
University of Sheffield

Doctoral Thesis

# Data-Integrity Attacks of Linear Control Systems

**William Casbolt**

The Control, Monitoring and Systems Engineering UTC

*within*

The Department of Automatic Control and System Engineering

This thesis is submitted for the degree of
*PhD - Automatic Control and Systems Engineering*

September 2021

# Abstract

We analyse the performance of control systems that are subject to stealthy data-integrity attacks. We derive different attack strategies on multiple control system architectures and study the effect of these attack on control systems. These attack strategies range from deterministic Denial of Service (DoS) attack to random data-injection attacks. All of these attack construction alter the integrity of the data sent over a communication channel. Namely, for the DoS attacks the attacker drops the packet containing the information and through a data-injection attack the attacker degrades the signal with additive noise.

The performance of control systems with input packet losses on both communication channels in a control system is analysed. We conduct this analysis for two separate communication protocols. Namely, the TCP-like and the UDP-like communication protocols. The TCP-like protocol provides the controller of the control system with additional information, and therefore, the comparison between TCP-like and UDP-like is equivalent to a comparison between systems with differing information. We provide a proof that linear optimal control systems operating with limited information, i.e. the UDP-like communication protocol, have a larger quadratic cost. This holds for multidimensional communication channels including communication channels that are characterised by non-stationary sequences of packet loss. The difference in cost that results from operating with limited information is analysed, enabling a quantification of the maximal difference. We also provide a scheme for the joint optimisation of the cost of communication and the cost of optimal control. We show that for the operator using the maximum likelihood detector the attacker can construct a stealthy attack. The performance of the attack is measured in terms of the increase of the linear quadratic cost function of the operator subject to a given detection constraint. The explicit characterisation of the expected cost increase of the optimal stealthy attack construction is provided and the for the IID attack bounds on the probability of detection are given.

Following the analysis of control systems with packet loss we consider systems with additive white Gaussian noise (AWGN) communication channels. We provide explicit characterisation of the cost increase caused by the error within each of the AWGN com-

munication channels. Once more we consider systems with differing levels of information. Namely, we provide this characterisation for three separate system architectures which are reminiscent of the UDP-like and the TCP-like protocols from the prior chapters. From this analysis it is seen that once again by limiting the information available to the controller the operator of a control system necessarily increases the cost of controlling a system. We characterise this cost increase explicitly for each system architecture and each AWGN channel within each system architecture. After presenting the framework for optimal control over AWGN channels we present a random data-injection attack construction and characterise the cost increase caused by the data-injection attack on each multidimensional AWGN channel. The attack is analysed and we provide a lower bound on the optimal attack strategy that enables the attack to remain undetected. Additionally, we provide an exact solution to the optimal stealthy attack construction for scalar communication channels. For all analytical results we also provide case studies on control systems to numerically evaluate the results presented.

# Table of contents

# List of figures

# List of tables

# Glossary of Notation

## General Definitions

| | |
|---|---|
| $a$ | A constant scalar |
| $\mathbf{X}$ | A constant matrix |
| $\mathcal{X}$ | A partitioned vector/matrix variable |
| $\mathbf{A}^\mathsf{T}$ | The transpose of matrix $\mathbf{A}$ |

## Random Variables

| | |
|---|---|
| $X$ | A scalar/vector random variable |
| $\mathbf{X}$ | A matrix random variable |
| $\{X_k\}_{k=1}^{\infty}$ | A random process for which $X_k$ denotes the random variable at time step $k$. |
| $\mathcal{X}$ | A partitioned vector/matrix random variable |
| $x$ | A realisation of a vector random variable |
| $\mathcal{I}_k$ | An information set at time instant $k$ |
| $X^k$ | The vector of random variables given by the sequence of variables $X^k \triangleq (X_1, X_2, \ldots, X_k)$. |
| $\widehat{X}(\mathcal{I}_k)$ | An estimate of a random variable obtained with information set $\mathcal{I}_k$ |
| $X_{k,i}$ | The entry $i$ of the random variable $X_k$ |
| $\widehat{X}_k\left(\mathcal{I}_{k-1}\right)$ | Prediction of a random variable with the information set $\mathcal{I}_{k-1}$ |

## Special Operators

| | |
|---|---|
| sup | Supremum |
| inf | Infimum |
| max | Maximum |
| min | Minimum |
| $\to$ | Tends to |
| $\xrightarrow[n\to m]{}$ | Tends to as $n$ tends to $m$ |
| $\mathbf{A} \succeq 0$ | $\mathbf{A}$ is symmetric non-negative definite, i.e. $X^\mathsf{T}\mathbf{A}X \geq 0$ |
| $\mathbf{A} \preceq 0$ | $-\mathbf{A}$ is symmetric non-negative definite, i.e. $-X^\mathsf{T}\mathbf{A}X \geq 0$ |
| $\mathbf{A} \succeq \mathbf{B}, \mathbf{B} \preceq \mathbf{A}$ | $\mathbf{A} - \mathbf{B}$ is symmetric non-negative definite, $X^\mathsf{T}(\mathbf{A} - \mathbf{B})X \geq 0$ |
| $\mathbf{A} \succ 0$ | $\mathbf{A}$ is symmetric positive definite, i.e. $X^\mathsf{T}\mathbf{A}X > 0$ |
| $\mathbf{A} \prec 0$ | $-\mathbf{A}$ is symmetric positive definite, i.e. $-X^\mathsf{T}\mathbf{A}X > 0$ |
| $\mathbf{A} \succ \mathbf{B}, \mathbf{B} \prec \mathbf{A}$ | $\mathbf{A} - \mathbf{B}$ is symmetric positive definite, i.e. $X^\mathsf{T}(\mathbf{A} - \mathbf{B})X > 0$ |
| $\mathbf{A}^{-1}$ | The inverse of $\mathbf{A}$ when $\mathbf{A}$ is non-singular |
| $\mathrm{rank}(\mathbf{A})$ | The rank of $\mathbf{A}$ |
| $\mathrm{tr}(\mathbf{A})$ | The trace of $\mathbf{A}$ |
| $\mathrm{diag}(x_1, x_2, \ldots, x_n)$ | A diagonal matrix with the elements $x_1, x_2, \ldots, x_n$ along the main diagonal |
| $\mathrm{diag}(\mathbf{A})$ | A diagonal matrix with the same diagonal elements as the matrix $\mathbf{A}$ |
| $\mathrm{vec}(\mathbf{A})$ | The $nm \times 1$ vector formed by writing the columns of $\mathbf{A} \in \mathbb{M}^{n\times m}$ one below the other |

| | |
|---|---|
| $\lvert\mathbf{A}\rvert$ | The determinant of a square matrix $\mathbf{A}$ |
| $\lVert X\rVert_2$ | The 2-norm of a vector $X$ |
| $\lVert\mathbf{A}\rVert_F$ | The Frobenius norm of a square matrix $\mathbf{A}$ |
| $\mathbf{A} \odot \mathbf{B}$ | The Hadamard (element-wise) product of $\mathbf{A}$ and $\mathbf{B}$ |
| $\mathbf{A} \otimes \mathbf{B}$ | The Kronecker product of $\mathbf{A}$ and $\mathbf{B}$ |
| $\lambda_i(\mathbf{A})$ | The i-th eigenvalue of a square matrix $\mathbf{A}$ |

## Special Objects

| | |
|---|---|
| $\mathbf{0}$ | The zero vector of appropriate dimension |
| $\mathbb{0}$ | The zero matrix of appropriate dimension |
| $\mathbf{1}$ | A vector of all ones |
| $\mathbf{I}_n$ | The $n \times n$ identity matrix |
| $e_i$ | The $i$-th column of the identity matrix |

## Scalar Spaces

| | |
|---|---|
| $\{\cdot\}$ | A set |
| $\mathbb{N}$ | The set of natural numbers |
| $\mathbb{R}$ | The set of real numbers |
| $\mathbb{C}$ | The set of complex numbers |
| $\mathbb{F}$ | $\mathbb{R}$ or $\mathbb{C}$ |
| $\mathbb{Z}_+$ | The set of non-negative integers |
| $\mathbb{Z}_{++}$ | The set of positive integers |

## Vector Spaces

| | |
|---|---|
| $\mathbb{F}^n$ | n-dimensional coordinate space |
| $\mathbb{R}^n$ | $\mathbb{F}^n$ with $\mathbb{F} = \mathbb{R}$ |
| $\mathbb{C}^n$ | $\mathbb{F}^n$ with $\mathbb{F} = \mathbb{C}$ |
| $\mathbb{M}^{n\times m}$ | n by m-dimensional coordinate space |
| $\mathbb{M}^n$ | n by n-dimensional coordinate space |
| $\mathbb{C}^{n\times m}$ | $\mathbb{M}^{n\times m}$ with $\mathbb{M} = \mathbb{C}$ |
| $S^n_{++}$ | The set of n by n symmetric positive definite matrices |
| $S^n_{+}$ | The set of n by n symmetric non-negative definite matrices |
| $X \in \mathscr{I}$ | The object $X$ is an element of the set $\mathscr{I}$ |

# Chapter 1

# Introduction

There are three pillars in cyber security: authentication, privacy, and integrity of communication channels. Conventionally, this consists of preventing access to the system through cryptographic techniques. However, encryptions are breakable. Specifically, given enough time and computational power, any encryption key can be broken, or alternatively, secure encryption keys can be stolen. It should be noted that current encryptions, with current computing power, typically take longer than the age of the observable universe to crack [42, 74]. However, these time frames are given under the assumption of brute force methods. Namely, attempting every possible combination of a cryptographic key. Encryption keys can also be broken through use of what is known as side information. This practice is the use of information outside of the encryption to help guess the encryption key. It is shown in [26] that it is possible to crack a 4096-bit RSA encryption through side information. Specifically, they crack the encryption key through monitoring the sound of a system using the encryption key to decode a file. When an encryption key is cracked, all three pillars of cyber security fail for the entire system. However, a control system that is secure in an information-theoretic sense is unbreakable in a given time frame or computational power [23]. This claim is sometimes able to be extended to include future computing power e.g. quantum computers [10], where all current encryption schemes become redundant [22]. An example of an information theoretically secure system is the One Time Pad. This encryption scheme is provably secure and termed to have perfect

secrecy [23, 76]. Therefore, a system operator guarantees fundamental limits on the systems security when the system is secure in an information-theoretic sense. These limits are never exceeded under the conditions they are valid for.

There is a growing interest in the community for the security of control systems operating over critical systems and infrastructure. This increase in interest has been driven by recent security incidents, such as [39, 35, 70, 16]. These attacks highlight the risk of interconnecting control systems with sensing and communication infrastructure. In particular, these malicious agents compromise part of the observation and/or actuation of the control system. In doing so, the attacks upon these systems have attracted significant interest in the control, communication, and signal-processing communities.

An attack that is able remain undetected while penetrating the encryption layer and compromising at least one of the three security pillars is known as a stealthy attack. This project grounds itself in this scenario. Namely, the scenario of an attacker/attack upon a control system that has bypassed the encryption layer whilst remaining undetected. Therein we develop methodologies that provide security in situations where traditional cyber security fails.

The Stuxnet worm [51, 39, 52] achieved precisely the objectives stated above. Namely, the Stuxnet worm bypassed the encryption layer and compromised a control system while remaining undetected. Stuxnet was the first cyber-weapon to physically damage a control system and in doing so it crossed the boundary from a cyber attack to a cyber physical attack. This is a direct result of the interconnectivity of sensing and control systems. By compromising the cyber portion of the control system, the Stuxnet worm was able to affect and damage the physical world. In particular, the worm targeted the programmable logic controllers of the centrifuges responsible for separating nuclear material in approximately 1000 [51] Iranian plants [51, 40]. It infiltrated, replicated, and spread throughout the system. This is the first case of a malware worm using the supervisory control and data acquisition (SCADA) systems in place [51, 38, 24]. However, unlike other programs, it specifically selected which systems to infect. Once it had gained access to control of the system, it intentionally withheld its full potential for damage

in order to remain undetected. In fact, Stuxnet performed what is known as a replay attack on the system [51, 49]. This entails recording the nominal function of the control system and *replaying* this back to the controller while intentionally perturbing the system. These perturbations were achieved through the actuators of the system that already existed. The worm remained undetected for months and is thought to be the reason why Iran decommissioned nearly $1,000$ centrifuges between 2009 and 2011. The strategy of withholding potential for immediate damage in order to remain undetected and, therefore, cause more damage over a longer period of time is a trade-off that appears multiple times throughout this thesis.

In a similar vein to Stuxnet, NotPetya is another cyber worm. NotPetya however, is known as a Ransomware worm. This is because the NotPetya worm locks the user out of the system until a bitcoin ransom is paid. Note however, that this worm is not stealthy. This is due to the fact that although it has bypassed layers of encryption, it does not remain undetected throughout this process. The attack performed by NotPetya is be modelled as a Denial of Service (DoS) attack on the control systems. This attack strategy is common and is explored throughout the literature [78, 58]. Although this is not the aim of the NotPetya worm, a DoS attack can be utilised for a stealthy attack construction given that the control system already postulates a portion of packet losses. This is intuitively termed as hiding in the noise. NotPetya infiltrated several systems including control systems in Ukraine, among these, the radiation sensors outside Chernobyl. The control systems that were affected were mainly power substations. On 30 substations not only did the malware shut them down and cause power outages, but NotPetya simultaneously performed Distributed Denial of Service (DDoS) attacks on call centres in parallel to cause delays in getting the substations back on-line [16]. If a worm of this nature were to specifically attack a control system, there could be safety critical failures. If the operator of the system is locked out of the controls via a DoS attack, the closed loop control system becomes open loop. For any health or safety critical control systems this could result in serious harm, either physically or economically.

Another Ransomware worm is WannaCry. This worm demands payment for access back into the system. However, instead of locking the user out of the system, it encrypts all of the data and demands payment. Although both WannaCry and NotPetya infiltrated and affected systems, they lacked the stealthiness and sophistication of Stuxnet. For example another Ransomware program, known as CryptoLocker, infected a utility in Brazil [16], but this infection was instantly detected and control of the system was transferred to a back up system. The infected machines were then destroyed [16]. Whereas if Stuxnet had been used, the worm could have infected far more machines before becoming detected. At which point it would have caused more damage over a longer period of time before being discovered. This in turn would result in more financial damage to the company than CryptoLocker achieved.

All examples above are scenarios where traditional cyber security mechanisms failed. All of these attacks occurred in the last ten years. Given that these cyber worms have been released, their behaviour can be analysed and replicated. This exact process is seen in laboratory studies [6]. The above highlights the need for a system (potentially safety critical) to be able to ensure its safety, even when subjected to a cyber-physical attack, is becoming evident in the current geopolitical climate.

With this in mind the PhD project focused upon the effect of optimal attacks within control systems that remain undetected. For this PhD an optimal attack is defined as the attack, or set of attacks that maximise the operator's optimal control cost while remaining undetected. A detection constraint is simultaneously imposed as a constraint in the optimisation of the attack strategy, but is also operator's mechanism for detecting a malicious attacker in the system. Namely, the detection constraint ensures a given outcome of the hypothesis test, on average. We derive these optimal attacks on control systems and the resultant optimal control laws for those systems. Our aim is to inform system operators of the degrees of security that detection constraints give them. Namely, for a given detection constraint, what is the most damaging attack that can occur? This question rests at the core of our work. Answering this question for given system constraints

allows an operator to control not only the system, but the security and the maximal damage a given attack can cause before the attack is detected.

Within this thesis we consider both DoS attacks and data-injection attacks upon control systems. We show that not only do optimal stealthy attack constructions exist for control systems, but we are able to quantify the damage each of these optimal attacks cause. In doing so we provide analysis of different control system architectures. Namely, we study the use of feedback communication channels to combat DoS attacks and introduce the use of an auxiliary channel within a control system experiencing a data-injection attacks. We explicitly quantify the additional safety these communication channels give in addition to showing how the expected cost of a control system under nominal conditions is reduced with the presence of these additional communication channels.

The thesis is structured as follows, Chapter 2 contains the literature review of the subject matter and the surrounding areas; Chapter 3 utilises the framework within [59] for the operator of a system and derives an optimal stealthy DoS attack upon the system; Chapter 4 takes the framework of [59] and extends the scalar channels therein to the multidimensional channel scenario, in doing which we provide analytic proofs of cost differences caused by the feedback channels; Chapter 5 builds upon the multidimensional communication channels constructed within Chapter 4 and derives an optimal *random* DoS attack upon the system, where the attacks derived are able to be tuned for a trade-off between probability of detection and the magnitude of cost increased; Chapter 6 steps away from the DoS regime and considers a control system with multidimensional Gaussian channels, in doing which we derive the optimal cost of the control systems and explicitly show the additional cost induced by controlling a system over imperfect communication channels; Chapter 7 builds upon the system structure outlined within Chapter 6 and derives the optimal *random* stealthy data-injection attack, where the derivation is performed for multiple system architectures and the differences in resultant cost are quantified; Chapter 8 is concerned with the implementation of the control laws and attack strategies of all of the previous chapters; Chapters 9 and 10 discuss the future of the work and conclusion of the thesis, respectively.

In addition to this thesis there have been publications such as [19] that focuses on the DoS attacks contained within Chapter 5, and the recently submitted work [20] which contains the some of the work within Chapter 4.

# Chapter 2

# Literature Review

When studying the surrounding literature there is a clear divide between approaches. The first approach is system analysis. This approach does not consider the presence of an attacker within the system construction. However, these areas of work could be interpreted in that way, an example of this is seen in [59]. Within [59] the authors consider a system that randomly drops packets upon the communication channels, and although they do not consider these drops to be caused by an attack, it is easily interpreted as a DoS attack. Another approach is where authors analyse an attack on a system from a system theoretic approach. The third approach is similar to the previous. However, with the exception that the problem is assessed from an information theoretic perspective. This approach is taken within [34]. Unfortunately however, this work does not consider control systems. Therefore in doing so, their work does not readily transfer to the control system architecture. This is due to the fact that there is memory within a control system. Specifically, a control system is Markovian in nature and therefore future states depend on the previous. The work within [34] only considers Independently and Identically Distributed (IID) states.

When considering the cyber security of any system, first the vulnerabilities must be mapped. Therein [48] highlights some of the security concerns of the smart grid. These vulnerabilities range anywhere from gas and electric meter bypassing to the Stuxnet computer worm [39]. A model of the smart grid is proposed in [48] to analyse the security challenges of the system. The model proposed contains all the layers of the smart grid.

These are known as: the Wide-Area Network (WAN), the Neighbour-Area Network (NAN), and the Home-Area Network (HAN). Through introducing each layer, the authors propose attacks that have the ability to be launched on the system at each of these layers. In doing so they highlight what they consider the three main security requirements from a system: confidentiality, integrity, and availability. It is clear why these three properties are required for a system to be considered secure. Confidentiality is required so that a system is able to guarantee it is communicating with an authorised user, or similarly it must be certain that there is no eavesdropping over the communication channel between the two systems. This relates to the authenticity and privacy pillars we have proposed. This pillar is usually safeguarded with standard encryption techniques, using either public or private keys for encryption. Within [48] the customers power usage is considered as the smart grids confidentiality pillar. This stems from the fact that an unauthorised user knowing the usage pattern of a customer reveals the personal activities of the customer [4]. Integrity is needed such that any data received is considered reliable and unaltered. For the smart grid, this is ensuring that the metering costs are unaltered, genuine and from the energy provider. Finally, availability is needed to ensure attacks that take the form of denial of service (DoS) do not damage the system. In the smart grid no availability of power results in black outs. Counter measures for attacks are proposed after the clear vulnerabilities of the smart grid are shown, such as its entry points and a range of possible actions that can be performed once access is granted. These countermeasures range from careful key management, in order to inhibit unauthorized entries, to the redesigning of the network topology entirely, in an effort to build a secure network from the ground up. The key element is that for the smart grid to be secure, it is not enough to consider the problem solely from a cyber security or system-theoretic perspective. Cyber-physical security is introduced and it highlights this area as a research challenge for the forthcoming years. Only a few years after [48] was published, the NotPetya malware exploited a lot of these vulnerabilities, highlighting the need for improved security. These points have motivated the need for a combined cyber and physical security approach in order to solve the problems we face.

## 2.1 Control Systems with Lossy Communication Channels

When considering malicious attacks on control systems, random packets drops in the communication links arise naturally. Packet drops are a result of multiple effects within communication. They can be the effect of high traffic within a network, noise during wireless communication, or even the result of a DoS attack. In [59, 58, 66, 46, 65, 63, 56], control systems with packet loss in the communication channels between the plant and the controller are modelled and analysed. In doing so, the foundations for control and estimation over lossy communication channels are established. The optimal control law and estimator is derived for both protocols in [59] using dynamic programming. A control system that is susceptible to packet loss on the communication channel from the plant to the controller is considered in [63]. In [59] and [46] the work of [63] is extended to systems with packet loss in both the sensing (plant to controller channel) and the actuation (controller to plant channel) communication channels. In [65] and [66], systems with and without an acknowledgement link respectively are considered. These approaches analyse the performance of the controller and characterise the trade-off between the control system cost, stability, and the properties of the communication channel. More specifically, in [59] the authors model the performance of a Linear Quadratic Gaussian (LQG) controller that is experiencing packet drops on the communication channels between the plant and the controller. The loss of a packet between the plant and the controller is modelled as a Bernoulli random variable. An IID sequence of Bernoulli variables, although sufficient for the purpose, do not accurately model a real packet drop channel within a wireless network. This is due to the fact that losses tend to be dependent on previous time instances [13]. Intuitively, if there is interference in a signal at a given time instance it is more likely that the same interference will also cause interference with the following time instance. In an effort to model this effect more accurately in [47], the authors consider a two-state Markov chain to model the memory in the packet losses. Therein the authors investigate how, under different protocols, the stability region of the system differs due to the lossy links

connecting the system. Within both of the works, [59, 47], two protocols are considered: TCP-like and UDP-like. The scenario where a system that has an imperfect communication protocol is discussed in [29]. The UDP-like protocol considered in these works is currently the more realistic scenario for most control systems. Namely, the standard form of practice has no auxiliary feedback channel that is present in the TCP-like protocol. The authors conclude in these papers, [59, 47, 29], that the infinite horizon cost of the system is bounded if and only if the probability of packet loss is below a critical threshold. It is also shown that in the UDP-like case, the separation principle between control and separation no longer holds unless there is a perfect communication link between the controller and the plant. This is caused by the fact that the estimation error covariance depends on the input distribution, which in turn is dependent on the distribution of the packet arrivals on the plant to controller link. Within [75] the authors consider the problem of optimising the schedule of control signals within a networked control system. The authors utilise a time based schedule as opposed to an event driven schedule but show that they are able to minimise the average transmission power whilst maintaining the stability of the networked control system.

A natural question that arises from the study in [59] is: given that the feedback link in the TCP-like protocol is the only differing feature between the two separate protocols, under which circumstances does the performance of the TCP-like case tend to performance of the UDP-like case? This question is approached by Garone et al. [29] who consider an acknowledgement link that also has a probabilistic loss parameter. This loss parameter is also a Bernoulli variable. It is shown that in line with [59], if the Bernoulli parameter governing the acknowledgement link tends to perfect transmission then the systems stability region converges to the TCP-like case as seen in. Conversely, as this parameter tends to a broken link, i.e. no transmission for all time instances, the systems stability region converges to the UDP-like protocol case. It is also shown that as this parameter for acknowledgement varies, the stability regions of the system also vary, although it is worth mentioning that the systems stability region never exceeds either of the two extreme cases. Therefore, given no communication link is perfect, this work highlights exactly what a

particular system achieves and presents the worst case scenario for the system. On the other hand it also presents the best possible scenario for a system operator i.e. TCP-like, meaning that provided the system is performing sub-TCP-like then there is room for improvement. It should be noted that if the acknowledgement link is not a perfect channel then, as in the UDP-like case, the separation principle does not hold, and therefore, design of the controller and the estimator must be conducted simultaneously.

Following on from [59], Mo et al. [47] extend the IID Bernoulli packet drop model to a Markovian packet drop model. This choice is made to reflect the characteristics of wireless channels more realistically. In this setting the system is assumed to be operating under a perfect TCP-like protocol. As in [59], the TCP-like architecture means the controller has access to the previous realisation of the loss variable. This allows the operator to include this information in their computations of the optimal control law. Unlike [59], the closed loop system only drops packets on the actuation link. This implies the controller is co-located on the sensing side of the plant. The communication channel loss model is governed by a two state irreducible and stationary Markov chain. The authors consider an LQG optimal control problem. Therein it is shown that the system is stable provided that the elements of the transition matrix for the Markov chain are within a specified region. This region, surprisingly, is fragmented and the elements have dependence with one another. This region resembles the stability region of the UDP-like protocol from [59]. It is shown that when the transition matrix is such that the realisation of packet delivery is alternating at every time instance i.e. only actuating at odd or even time instances, then the closed loop system is unstable. It should be noted that the if communication channel of the systems is modelled as a Bernoulli process, the system remains stable if the system is expected to lose half of its packets. It is also shown, in accordance with the TCP-like protocol, that the optimal control input at each time instance is a linear function of the states. In addition to this, the separation principle is shown to hold for the closed loop system, provided it is operating with a TCP-Like communication protocol. Therefore, the work in [47] shows that increasing the complexity of the loss variable, has surprising results on the region of stability when compared with the IID Bernoulli case.

Similar to [47], a Markov chain of losses in considered in [56], specifically the losses are modelled with a Gilbert-Elliot model [31]. As an alternative to [47] the authors of [56] analyse the problem of packet losses on the sensory link and assume the actuation link to be perfect. However, in doing so they are able to show stabilising control laws exist and present examples of these control laws stabilising a system even outside of the sufficient conditions they provide.

## 2.2 Control Theoretic Analysis of Systems under Attack

To effectively detect attacks it is necessary to understand the advantages and limitations of different detection strategies. In [54] the fundamental limits of monitoring within Linear Time-Invariant (LTI) systems are analysed. Formal definitions of undetectability and unidentifiability are provided. An unidentifiable attack is one that can be detected, but cannot be distinguished from another attack. For example, two separate attacks may be indistinguishable from a single attack on the same system, even though the presence of an attack is detected. This is considered the problem of assigning ownership to an attack. An undetectable attack is by definition also unidentifiable, and therefore, an undetectable attack has a stronger sense of stealth. The authors also introduce the idea of active and inactive monitors. Active monitors inject their own auxiliary input signal, as seen in [49], for detection purposes. Conversely, inactive monitors only assess the incoming data. Additionally, the authors consider both centralised and decentralised attack detection. The difficulties in identifying distributed attacks are highlighted. Naturally, as mentioned above, a single attack that is distributed on separate systems is difficult to distinguish from two separate attacks on separate systems. The problem is approached using system theoretic and graph theoretic tools. It is concluded, in line with [53], that an attack on the IEEE 14 bus test system is undetectable to a static monitor, if and only if more than three sensors are corrupted. These findings are concurrent with those in [49], although the case study is not on the IEEE 14 bus within [49]. On the same test system it is shown that a

dynamic detector detects any attack of this construction, independent of the proportion of sensor corruption. There is also a case study on the IEEE 118 bus test system in which it is divided into five zones where it is assumed that all generators in a zone are compromised. The simulations corroborate that the attacks are detected using their proposed distributed detection filter.

Within [78] the authors consider wireless networked control systems (WNCS) that are subjected to Denial of Service (DoS) attacks. Unlike other works, [78] considers the problem from the standpoint of the attacker as opposed to the operator of an unstable system. The objective of their investigation is to produce an optimal schedule of when to attack the system. As mentioned above, their attack is constructed as a DoS attack. The scheduling of the attack is restricted such that the attacker has a finite amount of energy to expend. The objective of the attacker is to maximise the cost function of the operator. This work uses the same framework as in [59], i.e. an erasure communication channel [25]. The attacker is assumed to have full knowledge of the system and attacks the sensing communication channel. The attacker is also given a selected period of 'active time', this is a predetermined window in which the attacker has the ability to jam the communication channel. Outside of this active period, the attacker can not jam the system and must remain inactive. When the operator is implementing the optimal control strategy, as presented in [59], the best attack for any given active window is a constant stream of jamming for as long as the attacker can allow with the allotted energy. It is shown that the system remains stable, in the sense of bounded state covariance. The only situation where the system is not stable is when the 'active' window for the attack tends to infinity. Naturally, this scenario corresponds to the system running open loop. This is due to not being able to measure the control system states, and therefore, the system tends to instability. Within [78] the authors also present case studies on single and multiple subsystems. In these case studies it is consistently shown that the optimal attack schedule drives up the cost of the system. However when looking at the case studies, there are signs that there is room for improvement with this attack strategy. Namely, the optimal schedule derived gives rise to 'spikes' in state magnitudes. This spike in state

would cause the attack to be detected for most attack detection methods described in the above literature, for example, the detection constraints seen within [49, 54, 53]. Due to this, an optimal attack in this framework needs to take more into consideration than the sole objective of maximising the cost of the operator. Specifically, the attack construction also needs to consider limiting the short term cost increase in order to remain undetected. In doing so, an attack would be able to cause a larger cost increase over a longer period of time.

A more sophisticated attacker may be able to not just drop packets, they could potentially also inject their own signals. In [49] a standard LQG optimal controller is considered and for detection purposes, the authors employ a $\chi^2$ failure detector with a monitoring signal. The system is subjected to a replay attack. This attack is implemented after a fixed training window for the $\chi^2$ detector. In this scenario the detector requires a guaranteed time window with no attack present for the detector to be effective. This means the system does not account for attacks that are present from day zero of the system operating. A replay attack entails the attacker recording the incoming measured data and then 'replaying' the recorded data back to the controller whilst perturbing the actuators if desired. This method is the attack technique used by Stuxnet [39]. This leaves the operator unaware of the attack, provided that the attack is stealthy. Whilst in operation, the $\chi^2$ detector monitors the measurement and decides whether these values correspond to nominal operation. The setting in [49] assumes that the attacker injects the attack signal at any time outside the training window. It is also assumed that the attacker has access, and the ability to record signals coming from the plant whilst simultaneously modifying the packets on the actuation link. In order to detect the replay attack, a monitoring signal is used. The monitoring signal is an IID sequence of random variables with a Gaussian distribution of zero mean and covariance matrix $\mathcal{L}$. This signal is injected into the control law. The $\chi^2$ failure detector is used to determine whether this lies in the characteristics of normal operation or if the signal representative of an attack. In the simulations it is shown that systems without a monitoring signal are susceptible to replay attacks. It is concluded that the larger the covariance of the monitoring signal between time instances,

the higher the probability of detecting a replay attack. It is also investigated whether the training window size affects attack detection. Interestingly, the $\chi^2$ has a faster response to the attack with a smaller training window. However, it has a lower detection rate overall when compared with a larger training window. It is noted that by including the monitoring signal, the system loses 9% efficiency, with respect to the optimal LQG cost, but the detector gains 35% increase in probability of detection. Once again, a trade-off appears between security and efficiency.

Cyber-physical attacks in power networks are the main focus of [53]. The authors investigate the performance of different types of attack detectors. The discussion revolves around how static and dynamic detectors determine differ in their performance during a malicious attack. A static detector checks a data signal at discrete time intervals and does not take into account the system dynamics whereas a dynamic detector checks signals on a continuously. This work defines detectability as whether an attack is distinguishable from nominal operation. The paper concludes that, for the IEEE 14 bus test system, the static detector only detects the attack if the attack compromises four or more sensors, whereas the dynamic detector detects an attack independently of the number of sensors compromised. This suggests dynamic detectors are more effective at detecting malicious attacks.

## 2.3 Information Theoretic Analysis of Systems under Attack

In the above attack scenarios, [53, 54, 49, 78], the authors approached the problem using control and system theoretic techniques. The following works address similar issues, however, they approach the problem from an information theoretic standpoint. The definitive starting point for information theory is with Shannon [60]. In this paper, Shannon quantified exactly what society meant by information and communication. In doing so he simultaneously addresses the limit at which it is impossible to guarantee perfect communication. This is known as the channel capacity. This is where the field began, but

quickly the topic grew, measures such as the Kullback-Leibler divergence (KL divergence) and mutual information appeared. We utilise some of these measures throughout this thesis.

Yu et al. [77] asses the effectiveness of an information-theoretic measure, the KL divergence. The authors assess its effectiveness as an attack detection filter. They assess the effectiveness for a Distributed DoS (DDoS) attack. The attack is designed such that it mimics network traffic. It is particularly difficult to discern this attack construction from an unusually high amount of legitimate network flow. This issue of identifying a genuine traffic surge within a network compared with a malicious attack is addressed throughout [77]. The paper assumes the attacker creates packets according to either a Poisson or chi-squared distribution. These packets are created at all of the 'zombie' IP addresses. A zombie address is an address that has been made a slave to the attackers computer. It is also assumed that the attacker only targets a single server. The background network traffic, or nominal network traffic, is assumed to follow a Poisson distribution. The paper addresses the need for a fast detection window in an attack scenario, whilst maintaining a low false alarm rate. In order to apply the information metric, the authors look at the packet flow through the routers in the network. When a suspicious amount of traffic is detected, the routers begin to count the packets travelling through them. After doing so, they monitor the KL-divergence of the separate flows throughout the routers, following which a decision on the attack presence is declared. In simulations the authors consider a network of 21 routers and 336 network nodes. The KL-divergence of the flow between nominal traffic and the flow caused by an attack, as well as the KL divergence of two attack flows is considered. In doing so, it is identified that a clear difference between the two cases of traffic flow exists. However, the authors fail to explore the KL-divergence of two normal traffic flows. In neglecting this possibility there is a chance that an influx of legitimate requests flag as an attack. This raises the potential for a false alarm. Similarly, by considering the difference between an attacked and nominal traffic flow as the normal case there is a non-zero possibility of a DoS slipping through the detection filter.

An additive attack within the smart-grid is considered in [34]. This is done using information theoretic tools. The additive attack used is a more general attack construction than a DoS attack. In [34] the problem of estimation whilst under attack is considered. However, it should be noted that the states of the system are modelled as IID states, and therefore, the results derived do not apply directly to control systems. This is due to the attacks constructed not taking into account the memory in the states. Ke Sun et al. [34] consider a stealthy IID attack strategy. In this scenario this assumption is valid, however, if an author were to extend this work to a control system there is reason to believe an attacker could take advantage of the structure within the system. The authors construct a utility function that consists of two terms. One term governs the attacker's objective for damage to the system, the mutual information. The other term is responsible for the attack detection, KL divergence. The attacker aims to minimise this function so that there is maximum damage caused with the minimum chance of detection. Note that minimising the mutual information between two distributions causes greater errors in the estimation of one random variable through use of the other [25]. The case when the attacker has finite training data to construct the attack is considered. It is shown that an attack constructed from the training data converges to an attack with full knowledge. The rate of convergence of this attack construction is also assessed. During simulations, the Signal to Noise Ratio (SNR) is adjusted to assess the performance of the attacker. In addition to this, Ke Sun et al. [34] also vary the covariance of the random variable being estimated. It is seen that when there is an abundance of noise, the attacker can attempt to 'hide' amongst it. This means that the KL divergence is smaller when compared with a higher SNR signal. It is also seen that the smaller the correlation, the faster the attack converges to the optimal attack. This convergence is quantified in terms of number of samples needed. However, it is also seen that the optimal attack is when there is a high correlation in the system, therefore, a trade-off appears between rate of convergence to the optimal attack and the performance of the optimal attack.

## 2.4 Information Theoretic Approaches to Control Theory

There are approaches that have attempted to integrated information theory into control theory. The main goals of these works are to generalise the communication channels within control [21] or to quantify the cost of communication [37]. Specifically, within [37] the authors quantify the trade-off between the communication rate over the communication channels and the the expected quadratic cost function of a control system. In doing so they present a lower bound on the communication rate necessary to attain a given quadratic cost. It is not however considered within an attack framework. Namely, [37] does not consider the presence of an additional malicious agent that is attempting to increase the quadratic cost of the control system. In a similar vein, [21] generalises the model of the sensory communication channel within a control system. The authors characterise the resultant cost of a control system that transmits the sensory information over an imperfect communication channel. They show that the resultant control system cost increase caused by communicating over an imperfect sensory communication channel is able to be decoupled from the cost of controlling a system over a perfect communication channel. In doing so, this allows the problem of control optimisation and communication optimisation to be considered separately. It is however assumed in [21] that there is a perfect communication channel from the controller to the plant. Once again, there is no consideration of the malicious presence of an attack in the system model within [21].

The surrounding literature is mainly focused on the control theoretic side of the cyber security problem, [49, 54, 53], where a similar problem to ours is approached. However, the methodology used differs greatly. Conversely, as seen in the field of information theory, the cyber-physical security aspects of control systems are still not well understood. However, the problem of cyber security is addressed outside of a control system setting [34]. As seen above there is a clear gap between the information theoretic and the control theoretic approaches. This thesis aims to explore the gap between these two fields by using information theoretic tools to study the security issues within control systems.

# Chapter 3

# Deterministic Denial of Service Attacks in Control Systems

## 3.1 Chapter Introduction

Under normal operation a communication network drops packets as a result of many factors. These factors include congestion within the network; errors within the channel; and delays within the network. Therefore, it is reasonable to assume that the operator of a wireless or networked control system assumes a proportion of packet loss over a communication channel. In [57] packet loss in wireless control systems is studied, and a nominal level of packet loss is established for normal operation conditions. In view of this, an attacker may attempt to disguise an attack that induces packet loss as nominal packet loss. In doing so, the attacker is able to strategically drop packets without being detected. This idea is analogous to an attacker hiding among the noise in an additive attack [34]. To that end, the derivation of an optimal and stealthy Denial of Service (DoS) attack is the focus of this chapter, specifically, a stealthy deterministic DoS attack. The first step to achieve this is to establish how an optimal deterministic DoS attack affects a system and, more importantly, how it differs from the probabilistic case in [59]. In our first approach we do not consider a detection constraint, the stealth of the attack is studied later.

The problem contains two different perspectives: the operator of the system, that assumes IID packet loss, and the attacker, that wishes to attack this system whilst remaining undetected. It should be noted that the attacker is assumed to have full knowledge of the system model. This includes the probability of packet loss postulated by the operator. The attacker having *a priori* knowledge of the system is a reasonable assumption given that with full knowledge of the system the attacker can only do better than an attacker with a subset of the full information [72]. Therefore, with full knowledge of the system, the attack is considered the worst case attack of that type for the operator. Naturally, if the operator of the system is armed with the knowledge of the worst possible attack scenario and it is within acceptable limits, the system is considered safe for that attack strategy.

### 3.1.1 Communication Protocol

In the following derivation in this chapter, the operator chooses to implement the TCP-like communication protocol. The TCP-like protocol differs from the TCP protocol used in communication literature in that a lost packet is not automatically re-transmitted to the plant, since there is no reason for this to be useful any longer to the optimal control input. This is a result of the most recently calculated control signal being the most vital for the plant to receive. For example, due to the fact that there is no estimation performed at the plant, in addition to the presence of uncertainty within the system, the most recent measurement contains the least uncertainty of the current state of the system. Due to this, in the event of a packet loss, the plant performs no actuation as is assumed in [59, 65, 66, 46] and is the main focus of [58]. In [58], a comparison of different control strategies in the event of packet loss is studied. They study the effect of a smart actuator that supplies the previous input in the event of a packet loss. Therein they conclude that there exists a trade-off between the zero-input and the hold-input strategies. Specifically, in the high packet loss percentage scenario or the 'cheap control' scenario, where the zero-input strategy is superior in terms of Linear Quadratic Gaussian (LQG) cost. The 'cheap control' terminology corresponds to a control law that does not

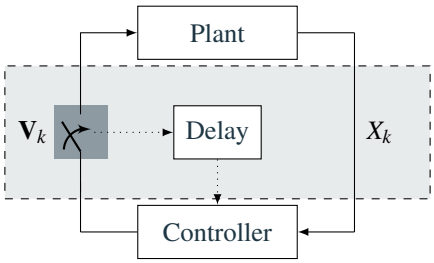


Fig. 3.1 The TCP-like system model, where the dotted line represents the transmission of information and the dashed box shows the communication channel between the plant and controller.

penalise the actuators heavier than the states. Furthermore, the stability regions for both strategies are the same. For that reason, the work below adopts the zero-input strategy for mathematical convenience. A control system communicating with a TCP-like protocol is depicted in Fig. 3.1. The presence of the information link that transmits the packet loss information back to the controller enables the operator to update the *state estimate* with the realisation of the random variable. It does not however allow the operator to know the realisation of the random variable before transmitting the control signal over the communication channel to the plant. In, [59] the operator communicates over two different protocols. Namely, UDP-like or TCP-like. UDP-like lacks the acknowledgement link that the TCP-like protocol has. In the remaining sections of this chapter we do not consider the possibility that the operator communicates using a UDP-like protocol. The reason for this is if the operator implements a UDP-like protocol, the operator will have no access to the realisations of the random variable $V_k$. Therefore, the detection constraints implemented later on would have to be radically different from the detection constraints of the TCP-like protocol. Namely, the operator would have to implement an additional hypothesis test in tandem with the attack test to decide if the packet was dropped. At each time instant, the additional hypothesis test would be to decide if at the previous time instant the system was open loop or closed loop.

## 3.2 System Model

The state space system under DoS attack is modelled as

$$X_{k+1} = \mathbf{A}X_k - V_k\mathbf{B}\mathbf{K}\widehat{X}_k + W_k, \tag{3.1a}$$

where $\mathbf{A} \in \mathbb{M}^n$ represents the dynamics matrix; $X_k \in \mathbb{R}^n$ is the state vector at time $k$ with $k \in \mathbb{N}$; $X_0$ is drawn from the Gaussian distribution $\mathcal{N}(\overline{X}_0, \mathbf{P}_0)$ where $\overline{X}_0 \in \mathbb{R}^n$ and $\mathbf{P}_0 \in S^m_{++}$ are the mean and covariance of $X_0$ respectively; $V_k \in [0, 1]$ is the packet loss variable modelled as an IID Bernoulli random variable with mean $\overline{V}$; $\mathbf{B} \in \mathbb{M}^{n\times m}$ is the control matrix; $W_k \in \mathbb{R}^n$ is a Gaussian distributed independent random variable with mean $\mathbf{0} \in \mathbb{R}^n$ and covariance matrix $\Sigma_W \in S^n_{++}$ ; and $\mathbf{K} \in \mathbb{M}^{m\times n}$ is the constant gain determined by the system dynamics. Note that with the system model in (3.1a), we adopt the same framework as in [59]. We require no specific restrictions on the relations of the pair $(\mathbf{A}, \mathbf{B})$ in order to perform the analysis below. However, it follows from standard theory that in order to have a stabilising control law the pair must be reachable. Similarly this statement holds for the dual problem of the observability of the system.

Prior to the attack, the system is assumed to achieve a steady state input. It is shown in [59] that the optimal input for any time instant $k$ after steady state is reached, is a constant linear function of the state estimate, i.e. $U^*_k = -\mathbf{K}\widehat{X}_{k|k}$ where $\widehat{X}_{k|k}$ is the optimal state estimate at time instant $k$ given all previous measurements. It should be noted that the steady state input does not mean the system is in steady state. The system is considered stable in the sense that the covariance is bounded, and therefore, the states do not approach 0. The system communicates over the channel with a TCP-like protocol, as in [59], i.e. the controller always knowledge of the previous loss realisation $v_k$ for estimation purposes.

The observations are modelled as

$$Y_k = \mathbf{C}X_k + Z_k, \tag{3.1b}$$

where $Y_k \in \mathbb{R}^q$ are the observations at time $k$; $\mathbf{C} \in \mathbb{M}^{q\times n}$ is the observation matrix; and $Z_k \in \mathbb{R}^q$ is the observation noise at time $k$ that is modelled as an independent Gaussian random variable with mean $\mathbf{0} \in \mathbb{R}^q$ and covariance matrix $\Sigma_Z \in S^q_{++}$.

## 3.3 Operator Model

At every time instant, the operator has access to a given amount of information determined by their information set. For the TCP-like protocol the information set is defined as

$$\mathcal{O}_k \triangleq \{\mathcal{V}_{k-1}, \mathcal{Y}_k, \mathcal{O}_{k-1}\}, \tag{3.2}$$

where $\mathcal{V}_{k-1} = \{v_0, \ldots, v_{k-1}\}$; $\mathcal{Y} = \{y_0, \ldots, y_{k-1}\}$; $v_k$ represents a realisation of the random variable $V_k$ at time instant $k$; $y_k$ represents a realisation of the random variable $Y_k$ at time instant $k$; and by definition $\mathcal{O}_k$ contains all realisations of $V_k$ up to time instance $k-1$, in addition to the current and all previous measurements $Y_k$. In order to assess to the efficiency of the control system we introduce a Linear Quadratic Gaussian (LQG) cost function. The cost of the system for the operator is

$$J_N(\overline{X}_0, \mathbf{P}_0) = \mathbb{E}\left[X_N^\mathsf{T}\mathbf{Q}_X X_N + \sum_{k=0}^{N-1} \begin{pmatrix} X_k \\ \mathbf{K}\widehat{X}_k \end{pmatrix}^\mathsf{T} \begin{pmatrix} \mathbf{Q}_X & 0 \\ 0 & V_k\mathbf{Q}_U \end{pmatrix} \begin{pmatrix} X_k \\ \mathbf{K}\widehat{X}_k \end{pmatrix} \middle| \overline{X}_0, \mathbf{P}_0 \right], \tag{3.3}$$

where $\mathbf{Q}_X \in S^{n\times n}_{++}$ is the state penalty matrix; $\mathbf{Q}_U \in S^{m\times m}_{++}$ is the input penalty matrix; $N \in \mathbb{N}$ represents the time horizon; and $\mathbf{K} \in \mathbb{M}^{m\times n}$ is the constant gain of the control law. The optimal cost for the operator is defined as

$$J^*_N(\overline{X}_0, \mathbf{P}_0) = \min_{\mathbf{K}} \left\{ \mathbb{E}\left[X_N^\mathsf{T}\mathbf{Q}_X X_N + \sum_{k=0}^{N-1} \begin{pmatrix} X_k \\ \mathbf{K}\widehat{X}_k \end{pmatrix}^\mathsf{T} \begin{pmatrix} \mathbf{Q}_X & 0 \\ 0 & V_k\mathbf{Q}_U \end{pmatrix} \begin{pmatrix} X_k \\ \mathbf{K}\widehat{X}_k \end{pmatrix} \middle| \overline{X}_0, \mathbf{P}_0 \right] \right\}. \tag{3.4}$$

It follows from [59] that $\mathbf{K}$ is determined by the solution of a Modified Algebraic Riccatti Equation (MARE). Specifically, the optimal gain $\mathbf{K}^*$ is given by

$$\mathbf{K}^* = \left(\mathbf{Q}_U + \mathbf{B}^\mathsf{T}\mathbf{S}_\infty\mathbf{B}\right)^{-1}\mathbf{B}^\mathsf{T}\mathbf{S}_\infty\mathbf{A}, \tag{3.5}$$

where $\mathbf{S}_\infty$ is defined as the steady state solution of the MARE

$$\mathbf{S}_k = \mathbf{A}^\mathsf{T}\mathbf{S}_{k+1}\mathbf{A} + \mathbf{Q}_X - \overline{V}\mathbf{A}^\mathsf{T}\mathbf{S}_{k+1}\mathbf{B}\left(\mathbf{Q}_U + \mathbf{B}^\mathsf{T}\mathbf{S}_{k+1}\mathbf{B}\right)^{-1}\mathbf{B}^\mathsf{T}\mathbf{S}_{k+1}\mathbf{A}. \tag{3.6}$$

It should be noted that this "optimal gain" is in fact suboptimal, we have used this terminology due to the fact that it is the gain matrix that comes from the steady state solution of the optimal time-varying Riccati equation. This restriction is dropped later on and the operator uses the true time-varying optimal gain matrix. The proof of the derivation of the time-varying gain matrix is, for convenience, reported in Appendix A.2 and follows a dynamic programming argument. Following the same approach as in [59], the estimation of this process rewritten in terms of the constant gain $\mathbf{K}$ is

$$\begin{aligned}
\widehat{X}_{k+1|k} &= \mathbb{E}\left[\mathbf{A}X_k - V_k\mathbf{B}\mathbf{K}\widehat{X}_k + W_k \middle| \mathcal{O}_k, v_k\right] \\
&= (\mathbf{A} - V_k\mathbf{B}\mathbf{K})\,\widehat{X}_{k|k}, && \text{(3.7a)} \\
E_{k+1|k} &= X_{k+1} - \widehat{X}_{k+1|k} \\
&= \mathbf{A}E_{k|k} + W_k, && \text{(3.7b)} \\
\mathbf{P}_{k+1|k} &= \mathbb{E}\left[E_{k+1|k}E_{k+1|k}^\mathsf{T} \middle| \mathcal{O}_k\right] \\
&= \mathbf{A}\mathbf{P}_{k|k}\mathbf{A}^\mathsf{T} + \Sigma_W, && \text{(3.7c)}
\end{aligned}$$

where it should be clear that the operator has access to the realisation of the packet drop parameter for estimation due to the TCP-like system architecture. As shown in [59], the

optimal cost at time $N$ the time horizon, is

$$J_N^*(\overline{X}_0, \mathbf{P}_0) = X_0^\mathsf{T}\mathbf{S}_0 X_0 + \mathrm{tr}(\mathbf{S}_0\mathbf{P}_0) + \sum_{k=0}^{N-1} \mathrm{tr}\left(\mathbf{S}_{k+1}\mathbf{Q}\right) + \sum_{k=0}^{N-1} \mathrm{tr}\left(\left(\mathbf{A}^\mathsf{T}\mathbf{S}_{k+1}\mathbf{A} + \mathbf{Q}_X - \mathbf{S}_k\right)\mathbf{P}_{k|k}\right), \tag{3.8}$$

where $\mathbf{S}_k$ is the MARE governed by (3.6).

Throughout later sections, the model for the operator does not change. Namely, the attack strategies derived below all assume that the operator performs the system control algorithms detailed above, unless stated otherwise.

## 3.4 Detection Constraint

In the previous section we define the operator's control and estimation process. However, the operator also monitors the communication channel and employs a detection strategy.

The operator postulates two properties from the sequence of packet drops. Namely, the sequence of packet drops $\{V_i\}_{i=0}^N$ is an IID sequence, and that the packet drops follow a Bernoulli distribution $V_i \sim Be\left(\overline{V}\right)$. With these postulates in mind, the operator constructs their hypothesis test. We define that hypothesis test as

$$H_0 : \text{There is no attack present,} \quad V_k \sim Be\left(\overline{V}\right), \tag{3.9a}$$

$$H_1 : \text{There is an attack present,} \quad V_k \nsim Be\left(\overline{V}\right). \tag{3.9b}$$

Naturally, due to the fact that this is a random sequence, there exists a non-zero probability that a sequence of nominal packet losses (packet losses from a communication channel with no attack present) causes result in an error in the hypothesis test decision. This is known as a false alarm rate. Due to this fact the operator decides to accept the null hypothesis for all sequences within a certain *distance* from the postulated statistics. Specifically, the operator constructs an estimator of the communication channel statistics that is a function of the measured packet losses $\widehat{V}_k = f\left(V_1, \ldots, V_k\right)$. From this estimator the operator then

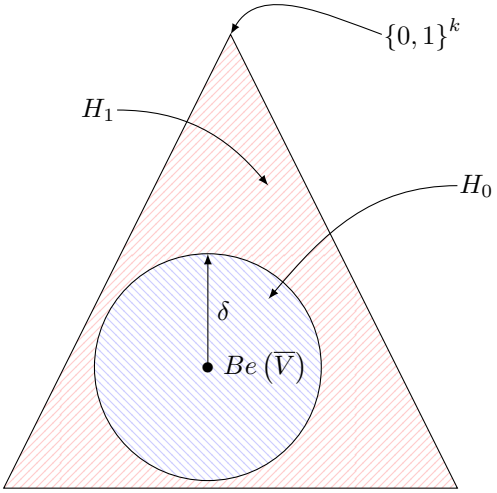


Fig. 3.2 The probability simplex of the hypothesis test, clearly showing the regions of acceptance and rejection of the null hypothesis.

measures the distance of this estimated distribution to the postulated distribution. Due to the fact we have kept the function that the operator chooses to be arbitrary, we define this distance in terms of the distributions. Therefore, the hypothesis test becomes

$$H_0 : d\left(\mathcal{P}_{\widehat{V}_k,V_1,\ldots,V_k}, \mathcal{P}_{\overline{V}}\right) < \delta, \tag{3.10a}$$

$$H_1 : d\left(\mathcal{P}_{\widehat{V}_k,V_1,\ldots,V_k}, \mathcal{P}_{\overline{V}}\right) \geq \delta, \tag{3.10b}$$

where $\delta > 0$ is a constant to be tuned by the operator for a desired trade-off between attack detection and false alarm rate and $d\left(\cdot,\cdot\right)$ is any distance measure between two distributions. The hypothesis test in (3.10) is depicted visually in Fig. 3.2. It should be noted that due to the fact that we are considering an IID sequence of Bernoulli random variables, this sequence is characterised entirely by the mean. Therefore, any chosen distance measure is a scaling of another.

We now consider the estimator function for the operator. Namely, the maximum likelihood estimator for this setting. The maximum likelihood (ML) estimator is defined as

$$\widehat{V}_{ML} \triangleq \arg\max_{\widehat{V}_k} \ \mathbb{P}\left[\left(V_1,\ldots,V_k\right)|\widehat{V}_k\right]. \tag{3.11}$$

Intuitively, this is interpreted as deciding the $\widehat{V}_k$ that maximises the probability of obtaining the sequence $\{V_1, \ldots, V_k\}$. For this particular problem, we have an IID sequence of Bernoulli trials. This is the definition of a Binomial distribution. Therefore,

$$\mathbb{P}\Big[(V_1, \ldots, V_k)\,|\widehat{V}_k\Big] = \begin{pmatrix} k \\ s \end{pmatrix} \widehat{V}_k^{\,s} \left(1 - \widehat{V}_k\right)^{k-s}, \tag{3.12}$$

where $s \in \mathbb{N}$ denotes the number of successful packet transmissions. Namely,

$$s = \sum_{i=1}^{k} V_i. \tag{3.13}$$

In order to find the maximal points of this function we take the derivative with respect to $\widehat{V}_k$

$$\frac{\partial \mathbb{P}\Big[(V_1, \ldots, V_k)\,|\widehat{V}_k\Big]}{\partial \widehat{V}_k} = \begin{pmatrix} k \\ s \end{pmatrix} \Big[ s\widehat{V}_k^{\,s-1} \left(1 - \widehat{V}_k\right)^{k-s} - (k-s)\,\widehat{V}_k^{\,s} \left(1 - \widehat{V}_k\right)^{k-s-1} \Big]. \tag{3.14}$$

Setting this equal to zero while noting that $\begin{pmatrix} k \\ s \end{pmatrix}$ is a strictly positive real number yields

$$s\widehat{V}_k^{\,s-1} \left(1 - \widehat{V}_k\right)^{k-s} - (k-s)\,\widehat{V}_k^{\,s} \left(1 - \widehat{V}_k\right)^{k-s-1} = 0 \tag{3.15}$$

$$\widehat{V}_k^{\,s-1} \left(1 - \widehat{V}_k\right)^{k-s-1} \left(s - k\widehat{V}_k\right) = 0. \tag{3.16}$$

This manipulation has resulted in three stationary points for the maximum likelihood estimator. Two of these points are not of interest as they correspond to the edge cases, namely $\widehat{V}_{ML} = 0$ and $\widehat{V}_{ML} = 1$. However, the third stationary point gives the maximum of the ML estimator as

$$\widehat{V}_{ML} = \frac{s}{k} = \frac{1}{k} \sum_{i=1}^{k} V_i. \tag{3.17}$$

With this in mind, the hypothesis detection problem becomes

$$H_0 : \left| \sum_{i=0}^{k} \frac{V_i}{k} - \overline{V} \right| < \delta, \tag{3.18a}$$

$$H_1 : \left| \sum_{i=0}^{k} \frac{V_i}{k} - \overline{V} \right| \geq \delta. \tag{3.18b}$$

Note that due to the absolute value of the distance, this hypothesis test is two sided.

## 3.5 Attacker Model

Our work diverges from the literature by introducing an attacker that controls the packet drops within the communication channel. From the point of view of the attacker, the loss parameter $V_k$ becomes the control variable to achieve their objective. Specifically $V_k$ is not a random variable and $U_k$ is no longer a control variable. Instead, in this setting $V_k$ is a deterministic input sequence that the attacker constructs based on the available information set. This control input is optimised at each time instant by the attacker, with the aim of maximising the cost function of the operator. It is assumed that the attacker has access to the entire system architecture in addition to the observation and state estimate, i.e. $Y_k, \widehat{X}_k$. Naturally, this implies that the attacker has access to the same information as the operator in addition to control of packet drops $V_k$. Bear in mind that the attacker has no control over the choice of $U_k$. Therefore, the information set available to the attacker is

$$\mathscr{A}_k \triangleq \left\{ V_k^A, \mathscr{Y}_k, \widehat{\mathscr{X}}_k, \mathscr{A}_{k-1} \right\}, \tag{3.19}$$

where $V_k^A \in \{0, 1\}$ is a deterministic control variable controlled by the attacker and $\widehat{\mathscr{X}}_k = \left\{ \widehat{X}_0, \ldots, \widehat{X}_k \right\}$ is the set of all state estimates up until time instant $k$. As with the operators information set $\mathscr{A}_k$ is a monotonically increasing set. Note that the information set of the attacker differs in that it contains the current realisation of $V_k^A$. Due to these fundamental

changes in the control system, the system model is redefined for the attacker as

$$X_{k+1} = \mathbf{A}X_k + V_k^A \mathbf{B}\mathbf{K}\widehat{X}_k + W_k, \tag{3.20a}$$

$$Y_k = \mathbf{C}X_k + Z_k. \tag{3.20b}$$

The cost function of the attacker is similar to that of the operator, but in this case, the attacker aims to *maximise* the cost at each time instant with respect to $V_k^A$ as opposed to a minimisation with respect to $\mathbf{K}$. This formulation yields the optimal cost function of the attacker

$$J_N^{A^*}(\overline{X}_0, \mathbf{P}_0) = \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{ \mathbb{E}\left[ X_N^{\mathsf{T}} \mathbf{Q}_X X_N + \sum_{k=0}^{N-1} \begin{pmatrix} X_k \\ \mathbf{K}\widehat{X}_k \end{pmatrix}^{\mathsf{T}} \begin{pmatrix} \mathbf{Q}_X & 0 \\ 0 & V_k^A \mathbf{Q}_U \end{pmatrix} \begin{pmatrix} X_k \\ \mathbf{K}\widehat{X}_k \end{pmatrix} \middle| \overline{X}_0, \mathbf{P}_0 \right] \right\}, \tag{3.21}$$

where the decision at time $k$ of the realisation of $V_k^A$ is a function of the information set $\mathscr{A}_k$. For the attacker, the optimal estimation procedure is the same as for the operator. Thus, in the case in which the attacker is not able to directly access $\widehat{X}_k$ the variable is computed using the same process as the operator, i.e. (3.7). Note that in (3.21) the attacker does not initially penalise the attack construction in any way to induce stealth. This assumption is later introduced for attack constructions that almost target minimising the probability of detection. We term these differing attack constructions as unconstrained and constrained. This is due to the fact that, in the constrained setting, the attacker limits their damage potential in order to remain undetected.

## 3.6 Optimal Unconstrained Attack

The first attack construction is a *naive attack*. Additionally, the operator's MARE (3.6), is assumed to have converged before the attack takes place i.e. $\mathbf{S}_k = \mathbf{S}_\infty$. As a result

of this assumption, the operator implements the optimal steady state input gain $\mathbf{K}^*$. This assumption is dropped in later derivations. This simpler setting is first presented as an introduction to the problem that captures the main features of the problem. The attacker maximises the cost of the operator without any detection constraints. In order to compute the sequence of optimal packet drops that maximise the cost function (3.43), a dynamic programming formulation is used. To that end, the optimal value function for the attacker $f_k(X_k)$ is defined as

$$f_N\left(X_N\right) \triangleq \mathbb{E}\left[X_N^{\mathsf{T}}\mathbf{Q}_X X_N \middle| \mathscr{A}_N\right], \tag{3.22a}$$

$$f_k\left(X_k\right) \triangleq \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{Q}_X X_k + V_k^{A^*}\widehat{X}_k^{\mathsf{T}}\mathbf{K}^{*\mathsf{T}}\mathbf{Q}_U\mathbf{K}^*\widehat{X}_k + f_{k+1}(X_{k+1}) \middle| \mathscr{A}_k\right]\right\}, \tag{3.22b}$$

where $N \in \mathbb{N}$ is the time horizon for the system. This leads to the following lemma

**Lemma 1.** *The optimal value function (3.22) for the system defined in (3.20) is equivalent to*

$$f_k(X_k) \triangleq \mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{R}_k X_k \middle| \mathscr{A}_k\right] + \ d_k, \quad k = N, \ldots, 0, \tag{3.23}$$

*where the matrix $\mathbf{R}_k \in \mathbb{M}^n$ and the scalar $d_k \in \mathbb{R}$ are recursively calculated according to*

$$\mathbf{R}_k = \mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X + V_k^{A^*}\left(\mathbf{K}^{\mathsf{T}}\left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\right)\mathbf{K} - 2\mathbf{K}^{\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A}\right), \tag{3.24a}$$

$$d_k = \operatorname{tr}\left(\left(\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X - \mathbf{R}_k\right)\mathbf{P}_{k|k}\right) + \operatorname{tr}\left(\Sigma_W\mathbf{R}_{k+1}\right) + \mathbb{E}[d_{k+1}|\mathscr{A}_k], \tag{3.24b}$$

*where $V_k^{A^*}$ is the optimal choice that maximises the cost function (3.21) at time instant $k$ that satisfies*

$$V_k^{A^*} = \begin{cases} 1 & \text{for} \quad \widehat{X}_k^{\mathsf{T}}\left(\mathbf{K}^{\mathsf{T}}\left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\right)\mathbf{K} - 2\mathbf{K}^{\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A}\right)\widehat{X}_k \geq 0, \\ 0 & \text{otherwise.} \end{cases} \tag{3.25}$$

*Proof.* See Appendix A.

The dynamic programming algorithm guarantees that $f_0(X_0) = J_N^{A^*}$. Therefore, the cost whilst under the optimal attack is

$$J_N^{A^*}(\overline{X}_0, \mathbf{P}_0) = X_0^{\mathsf{T}}\mathbf{R}_0 X_0 + \operatorname{tr}(\mathbf{R}_0\mathbf{P}_0) + \sum_{k=0}^{N-1} \operatorname{tr}\left(\mathbf{R}_{k+1}\mathbf{Q}\right) + \sum_{k=0}^{N-1} \operatorname{tr}\left(\left(\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X - \mathbf{R}_k\right)\mathbf{P}_{k|k}\right), \quad (3.26)$$

where it should be noted that $\mathbf{R}_k \neq \mathbf{S}_k$ for all $k > 0$ and $\mathbf{R}_0 = \mathbf{S}_0 = \mathbf{0}$. Analysis of the behaviour of the $\mathbf{R}_k$ matrix is not straight forward, and therein the attack construction. Particularly it should be noted that the variable $\mathbf{R}_k$ is not monotonic, this is displayed graphically in Chapter 8. Due to this property the analysis of the attack constructions behaviour is non-trivial and an open problem. However, it is seen within the simulations in Chapter 8 that the optimal attack for this construction is a sequence of all zeros.

Although the above attack construction is optimal under the circumstances given, it has significant practical limitations. Specifically, the attack construction can only be used once the operator has reached steady state operation. Additionally, the attack derived above does not consider any form of attack detection, which is why we have termed it the 'naive attack'. In the following section, the attack construction is extended to the case where the operator is implements a time-varying gain matrix $\mathbf{K}_k$. This enables attacks to be implemented at any point during the operation of the system.

## 3.7 Optimal Unconstrained Attack with Time-Varying Gain

In this section we consider the case in which the operator employs a time-varying gain. This means the operator is no longer operating according to the steady state MARE $\mathbf{S}_\infty$ and instead uses the time-varying MARE $\mathbf{S}_k$. This in turn induces a time-varying gain $\mathbf{K}_k$. The method to optimally compute this gain is shown in [59]. A lemma from [59] that is

central to this result is reported below with the difference that the minimisation is over the gain $\mathbf{K}_k$ instead of over $U_k$.

**Lemma 2.** *[lemma 5.1, [59]]*

*Assume a linear time-varying gain such that* $u_k^* = -\mathbf{K}_k^* \widehat{x}_{k|k}$. *Then the value function of the system under TCP-like operation is*

$$g_k(X_k) \triangleq \mathbb{E}\left[X_k^{\mathsf{T}} \mathbf{S}_k X_k \middle| \mathcal{A}_k\right] + c_k, \quad k = N, \ldots, 0, \tag{3.27}$$

*and it is known that* $\mathbf{S}_k$ *and* $c_k$ *are*

$$\mathbf{S}_k = \mathbf{A}^{\mathsf{T}} \mathbf{S}_{k+1} \mathbf{A} + \mathbf{Q}_X - \overline{V} \mathbf{A}^{\mathsf{T}} \mathbf{S}_{k+1} \mathbf{B} \mathbf{K}_k^*, \tag{3.28}$$

$$c_k = \overline{V} \mathrm{tr}(\mathbf{A}^{\mathsf{T}} \mathbf{S}_{k+1} \mathbf{B} \mathbf{K}_k^* \mathbf{P}_{k|k}) + \mathrm{tr}\left(\mathbf{Q} \mathbf{S}_{k+1}\right) + \mathbb{E}[c_{k+1} | \mathcal{O}_k], \tag{3.29}$$

*and the resultant optimal gain,* $\mathbf{K}_k^*$ *is*

$$\mathbf{K}_k^* = \left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}} \mathbf{S}_{k+1} \mathbf{B}\right)^{-1} \mathbf{B}^{\mathsf{T}} \mathbf{S}_{k+1} \mathbf{A}. \tag{3.30}$$

*Proof.* See Appendix A.2.

The time-varying gain changes the formulation of the innovation step, as well as the source and observation models defined in (3.7), (3.1a), and (3.1b), respectively. Specifically, the gain matrices in each of the relations are replaced with their time-varying versions. The cost for the operator remains as in (3.8),but note that $\mathbf{S}_k$ and $U_k^*$ are now equivalent to

$$\mathbf{S}_k = \mathbf{A}^{\mathsf{T}} \mathbf{S}_{k+1} \mathbf{A} + \mathbf{Q}_X - \overline{V} \mathbf{A}^{\mathsf{T}} \mathbf{S}_{k+1} \mathbf{B} \mathbf{K}_k, \tag{3.31}$$

$$\mathbf{K}_k = \left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}} \mathbf{S}_k \mathbf{B}\right)^{-1} \mathbf{B}^{\mathsf{T}} \mathbf{S}_k \mathbf{A}, \tag{3.32}$$

$$U_k^* = -\mathbf{K}_k^* \widehat{X}_{k|k}. \tag{3.33}$$

The expected cost for the operator is also equivalent to that in[59][Lemma 5.1]

$$J_N^* = X_0^\mathsf{T}\mathbf{S}_0X_0 + \mathrm{tr}(\mathbf{S}_0\mathbf{P}_0) + \sum_{k=0}^{N-1}\mathrm{tr}\left(\mathbf{S}_{k+1}\mathbf{Q}\right) + \sum_{k=0}^{N-1}\mathrm{tr}\left(\left(\mathbf{A}^\mathsf{T}\mathbf{S}_{k+1}\mathbf{A} + \mathbf{Q}_X - \mathbf{S}_k\right)\mathbf{P}_{k|k}\right). \quad (3.34)$$

It should be noted that this is the expected cost given that there is no attack present. Otherwise, this expected cost is invalid because the control law and the cost function are calculated with an incorrect percentage of packet drops in the channel.

From the perspective of the attacker, Lemma 1 must also be modified to account for the time-varying gain. It is assumed that the attacker has access to $\mathbf{K}_k^*$ which can be computed from the attack information set if required. The optimal attack in this setting is described in the following lemma.

**Theorem 1.** *The optimal value function of the attacker for the system (3.20) is defined as*

$$f_N\left(X_N\right) \triangleq \mathbb{E}\left[X_N^\mathsf{T}\mathbf{Q}_X X_N \middle| \mathscr{A}_N\right], \quad (3.35a)$$

$$f_k\left(X_k\right) \triangleq \max_{V_k^A}\left\{\min_{K_k=g_k(\mathscr{A}_k)}\left\{\mathbb{E}\left[X_k^\mathsf{T}\mathbf{Q}_X X_k + V_k^{A^*}\widehat{X}_k^\mathsf{T}\mathbf{K}_k^\mathsf{T}\mathbf{Q}_U K_k\widehat{X}_k + f_{k+1}\left(X_{k+1}\right)\middle|\mathscr{A}_k\right]\right\}\right\}, \quad (3.35b)$$

*where the minimising $\mathbf{K}_k$ is (3.30). It is shown that (3.35) is equivalent to*

$$f_k(X_k) \quad = \quad \mathbb{E}\left[X_k^\mathsf{T}\mathbf{R}_k X_k\middle|\mathscr{A}_k\right] + \ d_k, \quad k = N,\ldots,0, \quad (3.36)$$

*where the matrix $\mathbf{R}_k \in \mathbb{M}^n$ and the scalar $d_k \in \mathbb{R}$ are recursively calculated according to*

$$\mathbf{R}_k = \ \mathbf{A}^\mathsf{T}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X + V_k^{A^*}\left(\mathbf{K}_k^{*\mathsf{T}}\left(\mathbf{Q}_U + \mathbf{B}^\mathsf{T}\mathbf{R}_{k+1}\mathbf{B}\right)\mathbf{K}_k^* - 2\mathbf{K}_k^{*\mathsf{T}}\mathbf{B}^\mathsf{T}\mathbf{R}_{k+1}\mathbf{A}\right), \quad (3.37)$$

$$d_k = \ V_k^{A^*}\mathrm{tr}\left(\left(\mathbf{A}^\mathsf{T}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X - \mathbf{R}_k\right)\mathbf{P}_{k|k}\right) + \mathrm{tr}\left(\Sigma_W\mathbf{R}_{k+1}\right) + \mathbb{E}[d_{k+1}|\mathscr{A}_k], \quad (3.38)$$

*where $V_k^{A^*}$ represents the optimal value at time $k$ that maximises the cost function of the operator and $\mathbf{K}_k^*$ is the optimal time-varying gain that the operator implements at time $k$.*

*The optimal value of* $V_k^{A^*}$ *is determined by the inequality*

$$V_k^{A^*} = \begin{cases} 1 & \text{for} \quad \widehat{X}_k^{\mathsf{T}}\Big(\mathbf{K}_k^{*\mathsf{T}}\Big(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\Big)\mathbf{K}_k^* - 2\mathbf{K}_k^{*\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A}\Big)\widehat{X}_k > 0, \\ 0 & \text{otherwise,} \end{cases} \tag{3.39}$$

*with*

$$\mathbf{K}_k^* \triangleq \left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\right)^{-1}\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}. \tag{3.40}$$

*Proof.* The proof is moved to Appendix A.3. As before the characteristics of the $\mathbf{R}_k$ variable are difficult and non-trivial to characterise. However, as with the scenario in the previous section we show in the simulations in Chapter 8 that the optimal attack sequence for this construction remains a sequence of all zeros.

Under the same principles as before the expected cost of the system, (3.21), while under this attack construction is

$$J_N^A(\overline{X}_0, \mathbf{P}_0) = X_0^{\mathsf{T}}\mathbf{R}_0 X_0 + \operatorname{tr}(\mathbf{R}_0\mathbf{P}_0) + \sum_{k=0}^{N-1}\operatorname{tr}\left(\mathbf{R}_{k+1}\mathbf{Q}\right) + \sum_{k=0}^{N-1}\operatorname{tr}\left(\left(\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X - \mathbf{R}_k\right)\mathbf{P}_{k|k}\right). \tag{3.41}$$

## 3.8 Optimal Attack with a Constant Detection Constraint

In the previous sections, the attacker increased the cost of the operator with no regard as to whether the operator detects the attack. In this section it is assumed that the attacker wishes to remain undetected while increasing the operators cost function. To that end, a detection constraint is introduced to ensure the hypothesis test (3.18) remains null. In order for the hypothesis test to remain null the attacker must incorporate the test seen in (3.18) within their attack construction. Namely, this term must be included into the cost function in such a way that any deviations from the operator's postulated mean $\overline{V}$

penalise the attacker. This is done by introducing the optimal detection constraint as seen in (3.17). The attacker employs the following as their *penalty* for a stealthy attack

$$t\left(\Lambda\right) = -\Lambda\left(\sum_{i=0}^{k}\frac{V_i^A}{k} - \overline{V}\right), \tag{3.42}$$

where $\Lambda \in \mathbb{R}$ is to be treated as the penalty term for the degree of stealth of the attack. This is similar to the purpose of $\mathbf{Q}_X$ and $\mathbf{Q}_U$ for the operator.

The penalty variable $\Lambda$ has the same purpose for the attacker as the state and input penalty matrices do for the operator, i.e. it is a tuning parameter for the attacker to determine the stealth of the attack. It is clear that when $\Lambda = 0$ the constrained attacked is equivalent to the unconstrained attack. Assuming the operator uses (3.18) as the detection hypothesis test, then the cost function of the attacker takes the form

$$\begin{aligned} J_N^A\left(\overline{X}_0, \mathbf{P}_0\right) = \max_{V_k^A = f_k(\mathscr{A}_k)} \Bigg\{ \mathbb{E}\Bigg[ & X_N^{\mathsf{T}}\mathbf{Q}_X X_N \\ & + \sum_{k=0}^{N-1} \begin{pmatrix} X_k \\ \mathbf{K}\widehat{X}_k \\ \widehat{X}_k \end{pmatrix}^{\mathsf{T}} \begin{pmatrix} \mathbf{Q}_X & 0 & 0 \\ 0 & V_k^A\mathbf{Q}_U & 0 \\ 0 & 0 & t\left(\Lambda\right) \end{pmatrix} \begin{pmatrix} X_k \\ \mathbf{K}\widehat{X}_k \\ \widehat{X}_k \end{pmatrix} \Bigg| \overline{X}_0, \mathbf{P}_0 \Bigg] \Bigg\}, \end{aligned} \tag{3.43}$$

where the inclusion of (3.42) with scaling proportional to the current state estimate is the only change from (3.21).

The reason for the appearance of $\widehat{X}_k$ in the detection term may not be obvious. However, as seen in (3.25) and (3.39), the optimal choice for $V_k^{A^*}$ is scaled by the magnitude of $\widehat{X}_k$. If the system becomes rapidly unstable, through no fault of the attacker $\widehat{X}_k$ also increases rapidly at which point the contribution of the detection term reduces. Therefore, the detection term must also be scaled to maintain a stealthy attack under these circumstances. The system for the operator remains as in the time-varying gain scenario. To that end, we present the following lemma

**Lemma 3.** *The optimal value function for the attack on the system (3.20) where the operator assumes IID packet drops, is defined as*

$$f_N\left(X_N\right) \triangleq \mathbb{E}\left[X_N^{\mathsf{T}}\mathbf{Q}_X X_N \middle| \mathscr{A}_N\right], \tag{3.44a}$$

$$f_k\left(X_k\right) \triangleq \max_{V_k^A = f_k(\mathscr{A}_k)} \Big\{\mathbb{E}\Big[X_k^{\mathsf{T}}\mathbf{Q}_X X_k + V_k^A \widehat{X}_k^{\mathsf{T}}\mathbf{K}_k'^{*}\mathbf{Q}_U\mathbf{K}_k^{*}\widehat{X}_k + \widehat{X}_k^{\mathsf{T}} t\left(\Lambda\right)\widehat{X}_k + f_{k+1}\left(X_{k+1}\right)\Big|\mathscr{A}_k\Big]\Big\}. \tag{3.44b}$$

*It holds that (3.44) is equivalent to*

$$f_k(X_k) \quad = \quad \mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{R}_k X_k \middle| \mathscr{A}_k\right] + \ d_k, \quad k = N, \ldots, 0, \tag{3.45}$$

*with the matrix $\mathbf{R}_k \in \mathbb{M}^n$ and $d_k \in \mathbb{R}$ are recursively calculated according to*

$$\begin{aligned}\mathbf{R}_k = {} & \mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X \\ & + V_k^{A^*}\left(\mathbf{K}_k^{*\mathsf{T}}\left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\right)\mathbf{K}_k^{*} - 2\mathbf{K}_k^{*\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A}\right), \end{aligned} \tag{3.46}$$

$$\begin{aligned} d_k = {} & V_k^{A^*}\mathrm{tr}\left(\left(\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X - \mathbf{R}_k\right)\mathbf{P}_{k|k}\right) + \mathrm{tr}\left(\Sigma_W\mathbf{R}_{k+1}\right) + \mathbb{E}[d_{k+1}|\mathscr{A}_k] \\ & + \widehat{X}_k t\left(\Lambda\right)\widehat{X}_k, \end{aligned} \tag{3.47}$$

*where $V_k^{A^*}$ represents the optimal realisation that maximises the cost function of the operator. The value is determined by the inequality*

$$V_k^{A^*} = \begin{cases} 1 & \text{for} \quad \widehat{X}_k^{\mathsf{T}}\left(\mathbf{K}_k^{*\mathsf{T}}\left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\right)\mathbf{K}_k^{*} - 2\mathbf{K}_k^{*\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A}\right)\widehat{X}_k \\ & \qquad\qquad > \widehat{X}_k t\left(\Lambda\right)\widehat{X}_k, \\ 0 & \text{otherwise}, \end{cases} \tag{3.48}$$

*where*

$$\mathbf{K}_k^{*} \triangleq \left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\right)^{-1}\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}. \tag{3.49}$$

*Proof.* The proof of this Lemma follows the exact same process as Lemma 1 with the detection term following throughout.

The above attack construction differs from the previous in that the actuation law, (3.48) requires the left hand side to be only less negative than the right hand side. This differs from the previous unconstrained construction where an actuation would require the left hand side to be positive definite. Additionally it should be clear that the right hand side changes it's positivity depending on the choice of the sequence of $V^A$. Due to this fact analytical analysis of this construction is non-trivial.

Unfortunately, this attack construction is not perfect. Specifically, this attack construction remains undetectable for a finite period of time proportional to the magnitude of $\Lambda$. Furthermore, within this period of time of stealthiness, the attack variable choice is completely dominated by the detection constraint. In fact, as seen in the simulations within Section 8.1, this gives the operator a better cost than expected before reverting to the unconstrained attack construction. To see the this convergence see the following.

$$t\left(\Lambda\right) = -\Lambda\left(\sum_{i=0}^{k}\frac{V_i^A}{k} - \overline{V}\right). \tag{3.50}$$

This term converges to $\epsilon > 0$ for a sequence of $V_i^A$ that are statistically similar to a sequence of nominal losses $V_i$. To see this, note the following lemmas.

**Lemma 4.** *The ML estimator is unbiased Specifically,*

$$\mathbb{E}\left[\widehat{V}_{ML}\right] \xrightarrow[k\to\infty]{} \overline{V}. \tag{3.51}$$

*Proof.* By the weak law of large numbers

$$\lim_{k\to\infty}\mathbb{P}\left[\left|\sum_{i=0}^{k}\frac{V_i}{k} - \overline{V}\right| > \epsilon\right] = 0, \tag{3.52}$$

where $\epsilon > 0$ is an arbitrarily small scalar value. This concludes the proof. □

With the above lemma it is able to be shown that the convergence of this value is of order $\sqrt{k}$.

**Lemma 5.** *Due to the relation (3.51), it holds that*

$$\mathbb{E}\left[\left(\widehat{V}_{ML} - \overline{V}\right)^2\right] = \frac{1}{k}\overline{V}\left(1 - \overline{V}\right), \tag{3.53}$$

*and therefore the variance of the square error in the ML estimator decreases with order* $\frac{1}{k}$.

*Proof.* Beginning with the definition

$$k\widehat{V}_{ML} = \sum_{i=1}^{k} V_i, \tag{3.54}$$

it is then seen that taking expectations of both sides yields

$$\mathbb{E}\left[k\widehat{V}_{ML}\right] = k\overline{V}. \tag{3.55}$$

Similarly, taking the variance of both sides yields

$$\mathbb{E}\left[\left(k\widehat{V}_{ML} - k\overline{V}\right)^2\right] = k\overline{V}\left(1 - \overline{V}\right), \tag{3.56}$$

pulling the $k$ term outside of the expectation and dividing yields the desired relation. This concludes the proof. □

The attacker is constructing a sequence of variables that are statistically similar to the nominal statistics. However, the attacker picks a sequence of variables that maximise the cost whilst remaining $\epsilon$ close to the nominal statistics. In doing so, the detection constraint converges, as predicted by Lemma 5. As a result of this convergence, the attack decision becomes equivalent to (3.39) i.e. the unconstrained attack construction. However, in Section 8.1 it is seen that the MARE corresponding to the unconstrained attack grows exponentially. Unfortunately, the detection constraint of the attacker grows linearly for the case of $V_i^A = 0$ for all $i$. Therefore, after a period of time that is proportional to

the magnitude of $\Lambda$ the detection constraint converges to $\epsilon$. By this it is meant that the detection term (3.50) converges at a rate of order $\Lambda\frac{1}{k}$. After this point, the attack construction reverts to the unconstrained attack construction and the attack is detected. However, as seen within Lemma 5, the rate at which the detection term converges is known. This construction therefore, is able to be improved upon.

## 3.9 Optimal Attack construction with Time Varying Detection Constraint

This attack behaviour seen from the constant detection term is not practical since the attack is only stealthy for a finite period of time. Instead, it is desirable that a practical attack implementation maintains stealth for an arbitrary time duration. In an attempt to mitigate the convergence of the detection constraint, as seen in Lemma 5, the attacker employs a time-varying detection constraint. This time-varying detection constraint mitigates the convergence of the constant detection term in the previous section. Specifically, the constraint scales with $\sqrt{k}$. Time varying constraint also ensures that if there is a convergence, the detection constraint grows linearly with the MARE of the attacker, as opposed to sub-linearly.

The operator performs the same hypothesis test that takes place in (3.18), as in previous sections. The attacker employs the following as their *penalty* for a stealthy attack

$$t\left(\Lambda_k\right) = -\Lambda_k \left(\sum_{i=0}^{k} \frac{V_i^A}{k} - \overline{V}\right), \tag{3.57}$$

where $\Lambda_k \in \mathbb{R}$ is to be treated as the penalty term for the degree of stealth of the attack. The time-varying stealth penalty term $\Lambda_k$ is defined as

$$\Lambda_k = \Lambda \mathbf{R}_{k+1} \sqrt{k}. \tag{3.58}$$

As with the the previous attack, the penalty term $\Lambda$ is similar to the purpose of $\mathbf{Q}_X$ and $\mathbf{Q}_U$ for the operator. Observe that the time-varying stealth penalty term is weighted by the square root of $k$ to counter the convergence of the packet drop sequence. Additionally, the inclusion of the term $\mathbf{R}_{k+1}$ ensures that the detection constraint grows linearly with the MARE. As before, the larger $\Lambda$ is, the stealthier the attack, and when it is set to 0 the attack is equivalent to the unconstrained attack. However, with the time-varying constraint, the $\Lambda$ variable does not control the time window for the attack. Therefore, this attack construction provides stealth for an arbitrary period of time. Again, the penalty term is included in the cost function of the attacker just as any other penalty term. Therefore, the resulting cost function of the attacker including the time-varying detection constraint is

$$J_N^A\left(\overline{X}_0, \mathbf{P}_0\right) = \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{ \mathbb{E}\left[ X_N^{\mathsf{T}} \mathbf{Q}_X X_N + \sum_{k=0}^{N-1} \begin{pmatrix} X_k \\ \mathbf{K}_k^* \widehat{X}_k \\ \widehat{X}_k \end{pmatrix}^{\mathsf{T}} \begin{pmatrix} \mathbf{Q}_X & 0 & 0 \\ 0 & V_k^A \mathbf{Q}_U & 0 \\ 0 & 0 & t\left(\Lambda_k\right) \end{pmatrix} \begin{pmatrix} X_k \\ \mathbf{K}_k^* \widehat{X}_k \\ \widehat{X}_k \end{pmatrix} \middle| \overline{X}_0, \mathbf{P}_0 \right] \right\}, \tag{3.59}$$

where the inclusion of (3.57) is the only change from (3.42). Which brings us to the next lemma.

**Lemma 6.** *The optimal value function for the attack on the system system (3.20), where the operator assumes IID packet drops, with a time-varying detection constraint is defined*

*as*

$$f_N\left(X_N\right) \triangleq \mathbb{E}\left[X_N^{\mathsf{T}}\mathbf{Q}_X X_N \middle| \mathscr{A}_N\right], \tag{3.60a}$$

$$f_k\left(X_k\right) \triangleq \max_{V_k^A = f_k(\mathscr{A}_k)} \Big\{\mathbb{E}\Big[X_k^{\mathsf{T}}\mathbf{Q}_X X_k + V_k^A \widehat{X}_k^{\mathsf{T}}\mathbf{K}_k'^{*}\mathbf{Q}_U\mathbf{K}_k^{*}\widehat{X}_k + \widehat{X}_k^{\mathsf{T}} t\left(\Lambda_k\right)\widehat{X}_k + f_{k+1}\left(X_{k+1}\right)\Big|\mathscr{A}_k\Big]\Big\}, \tag{3.60b}$$

*where* $\Lambda_k$ *is defined as*

$$\Lambda_k = \Lambda\mathbf{R}_{k+1}\sqrt{k}. \tag{3.61}$$

*It holds that (3.60) is equivalent to*

$$f_k(X_k) \quad \triangleq \quad \mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{R}_k X_k\middle|\mathscr{A}_k\right] + \ d_k, \quad k = N,\ldots,0, \tag{3.62}$$

*where the matrix* $\mathbf{R}_k \in \mathbb{M}^n$ *and* $d_k \in \mathbb{R}$ *are recursively calculated according to*

$$\mathbf{R}_k = \mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X + V_k^{A^*}\left(\mathbf{K}_k^{*\mathsf{T}}\left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\right)\mathbf{K}_k^{*} - 2\mathbf{K}_k^{*\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A}\right), \tag{3.63}$$

$$d_k = V_k^{A^*}\mathrm{tr}\left(\left(\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X - \mathbf{R}_k\right)\mathbf{P}_{k|k}\right) + \mathrm{tr}\left(\Sigma_W\mathbf{R}_{k+1}\right) + \mathbb{E}[d_{k+1}|\mathscr{A}_k] + \widehat{X}_k t\left(\Lambda_k\right)\widehat{X}_k, \tag{3.64}$$

*where* $V_k^{A^*}$ *represents the optimal decision of* $V_i^A$ *that maximises the cost function of the operator. The decision is determined by the inequality*

$$V_k^{A^*} \triangleq \begin{cases} 1 & \text{for} \quad \left(\mathbf{K}_k^{*\prime}\left(\mathbf{Q}_U + \mathbf{B}'\mathbf{R}_{k+1}\mathbf{B}\right)\mathbf{K}_k^{*} - 2\mathbf{K}_k^{*\prime}\mathbf{B}'\mathbf{R}_{k+1}\mathbf{A}\right) > t\left(\Lambda_k\right) \\ 0 & \text{otherwise,} \end{cases}, \tag{3.65}$$

*Proof.* The proof is moved to Appendix A.5.

The resultant cost of this attack is

$$J_N^{A^*}(\overline{X}_0, \mathbf{P}_0) = X_0^\mathsf{T}\mathbf{R}_0 X_0 + \operatorname{tr}(\mathbf{R}_0\mathbf{P}_0) + \sum_{k=0}^{N-1} \operatorname{tr}\left(\mathbf{R}_{k+1}\mathbf{Q}\right) + \sum_{k=0}^{N-1} \operatorname{tr}\left(\left(\mathbf{A}^\mathsf{T}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X - \mathbf{R}_k\right)\mathbf{P}_{k|k}\right). \tag{3.66}$$

However, it should be noted that the variables present within (3.66) refer to different realisations of each of the variables when compared to (3.41).

## 3.10 Chapter Conclusion

The attack strategies presented in this chapter result in optimal DoS attacks for the constraints considered in each construction. The constrained time-varying attack construction presented remains stealthy indefinitely. This construction is derived for the given hypothesis test that the operator is performing. Namely, the hypothesis test in (3.18). Were the operator to implement a different detection strategy, then the attack construction would take a different form. This back and forth is reminiscent of a game. Namely, each of the *players*, the operator and the attacker, take turns optimising their respective strategies. Under this interpretation we have stopped the *game* after a single turn each, with the operator going first. In the following chapters this stance remains. Namely, the operator taking the first turn in the *game* with the attacker going second. Note we calls this a *game* for descriptive purposes and do not present the following results as a game in the mathematically rigorous sense of a game.

The constrained time-varying attack strategy presented allows the attacker to tune the attack to trade-off the stealth of the attack for attack performance. This is achieved through use of the $\Lambda$ variable. As mentioned prior, the $\Lambda$ variable is a tuning parameter for the attack. This means that a larger value of $\Lambda$ results in the detection constraint dominating the cost function with either very little or no cost increase of the system. In fact for large enough $\Lambda$ the attacker improves the expected cost of the operator. This is explored further within Chapter 8. If however the value of $\Lambda$ is made small, or even 0,

the attack designed becomes aggressive causing large cost increases in the expected cost at the drawback of becoming more likely to be detected. This behaviour is comparable to that of the operators design of the penalty matrices $\mathbf{Q}_X$ and $\mathbf{Q}_U$ i.e. tuning these matrices in order to create desired system behaviours. The final attack strategy designed, the attack derived in Section 3.9, is not perfect in practice. For example, it has a high computational cost and requires full knowledge of the system and the operators choices. This strategy requires the attacker to calculate their own Ricatti equation in addition to then calculating the term in (3.65). Additionally, in order to calculate these objects, the attacker also requires knowledge of the current realisation of the operators gain, state estimation, and the Ricatti equation of the operator. With all of these drawbacks, an optimal stealthy attack strategy that requires less knowledge of the operators system choices or less computing power may be a more appealing choice.

# Chapter 4

# Control Systems with Communication Channel Packet Loss

## 4.1 Chapter Introduction

In the previous chapter the focus was upon the derivation of an optimal deterministic DoS attack strategy for a system experiencing packet loss. This was achieved by allowing the operator to design the optimal control law for a given system, and then switching perspectives to the attacker to design the optimal attack. This chapter focuses on the effect of packet loss on different control strategies. The effect of the attacker is studied in Chapter 5.

As mentioned above the system considered is changed in this chapter. Specifically, the communication channel that the control system operates over is altered. The optimal control and the resultant cost of controlling a system over a scalar packet loss communication channel is derived in [59]. This derivation is utilised in the previous chapter. In fact it is this control law that the operator utilises during the attacks derived. However, in the following chapter the system communicates over a multidimensional packet loss communication channel. This is a generalisation of the scalar communication channel. In generalising this, we derive the optimal control law for a system communicating over multiple *independent* packet loss communication channels. Additionally, unlike the previous

chapter, the operator is assumed to communicate over one of two different communication protocols. This enables the characterisation of the cost difference between the communication protocols. In [59, 65, 66, 46], two communication protocols are proposed for analysis. Namely, a TCP-like protocol and a UDP-like protocol. The TCP-like protocol remains as in the previous chapter, in that it implements an auxiliary acknowledgement signal that is transmitted back to the controller, confirming whether or not the control signal has been successfully received by the plant. In contrast to this, the UDP-like protocol lacks this acknowledgement link. As in Chapter 3 we adopt the zero input strategy. Therefore, in the event that the communication channel drops a packet, the actuators perform no actuation. It should be noted however, that each of the multiple dimensions within the channel operate independently. Namely, different actuators receive different realisations from the communication channel, and therefore, each actuator at any given time instant could perform a zero input due to a packet loss, while the other actuators receive a packet and perform the optimal actuation.

The actuation communication channel is extended from [59] and Chapter 3 to allow for multiple independent channels as opposed to a single channel shared by all actuators. As a result of this, we provide an analytical proof that the system cost is always greater as a result of not monitoring realisations of packet loss in the channel. Due to the communication channel being a generalisation of the result in [59], these results also apply to a simplified scalar communication channel. The maximal cost difference between the two protocols is also characterised. The packet loss in the communication channel is modelled as a set of Independent and Identically Distributed (IID) Bernoulli random variables. As a result, each actuator either receives the optimal input, or it receives zero input. The optimal control law is obtained by formulating the problem in a Model Predictive Control (MPC) framework. This subsequently enables the analytical comparison of the cost incurred by both protocols in a more tractable fashion that a dynamic programming approach.

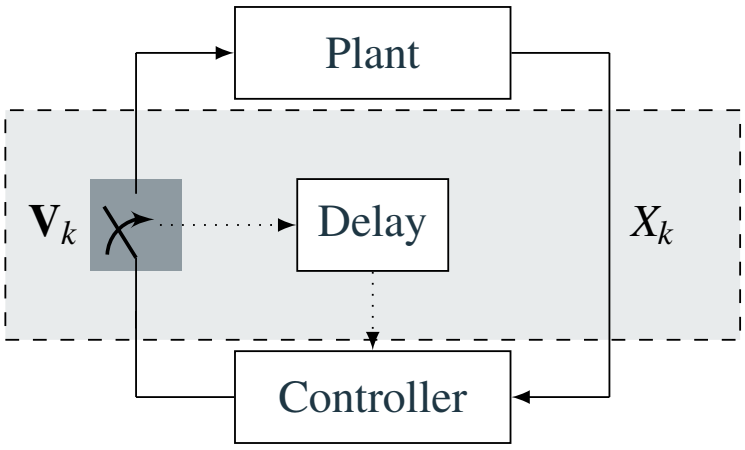


Fig. 4.1 Control system with TCP-like protocol where realisations of the packet transmission variable are transmitted to the controller.

## 4.2 System Model and Problem Formulation

We consider systems that consist of a plant, a controller and a communication channel, as shown in Fig. 4.1 and 4.2. Initially, packet loss only occurs in the controller to actuator communication channel; the sensor to controller communication channel is initially assumed to be perfect. However, later on in the Chapter this assumption is dropped. We consider the plant model described by

$$X_{k+1} = \mathbf{A}X_k + \mathbf{B}\mathbf{V}_k U_k + W_k, \tag{4.1}$$

where $\mathbf{A} \in \mathbb{R}^{n\times n}$ is the dynamics matrix; $X_k \in \mathbb{R}^n$ describes the state of the plant at time step $k \in \mathbb{N}$; $\mathbf{B} \in \mathbb{R}^{n\times m}$ is the control matrix; $U_k \in \mathbb{R}^m$ is the vector of control inputs; $W_k \in \mathbb{R}^n$ is the process noise modelled as a vector of Gaussian random variables with mean $\mathbf{0} \in \mathbb{R}^n$ and covariance matrix $\Sigma_W \in S^n_{++}$; where $S^n_{++}$ is the set of $n$ by $n$ symmetric positive definite matrices; $\mathbf{V}_k \in S^m_+$ is the packet transmission variable modelled as a diagonal matrix where the $i$-th diagonal entry is an IID Bernoulli random variable with mean $\mu_i \in [0,1]$ ; and $S^m_+$ is the set of $m$ by $m$ symmetric non-negative definite matrices. The initial state of the plant is determined by the Gaussian distributed vector of random variables $X_k$ with mean $\overline{X}_k$ and covariance matrix $\Sigma_{X_k} \in S^n_{++}$. Additionally, the expected

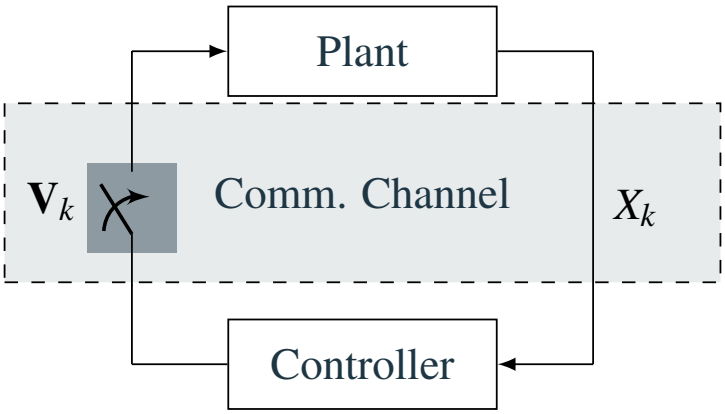


Fig. 4.2 Control system with UDP-like protocol where the realisations of the packet transmission variable are not transmitted to the controller

value of $\mathbf{V}_k$ is $\mathbb{E}[\mathbf{V}_k] = \mathbf{M}$, where $\mathbf{M} \in S^m_{++}$ is a diagonal matrix in which the i-th diagonal element is $\mu_i$.

It is in the structure of $\mathbf{V}_k$ and $\mathbf{M}$ that the system model differs from [59, 67, 46, 65, 63]. Defining $\mathbf{M}$ as a matrix models the case in which the system communicates over $m$ independent channels, where each actuator has a single dedicated communication channel. Specifically, the $m$-th control input communicates through the $m$-th channel which is completely solely by the $m$-th diagonal entry of $\mathbf{M}$. In contrast, were $\mathbf{M}$ and $\mathbf{V}_k$ to be defined as a scalars, all control inputs would share a single communication channel that is fully characterised by these scalars. Due to the imperfect communication between the controller and the plant, the operator implements a communication protocol. We adopt the two protocol paradigms mentioned previously. Namely, a UDP-like protocol that does not monitor the communication channel, and a TCP-like protocol that acknowledges receipt of the packet from the controller by sending an *acknowledgement* message to the controller over an auxiliary channel. As in [59], it is assumed that the auxiliary channel has perfect communication. The difference between both protocol paradigms is depicted in Fig. 4.1 and Fig. 4.2. The choice of protocol paradigm for a system results in different information available for the controller. We define the information available at the controller for each

protocol with the following two information sets

$$\mathscr{I}_k \triangleq \begin{cases} \mathscr{F}_k = \left\{\mathscr{X}^k, \mathscr{V}^{k-1}\right\}, & \text{TCP-like,} \\ \mathscr{G}_k = \left\{\mathscr{X}^k\right\}, & \text{UDP-like,} \end{cases} \tag{4.2}$$

where $\mathscr{V}^{k-1} \triangleq \left\{\mathbf{V}_0, \mathbf{V}_1, \ldots, \mathbf{V}_{k-1}\right\}$ and $\mathscr{X}^k \triangleq \{X_0, X_1, \ldots, X_k\}$. Note that all sets are monotonically increasing, i.e. $\mathscr{I}_k \subseteq \mathscr{I}_{k+1}$. Additionally, the lower indices represent the time index whereas upper indices refers to the dimension of the information sets. The information set at each time step contains the information from all previous time steps in addition to the information from the current time step.

Under the TCP-like protocol, the controller has access to the realisation of the packet transmission variable $\mathbf{V}_k$ when performing state estimation and incorporates it in the error prediction to obtain an estimate with error

$$\begin{aligned} E_{k+1}(\mathscr{F}_k) &\triangleq X_{k+1} - \mathbb{E}\left[X_{k+1}\middle|\mathscr{F}_k, \mathbf{V}_k\right] \\ &= \mathbf{A}X_k + \mathbf{B}\mathbf{V}_k U_k(\mathscr{F}_k) + W_k - \mathbf{A}\widehat{X}_k - \mathbf{B}\mathbf{V}_k U_k(\mathscr{F}_k) \\ &= \mathbf{A}E_k\left(\mathscr{F}_{k-1}\right) + W_k, \end{aligned} \tag{4.3a}$$

where $\widehat{X}_k \triangleq \mathbb{E}[X_k]$. The control law is redefined as $U_k(\mathscr{I}_k) \in \mathbb{R}^m$ to explicitly show the functions dependency on the information set $\mathscr{I}_k$. Additionally, the control law takes the form of a state feedback law, and is therefore, a random variable. The UDP-like protocol error prediction differs from the TCP-like protocol in that there is no knowledge of the realisation of $\mathbf{V}_k$, and therefore, the error for the UDP-like protocol is given by

$$\begin{aligned} E_{k+1}(\mathscr{G}_k) &\triangleq X_{k+1} - \mathbb{E}\left[X_{k+1}\middle|\mathscr{G}_k\right] \\ &= \mathbf{A}X_k + \mathbf{B}\mathbf{V}_k U_k(\mathscr{G}_k) + W_k - \mathbf{A}\widehat{X}_k - \mathbf{B}\mathbf{M}U_k(\mathscr{G}_k) \\ &= \mathbf{A}E_k\left(\mathscr{G}_{k-1}\right) + \mathbf{B}\left(\mathbf{V}_k - \mathbf{M}\right)U_k(\mathscr{G}_k) + W_k. \end{aligned} \tag{4.3b}$$

Note that the error prediction for both the UDP-like and the TCP-like protocol resemble those in [59]. As shown in [59], the optimal linear control law for the UDP-like protocol can only be obtained when perfect state information is available. Indeed, the lack of knowledge about the packet loss breaks the separation structure between optimal estimation and optimal control. It is here our derivation diverges again from [59]. Assuming perfect knowledge of the realisation of $X_k$, (4.1) is expanded over a time horizon $N \in \mathbb{N}$ as follows

$$\begin{aligned}
X_{k+1} &= \mathbf{A}X_k + \mathbf{B}\mathbf{V}_k U_k(\mathcal{I}_k) + W_k \\
X_{k+2} &= \mathbf{A}X_{k+1} + \mathbf{B}\mathbf{V}_{k+1} U_{k+1}(\mathcal{I}_k) + W_{k+1} \\
&\vdots \quad\quad \vdots \quad\quad\quad\quad \vdots \quad\quad\quad\quad \vdots \\
X_{k+N} &= \mathbf{A}X_{k+N-1} + \mathbf{B}\mathbf{V}_{k+N-1} U_{k+N-1}(\mathcal{I}_k) + W_{k+N-1}.
\end{aligned} \tag{4.4}$$

Exploiting the recursive structure of the above allows the states to be expressed in terms of the initial state $X_k$. This is seen to be

$$\begin{aligned}
X_{k+1} &= \mathbf{A}X_k + \mathbf{B}\mathbf{V}_k U_k(\mathcal{I}_k) + W_k \\
X_{k+2} &= \mathbf{A}^2 X_k + \mathbf{A}\mathbf{B}\mathbf{V}_k U_k(\mathcal{I}_k) + \mathbf{B}\mathbf{V}_{k+1} U_{k+1}(\mathcal{I}_k) + \mathbf{A}W_k + W_{k+1} \\
&\vdots \\
X_{k+N} &= \mathbf{A}^N X_k + \mathbf{A}^{N-1}\mathbf{B}\mathbf{V}_k U_k(\mathcal{I}_k) + \dots \\
&\quad + \mathbf{B}\mathbf{V}_{k+N-1} U_{k+N-1}(\mathcal{I}_k) + \mathbf{A}^{N-1} W_k + \cdots + W_{k+N-1}.
\end{aligned}$$

This can be expressed as a matrix equation. Re-writing (4.5) in that form yields

$$\underbrace{\begin{pmatrix} X_{k+1} \\ X_{k+2} \\ \vdots \\ X_{k+N} \end{pmatrix}}_{\mathcal{X}_k} = \underbrace{\begin{pmatrix} \mathbf{A} \\ \mathbf{A}^2 \\ \vdots \\ \mathbf{A}^N \end{pmatrix}}_{\Phi} X_k + \underbrace{\begin{pmatrix} \mathbf{B} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{AB} & \mathbf{B} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{A}^{N-1}\mathbf{B} & \dots & \mathbf{AB} & \mathbf{B} \end{pmatrix}}_{\Gamma} \underbrace{\begin{pmatrix} \mathbf{V}_k & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{V}_{k+1} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{V}_{k+N-1} \end{pmatrix}}_{\Upsilon_k} \underbrace{\begin{pmatrix} U_k(\mathcal{I}_k) \\ U_{k+1}(\mathcal{I}_k) \\ \vdots \\ U_{k+N-1}(\mathcal{I}_k) \end{pmatrix}}_{\mathcal{U}_k(\mathcal{I}_k)} + \underbrace{\begin{pmatrix} \mathbf{I} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{A} & \mathbf{I} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{A}^{N-1} & \dots & \mathbf{A} & \mathbf{I} \end{pmatrix}}_{\Lambda} \underbrace{\begin{pmatrix} W_k \\ W_{k+1} \\ \vdots \\ W_{k+N-1} \end{pmatrix}}_{\mathcal{W}_k}. \tag{4.5}$$

Re-casting (4.5) as a prediction matrix equation gives

$$\mathcal{X}_k \triangleq \Phi X_k + \Gamma \Upsilon_k \mathcal{U}_k(\mathcal{I}_k) + \Lambda \mathcal{W}_k, \tag{4.6}$$

where $\Phi \in \mathbb{R}^{Nn \times n}$ is the dynamics matrix over the prediction horizon; $\mathcal{X}_k \in \mathbb{R}^{Nn}$ is the state prediction vector; $\Gamma \in \mathbb{R}^{Nn \times Nm}$ is the propagation matrix for the control over the prediction horizon; $U_k(\mathcal{I}_k) \in \mathbb{R}^{Nm}$ is the realisation at time step $k$ of the control law computed with access to the information set $\mathcal{I}_k$; $\Lambda \in \mathbb{R}^{Nn \times Nn}$ is the propagation matrix for the process noise; $\mathcal{W}_k \in \mathbb{R}^{Nn}$ is the process noise over the prediction horizon with mean $\mathbf{0}$ and covariance $\Sigma_{\mathcal{W}}$; $\Sigma_{\mathcal{W}} \in S_{++}^{Nn}$ is the diagonal block matrix where the $i$-th block is $\Sigma_W$; $\Upsilon_k \in S_{+}^{Nm}$ is a diagonal matrix with the Bernoulli random variables describing the packet transmission over the prediction horizon in the diagonal;and $\overline{\Upsilon} \in S_{++}^{Nm}$ is the block diagonal matrix where the $i$-th block is $\mathbf{M}$, and therefore $\mathbb{E}[\Upsilon_k] = \overline{\Upsilon}$. To control the system over the horizon, N, the controller calculates the expected state trajectory $\widehat{\mathcal{X}}_k$. Note that, for both protocols, the estimate coincides due to the fact that neither protocol knows the realisation of $\mathbf{V}_k$ before actuating. The expected state trajectory for both

protocols is therefore given by

$$\widehat{\mathcal{X}}_k \triangleq \mathbb{E}\left[\mathcal{X}_k \middle| \mathcal{J}_k\right] = \Phi X_k + \Gamma\overline{\Upsilon}\mathcal{U}_k(\mathcal{J}_k). \tag{4.7}$$

In the TCP-like regime the operator does not know the realisation of a packet transmission before actuating, which results in (4.7), but knows the packet transmission realisation when updating the state estimate, which results in (4.3a). The TCP-like protocol only estimates the packet transmission for the optimal control problem. In contrast, the UDP-like protocol packet transmission variables are estimated for both the estimation and the optimal control problem. Expanding the update error terms in (4.3) over the prediction horizon of $N$ time-steps results in

$$\begin{aligned}
\mathcal{E}_k(\mathcal{F}_k) &\triangleq \mathcal{X}_k - \mathbb{E}\left[\mathcal{X}_k \middle| \mathcal{F}_k, \Upsilon_k\right] \\
&= \Phi X_k + \Gamma\Upsilon_k\mathcal{U}_k(\mathcal{F}_k) + \Lambda\mathcal{W}_k - \widehat{\mathcal{X}}_k \\
&= \Phi X_k + \Gamma\Upsilon_k\mathcal{U}_k(\mathcal{F}_k) + \Lambda\mathcal{W}_k - \Phi X_k - \Gamma\Upsilon_k\mathcal{U}_k(\mathcal{F}_k) \\
&= \Lambda\mathcal{W}_k, \qquad (4.8a) \\
\mathcal{E}_k(\mathcal{G}_k) &\triangleq \mathcal{X}_k - \mathbb{E}\left[\mathcal{X}_k \middle| \mathcal{G}_k\right] \\
&= \Phi X_k + \Gamma\Upsilon_k U_k(\mathcal{G}_k) + \Lambda\mathcal{W}_k - \widehat{\mathcal{X}}_k \\
&= \Phi X_k + \Gamma\Upsilon_k\mathcal{U}_k(\mathcal{G}_k) + \Lambda\mathcal{W}_k - \Phi X_k - \Gamma\overline{\Upsilon}\mathcal{U}_k(\mathcal{G}_k) \\
&= \Gamma\left(\Upsilon_k - \overline{\Upsilon}\right)\mathcal{U}_k(\mathcal{G}_k) + \Lambda\mathcal{W}_k. \qquad (4.8b)
\end{aligned}$$

In this setting we formulate a Linear Quadratic Gaussian (LQG) control problem, i.e. the system operator minimises a quadratic function of the states and inputs. This function is weighted with diagonal state penalty matrix $\Omega \in S_{++}^{Nn}$, diagonal input penalty matrix $\Psi \in S_{++}^{Nm}$, and diagonal matrix $\mathbf{Q} \in S_{++}^{n}$. Note that the penalties at each time step vary. Since $\mathcal{W}_k$ is random, the state of the plant is random, which yields a stochastic model predictive control problem [2]. The cost function to be minimised is the expected

cost, defined as

$$J\left(\mathcal{J}_k\right) \triangleq \mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{Q}X_k + \mathcal{X}_k^{\mathsf{T}}\Omega\mathcal{X}_k + \mathcal{U}_k^{\mathsf{T}}(\mathcal{J}_k)\Upsilon_k^{\mathsf{T}}\Psi\Upsilon_k\mathcal{U}_k(\mathcal{J}_k)\middle|\mathcal{J}_k\right], \tag{4.9a}$$

where the expectation in (4.56a) is with respect to the joint distribution of $\Upsilon_k$ and $\mathcal{W}_k$. The expectation is taken sequentially as in [65, Lemma 1(c)] to account for the causality constraints imposed by the system. Therein, the expectation at each time step is conditioned on all previous time steps. This is due to the fact that the sequence of states at each time step forms a Markov chain, i.e. $X_k \to X_{k+1} \to \cdots \to X_{k+N}$. The state trajectory $\mathcal{X}_k$ is re-written in terms of the estimate $\widehat{\mathcal{X}}_k$ and the error induced by the estimate $\mathcal{E}_k$. Substituting $\mathcal{X}_k = \widehat{\mathcal{X}}_k + \mathcal{E}_k$ into (4.56a) yields

$$J(\mathcal{J}_k) = \mathbb{E}\Big[X_k^{\mathsf{T}}\mathbf{Q}X_k + \left(\widehat{\mathcal{X}}_k + \mathcal{E}_k\right)^{\mathsf{T}}\Omega\left(\widehat{\mathcal{X}}_k + \mathcal{E}_k\right) + \mathcal{U}_k^{\mathsf{T}}(\mathcal{J}_k)\Upsilon_k^{\mathsf{T}}\Psi\Upsilon_k\mathcal{U}_k(\mathcal{J}_k)\Big|\mathcal{J}_k\Big]. \tag{4.9b}$$

The optimal control problem is to find the input sequence $\mathcal{U}_k(\mathcal{J}_k)_k^*$ that minimises (4.9b). Additionally, it should be noted that $\mathbb{E}\left[\mathcal{E}_k\middle|\mathcal{J}_k\right] = 0$ and the state error and the state estimate are independent for both protocols. The proofs of these statements are provided in [65], which leads to the following optimal cost definition:

$$J^*\left(\mathcal{J}_k\right) \triangleq \min_{\mathcal{U}_k(\mathcal{J}_k)} \Big\{\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{Q}X_k + \widehat{\mathcal{X}}_k^{\mathsf{T}}\Omega\widehat{\mathcal{X}}_k + \mathcal{E}_k^{\mathsf{T}}\Omega\mathcal{E}_k + \mathcal{U}_k^{\mathsf{T}}(\mathcal{J}_k)\,\Upsilon_k{}^{\mathsf{T}}\Psi\Upsilon_k\,\mathcal{U}_k(\mathcal{J}_k)\middle|\mathcal{J}_k\right]. \tag{4.10}$$

## 4.3 MPC Optimal Cost Derivation and Analysis

The above section has vectorised the state space equations and formed a vectorised LQG cost function with the aim of solving the optimal control problem using MPC. However, this is just an alternate way of solving the optimal control problem. This optimal control problem can be solved using the available tools within Chapter 3, namely the Dynamic Programming (DP) approach. In fact, as will be shown later, the DP approach is used in order to give the infinite horizon solution. Specifically, the solution to the Ricatti equation is used as a penalty matrix to give the equivalence. The reason for the switch to MPC is

due to the following chapter, Chapter 5. Within Chapter 5 the problem of solving the optimal attack becomes simplified when the system is viewed in the vectorised state.

The derivation of the optimal control law is therefore recast into solving the minimisation in (4.10) for both communication protocols. The first and second term on the right hand side of (4.10) are not random due to the information available and are therefore unaffected by the expectation. Furthermore, since the first term does not depend on $\mathcal{U}_k(\mathcal{I}_k)_k$ the minimisation is rewritten as

$$J^*(\mathcal{I}_k) = X_k^{\mathsf{T}}\mathbf{Q}X_k + \min_{\mathcal{U}_k(\mathcal{I}_k)} \left\{ \widehat{\mathcal{X}}_k^{\mathsf{T}}\Omega\widehat{\mathcal{X}}_k + \mathbb{E}\left[\mathcal{E}_k^{\mathsf{T}}\Omega\mathcal{E}_k + \mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k)\,\Upsilon_k^{\mathsf{T}}\Psi\Upsilon_k\,\mathcal{U}_k(\mathcal{I}_k)\middle|\mathcal{I}_k\right]\right\}. \tag{4.11}$$

The computation of the expectation of the last term can be simplified by using the commutation properties of diagonal matrices and the idempotency of the matrix $\Upsilon_k$. Additionally, due to the causality imposed on the system $\mathcal{U}_k(\mathcal{I}_k)$ does not depend on the future *realisations* of $\mathbf{V}_k$ or $W_k$, and therefore, is not affected by the expectation. Note, that this still allows for a $\mathcal{U}_k(\mathcal{I}_k)$ that depends on the statistics of each of these variables, just not the future *realisations*. The last term in (4.11) is

$$\mathbb{E}\left[\mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k)\,\Upsilon_k{}^{\mathsf{T}}\Psi\Upsilon_k\,\mathcal{U}_k(\mathcal{I}_k)\middle|\mathcal{I}_k\right] = \mathcal{U}_k(\mathcal{I}_k)^{\mathsf{T}}\,\overline{\Upsilon}\Psi\,\mathcal{U}_k(\mathcal{I}_k). \tag{4.12}$$

Therefore, (4.11) is equivalent to

$$J^*(\mathcal{I}_k) = X_k^{\mathsf{T}}\mathbf{Q}X_k + \min_{\mathcal{U}_k(\mathcal{I}_k)} \left\{ \widehat{\mathcal{X}}_k^{\mathsf{T}}\Omega\widehat{\mathcal{X}}_k + \mathcal{U}_k(\mathcal{I}_k)^{\mathsf{T}}\overline{\Upsilon}\Psi\mathcal{U}_k(\mathcal{I}_k) + \mathbb{E}\left[\mathcal{E}_k^{\mathsf{T}}\Omega\mathcal{E}_k\middle|\mathcal{I}_k\right]\right\}. \tag{4.13}$$

The term involving the expected state trajectory is combined with (4.7) to give

$$\begin{aligned} J^*(\mathcal{I}_k) = {} & X_k^{\mathsf{T}}\left(\mathbf{Q} + \Omega_p\right)X_k \\ & + \min_{\mathcal{U}_k(\mathcal{I}_k)} \left\{ \mathbb{E}\left[\mathcal{E}_k^{\mathsf{T}}\Omega\mathcal{E}_k\middle|\mathcal{I}_k\right] + \mathcal{U}_k(\mathcal{I}_k)^{\mathsf{T}}\overline{\Upsilon}\left(2\Omega_{gp}X_k + \left(\Omega_g\overline{\Upsilon} + \Psi\right)\mathcal{U}_k(\mathcal{I}_k)\right)\right\}, \end{aligned} \tag{4.14}$$

where $\Omega_p = \Phi^{\mathsf{T}}\Omega\Phi$, $\Omega_g = \Gamma^{\mathsf{T}}\Omega\Gamma$, and $\Omega_{gp} = \Gamma^{\mathsf{T}}\Omega\Phi$.

Evaluating the quadratic error requires knowledge of second-order statistics. It is in this step that the differences between the UDP-like protocol and the TCP-like protocol become apparent. This observation leads to the first lemma.

**Lemma 7.** *Consider the system modelled by (4.1) with access to (4.2). Then the following holds*

$$\mathbb{E}\Big[\mathcal{E}_k^{\mathsf{T}}\Omega\mathcal{E}_k\Big|\mathcal{F}_k\Big] = \operatorname{tr}(\Omega_l\Sigma_{\mathcal{W}}), \tag{4.15a}$$

$$\mathbb{E}\Big[\mathcal{E}_k^{\mathsf{T}}\Omega\mathcal{E}_k\Big|\mathcal{G}_k\Big] = \mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k)\overline{\Upsilon}(\mathbf{I}\odot\Omega_g)\Big(\mathbf{I}-\overline{\Upsilon}\Big)\mathcal{U}_k(\mathcal{G}_k) + \operatorname{tr}(\Omega_l\Sigma_{\mathcal{W}}), \tag{4.15b}$$

*where* $\Omega_l = \Lambda\Omega\Lambda$ *and* $\odot$ *denotes the Hadamard product.*

*Proof.* See Appendix.

Lemma 7 highlights that the UDP-like quadratic error term depends on $\mathcal{U}_k(\mathcal{G}_k)$, whereas the TCP-like protocol does not. Additionally, (4.14) shows that the quadratic error term lies within the minimisation. Therefore, the term for the TCP-like quadratic error is removed from the minimisation in (4.14) whereas the UDP-like term is not. Due to this, the derivation of the optimal control law is at this point split into two cases.

**Theorem 2.** *Consider the closed-loop systems shown in Fig. 4.1 and Fig. 4.2, with plant dynamics given in (4.1), protocol dependent information sets given in (4.2), and controller cost function given in (4.10), respectively. Then the optimal cost for the TCP-like protocol is*

$$J^*(\mathcal{F}_k) = X_k^{\mathsf{T}}(\mathbf{Q}+\Omega_p)X_k + \operatorname{tr}(\Sigma_{\mathcal{W}}\Omega_l) - X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathcal{F}_k)\overline{\Upsilon}\Omega_{gp}X_k, \tag{4.16a}$$

*and the optimal cost for the UDP-like protocol is*

$$J^*(\mathcal{G}_k) = X_k^{\mathsf{T}}(\mathbf{Q}+\Omega_p)X_k + \operatorname{tr}(\Sigma_{\mathcal{W}}\Omega_l) - X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathcal{G}_k)\overline{\Upsilon}\Omega_{gp}X_k. \tag{4.16b}$$

*The corresponding optimal control laws are*

$$\begin{aligned}\mathcal{U}_k^*(\mathcal{F}_k) &\triangleq -\left(\Omega_g \overline{\Upsilon} + \Psi\right)^{-1} \Omega_{gp} X_k \qquad (4.17a)\\ &= -\mathbf{G}^{-1}(\mathcal{F}_k)\, \Omega_{gp} X_k,\\ \mathcal{U}_k^*(\mathcal{G}_k) &\triangleq -\left(\Psi + (\mathbf{I} \odot \Omega_g)\left(\mathbf{I} - \overline{\Upsilon}\right) + \Omega_g \overline{\Upsilon}\right)^{-1} \Omega_{gp} X_k \qquad (4.17b)\\ &= -\mathbf{G}^{-1}(\mathcal{G}_k)\, \Omega_{gp} X_k,\end{aligned}$$

*for the TCP-like and the UDP-like protocols, respectively.*

*Proof.* See Appendix.

**Remark 1.** *In the TCP-like regime the optimal control law, (4.17a), only depends on the mean number of packet transmissions* $\overline{\Upsilon}$ *and this term weights how the actuation propagates through the system via the* $\Omega_g$ *term. On the other hand, the optimal control law of the UDP-like regime, (4.17b), contains an additional term that weighs the control law with the probability of packet loss* $\mathbf{I} - \overline{\Upsilon}$*.*

**Corollary 1.** *It is possible to show that the for the TCP-like protocol the resultant MPC LQG cost, (4.16a), is equivalent to the optimal Dynamic Programming infinite horizon cost. Namely, with the penalty matrices defined such that* $\mathbf{Q} = \Omega_1, \Omega_1 = \Omega_1, \ldots, \Omega_{N-1} = \Omega_1$ *and the final penalty matrix,* $\Omega_N$ *is defined as the steady state solution of the ARE*

$$\mathbf{P}_k = \mathbf{A}\mathbf{P}_{k+1}\mathbf{A} + \Omega_1 - \mathbf{A}\mathbf{B}\mathbf{P}_{k+1}\left(\mathbf{B}\mathbf{P}_{k+1}\mathbf{B}\mathbf{M} + \Psi_1\right)^{-1}\mathbf{M}\mathbf{B}\mathbf{P}_{k+1}\mathbf{A}$$

*and noting that the optimal control law under DP is*

$$u_k = -\left(\mathbf{B}\mathbf{P}_{k+1}\mathbf{B}\mathbf{M} + \Psi_1\right)^{-1}\mathbf{B}\mathbf{P}_{k+1}\mathbf{A}x_k. \qquad (4.18)$$

*results in equivalence between the MPC and the DP infinite horizon solutions.*

Note that the matrix $\mathbf{G}(\mathcal{J}_k)$ is invertible, due to the fact that $\Omega_g \succeq 0$ as a result of the controllability condition on the system and $\Psi \succ 0$ by definition. The optimal control

laws presented in (4.17a) and (4.17b) and the corresponding optimal cost functions (4.16a) and (4.16b) depend on $\overline{\Upsilon}$. Therefore, the current formulation makes no assumption on the stationarity of the random process governing the channel-loss statistics. Specifically, much like how the penalty matrices $\Psi$ and $\Omega$ vary along the time horizon, the mean of packet transmission for each channel may also vary over the time horizon. This allows for a wider class of packet loss models to be utilised. For example, a sequence of packet losses that form a Markov chain. In this scenario the expected value of a packet transmission, $\mathbf{V}_k$ is modelled as $\mathbf{V}_k \sim \mathscr{B}e\left(\mathbf{M}_k\right)$ where $\mathbf{M}_k \in S_{++}^m$ is a diagonal matrix in which the i-th diagonal element is $\mu_{i,k}$ which describes the probability of a packet transmission in the $i$-th channel at the $k$-th time step. Therefore, $\mathbb{E}[\mathbf{V}_k] = \mathbf{M}_k$ and $\mathbb{E}\left[\Upsilon_k\right] = \overline{\Upsilon}$ where $\overline{\Upsilon}$ is the block diagonal matrix where the $i$-th block is $\mathbf{M}_k$. Substitution of these definitions into the above derivation does not break any assumptions made and results in a control law and optimal cost function for a non-stationary sequence of packet losses.

It should also be noted that the control laws presented are the vectorised control laws. In practise only the first entry in the optimal control law should be implemented on a feedback control law. Namely, the first $m$ entries in the vector $\mathscr{U}_k\left(\mathscr{I}_k\right)$. This entry will then be used recursively with the updated state estimate in the next time step.

## 4.4 Cost Difference Analysis

The difference in the information sets leads to different optimal control laws, as seen in (4.17), and results in differing costs over the horizon. In the following section it is shown that the expected optimal control cost incurred by the information set of the UDP-like protocol is strictly greater than the expected optimal control cost incurred by using the information set of the TCP-like protocol.

**Theorem 3.** *Let* $\mathbf{M}$ *such that* $\mathbf{0} \prec \mathbf{M} \prec \mathbf{I}$*, with information sets given in (4.2). Then*

$$J^*\left(\mathscr{G}_k\right) - J^*\left(\mathscr{F}_k\right) > 0,$$

*where the optimal cost is as defined in (4.10).*

*Proof.* The optimal control laws for each communication protocol are defined in (4.17a) and (4.17b). Note that $\mathbf{G}\left(\mathscr{I}_k\right) \succ 0$ and that,

$$\mathbf{G}(\mathscr{G}_k) - \mathbf{G}(\mathscr{F}_k) = \left(\mathbf{I} \odot \Omega_g\right)\left(\mathbf{I} - \overline{\Upsilon}\right) \succ 0. \tag{4.19}$$

Therefore, [30, 10.53] implies that

$$\begin{aligned}
\mathbf{G}^{-1}(\mathscr{G}_k) &\prec \mathbf{G}^{-1}(\mathscr{F}_k)\,, \\
\mathbf{G}^{-1}(\mathscr{G}_k)\,\overline{\Upsilon} &\prec \mathbf{G}^{-1}(\mathscr{F}_k)\,\overline{\Upsilon}, \\
\mathbf{C} - X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathscr{G}_k)\,\overline{\Upsilon}\Omega_{gp}X_k &> \mathbf{C} - X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathscr{F}_k)\,\overline{\Upsilon}\Omega_{gp}X_k,
\end{aligned}$$

where $\mathbf{C} = X_k^{\mathsf{T}}\left(\mathbf{Q} + \Omega_p\right)X_k + \operatorname{tr}\left(\Sigma_{\mathcal{W}}\Omega_l\right)$. Therefore, for any $\mathbf{0} \prec \mathbf{M} \prec \mathbf{I}$ it holds that

$$J^*\left(\mathscr{G}_k\right) - J^*\left(\mathscr{F}_k\right) > 0. \tag{4.20}$$

This concludes the proof. □

As is shown in Theorem 3, the cost difference between the UDP-like and the TCP-like protocol is strictly positive for a channel without deterministic packet transmissions. The cost difference is zero only in the cases of no communication $\mathbf{M} = \mathbf{0}$ or perfect communication $\mathbf{M} = \mathbf{I}$.

Additional insight can be obtained from Theorem 3. Specifically, the TCP-like protocol achieves a lower quadratic cost by using larger control signals to drive the states to zero quicker than the UDP-like protocol. This difference is a result of the larger information set that the TCP-like protocol has access to, which is shown in the following corollary.

**Corollary 2.** *It holds that*

$$\left\|\mathcal{U}_k^*(\mathscr{G}_k)\right\|_2 < \left\|\mathcal{U}_k^*(\mathscr{F}_k)\right\|_2, \tag{4.21}$$

*where* $\|\cdot\|_2$ *denotes the 2-norm.*

*Proof.* Starting with (4.19), it is seen that

$$\mathbf{G}(\mathcal{G}_k) - \mathbf{G}(\mathcal{F}_k) = (\mathbf{I} \odot \Omega_g)\left(\mathbf{I} - \overline{\Upsilon}\right) \succ 0, \tag{4.22}$$

$$\mathbf{G}^{-1}(\mathcal{G}_k) \prec \mathbf{G}^{-1}(\mathcal{F}_k)\,, \tag{4.23}$$

$$\mathbf{G}^{-1}(\mathcal{G}_k)\,\Omega_{gp} X_k < \mathbf{G}^{-1}(\mathcal{F}_k)\,\Omega_{gp} X_k, \tag{4.24}$$

$$\left\|\mathbf{G}^{-1}(\mathcal{G}_k)\,\Omega_{gp} X_k\right\|_2 < \left\|\mathbf{G}^{-1}(\mathcal{F}_k)\,\Omega_{gp} X_k\right\|_2, \tag{4.25}$$

$$\|-\mathcal{U}_k^*(\mathcal{G}_k)\|_2 < \|-\mathcal{U}_k^*(\mathcal{F}_k)\|_2\,, \tag{4.26}$$

$$\|\mathcal{U}_k^*(\mathcal{G}_k)\|_2 < \|\mathcal{U}_k^*(\mathcal{F}_k)\|_2\,. \tag{4.27}$$

This concludes the proof. □

In addition to showing that the cost of the UDP-like protocol is strictly greater than the cost of the TCP-like protocol. The MPC formulation derived above allows for an analytic proof that the cost of the system under either protocol is monotonic with respect to the variable $\mathbf{M}$. The following theorem shows that the cost function is a monotonically decreasing function in $\mathbf{M}$ for both protocols.

**Theorem 4.** *Let* $\mathbf{M}_1 \in S_{++}^m$ *and* $\mathbf{M}_2 \in S_{++}^M$ *be diagonal matrices. If* $\mathbf{M}_2 \succ \mathbf{M}_1$ *then*

$$J^*_{\Delta\mathbf{M}} = J^*_{\mathbf{M}_1}(\mathcal{I}_k) - J^*_{\mathbf{M}_2}(\mathcal{I}_k) > 0, \tag{4.28}$$

*where* $J^*_{\mathbf{M}_1}(\mathcal{I}_k)$ *is the optimal expected cost obtained with the value of* $\mathbf{M}_i$*, where* $\mathbf{M}_i$ *as the mean of the channel transmission variable* $\mathbf{V}_k$*.*

*Proof.* The proof is constructed for the TCP-like protocol. However, with the substitutions of $\Omega_g$ for $\Omega_h$ and $\Psi$ for $(\mathbf{I} \odot \Omega_g) + \Psi$ the corresponding UDP-like proof is identical. For a given $\mathbf{M}_1$ and $\mathbf{M}_2$ the cost difference between the optimal expected costs calculated for

each $\mathbf{M}_i$ respectively is

$$J^*_{\mathbf{M}_1}(\mathcal{J}_k) = \mathbf{C} - X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\left(\overline{\Upsilon}_1\Omega_g + \Psi\right)^{-1}\overline{\Upsilon}_1\Omega_{gp}X_k, \tag{4.29}$$

$$J^*_{\mathbf{M}_2}(\mathcal{J}_k) = \mathbf{C} - X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\left(\overline{\Upsilon}_2\Omega_g + \Psi\right)^{-1}\overline{\Upsilon}_2\Omega_{gp}X_k, \tag{4.30}$$

where $\overline{\Upsilon}_1$ and $\overline{\Upsilon}_2$ are the diagonal matrices constructed from the matrices $\mathbf{M}_1$ and $\mathbf{M}_2$, such that $\overline{\Upsilon}_i = \mathbf{I}_N \otimes \mathbf{M}_i$. Additionally, as in the previous proof, the constant $\mathbf{C}$ is defined as $\mathbf{C} = X_k^{\mathsf{T}}(\mathbf{Q} + \Omega_p)X_k + \mathrm{tr}(\Sigma_{\mathcal{W}}\Omega_l)$. Consequently $\overline{\Upsilon}_2 \succ \overline{\Upsilon}_1$ due to the assumption $\mathbf{M}_2 \succ \mathbf{M}_1$. Therefore, the cost difference between the two optimal expected costs is

$$\begin{aligned}
J^*_{\Delta\mathbf{M}} &= J^*_{\mathbf{M}_1}(\mathcal{J}_k) - J^*_{\mathbf{M}_2}(\mathcal{J}_k) \qquad (4.31)\\
&= \mathbf{C} - X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\left(\overline{\Upsilon}_1\Omega_g + \Psi\right)^{-1}\overline{\Upsilon}_1\Omega_{gp}X_k - \left(\mathbf{C} - X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\left(\overline{\Upsilon}_2\Omega_g + \Psi\right)^{-1}\overline{\Upsilon}_2\Omega_{gp}X_k\right)\\
&= X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\left[\left(\overline{\Upsilon}_2\Omega_g + \Psi\right)^{-1}\overline{\Upsilon}_2 - \left(\overline{\Upsilon}_1\Omega_g + \Psi\right)^{-1}\overline{\Upsilon}_1\right]\Omega_{gp}X_k\\
&= X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\left(\overline{\Upsilon}_2\Omega_g + \Psi\right)^{-1}\overline{\Upsilon}_2\left[\overline{\Upsilon}_1^{-1}\left(\overline{\Upsilon}_1\Omega_g + \Psi\right)\right.\\
&\qquad\qquad \left. - \overline{\Upsilon}_2^{-1}\left(\overline{\Upsilon}_2\Omega_g + \Psi\right)\right]\left(\overline{\Upsilon}_1\Omega_g + \Psi\right)^{-1}\overline{\Upsilon}_1\Omega_{gp}X_k\\
&= X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\left(\overline{\Upsilon}_2\Omega_g + \Psi\right)^{-1}\overline{\Upsilon}_2\left(\overline{\Upsilon}_1^{-1} - \overline{\Upsilon}_2^{-1}\right)\Psi\left(\overline{\Upsilon}_1\Omega_g + \Psi\right)^{-1}\overline{\Upsilon}_1\Omega_{gp}X_k. \qquad (4.32)
\end{aligned}$$

Only the term $\overline{\Upsilon}_1^{-1} - \overline{\Upsilon}_2^{-1}$ within (4.32) determines the positivity of the expected cost difference. The term is positive if $\mathbf{M}_2 \succ \mathbf{M}_1$, as is assumed above. Therefore, $\overline{\Upsilon}_2 \succ \overline{\Upsilon}_1$ and $\overline{\Upsilon}_1^{-1} - \overline{\Upsilon}_2^{-1} \succ 0$ and the expected cost difference is strictly positive. This concludes the proof. □

**Corollary 3.** *Theorem 3 combined with Theorem 4 implies that with both protocols operating at a fixed cost value, the TCP-like protocol communicates with a larger packet loss rate. Therefore, where* $\mathbf{M}_1 \succ \mathbf{M}_2$.

$$J^*_{\mathbf{M}_1}(\mathcal{G}_k) = J^*_{\mathbf{M}_2}(\mathcal{F}_k). \tag{4.33}$$

*Proof.* From Theorem 3

$$J^*_{\mathbf{M}_1}\left(\mathscr{G}_k\right) = J^*_{\mathbf{M}_1}\left(\mathscr{F}_k\right) + \epsilon,$$

where $\epsilon \in \mathbb{R}^+$. From Theorem 4 it is known that

$$J^*_{\mathbf{M}_1}\left(\mathscr{F}_k\right) + \epsilon = J^*_{\mathbf{M}_2}\left(\mathscr{F}_k\right).$$

Therefore,

$$J^*_{\mathbf{M}_1}\left(\mathscr{G}_k\right) = J^*_{\mathbf{M}_2}\left(\mathscr{F}_k\right).$$

This concludes the proof. □

**Remark 2.** *Theorem 4 and Corollary 3 also apply to a non-stationary communication channel with a slight adjustment of the conditions. Both are true for a non-stationary channel when the stronger condition* $\overline{\Upsilon}_2 \succ \overline{\Upsilon}_1$ *holds, or more precisely,* $\mathbf{M}_{2\ k} \succ \mathbf{M}_{1\ k}$ *for all* $k$*.*

### 4.4.1 Scalar Communication Channel

The maximum difference in the expected cost and the maximising value of the expected packet transmission variable is characterised when the expected cost difference, as established in Theorem 3, is simplified to the scalar case i.e. $\overline{\Upsilon} \in [0, 1]$. In doing so, the channel is simplified to a single channel that all actuators share. Due to this, the following results do not apply to a non-stationary communication channel.

Assuming the same plant dynamics as (4.1), the cost difference between the two protocols as a function of $\overline{\Upsilon}$ is given by

$$J^*_{\Delta}\left(\overline{\Upsilon}\right) \triangleq J^*\left(\mathscr{G}_k\right) - J^*\left(\mathscr{F}_k\right). \tag{4.34}$$

Note that Theorem 3 states that (4.34) is positive, and therefore, the cost difference is

$$\begin{aligned} J_{\Delta}^{*}\left(\overline{\Upsilon}\right) &= \mathbf{C} - X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\,\overline{\Upsilon}\mathbf{G}^{-1}(\mathcal{G}_k)\,\Omega_{gp}X_k - \left(\mathbf{C} - X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\,\overline{\Upsilon}\mathbf{G}^{-1}(\mathcal{F}_k)\,\Omega_{gp}X_k\right) \\ &= X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\overline{\Upsilon}\mathbf{G}^{-1}(\mathcal{G}_k)\left(1-\overline{\Upsilon}\right)(\mathbf{I}\odot\Omega_g)\mathbf{G}^{-1}(\mathcal{F}_k)\Omega_{gp}X_k \\ &= \overline{\Upsilon}\left(1-\overline{\Upsilon}\right)\mathrm{tr}\left(\mathbf{G}^{-1}(\mathcal{G}_k)\,(\mathbf{I}\odot\Omega_g)\,\mathbf{G}^{-1}(\mathcal{F}_k)\,\mathbf{L}\right), \end{aligned} \tag{4.35}$$

where $\mathbf{L} = \Omega_{gp}X_kX_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}$. From (4.35) it is seen that the cost difference between the protocols depends on a scaling of the variance of the packet transmission variable $\overline{\Upsilon}\left(1-\overline{\Upsilon}\right)$ over the prediction horizon $N$. Intuitively, this means that for a channel with a high variance, the cost difference is larger. The TCP-like protocol has access to more information and is better able to reduce the uncertainty in the state caused by the variable $\Upsilon_k$ than the UDP-like protocol, and therefore, has a smaller cost. However, the cost difference in (4.35) is a non-linear function of $\overline{\Upsilon}$ owing to the dependence of $\mathbf{G}^{-1}(\mathcal{F}_k)$ and $\mathbf{G}^{-1}(\mathcal{G}_k)$ on $\overline{\Upsilon}$. At this point, we characterise the maximum cost difference as a function of $\overline{\Upsilon}$. This maximum cost difference corresponds to the greatest cost difference incurred by the operator choosing to communicate using a UDP-like communication protocol instead of a TCP-like protocol.

**Lemma 8.** *The derivative of the cost difference in (4.35) is*

$$\begin{aligned} \frac{\partial}{\partial\overline{\Upsilon}}J_{\Delta}^{*}\left(\overline{\Upsilon}\right) = X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\Big(\mathbf{G}^{-1}(\mathcal{G}_k)\Big(\left(1-2\overline{\Upsilon}\right)\Omega_d \\ -\overline{\Upsilon}\left(1-\overline{\Upsilon}\right)\left[\Omega_h\mathbf{G}^{-1}(\mathcal{G}_k)\,\Omega_d+\Omega_d\mathbf{G}^{-1}(\mathcal{F}_k)\Omega_g\right]\Big)\mathbf{G}^{-1}(\mathcal{F}_k)\Big)\Omega_{gp}X_k, \end{aligned} \tag{4.36}$$

*where* $\Omega_d = (\mathbf{I}\odot\Omega_g)$ *and* $\overline{\Upsilon}\in[0,1]$.

*Proof.* See Appendix.

Finding the critical points of the cost difference (4.36) is non-trivial for this function due to the outer products. In order to find the stationary points of (4.36) it is required that the maximum eigenvalue of the matrix inside the quadratic tends to 0. The maximum eigenvalue of a matrix can be written as [32]

$$\lambda_{\max}(\mathbf{C}) = \max_{\|x\|\neq 0}\frac{\mathbf{x}^{\mathsf{T}}\mathbf{C}\mathbf{x}}{\mathbf{x}^{\mathsf{T}}\mathbf{x}}, \tag{4.37}$$

where $\mathbf{x} \in \mathbb{R}^n$ is a column vector, $\mathbf{C}$ is a square matrix of appropriate dimension, and $\lambda_{\max}(\mathbf{C})$ is the maximum eigenvalue of $\mathbf{C}$. Any matrix for which all eigenvalues are equal to 0 also satisfies that the determinant is zero. However, not all matrices with a 0 determinant have a maximum eigenvalue equal to 0. Solving for a zero determinant of (4.36) results in a finite number of values for $\overline{\Upsilon}$, at which point the condition (4.37) reveals the critical points. This leads to the next theorem.

**Lemma 9.** *The equation*

$$det\left(\mathbf{G_G}\left(\overline{\Upsilon}\right)\left[\left(1-2\overline{\Upsilon}\right)\Omega_d - \overline{\Upsilon}\left(1-\overline{\Upsilon}\right)\left[\Omega_h \mathbf{G_G}\left(\overline{\Upsilon}\right)\Omega_d + \Omega_d \mathbf{G_F}\left(\overline{\Upsilon}\right)\Omega_g\right]\right]\mathbf{G_F}\left(\overline{\Upsilon}\right)\right) = 0, \quad (4.38)$$

*has $2Nm$ solutions, given by,*

$$\overline{\Upsilon}^D_{2i-1} = \frac{1}{1+\sqrt{1+\lambda_i}}, \quad (4.39a)$$

$$\overline{\Upsilon}^D_{2i} = \frac{1}{1-\sqrt{1+\lambda_i}}, \quad (4.39b)$$

*where $\overline{\Upsilon}^D_i$ correspondences to the i-th solution of (4.38) and $\lambda_i$ is the i-th eigenvalue of the matrix,*

$$\left(\Omega_g \Omega_d^{-1}\left(\Omega_g + \Psi\right) + \Psi \Omega_d^{-1} \Omega_h\right)\left(\Omega_g + \Psi\right)^{-1} \Omega_d \Psi^{-1}. \quad (4.40)$$

*Proof.* See Appendix.

The above theorem gives a solution in $\overline{\Upsilon}$ for all of the points for which (4.38) holds true. However, as mentioned above this does not correspond to all of the critical points of (4.34). In order for $\overline{\Upsilon}^D_i$ to be a critical point of (4.34) it must hold that the magnitude of the maximum eigenvalue of (4.36) must also be 0. We address this by solving the following numerical evaluation problem.

**Theorem 5.** *The cost difference between the UDP-like and the TCP-like protocols as a function of* $\overline{\Upsilon}$*, is defined as*

$$J_{\Delta}^{*}\left(\overline{\Upsilon}\right) \triangleq J^{*}\left(\mathcal{G}_{k}\right) - J^{*}\left(\mathcal{F}_{k}\right) \;>\; 0. \tag{4.41}$$

*This function has a maximum point that occurs at* $\overline{\Upsilon}^{D^{*}}$*, where* $\overline{\Upsilon}^{D^{*}}$ *is defined as*

$$\overline{\Upsilon}^{D^{*}} \triangleq \sup_{\overline{\Upsilon}_{i}^{D} \in [0,1]} \; J_{\Delta}^{*}\left(\overline{\Upsilon}_{i}^{D}\right) \;\; s.t. \left\| \max_{\|x\| \neq 0} \frac{x^{\mathsf{T}} f\left(\overline{\Upsilon}_{i}^{D}\right) x}{x^{\mathsf{T}} x} \right\| = 0, \tag{4.42}$$

*and where* $f\left(\overline{\Upsilon}_{i}^{D}\right)$ *is defined as*

$$\begin{aligned} f\left(\overline{\Upsilon}_{i}^{D}\right) = \mathbf{G_G}\left(\overline{\Upsilon}_{i}^{D}\right) \Big[ \left(1 - 2\overline{\Upsilon}_{i}^{D}\right) \Omega_{d} \\ - \overline{\Upsilon}_{i}^{D} \left(1 - \overline{\Upsilon}_{i}^{D}\right) \left[ \Omega_{h} \mathbf{G_G}\left(\overline{\Upsilon}_{i}^{D}\right) \Omega_{d} + \Omega_{d} \mathbf{G_F}\left(\overline{\Upsilon}_{i}^{D}\right) \Omega_{g} \right] \Big] \mathbf{G_F}\left(\overline{\Upsilon}_{i}^{D}\right). \end{aligned} \tag{4.43}$$

*Proof.* Lemma 9 states that every $\overline{\Upsilon}_{i}^{D}$ results in the determinant in (4.38) being equal to 0. However, this theorem does not guarantee that $\overline{\Upsilon}_{i}^{D}$ is a critical point of (4.34). It is also required that the magnitude of the maximum eigenvalue is 0 for a given $\overline{\Upsilon}_{i}^{D}$. Therefore, the condition on the $\overline{\Upsilon}_{i}^{D}$ is recast as

$$\begin{aligned} \max_{j} \Big| \lambda_{j} \Big( \mathbf{G_G}\left(\overline{\Upsilon}_{i}^{D}\right) \Big[ \left(1 - 2\overline{\Upsilon}_{i}^{D}\right) \Omega_{d} \\ - \overline{\Upsilon}_{i}^{D} \left(1 - \overline{\Upsilon}_{i}^{D}\right) \left[ \Omega_{h} \mathbf{G_G}\left(\overline{\Upsilon}_{i}^{D}\right) \Omega_{d} + \Omega_{d} \mathbf{G_F}\left(\overline{\Upsilon}_{i}^{D}\right) \Omega_{g} \right] \Big] \mathbf{G_F}\left(\overline{\Upsilon}_{i}^{D}\right) \Big) \Big| = 0. \end{aligned}$$

Therefore, the condition to ensure that $\overline{\Upsilon}_{i}^{D}$ is a critical point becomes

$$\left| \max_{\|x\| \neq 0} \frac{x^{\mathsf{T}} f\left(\overline{\Upsilon}_{i}^{D}\right) x}{x^{\mathsf{T}} x} \right| = 0, \tag{4.44}$$

where

$$f\left(\overline{\Upsilon}_{i}^{D}\right) \triangleq \mathbf{G_G}\left(\overline{\Upsilon}_{i}^{D}\right) \Big[ \left(1 - 2\overline{\Upsilon}_{i}^{D}\right) \Omega_{d} - \overline{\Upsilon}_{i}^{D} \left(1 - \overline{\Upsilon}_{i}^{D}\right) \Big[ \Omega_{h} \mathbf{G_G}\left(\overline{\Upsilon}_{i}^{D}\right) \Omega_{d} + \Omega_{d} \mathbf{G_F}\left(\overline{\Upsilon}_{i}^{D}\right) \Omega_{g} \Big] \Big] \mathbf{G_F}\left(\overline{\Upsilon}_{i}^{D}\right). \tag{4.45}$$

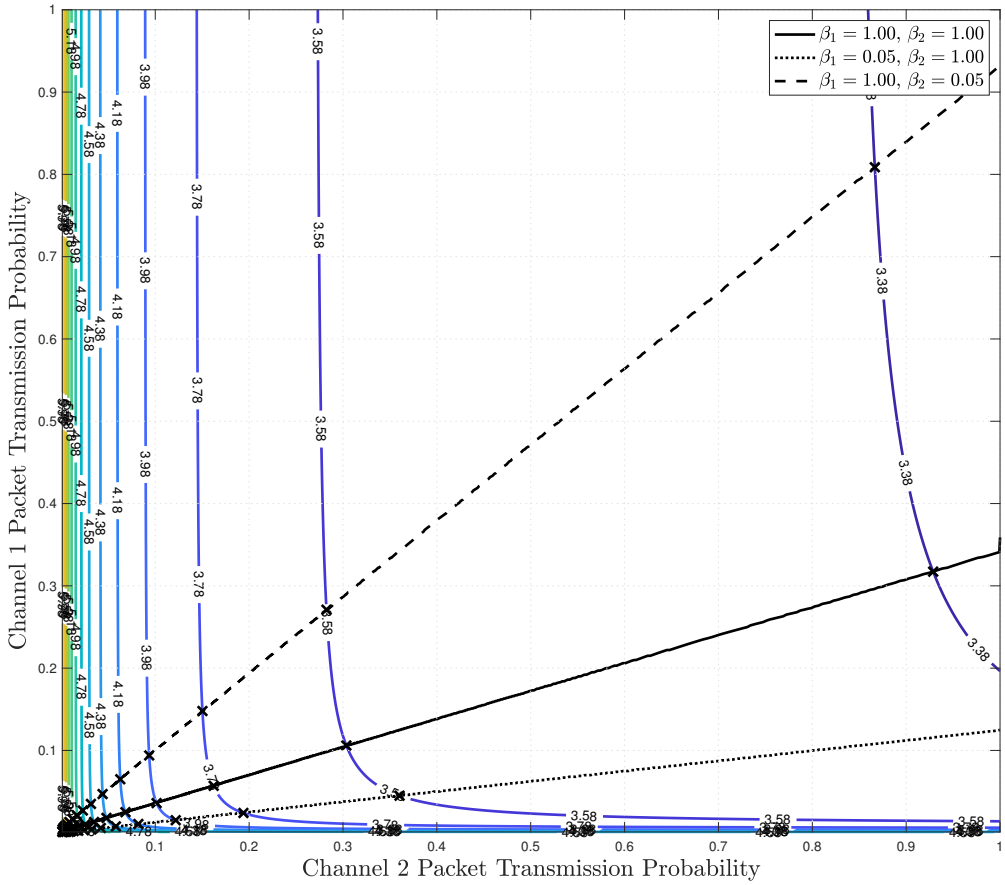


Fig. 4.3 Cost values for the TCP-like protocol operating on system (8.3) as a function of the channel packet packet transmission probabilities in both actuation channel dimensions.

Theorem 3 states that in $[0, 1]$ the cost difference is strictly positive. Therefore, there is at least one maximum in this interval. Taking the supremum of all critical points that lie within $[0, 1]$ results in the maximising $\overline{\Upsilon}_i^D$ in $[0, 1]$. This is denoted by $\overline{\Upsilon}^{D^*}$. This concludes the proof. □

## 4.5 Packet Loss Allocation Optimisation

In modern communication systems, the probability of packet loss is determined by the performance of multiple processes. These processes range from the modulation and coding,

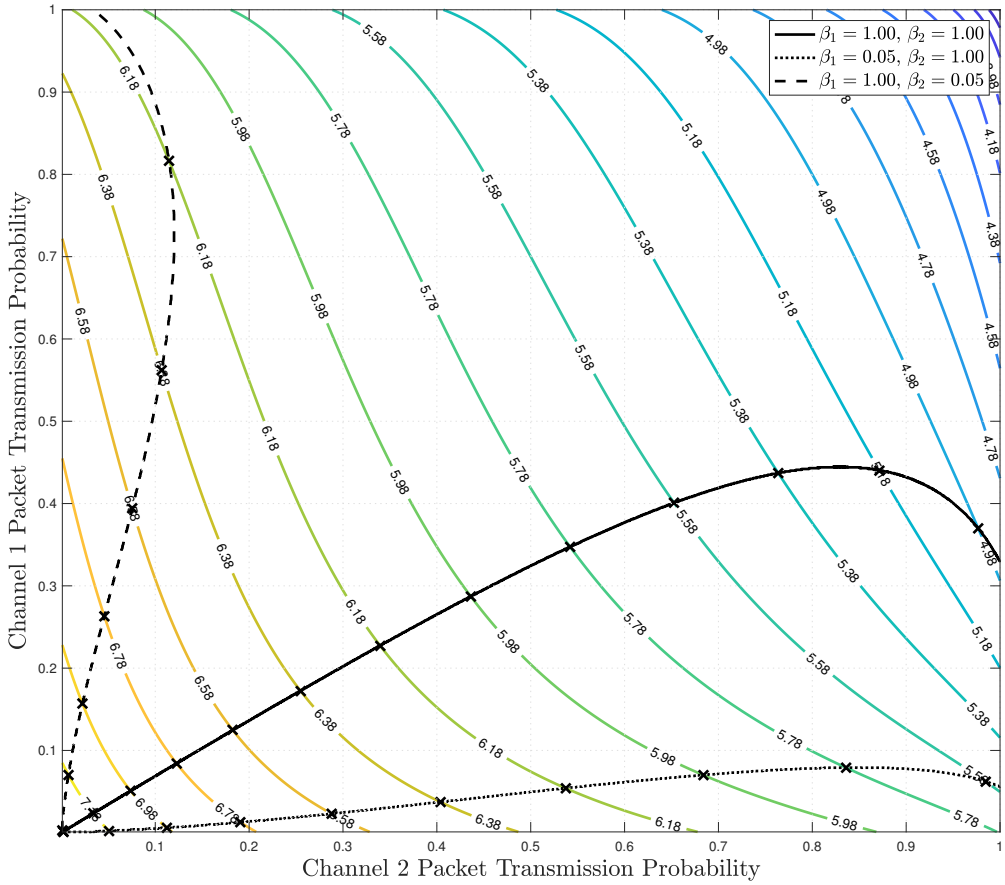


Fig. 4.4 Cost values for the UDP-like protocol operating on system (8.3) as a function of the channel packet packet transmission probabilities in both actuation channel dimensions.

which operate in the lower layers, to the routing and flow control, operating in the higher layers. While characterising the probability of packet transmission of a modern communication system is challenging in general, the probability of packet transmission decreases monotonically [8] with the resources allocated to the communication system, i.e. bandwidth, power, and delay. Indeed, resource allocation is a fundamental problem in communication systems and is often confronted with competing objectives for which the efficiency trade-offs are difficult to describe analytically. In our setting, the extension to the multidimensional actuation channel poses a central question that concerns the design of the communication system of the control system, namely the optimal allocation of

communication resources to each of the actuation channel dimensions. In the following section, we capitalise on the analytical framework developed above and provide a resource allocation framework that optimises the packet loss probabilities for each actuation dimension while satisfying a total budget constraint.

The set of packet loss probability matrices that achieve a given cost $\alpha \in \mathbb{R}_+$ is the set of channel matrices described by

$$\mathscr{M}_k(\mathscr{I}_k) = \{\mathbf{M} : J^*(\mathscr{I}_k) \leq \alpha\}. \tag{4.46}$$

All the matrices in the set induce a control cost that is upper bounded by $\alpha$, but differ in their use of communication resources, i.e. the packet transmission performance across different dimensions. To quantify the use of communication resources in global terms, a communication cost for the system is proposed, defined as

$$C(\mathbf{M}) \triangleq \sum_{i=1}^{m} \beta_i \mu_i = \operatorname{tr}(\boldsymbol{\beta}\mathbf{M}), \tag{4.47}$$

where $\boldsymbol{\beta} \in \mathbf{S}^+_{m\times m}$ is the non-negative definite diagonal penalty matrix where each diagonal entry $\beta_i \in \mathbb{R}$ is a penalty term corresponding to the cost of communication in that channel. The communication cost captures the notion of a total communication budget for the system. That being the case, the minimum communication cost is defined as

$$C_\alpha(\mathscr{I}_k) \triangleq \min_{\mathbf{M}\in\mathscr{M}_k(\mathscr{I}_k)} C(\mathbf{M}). \tag{4.48}$$

The maximum channel efficiency yields a communication setup that minimises the total number of packet losses while maintaining the system control performance. In view of this, the communication system configuration that minimises the amount of resources allocated to the actuation channel is

$$\mathbf{M}^* \triangleq \arg\min_{\mathbf{M}\in\mathscr{M}_k(\mathscr{I}_k)} C(\mathbf{M}). \tag{4.49}$$

This cost of communication formulation highlights the importance of Corollary 3. Specifically, if it is costly to communicate over a particular dimension, then allocating as few resources as possible whilst maintaining a set control cost is desirable. Indeed, as few resources as is dictated by the minimiser $\mathbf{M}^*$.

The optimisation of the communication channel for the pendulum case study presented in Section 8.2.1 is straightforward. There is a single communication channel, and therefore, the maximum channel efficiency is the packet transmission value that achieves the optimal control cost of $\alpha$ with equality. However, for the system presented in Section 8.2.2(8.3) there are fixed regions of expected cost for both the TCP-like protocol and the UDP-like protocol, as shown in Fig. 4.3 and Fig. 4.4, respectively. The black dashed lines plotted in Fig. 4.3 and Fig. 4.4 correspond to the channel matrices defined in (4.49) that achieve the maximum channel efficiency. The values of $\boldsymbol{\beta}$ are selected for three different cases. For the first case, the cost is symmetric in both channel dimensions, i.e. $\boldsymbol{\beta}$ is set to $\mathbf{I}$ and for the second and third cases the entries are set to $(0.05, 1)$ and $(1, 0.05)$, respectively. These cases model the situation in which communication across one of the channel dimensions induces larger cost. Additionally, we also mark the optimal allocation points for each contour line with a black cross. The same weighting matrices are used for both the UDP-like and the TCP-like figures. Note that for the point at which the minimum communication cost is achieved by a matrix $\mathbf{M}^*$ with either $\mu_1 = 1$ or $\mu_2 = 1$, the optimisation for the channel reduces to the single dimensional case, i.e. one of the channel dimensions is perfect and the other dimension incurs in all packet loss. Furthermore, Fig. 4.4 shows that for all the three weightings of the channel cost considered, the maximum channel efficiency for $\alpha \geq 4.78$ requires at least one of the channels to be perfect.

This packet loss allocation presented is not possible with the results [59], due to the scalar channel model.

## 4.6 Control with Sensor and Actuation Packet Loss

In the above it is assumed that the sensory channel has perfect communication. This means there is no chance of there being a packet drop on the sensory channel. This section is concerned with deriving an optimal control input to minimise the cost under an MPC framework, however, the system model is altered. This alteration is such that there are independent packet losses on the sensory channel in addition to the packet losses within the actuation channel. In doing so, we create a more general framework for systems experiencing packet loss. This system is modelled as

$$X_{k+1} = \mathbf{A}X_k + \mathbf{B}\mathbf{V}_k U_k(\mathscr{I}_k) + W_k, \tag{4.50a}$$

$$Y_k = \mathbf{L}_k X_k, \tag{4.50b}$$

where $Y_k$ is the received signal from the sensory communication channel and $\mathbf{L}_k \in S_+^n$ is the sensory channel packet transmission variable modelled as a diagonal matrix where the $i$-th diagonal entry is an IID Bernoulli random variable with mean $\gamma_i \in [0,1]$. Additionally, the expected value of $\mathbf{L}_k$ is $\mathbb{E}[\mathbf{L}_k] = \mathbf{T}$, where $\mathbf{T} \in S_{++}^n$ is a diagonal matrix in which the i-th diagonal element is $\gamma_i$. The initial state of the plant, as before, is determined by the Gaussian vector of random variables $X_k$ with mean $\overline{X}_k$ and covariance matrix $\Sigma_{X_k} \in S_{++}^n$. As in the previous derivation, the information sets available to the operator for each protocol are defined as

$$\mathscr{I}_k = \begin{cases} \mathscr{F}_k = \left\{\mathscr{X}^k, \mathscr{V}^{k-1}, \mathscr{L}^k\right\}, \\ \mathscr{G}_k = \left\{\mathscr{X}^k, \mathscr{L}^k\right\}, \end{cases} \tag{4.51}$$

where $\mathscr{L}^k = \{\mathbf{L}_0, \ldots, \mathbf{L}_{k-1}\}$ and as with $\mathscr{V}^k$ this set is monotonically increasing. Under TCP-like protocols, the operator has access to the realisation of the packet drop $\mathbf{V}_k$ and

therefore can utilise this in the error prediction

$$\begin{aligned} E_{k+1}(\mathscr{F}_k) &\triangleq X_{k+1} - \mathbb{E}\left[X_{k+1}\middle|\mathscr{F}_k, \mathbf{V}_k\right] \\ &= \mathbf{A}X_k + \mathbf{B}\mathbf{V}_k U_k(\mathscr{F}_k) + W_k - \mathbf{A}\widehat{X}_k - \mathbf{B}\mathbf{V}_k U_k(\mathscr{F}_k) \\ &= \mathbf{A}E_k\Big(\mathscr{F}_{k-1}\Big) + W_k, \end{aligned} \tag{4.52a}$$

As before, the function $U_k(\mathscr{I}_k)$ is a function of the information set $\mathscr{I}_k$ and takes the form of a state feedback law, and is therefore, a random variable. Similarly to before, the UDP-like error is defined as

$$\begin{aligned} E_{k+1}(\mathscr{G}_k) &\triangleq X_{k+1} - \mathbb{E}\left[X_{k+1}\middle|\mathscr{G}_k\right] \\ &= \mathbf{A}X_k + \mathbf{B}\mathbf{V}_k U_k(\mathscr{G}_k) + W_k - \mathbf{A}\widehat{X}_k - \mathbf{B}\mathbf{M}U_k(\mathscr{G}_k) \\ &= \mathbf{A}E_k\Big(\mathscr{G}_{k-1}\Big) + \mathbf{B}\left(\mathbf{V}_k - \mathbf{M}\right)U_k(\mathscr{G}_k) + W_k. \end{aligned} \tag{4.52b}$$

As before, the system is predicted over a horizon length $N$ to give the matrix equation

$$\mathcal{X}_k = \Phi X_k + \Gamma\Upsilon_k\mathcal{U}_k(\mathscr{I}_k) + \Lambda\mathcal{W}_k, \tag{4.53a}$$

$$\mathcal{Y}_k = \mathrm{T}_k\mathcal{X}_k, \tag{4.53b}$$

where $\mathcal{Y}_k \in \mathbb{R}^{nN}$ is the received sensory channel output over the time horizon; $\mathrm{T}_k \in \mathbb{M}^{nN}$ is the sensory channel transmission variable over the time horizon; and $\mathcal{U}_k(\mathscr{I}_k) \in \mathbb{R}^{mN}$ is the new control law over the time horizon with sensory channel packet loss. It should be noted that $\mathrm{T}_k$ is an idempotent matrix, meaning $\mathrm{T}_k^i = \mathrm{T}_k$ for all $i \in \mathbb{Z}_{++}$, this is due to the properties of the Bernoulli distribution. Additionally, $\Gamma^{\mathbf{A}}$ only differs from $\Gamma$ by the lack of $\mathbf{B}$ within it, i.e $\Gamma^{\mathbf{A}}\left(\mathbf{I}\otimes\mathbf{B}\right) = \Gamma$, where $\otimes$ is the Kronecker product. Also, due to the lack of a $\mathbf{C}$ in our description it should be clear that $p = n$. We define the following

predictions

$$\widehat{\mathcal{X}}_k = \mathbb{E}\left[\mathcal{X}|\mathcal{I}_k\right] = \Phi X_k + \Gamma\overline{\Upsilon}\mathcal{U}_k(\mathcal{I}_k)\,, \tag{4.54a}$$

$$\widehat{\mathcal{Y}}_k = \mathbb{E}\left[\mathcal{Y}_k|\mathcal{I}_k\right] = \mathbb{E}\left[\mathrm{T}_k\mathcal{X}_k|\mathcal{I}_k\right] = \overline{\mathrm{T}}\left(\Phi X_k + \Gamma\overline{\Upsilon}\mathcal{U}_k(\mathcal{I}_k)\right), \tag{4.54b}$$

where $\mathbb{E}\left[\mathrm{T}_k\right] = \overline{\mathrm{T}}$. As before, for the purposes of estimation, TCP-like protocols will have access to the both channels packet realisations, resulting in (4.52a). However, when computing the optimal control law the the operator will not have access to the packet drop realisations resulting in (4.54). This, as before, is to maintain causality. The operator does not know the realisation of a packet drop before actuating, but will know the packet transmission variables realisation when updating the state estimate. Under the UDP-like protocol, the packet drop must be estimated for both the estimation and optimal control problem on the actuation side but it does have access to the current realisation of the packet loss on the sensory communication channel, namely, $\mathbf{L}_k$. Stacking the error terms in the same fashion as the state trajectory results in the following matrix terms for the error predictions

$$\begin{aligned}\mathcal{E}_k(\mathcal{F}_k) &\triangleq \mathcal{X}_k - \mathbb{E}\left[\mathcal{X}_k\middle|\mathcal{F}_k, \Upsilon_k\right]\\ &= \Phi X_k + \Gamma\Upsilon_k U_k(\mathcal{F}_k) + \Lambda\mathcal{W}_k - \widehat{\mathcal{X}}_k\\ &= \Phi X_k + \Gamma\Upsilon_k U_k(\mathcal{F}_k) + \Lambda\mathcal{W}_k - \Phi X_k - \Gamma\Upsilon_k U_k(\mathcal{F}_k)\\ &= \Lambda\mathcal{W}_k,\end{aligned} \tag{4.55a}$$

for the TCP-like protocol and

$$\begin{aligned}\mathcal{E}_k(\mathcal{G}_k) &\triangleq \mathcal{X}_k - \mathbb{E}\left[\mathcal{X}_k\middle|\mathcal{G}_k\right]\\ &= \Phi X_k + \Gamma\Upsilon_k U_k(\mathcal{G}_k) + \Lambda\mathcal{W}_k - \widehat{\mathcal{X}}_k\\ &= \Phi X_k + \Gamma\Upsilon_k\mathcal{U}_k(\mathcal{G}_k) + \Lambda\mathcal{W}_k - \Phi X_k - \Gamma\overline{\Upsilon}\mathcal{U}_k(\mathcal{G}_k)\\ &= \Gamma\left(\Upsilon_k - \overline{\Upsilon}\right)\mathcal{U}_k(\mathcal{G}_k) + \Lambda\mathcal{W}_k,\end{aligned} \tag{4.55b}$$

for the UDP-like protocol. As in the previous derivation the cost function is an LQG cost function that the operator minimises, with the same penalty matrices as defined before. However, due to the loss of packets in the sensory communication channel, $\gamma_k$ the cost is redefined such that it is minimised with respect to $\mathcal{Y}_k$ and not $\mathcal{X}$. Therefore the cost function to be minimised is

$$J\left(\mathcal{I}_k\right) \triangleq \mathbb{E}\left[ X_k^{\mathsf{T}} \mathbf{Q} X_k + \mathcal{Y}_k^{\mathsf{T}} \Omega \mathcal{Y}_k + \mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k) \Upsilon_k^{\mathsf{T}} \Psi \Upsilon_k \mathcal{U}_k(\mathcal{I}_k) \middle| \mathcal{I}_k \right], \tag{4.56a}$$

where the expectation in (4.56a) is with respect to the joint distribution of $\Upsilon_k$, $\mathrm{T}_k$, and $\mathcal{W}_k$. The expectation is taken sequentially as in [65, Lemma 1(c)] to account for the causality constraints imposed by the system. Therein, the expectation at each time step is conditioned on all previous time steps. This is due to the fact that the sequence of states at each time step forms a Markov chain, i.e. $X_k \to X_{k+1} \to \cdots \to X_{k+N}$. The state trajectory $\mathcal{X}_k$ is re-written in terms of the estimate $\widehat{\mathcal{X}}_k$ and the error induced by the estimate $\mathcal{E}_k$. Substituting $\mathcal{X}_k = \widehat{\mathcal{X}}_k + \mathcal{E}_k$ into (4.56a) yields

$$J(\mathcal{I}_k) = \mathbb{E}\Big[ X_k^{\mathsf{T}} \mathbf{Q} X_k + \left(\widehat{\mathcal{X}}_k + \mathcal{E}_k\right)^{\mathsf{T}} \mathrm{T}_k \Omega \mathrm{T}_k \left(\widehat{\mathcal{X}}_k + \mathcal{E}_k\right) + \mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k) \Upsilon_k^{\mathsf{T}} \Psi \Upsilon_k \mathcal{U}_k(\mathcal{I}_k) \Big| \mathcal{I}_k \Big]. \tag{4.56b}$$

The optimal control problem is to find the input sequence $\mathcal{U}_k^*(\mathcal{I}_k)$ that minimises (4.9b). Additionally, it should be noted that $\mathbb{E}\left[\mathcal{E}_k \middle| \mathcal{I}_k\right] = 0$ and the state error and the state estimate are independent for both protocols.

$$\begin{aligned} J^*(\mathcal{I}_k) &= \min_{\mathcal{U}_k(\mathcal{I}_k)} \left\{ \mathbb{E}\Big[ X_k^{\mathsf{T}} \mathbf{Q} X_k + \left(\widehat{\mathcal{X}}_k + \mathcal{E}_k\right)^{\mathsf{T}} \mathrm{T}_k \Omega \mathrm{T}_k \left(\widehat{\mathcal{X}}_k + \mathcal{E}_k\right) + \mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k) \Upsilon_k^{\mathsf{T}} \Psi \Upsilon_k \mathcal{U}_k(\mathcal{I}_k) \Big| \mathcal{I}_k \Big] \right\} \\ &= \min_{\mathcal{U}_k(\mathcal{I}_k)} \Big\{ X_k^{\mathsf{T}} \mathbf{Q} X_k + \mathbb{E}\left[ \widehat{\mathcal{X}}_k^{\mathsf{T}} \mathrm{T}_k^{\mathsf{T}} \Omega \mathrm{T}_k \widehat{\mathcal{X}}_k + \mathcal{E}^{\mathsf{T}} \mathrm{T}_k^{\mathsf{T}} \Omega \mathrm{T}_k \mathcal{E} + \mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k)\, \Upsilon_k{}^{\mathsf{T}} \Psi \Upsilon_k \mathcal{U}_k(\mathcal{I}_k) \right] \Big\}. \end{aligned} \tag{4.57}$$

When looking at the expectation in (4.57), the three terms in the expectation are non-trivial. The two terms $U_k(\mathcal{I}_k)\, \Upsilon_k{}^{\mathsf{T}} \Psi \Upsilon_k \mathcal{U}_k(\mathcal{I}_k)$ and $\widehat{\mathcal{X}}_k^{\mathsf{T}} \mathrm{T}_k^{\mathsf{T}} \Omega \mathrm{T}_k \widehat{\mathcal{X}}_k$ are easier to evaluate and $\mathbb{E}\left[\mathcal{E}_k^{\mathsf{T}} \mathrm{T}_k^{\mathsf{T}} \Omega \mathrm{T}_k \mathcal{E}_k\right]$ can be simplified by using the commutation properties of diagonal

matrices and the idempotency of $\Upsilon_k$ and T. This is

$$\begin{aligned}
\mathbb{E}\left[\mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k)\Upsilon_k{}^{\mathsf{T}}\Psi\Upsilon_k\mathcal{U}_k(\mathcal{I}_k)\right] &= \mathbb{E}_{\Upsilon_k}\left[\mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k)\Upsilon_k{}^{\mathsf{T}}\Upsilon_k\Psi\mathcal{U}_k(\mathcal{I}_k)\right] \\
&= \mathbb{E}_{\Upsilon_k}\left[\mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k)\Upsilon_k\Psi\mathcal{U}_k(\mathcal{I}_k)\right] \\
&= \mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k)\overline{\Upsilon}\Psi\mathcal{U}_k(\mathcal{I}_k), && (4.58a) \\
\mathbb{E}\left[\widehat{\mathcal{X}}_k^{\mathsf{T}}\mathrm{T}_k^{\mathsf{T}}\Omega\mathrm{T}_k\widehat{\mathcal{X}}_k\right] &= \mathbb{E}_{\mathrm{T}_k}\left[\widehat{\mathcal{X}}_k^{\mathsf{T}}\mathrm{T}_k^{\mathsf{T}}\mathrm{T}_k\Omega\widehat{\mathcal{X}}_k\right] \\
&= \mathbb{E}_{\mathrm{T}_k}\left[\widehat{\mathcal{X}}_k^{\mathsf{T}}\mathrm{T}_k\Omega\widehat{\mathcal{X}}_k\right] \\
&= \widehat{\mathcal{X}}_k^{\mathsf{T}}\overline{\mathrm{T}_k}\Omega\widehat{\mathcal{X}}_k, && (4.58b) \\
\mathbb{E}_{\mathrm{T},\mathcal{E}}\left[\mathcal{E}_k^{\mathsf{T}}\mathrm{T}_k^{\mathsf{T}}\Omega\mathrm{T}_k\mathcal{E}_k\right] &= \mathbb{E}_{\mathcal{E},\mathrm{T}}\left[\mathcal{E}_k^{\mathsf{T}}\mathrm{T}_k^{\mathsf{T}}\mathrm{T}_k\Omega\mathcal{E}_k\right] \\
&= \mathbb{E}_{\mathcal{E},\mathrm{T}}\left[\mathcal{E}_k^{\mathsf{T}}\mathrm{T}_k\Omega\mathcal{E}_k\right] \\
&= \mathbb{E}_{\mathcal{E}}\left[\mathcal{E}_k^{\mathsf{T}}\overline{\mathrm{T}_k}\Omega\mathcal{E}_k\right], && (4.58c)
\end{aligned}$$

where the sub index on the expectation denotes with which variable the expectation is being taken with respect to. Note these variables are by definition independent which allows this. Substitution of these simplifications yields

$$J^*(\mathcal{I}_k) = \min_{\mathcal{U}_k(\mathcal{I}_k)}\Big\{X_k^{\mathsf{T}}\mathbf{Q}X_k + \mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k)\,\overline{\Upsilon}\Psi\mathcal{U}_k(\mathcal{I}_k) + \widehat{\mathcal{X}}_k^{\mathsf{T}}\overline{\mathrm{T}}\Omega\widehat{\mathcal{X}}_k + \mathbb{E}_{\mathcal{E}}\left[\mathcal{E}_k^{\mathsf{T}}\overline{\mathrm{T}}\Omega\mathcal{E}_k|\mathcal{I}_k\right]\Big\}, \quad (4.59)$$

substituting (4.54) gives

$$\begin{aligned}
J^*(\mathcal{I}_k) = \min_{\mathcal{U}_k(\mathcal{I}_k)}\Big\{&X_k^{\mathsf{T}}\mathbf{Q}X_k + \mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k)\,\overline{\Upsilon}\Psi\mathcal{U}_k(\mathcal{I}_k) + \Big(\Phi X_k + \Gamma\overline{\Upsilon}\mathcal{U}_k(\mathcal{I}_k)\Big)^{\mathsf{T}}\overline{\mathrm{T}}\Omega\left(\Phi X_k + \Gamma\overline{\Upsilon}\mathcal{U}_k(\mathcal{I}_k)\right) \\
&+\mathbb{E}_{\Upsilon,\mathcal{W}}\left[\mathcal{E}_k^{\mathsf{T}}\overline{\mathrm{T}}\Omega\mathcal{E}_k|\mathcal{I}_k\right]\Big\} && (4.60) \\
= \min_{\mathcal{U}_k(\mathcal{I}_k)}\Big\{&X_k^{\mathsf{T}}\left(\mathbf{Q} + \Omega_{pt}\right)X_k + \mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k)\,\overline{\Upsilon}\left(\Omega_{gt}\overline{\Upsilon} + \Psi\right)\mathcal{U}_k(\mathcal{I}_k) + 2\overline{\Upsilon}\mathcal{U}_k^{\mathsf{T}}(\mathcal{I}_k)\,\Omega_{gtp}X_k \\
&+\mathbb{E}_{\Upsilon,\mathcal{W}}\left[\mathcal{E}_k^{\mathsf{T}}\overline{\mathrm{T}}\Omega\mathcal{E}_k|\mathcal{I}_k\right]\Big\}, && (4.61)
\end{aligned}$$

where for ease of notation $\Phi^{\mathsf{T}}\overline{\mathrm{T}}\Omega\Phi = \Omega_{pt}$, $\Gamma^{\mathsf{T}}\overline{\mathrm{T}}\Omega\Gamma = \Omega_{gt}$, and $\Gamma^{\mathsf{T}}\overline{\mathrm{T}}\Omega\Phi = \Omega_{gtp}$. Also, as before, a number of terms do not depend on the control input, and therefore, are removed

from the minimisation to yield

$$J^*(\mathcal{I}_k) = X_k^\mathsf{T}\left(\mathbf{Q} + \Omega_{pt}\right) X_k + \min_{\mathcal{U}_k(\mathcal{I}_k)} \Big\{ \mathcal{U}_k^\mathsf{T}(\mathcal{I}_k)\,\overline{\Upsilon}\left(\Omega_{gt}\overline{\Upsilon} + \Psi\right)\mathcal{U}_k(\mathcal{I}_k) + 2\overline{\Upsilon}\mathcal{U}_k^\mathsf{T}(\mathcal{I}_k)\,\Omega_{gtp} X_k + \mathbb{E}_{\mathcal{E}}\left[\mathcal{E}_k^\mathsf{T}\overline{\mathrm{T}}\Omega\mathcal{E}_k|\mathcal{I}_k\right]\Big\}. \tag{4.62}$$

Evaluating the expectation of the final term is not trivial. It is in this step that the difference between UDP-like and TCP-like becomes clear. This leads to the following lemma

**Lemma 10.** *Consider the system modelled by (4.50) with access to (4.51). Then the following holds*

$$\mathbb{E}_{\Upsilon,\mathcal{W}}\left[\mathcal{E}_k^\mathsf{T}\overline{\mathrm{T}}\Omega\mathcal{E}_k \middle| \mathcal{F}_k\right] = \mathrm{tr}\left(\Omega_{lt}\Sigma_{\mathcal{W}}\right), \tag{4.63a}$$

$$\mathbb{E}_{\Upsilon,\mathcal{W}}\left[\mathcal{E}_k^\mathsf{T}\overline{\mathrm{T}}\Omega\mathcal{E}_k \middle| \mathcal{G}_k\right] = \mathcal{U}_k^\mathsf{T}(\mathcal{I}_k)\overline{\Upsilon}\left(\mathbf{I}\odot\Omega_{gt}\right)\left(\mathbf{I}-\overline{\Upsilon}\right)\mathcal{U}_k(\mathcal{G}_k) + \mathrm{tr}\left(\Omega_{lt}\Sigma_{\mathcal{W}}\right), \tag{4.63b}$$

*where* $\Omega_{lt} = \Lambda^\mathsf{T}\mathrm{T}\Omega\Lambda$ *and* $\odot$ *denotes the Hadamard product.*

*Proof.* The proof of this is identical to Lemma 7 with a transformation of the $\Omega$ matrix and is therefore omitted.

Due to this difference in quadratic error between the protocols, once again the derivation must be split. This is seen in the following theorem.

**Theorem 6.** *Consider the closed-loop control system, with plant dynamics given in (4.50), protocol dependent information sets given in (4.51), and controller cost function given in (4.62), respectively. Then the optimal cost for the TCP-like protocol is*

$$J^*\left(\mathcal{F}_k\right) = X_k^\mathsf{T}(\mathbf{Q}+\Omega_{pt})X_k + \mathrm{tr}\left(\Sigma_{\mathcal{W}}\Omega_{lt}\right) - X_k^\mathsf{T}\Omega_{gtp}^\mathsf{T}\mathbf{G}^{-1}(\mathcal{F}_k)\overline{\Upsilon}\Omega_{gtp}X_k, \tag{4.64a}$$

*and the optimal cost for the UDP-like protocol is*

$$J^*\left(\mathcal{G}_k\right) = X_k^\mathsf{T}(\mathbf{Q}+\Omega_{pt})X_k + \mathrm{tr}\left(\Sigma_{\mathcal{W}}\Omega_{lt}\right) - X_k^\mathsf{T}\Omega_{gtp}^\mathsf{T}\mathbf{G}^{-1}(\mathcal{G}_k)\overline{\Upsilon}\Omega_{gtp}X_k. \tag{4.64b}$$

*The corresponding optimal control laws are*

$$\mathcal{U}_k^*(\mathscr{F}_k) \triangleq -\left(\Omega_{gt}\overline{\Upsilon} + \Psi\right)^{-1}\Omega_{gtp}X_k \tag{4.65a}$$
$$= -\mathbf{G}^{-1}(\mathscr{F}_k)\,\Omega_{gtp}X_k,$$
$$\mathcal{U}_k^*(\mathscr{G}_k) \triangleq -\left(\Psi + (\mathbf{I}\odot\Omega_g)\left(\mathbf{I}-\overline{\Upsilon}\right) + \Omega_{gt}\overline{\Upsilon}\right)^{-1}\Omega_{gtp}X_k \tag{4.65b}$$
$$= -\mathbf{G}^{-1}(\mathscr{G}_k)\,\Omega_{gtp}X_k,$$

*for the TCP-like and the UDP-like protocols, respectively.*

*Proof.* As in the previous derivation of the optimal control laws and resultant cost functions, the derivation must be split into two sections, with one corresponding to each communication protocol.

**Remark 3.** *It should be noted that both of the above optimal control laws require access the state information $X_k$ in order to be implemented. However, in the case of sensory packet loss it is possible that this information may be unavailable at a given time instance. We propose implementing the next entry of the previous optimal control input. However, as with the other work in this thesis we don't analyse the potential stability repercussions of the system. Naturally, the drawback of this is we are dealing with random processes and therefore there is a non zero probability of running out control inputs in the horizon length, $N$. Therefore, it is suggested that the horizon length should be created long enough such that the probability of receiving a sequence of $N$ sequential zeros is below a threshold that the operator accepts. Alternatively the operator could perform no actuation when no sensory signal is received, this mirrors the zero input strategy assumed on the control optimisation.*

### TCP-like Protocol

From Lemma 10 it is clear that the error term for the TCP-like protocol does not depend on the control input and can therefore be removed from the control optimisation

$$J^*(\mathcal{F}_k) = X_k^\mathsf{T}\left(\mathbf{Q} + \Omega_{pt}\right) X_k + \mathbb{E}_{\Upsilon,\mathcal{W}}\left[\mathcal{E}_k^\mathsf{T}\overline{\mathrm{T}}\Omega\mathcal{E}_k|\mathcal{F}_k\right] + \min_{\mathcal{U}_k(\mathcal{F}_k)}\left\{\mathcal{U}_k^\mathsf{T}(\mathcal{F}_k)\,\overline{\Upsilon}\left(\Omega_{gt}\overline{\Upsilon} + \Psi\right)\mathcal{U}_k(\mathcal{F}_k) + 2\overline{\Upsilon}\mathcal{U}_k^\mathsf{T}(\mathcal{F}_k)\,\Omega_{gtp}X_k\right\}. \tag{4.66}$$

Using Lemma 10 the cost then becomes

$$J^*(\mathcal{F}_k) = X_k^\mathsf{T}\left(\mathbf{Q} + \Omega_{pt}\right) X_k + \mathrm{tr}\left(\Omega_{lt}\Sigma_{\mathcal{W}}\right) + \min_{\mathcal{U}_k(\mathcal{F}_k)}\left\{\mathcal{U}_k^\mathsf{T}(\mathcal{F}_k)\,\overline{\Upsilon}\left(\Omega_{gt}\overline{\Upsilon} + \Psi\right)\mathcal{U}_k(\mathcal{F}_k) + 2\overline{\Upsilon}\mathcal{U}_k^\mathsf{T}(\mathcal{F}_k)\,\Omega_{gtp}X_k\right\}. \tag{4.67}$$

Minimising with respect to $\mathcal{U}_k(\mathcal{F}_k)$ under the TCP-like protocol yields

$$\frac{\partial J(\mathcal{F}_k)}{\partial \mathcal{U}_k(\mathcal{F}_k)} = 2\overline{\Upsilon}\Omega_{gtp}X_k + 2\overline{\Upsilon}\left(\Omega_{gt}\overline{\Upsilon} + \Psi\right)\mathcal{U}_k(\mathcal{F}_k) \tag{4.68}$$

$$= 2\overline{\Upsilon}\left(\Omega_{gtp}X_k + \left(\Psi + \Omega_{gt}\overline{\Upsilon}\right)\mathcal{U}_k(\mathcal{F}_k)\right). \tag{4.69}$$

All terms within $\left(\Psi + \Omega_{gt}\overline{\Upsilon}\right)$ are either positive definite or positive semi-definite. This means the whole term is strictly positive definite, and therefore invertible. Therefore, assuming $\overline{\Upsilon}, \overline{\mathrm{T}} \neq 0$ yields the minimising $\mathcal{U}_k(\mathcal{F}_k)$ . Namely, it is found to be

$$\mathcal{U}_k^*(\mathcal{F}_k) = -\left(\Psi + \Omega_{gt}\overline{\Upsilon}\right)^{-1}\overline{\mathrm{T}}\Omega_{gtp}X_k \tag{4.70}$$

$$= -\mathbf{G}_t^{-1}(\mathcal{F}_k)\,\Omega_{gtp}X_k, \tag{4.71}$$

where $\mathbf{G}_t^{-1}(\mathcal{F}_k) = \left(\Psi + \Omega_{gt}\overline{\Upsilon}\right)^{-1}$. Substitution of the optimal control law into the expected cost function gives the optimal cost function under TCP-like protocols

$$\begin{aligned} J^*(\mathcal{F}_k) &= X_k^{\mathsf{T}}\left(\mathbf{Q} + \Omega_{pt}\right) X_k + \operatorname{tr}\left(\Omega_{lt}\Sigma_{\mathcal{W}}\right) \\ &\qquad + \mathcal{U}_k^{*\mathsf{T}}(\mathcal{F}_k)\,\overline{\Upsilon}\left(\Omega_{gt}\overline{\Upsilon} + \Psi\right)\mathcal{U}_k^*(\mathcal{F}_k) + 2\overline{\Upsilon}\mathcal{U}_k^{*\mathsf{T}}(\mathcal{F}_k)\,\Omega_{gtp}X_k \\ &= X_k^{\mathsf{T}}\left(\mathbf{Q} + \Omega_{pt}\right) X_k + \operatorname{tr}\left(\Omega_{lt}\Sigma_{\mathcal{W}}\right) - X_k^{\mathsf{T}}\Omega_{gtp}^{\mathsf{T}}\overline{\Upsilon}\mathbf{G}_t^{-1}(\mathcal{F}_k)\,\Omega_{gtp}X_k, \end{aligned} \tag{4.72}$$

### UDP-like Protocol

The main difference in how the protocols affect the optimal control law is that the UDP-like protocol error depends on the input to the system and therefore cannot be removed from the minimisation. However, the use of Lemma 10 allows simplification of the minimisation. The cost is transformed to

$$\begin{aligned} J^*(\mathcal{G}_k) &= X_k^{\mathsf{T}}\left(\mathbf{Q} + \Omega_{pt}\right) X_k + \operatorname{tr}\left(\Omega_{lt}\Sigma_{\mathcal{W}}\right) + \\ &\quad + \min_{\mathcal{U}_k(\mathcal{G}_k)} \left\{\mathcal{U}_k^{\mathsf{T}}(\mathcal{G}_k)\,\overline{\Upsilon}\left(\Omega_{gt}\overline{\Upsilon} + (\mathbf{I}\odot\Omega_{gt})\left(\mathbf{I} - \overline{\Upsilon}\right) + \Psi\right)\mathcal{U}_k(\mathcal{G}_k) + 2\overline{\Upsilon}\mathcal{U}_k^{\mathsf{T}}(\mathcal{G}_k)\,\Omega_{gtp}X_k\right\}. \end{aligned} \tag{4.73}$$

Minimising with respect to $\mathcal{U}_k(\mathcal{G}_k)$ under the UDP-like information set yields

$$\begin{aligned} \frac{\partial J(\mathcal{G}_k)}{\partial \mathcal{U}_k(\mathcal{G}_k)} &= 2\overline{\Upsilon}\Omega_{gtp}X_k + 2\overline{\Upsilon}\left(\Omega_{gt}\overline{\Upsilon} + (\mathbf{I}\odot\Omega_{gt})\left(\mathbf{I} - \overline{\Upsilon}\right) + \Psi\right)\mathcal{U}_k(\mathcal{G}_k) && (4.74) \\ &= 2\overline{\Upsilon}\left(\Omega_{gtp}X_k + \left(\Psi + (\mathbf{I}\odot\Omega_{gt})\left(\mathbf{I} - \overline{\Upsilon}\right) + \Omega_{gt}\overline{\Upsilon}\right)\mathcal{U}_k(\mathcal{G}_k)\right). && (4.75) \end{aligned}$$

All terms within $\left(\Psi + (\mathbf{I}\odot\Omega_{gt})\left(\mathbf{I} - \overline{\Upsilon}\right)\Omega_{gt}\overline{\Upsilon}\right)$ are either positive definite or positive semi-definite. This means the whole term is strictly positive definite, and therefore invertible. Therefore, assuming $\overline{\Upsilon}, \overline{\mathrm{T}} \neq 0$ yields the minimising $\mathcal{U}_k(\mathcal{G}_k)$. Namely, it is found to be

$$\begin{aligned} \mathcal{U}_k^*(\mathcal{G}_k) &= -\left(\Psi + (\mathbf{I}\odot\Omega_{gt})\left(\mathbf{I} - \overline{\Upsilon}\right) + \Omega_{gt}\overline{\Upsilon}\right)^{-1}\overline{\mathrm{T}}\Omega_{gtp}X_k && (4.76) \\ &= -\mathbf{G}_t^{-1}(\mathcal{G}_k)\,\Omega_{gtp}X_k, && (4.77) \end{aligned}$$

where $\mathbf{G}_t^{-1}(\mathcal{G}_k) = \left(\Psi + \Omega_{gt}\overline{\Upsilon}\right)^{-1}$. Substitution of the optimal control law into the expected cost function gives the optimal cost function under UDP-like protocols

$$\begin{aligned} J(\mathcal{G}_k) &= X_k^{\mathsf{T}}\left(\mathbf{Q} + \Omega_{pt}\right) X_k + \operatorname{tr}\left(\Omega_{lt}\Sigma_{\mathcal{W}}\right) \\ &\qquad + \mathcal{U}_k^{*\mathsf{T}}(\mathcal{G}_k)\,\overline{\Upsilon}\left(\Omega_{gt}\overline{\Upsilon} + \Psi\right)\mathcal{U}_k^{*}(\mathcal{G}_k) + 2\overline{\Upsilon}\mathcal{U}_k^{*\mathsf{T}}(\mathcal{G}_k)\,\Omega_{gtp}X_k \\ &= X_k^{\mathsf{T}}\left(\mathbf{Q} + \Omega_{pt}\right) X_k + \operatorname{tr}\left(\Omega_{lt}\Sigma_{\mathcal{W}}\right) - X_k^{\mathsf{T}}\Omega_{gtp}^{\mathsf{T}}\,\overline{\Upsilon}\mathbf{G}_t^{-1}(\mathcal{G}_k)\,\Omega_{gtp}X_k. \end{aligned} \tag{4.78}$$

This concludes the proof. □

## 4.7 Dual Channel Cost Difference Analysis

From the previous cost difference analysis, where there is only one multidimensional communication link, most results readily translate straight into this new system design. To that end, we restate them explicitly in the new system transformation.

**Theorem 7** (Main Result)**.** *Let* $\mathbf{M}$ *such that* $\mathbf{0} \prec \mathbf{M} \prec \mathbf{I}$*, and let* $\mathbf{0} \prec \mathbf{T} \prec \mathbf{I}$ *then with information sets given in (4.51). It holds that*

$$J^*\left(\mathcal{G}_k\right) - J^*\left(\mathcal{F}_k\right) > 0,$$

*where the optimal cost is as defined in (4.62).*

*Proof.* The optimal control laws for each communication protocol are defined in (4.71) and (4.77). Note that $\mathbf{G}_t(\mathcal{I}_k) \succ 0$ and that,

$$\mathbf{G}(\mathcal{G}_k) - \mathbf{G}(\mathcal{F}_k) = \left(\mathbf{I} \odot \Omega_{gt}\right)\left(\mathbf{I} - \overline{\Upsilon}\right) \succ 0. \tag{4.79}$$

Therefore, [30, 10.53] implies that

$$\begin{gathered}\mathbf{G}_t^{-1}(\mathcal{G}_k) \prec \mathbf{G}_t^{-1}(\mathcal{F}_k)\,,\\ \mathbf{G}_t^{-1}(\mathcal{G}_k)\,\overline{\Upsilon} \prec \mathbf{G}_t^{-1}(\mathcal{F}_k)\,\overline{\Upsilon},\\ \mathbf{C} - X_k^{\mathsf{T}}\Omega_{gtp}^{\mathsf{T}}\mathbf{G}_t^{-1}(\mathcal{G}_k)\,\overline{\Upsilon}\Omega_{gtp}X_k > \mathbf{C} - X_k^{\mathsf{T}}\Omega_{gtp}^{\mathsf{T}}\mathbf{G}_t^{-1}(\mathcal{F}_k)\,\overline{\Upsilon}\Omega_{gtp}X_k,\end{gathered}$$

where $\mathbf{C} = X_k^{\mathsf{T}}\left(\mathbf{Q} + \Omega_{pt}\right)X_k + \operatorname{tr}\left(\Sigma_{\mathcal{W}}\Omega_{lt}\right)$. Therefore, for any $\mathbf{0} \prec \mathbf{M} \prec \mathbf{I}$ and $\mathbf{0} \prec \mathbf{T} \prec \mathbf{I}$ holds that

$$J^*\left(\mathcal{G}_k\right) - J^*\left(\mathcal{F}_k\right) > 0. \tag{4.80}$$

This concludes the proof. □

Similarly to before, additional insight can be obtained from Theorem 7.

**Corollary 4.** *In the case where there are sensory communication channel packet loss. It still holds that*

$$\left\|\mathcal{U}_k^*(\mathcal{G}_k)\right\|_2 < \left\|\mathcal{U}_k^*(\mathcal{F}_k)\right\|_2, \tag{4.81}$$

*where* $\|\cdot\|_2$ *denotes the 2-norm.*

*Proof.* Starting with (4.79), it is seen that,

$$\mathbf{G}_t(\mathcal{G}_k) - \mathbf{G}_t(\mathcal{F}_k) = \left(\mathbf{I} \odot \Omega_{gt}\right)\left(\mathbf{I} - \overline{\Upsilon}\right) \succ 0, \tag{4.82}$$

$$\mathbf{G}_t^{-1}(\mathcal{G}_k) \prec \mathbf{G}_t^{-1}(\mathcal{F}_k)\,, \tag{4.83}$$

$$\mathbf{G}_t^{-1}(\mathcal{G}_k)\,\Omega_{gtp}X_k < \mathbf{G}_t^{-1}(\mathcal{F}_k)\,\Omega_{gtp}X_k, \tag{4.84}$$

$$\left\|\mathbf{G}_t^{-1}(\mathcal{G}_k)\,\Omega_{gtp}X_k\right\|_2 < \left\|\mathbf{G}_t^{-1}(\mathcal{F}_k)\,\Omega_{gtp}X_k\right\|_2, \tag{4.85}$$

$$\left\|-\mathcal{U}_k^*(\mathcal{G}_k)\right\|_2 < \left\|-\mathcal{U}_k^*(\mathcal{F}_k)\right\|_2, \tag{4.86}$$

$$\left\|\mathcal{U}_k^*(\mathcal{G}_k)\right\|_2 < \left\|\mathcal{U}_k^*(\mathcal{F}_k)\right\|_2. \tag{4.87}$$

This concludes the proof. □

The following theorem shows that the cost function is monotonically decreasing functions in $\mathbf{M}$ even with sensory channel packet loss for a fixed $\overline{\mathrm{T}}$.

**Theorem 8.** *Let* $\mathbf{M}_1 \in S_{++}^m$ *and* $\mathbf{M}_2 \in S_{++}^M$ *be diagonal matrices. If* $\mathbf{M}_2 \succ \mathbf{M}_1$ *then*

$$J^*_{\Delta\mathbf{M}} = J^*_{\mathbf{M}_1}(\mathscr{I}_k) - J^*_{\mathbf{M}_2}(\mathscr{I}_k) > 0, \tag{4.88}$$

*where* $J^*_{\mathbf{M}_1}(\mathscr{I}_k)$ *is the optimal expected cost obtained with the value of* $\mathbf{M}_i$*, where* $\mathbf{M}_i$ *as the mean of the actuation channel transmission variable* $\mathbf{V}_k$*.*

*Proof.* The proof of this theorem is identical the to the proof of Theorem 4 with the substitution of variables of $\Omega_{gp}$ for $\Omega_{gtp}$ and $\Omega_g$ for $\Omega_{gt}$. This concludes the proof. □

**Corollary 5.** *Theorem 7 combined with Theorem 8 implies that with both protocols operating at a fixed cost value, the TCP-like protocol communicates with a larger packet loss rate.*

$$J^*_{\mathbf{M}_1}(\mathscr{G}_k) = J^*_{\mathbf{M}_2}(\mathscr{F}_k), \tag{4.89}$$

*where* $\mathbf{M}_1 \succ \mathbf{M}_2$.

*Proof.* From Theorem 7

$$J^*_{\mathbf{M}_1}(\mathscr{G}_k) = J^*_{\mathbf{M}_1}(\mathscr{F}_k) + \epsilon,$$

where $\epsilon \in \mathbb{R}^+$. From Theorem 8 it is known that

$$J^*_{\mathbf{M}_1}(\mathscr{F}_k) + \epsilon = J^*_{\mathbf{M}_2}(\mathscr{F}_k).$$

Therefore,

$$J^*_{\mathbf{M}_1}(\mathscr{G}_k) = J^*_{\mathbf{M}_2}(\mathscr{F}_k).$$

This concludes the proof. □

**Remark 4.** *Theorem 4 and Corollary 5 also apply to a non-stationary communication channel with a slight adjustment of the conditions. Both are true for a non-stationary channel when the stronger condition* $\overline{\Upsilon}_2 \succ \overline{\Upsilon}_1$ *holds, or more precisely* $\mathbf{M}_{2\ k} \succ \mathbf{M}_{1\ k}$ *for all* $k$ *even with a constant, non-stationary* $\overline{\mathrm{T}}$*.*

As is shown in Theorem 7, the cost difference between the UDP-like and the TCP-like protocol is strictly positive for an actuation channel without deterministic packet transmissions. The cost difference is zero only in the cases of no actuation communication $\mathbf{M} = \mathbf{0}$ or perfect actuation communication $\mathbf{M} = \mathbf{I}$. Note that this conclusion is not necessarily true in the case of deterministic sensory channel communication. Namely, in the case with perfect communication on the sensory channel, the scenario reduces to the same as Theorem 3, in which case the TCP-like protocol still outperforms the UDP-like protocol.

It should be pointed out that transforming the $\Omega_{\bullet}$ matrices in the previous section, where there is perfect communication on the sensory channel, into the $\Omega_{\bullet t}$ matrices in this section, does not alter the positivity or symmetric properties of the matrices. Therefore, due to this fact, all of the results in those sections also apply to a system with sensory channel losses.

## 4.8 Dual Channel Packet Loss Allocation

With the above statement in mind, it allows us to inquire into the resource allocation problem for a system with packet loss on both communication channels.

To that end, we define some objects corresponding to a system with both actuation and sensory channel packet. The set of packet loss probability matrices that achieve a given cost $\alpha \in \mathbb{R}_+$ is the set of channel matrices described by

$$\mathcal{T}_k\left(\mathcal{I}_k\right) = \left\{\mathbf{M}, \mathbf{T} : J^*\left(\mathcal{I}_k\right) \leq \alpha\right\}. \tag{4.90}$$

All the matrices in the set induce a control cost that is upper bounded by $\alpha$, but differ in their use of communication resources, i.e. the packet transmission performance across different dimensions and different channels. To quantify the use of communication resources in global terms, a communication cost for the system is proposed, defined as

$$C\left(\mathbf{M},\mathbf{T}\right) \triangleq \sum_{i=1}^{m} \beta_i \mu_i + \epsilon_i \gamma_i = \mathrm{tr}\left(\boldsymbol{\beta}\mathbf{M} + \boldsymbol{\epsilon}\mathbf{T}\right), \tag{4.91}$$

where $\boldsymbol{\beta}, \boldsymbol{\epsilon} \in \mathbf{S}^{+}_{m\times m}$ are the non-negative definite penalty matrices where each diagonal entry $\beta_i \in \mathbb{R}$ and $\epsilon_i \in \mathbb{R}$, are penalty terms corresponding to the cost of communication in that channel. With the above definitions, the minimum communication cost for a system with packet loss in both communication channels is defined as

$$C_\alpha\left(\mathscr{J}_k\right) \triangleq \underset{\{\mathbf{M},\mathbf{T}\}\in\mathscr{T}_k(\mathscr{J}_k)}{\arg\min} \; C\left(\mathbf{M},\mathbf{T}\right). \tag{4.92}$$

The maximum dual channel efficiency yields a communication setup that minimises the total number of packet losses while maintaining a specified system control performance. In view of this, the communication channel configurations that minimise the amount of resources allocated to each channel is

$$\{\mathbf{M}^*,\mathbf{T}^*\} \triangleq \underset{\{\mathbf{M}^*,\mathbf{T}^*\}\in\mathscr{T}_k(\mathscr{J}_k)}{\min} \; C\left(\mathbf{M},\mathbf{T}\right). \tag{4.93a}$$

This cost of communication formulation highlights the importance of Corollary 5. Note that in the single channel version $\mathbf{M}^*$ is a single matrix. However, in this dual channel optimisation the set $\{\mathbf{M}^*,\mathbf{T}^*\}$ will not necessarily be two matrices and will most likely be a set of possible matrices that all achieve the same optimal cost.

## 4.9 Chapter Conclusion

We have obtained the optimal control laws for control systems with multidimensional communication channels subject to IID packet loss for both TCP-like and UDP-like packet

acknowledgement protocols. It is proved that for stationary packet loss processes, the cost incurred by the UDP-like protocol is strictly larger than that of the TCP-like protocol and that the difference between both increases monotonically with the probability of packet loss within each channel. These results provide an analytical framework to study the impact of communication channel resources in the performance of the control system. Capitalising on this notion, we have provided a guideline to optimally allocate channel resources for both the UDP-like and TCP-like protocol. This trade-off is explored via two case studies in Chapter 8.

We also provided the framework for MPC in the case where both of the communication channels are not perfect. Specifically, the sensory communication channel is another multidimensional packet loss communication channel. In doing so, it is seen that the formulation of the cost is similar. Namely, the matrices within the control law also depend on the probability of the sensory communication channel. In providing this extension the work above is a true generalisation of the system within [59].

This chapter has fully characterised a control system that operates with a multidimensional packet loss communication channel. Indeed, we derived the optimal control law for the operator and have provided the resultant optimal cost.

# Chapter 5

# Optimal Random Denial of Service Attacks

## 5.1 Introduction

The previous chapter outlines the optimal control law for the operator. The following chapter is from the perspective of the attacker. However, the following chapter derives the optimal stealthy *random* DoS attack. This is as opposed to the deterministic construction as seen within Chapter 3. Initially, this attack construction is restricted to the IID case, however, this assumption is later dropped.

The following attack construction differs from the derivation in Chapter 3 in that the attacker need not monitor the system after deriving their optimal attack strategy. This is due to the fact that since the attack construction is random, and therefore, after designing the optimal statistics for the attack the attacker needs only to implement the attack according to those statistics. Therefore, the random attack strategy derived is able to be implemented with a more restrictive information set than in the deterministic attack strategy. Specifically, once derived this attack construction requires no knowledge of the current realisation of the system or any system parameters. This means that the attack strategy can be implemented easier than the deterministic strategy. In doing so

this attack construction overcomes the main drawbacks of the attack construction seen within Section3.9.

In Section 5.7 the attack construction is extended from an IID sequence to a non-stationary random process describing the packet drops. By extending the attack construction in this way it acts as a middle ground between the deterministic attack in Chapter 3 and the IID attack initially derived in this chapter. In fact it is shown that the IID attack construction is a subset of the possible solutions of the non-stationary attack.

It should be noted that the following attack strategy is derived for a control system that only has packet loss on the actuation communication channel. However, as seen in Chapter 4, the following is trivially extended to a control system with packet loss on both channels with the relevant transformations of the $\Omega_\bullet$ variables. It should be noted that the attacker only performs an attack on the actuation communication channel and leaves the sensory communication channel unaltered.

## 5.2 Operator Model

The operator is assumed to be employing the optimal control strategies derived in Chapter 4. However, in this Chapter the operator is also conducting a hypothesis test as means of attack detection. Namely, we assume that the operator is monitoring the realisations of the packet drops in the communication channel and at each time step decides whether the drops in the channel are nominal or a sequence of drops induced by an attack. This detection strategy is explored in more detail in Section 5.4. The operator model remains as in Chapter 4, however, it is outlined briefly here for ease of reading. We consider the plant model given by

$$X_{k+1} = \mathbf{A}X_k + \mathbf{B}\mathbf{V}_k U_k + W_k, \tag{5.1}$$

where $\mathbf{A} \in \mathbb{M}^n$ is the dynamics matrix; $X_k \in \mathbb{R}^n$ describes the state of the plant at time step $k \in \mathbb{N}$; $\mathbf{B} \in \mathbb{M}^{n\times m}$ is the controls matrix; $U_k \in \mathbb{R}^m$ is the vector of control inputs at

the $k$-th time step; $W_k \in \mathbb{R}^n$ is the process noise modelled by a Gaussian distributed vector of random variables with mean $\mathbf{0} \in \mathbb{R}^n$ and covariance matrix $\Sigma_W \in S^n_{++}$; and the diagonal matrix $\mathbf{V}_k \in S^m_{++}$ is the packet loss variable, where the $i$-th diagonal entry is an IID Bernoulli random variable with mean $\mu_i \in [0, 1]$. It is assumed that the state of the plant at time instant $k$ is modelled by a vector of Gaussian distributed random variables $X_k$ with mean $\overline{X} \in \mathbb{R}^n$ and covariance matrix $\Sigma_X \in S^n_{++}$. The operator utilises an MPC formulation to expand the plant model given in (5.1) over a prediction horizon $N \in \mathbb{N}_+$. This results in the prediction model

$$\mathcal{X}_k \triangleq \Phi X_k + \Gamma \Upsilon_k \mathcal{U}_k(\mathcal{I}_k) + \Lambda \mathcal{W}_k, \tag{5.2}$$

where $\Phi \in \mathbb{M}^{Nn \times n}$ is the dynamics matrix over the prediction horizon; $\mathcal{X}_k \in \mathbb{R}^{Nn}$ is the state prediction vector; $\Gamma \in \mathbb{M}^{Nn \times Nm}$ is the propagation matrix for the control law over the prediction horizon; $\mathcal{U}_k(\mathcal{I}_k) \in \mathbb{R}^{mN}$ is the realisation at the $k$-th time step of the control law with access to the information set $\mathcal{I}_k$; $\Lambda \in \mathbb{M}^{Nn}$ is the propagation matrix for the process noise; $\mathcal{W}_k \in \mathbb{R}^{Nn}$ is the process noise over the prediction horizon; and $\Upsilon_k$ is a diagonal matrix with the independent Bernoulli random variables describing the packet losses over the prediction horizon along the diagonal. All terms in (5.2) are also described in (4.5) in Chapter 4. As before, due to the lossy communication between the controller and the plant, the operator implements a communication protocol to monitor the state of the packet transmission variable. Naturally, we adopt the two protocols outlined in Chapter 4. Namely, the UDP-like protocol that does not monitor the channel and the TCP-like protocol that acknowledges receipt of the packet from the controller by sending an *acknowledgement* message to the controller over an auxiliary channel. The information set available to the operator is determined by the choice of protocol. We define the information sets for the operator as

$$\mathcal{I}_k \triangleq \begin{cases} \mathcal{F}_k = \left\{ \mathcal{X}^k, \mathcal{V}^{k-1} \right\}, & \text{TCP-like,} \\ \mathcal{G}_k = \left\{ \mathcal{X}^k \right\}, & \text{UDP-like,} \end{cases} \tag{5.3}$$

where $\mathcal{V}^{k-1} = \left\{\mathbf{V}_0, \mathbf{V}_1, \ldots, \mathbf{V}_{k-1}\right\}$ and all sets are monotonically increasing, i.e. there is a filtration such that $\mathcal{I}_k \subseteq \mathcal{I}_{k+1}$. This is identical to the information sets seen in Chapter 4. Additionally, the system diagrams that correspond to the TCP-like and the UDP-like protocols are depicted in Fig. 4.1 and Fig. 4.2, respectively. As seen previously, the optimal control law is determined by the mean of the packet loss variable. The optimal performance of the controller is characterised by the optimal LQG cost function

$$J^*\left(\mathcal{I}_k\right) = X_k^{\mathsf{T}}(\mathbf{Q} + \Omega_p)X_k + \mathrm{tr}\left(\Sigma_{\mathcal{W}}\Omega_l\right) - X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathcal{I}_k)\overline{\Upsilon}\Omega_{gp}X_k, \tag{5.4}$$

where $\Omega \in S_{++}^{Nn}$ is the state penalty diagonal matrix, $\Psi \in S_{++}^{Nm}$ is the input penalty diagonal matrix, and the diagonal matrix $\mathbf{Q} \in S_{++}^{n}$ is the initial state penalty matrix. The control law that results in the optimal cost function, (5.4), for each protocol is

$$\mathcal{U}_k^*(\mathcal{I}_k) = \begin{cases} \mathcal{U}_k^*(\mathcal{F}_k) = -\left(\Psi + \Omega_g\overline{\Upsilon}\right)^{-1}\Omega_{gp}X_k, & \text{TCP-like} \\ \mathcal{U}_k^*(\mathcal{G}_k) = -\left(\Psi + \Omega_g\overline{\Upsilon} + (\mathbf{I}\odot\Omega_g)\left(1-\overline{\Upsilon}\right)\right)^{-1}\Omega_{gp}X_k, & \text{UDP-like} \end{cases} \tag{5.5}$$

as shown in Theorem 2.

## 5.3 Attack Model

The performance of the controller is dependent on the packet transmission variable, as shown explicitly in (5.5). In view of this, we study the security risk posed by an attacker that governs the statistics of the packet losses on the actuation channel. In practice, this can be achieved by the attacker via DoS attacks over the communication channel. We are not concerned with the particular implementation of the DoS attacks, instead we study the packet loss attack strategy that aims to disrupt the operation of the controller. Specifically, the attacker dictates the statistics of the actuation communication channel. The rationale for random attacks stems from the fact that the operator expects the packet losses to be IID, and therefore, the attacker mimics the *nominal* operation of the channel. That being the case, the optimal attack construction is characterised by the probability of

packet loss in the actuation channel, described by the diagonal matrix $\mathbf{V}_k^\alpha \in S_{++}^m$ where the $i$-th diagonal entry is an IID Bernoulli random variable with mean $\mu_i^\alpha \in [0,1]$. In Section 5.7, the IID assumption is dropped and a non-stationary sequence of Bernoulli random variables is considered instead. The attacker has access to the information set

$$\mathscr{A}_k = \left\{\mathbf{A}, \mathbf{B}, \Sigma_W, \overline{\Upsilon}, \Omega, \Psi, \mathscr{I}_k\right\}. \tag{5.6}$$

There is a slight abuse of notation in the above, this definition is given to show all of the information the attacker requires for the following derivations, including knowledge of matrices/system architecture. Furthermore, knowledge of the state of the plant is *not* necessary to construct the optimal attack and it is only required to compute the cost induced by the attack over a particular realisation of the state variables. The controller operates under the assumption that the packet losses over the actuation channel are IID with a mean of packet losses defined by $\mathbf{M} = \mathbb{E}[\mathbf{V}_k]$ for $k \in \mathbb{N}$ with $\mathbf{M} \in S_{++}^m$. By changing the statistics of the actuation channel, the attacker induces a different distribution over the sequence of packet losses. For notation clarity, this random variable is defined as the diagonal matrix $\mathbf{V}_k^\alpha$. Similarly, the channel is characterised by $\mathbf{M}^\alpha = \mathbb{E}[\mathbf{V}_k^\alpha]$ for $k \in \mathbb{N}$, with $\mathbf{M}^\alpha \in S_{++}^m$. Note that the mean does not depend on the time step $k$, and therefore, the sequence of random variables describing the packet loss in the $i$-th position is IID. The sequence of packet losses over the prediction horizon is described by the diagonal matrix $\Upsilon_k^\alpha$ with the Bernoulli sequences along the diagonal and $\overline{\Upsilon}^\alpha \triangleq \mathbb{E}[\Upsilon_k^\alpha]$. Namely, the communication channel under nominal conditions has statistics

$$\mathbb{E}\left[\mathbf{V}_k\right] = \mathbb{E}\left[\begin{pmatrix} V_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & V_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \dots & \mathbf{0} & V_m \end{pmatrix}\right] = \begin{pmatrix} \mu_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mu_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \dots & \mathbf{0} & \mu_m \end{pmatrix} = \mathbf{M}, \tag{5.7a}$$

and similarly the communication channel under attack has the statistics

$$\mathbb{E}\left[\mathbf{V}_k^\alpha\right] = \mathbb{E}\left[\begin{pmatrix} V_1^\alpha & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & V_2^\alpha & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \dots & \mathbf{0} & V_m^\alpha \end{pmatrix}\right] = \begin{pmatrix} \mu_1^\alpha & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mu_2^\alpha & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \dots & \mathbf{0} & \mu_m^\alpha \end{pmatrix} = \mathbf{M}^\alpha. \tag{5.7b}$$

When considering the statistics of the communication channels over the control horizon, the nominal statistics are seen to be

$$\mathbb{E}\left[\Upsilon_k\right] = \mathbb{E}\left[\begin{pmatrix} \mathbf{V}_k & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{V}_{k+1} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{V}_{k+N-1} \end{pmatrix}\right] = \begin{pmatrix} \mathbf{M} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{M} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{M} \end{pmatrix} = \overline{\Upsilon}, \tag{5.8a}$$

and similarly the communication channel over the control horizon under attack has the statistics

$$\mathbb{E}\left[\Upsilon_k^\alpha\right] = \mathbb{E}\left[\begin{pmatrix} \mathbf{V}_k^\alpha & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{V}_{k+1}^\alpha & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{V}_{k+N-1}^\alpha \end{pmatrix}\right] = \begin{pmatrix} \mathbf{M}^\alpha & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{M}^\alpha & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{M}^\alpha \end{pmatrix} = \overline{\Upsilon}^\alpha. \tag{5.8b}$$

The objective of the attacker, in contrast to the objective of the operator, is to maximise the cost function that the operator minimises. Therefore, the cost function of the attacker is defined as

$$J_A\left(\mathscr{A}_k, \overline{\Upsilon}^\alpha\right) \triangleq \min_{\mathcal{U}_k(\mathscr{I}_k)} \left\{\mathbb{E}\left[X_k^\mathsf{T}\mathbf{Q}X_k + \mathcal{X}_k^\mathsf{T}\Omega\mathcal{X}_k + \mathcal{U}_k^\mathsf{T}(\mathscr{I}_k){\Upsilon_k}^{\alpha\mathsf{T}}\Psi\Upsilon_k^\alpha\mathcal{U}_k(\mathscr{I}_k)\middle|\mathscr{A}_k\right]\right\},$$

and the optimal attack construction is defined as

$$J_A^*\left(\mathscr{A}_k, \overline{\Upsilon}^\alpha\right) \triangleq \max_{\overline{\Upsilon}^\alpha} J_A\left(\mathscr{A}_k, \overline{\Upsilon}^\alpha\right). \tag{5.9}$$

Note that the cost function of the operator lies inside the maximisation of (5.9), i.e. the attacker chooses the worst case packet loss mean under the assumption that the controller operates optimally. It should be noted that by putting the minimisation of the operator within the maximisation of the attacker we have explicitly decided that the operator performs their optimisation first.

The state estimation performed by the attacker accounts for the true statistics of the actuation channel to produce the state prediction

$$\widehat{\mathcal{X}}_k^\alpha \triangleq \mathbb{E}\left[\mathcal{X}_k \middle| \mathscr{A}_k\right] = \Phi X_k + \Gamma\overline{\Upsilon}^\alpha \mathcal{U}_k(\mathscr{I}_k), \tag{5.10}$$

and the state error prediction of the attack construction for the two protocols is given by

$$\mathcal{E}(\mathscr{F}_k)^\alpha \triangleq \mathcal{X}_k - \mathbb{E}\left[\mathcal{X}_k \middle| \mathcal{F}_k, \Upsilon_k^\alpha\right] = \Lambda\mathcal{W}_k, \tag{5.11a}$$

$$\mathcal{E}(\mathscr{G}_k)^\alpha \triangleq \mathcal{X}_k - \mathbb{E}\left[\mathcal{X}_k \middle| \mathcal{G}_k\right] = \Gamma\left(\Upsilon_k^\alpha - \overline{\Upsilon}^\alpha\right)\mathcal{U}_k(\mathscr{I}_k) + \Lambda\mathcal{W}_k, \tag{5.11b}$$

for the TCP-like protocol and the UDP-like protocol, respectively. The proof of the error trajectories is identical to the proof in Chapter 4. We describe the attack induced cost by rewriting (5.9) in terms of the state prediction and the state prediction error as in [20] which yields

$$\begin{aligned} J_A^*\left(\mathscr{A}_k, \overline{\Upsilon}^\alpha\right) = X_k^\mathsf{T}\left(\mathbf{Q} + \Omega_p\right)X_k + \max_{\overline{\Upsilon}^\alpha}\Bigg\{ &\min_{\mathcal{U}_k(\mathscr{I}_k)}\left\{\mathbb{E}\left[\mathbf{E}_k^{\alpha\mathsf{T}}\Omega\mathcal{E}_k(\mathscr{I}_k)\middle|\mathscr{A}_k\right]\right\} \\ &+\Upsilon_{k|\mathscr{I}_k}^{*\mathsf{T}}\overline{\Upsilon}^\alpha\left(2\Omega_{gp}X_k + \left(\Omega_g\overline{\Upsilon}^\alpha + \Psi\right)\mathcal{U}_k^*(\mathscr{I}_k)\right)\Bigg\}, \end{aligned} \tag{5.12}$$

where $\Omega_p = \Phi^\mathsf{T}\Omega\Phi$, $\Omega_g = \Gamma^\mathsf{T}\Omega\Gamma$, and $\Omega_{gp} = \Gamma^\mathsf{T}\Omega\Phi$.

## 5.4 Monitoring of Packet Losses and Attack Detection

The optimal control law for both protocols is determined by the mean number of packet drops. In view of this, the operator monitors the average number of packet drops on the actuation channel to check that it agrees with the postulated statistic used to construct the control law. Specifically, they perform the following hypothesis test

$$H_0 : \text{There is no attack present,} \quad \mathbf{V}_k \sim \text{diag}\left(Be\left(\mu_1\right), Be\left(\mu_2\right), \ldots, Be\left(\mu_m\right)\right), \tag{5.13a}$$

$$H_1 : \text{There is an attack present,} \quad \mathbf{V}_k \nsim \text{diag}\left(Be\left(\mu_1\right), Be\left(\mu_2\right), \ldots, Be\left(\mu_m\right)\right). \tag{5.13b}$$

Given that the packet losses within each channel of the multidimensional communication channel form a Bernoulli IID sequence, the ML estimator of each of these channels is the same as seen in Section 3.4. Therefore, the ML estimator for the multidimensional communication channel is a parallelisation of the ML estimator of each individual channel. This follows from the fact that each channel is independent of all other channels. To that end, the system computes the average number of packet losses over each dimension up to time step $k$. Thus, producing the ML estimate

$$\hat{\mu}_{iML} = \frac{1}{k} \sum_{j=1}^{k} \left(\mathbf{V}_j\right)_{i,i}, \tag{5.14}$$

where $\left(\mathbf{V}_j\right)_{i,i}$ describes the $i$-th diagonal element of $\mathbf{V}_j$. The resulting estimate of the mean probability of packet losses at time step $k$ is given by

$$\widehat{\mathbf{M}}_{ML} = \text{diag}(\hat{\mu}_{1ML}, \hat{\mu}_{2ML}, \ldots, \hat{\mu_{m}}_{ML}). \tag{5.15}$$

The system uses the estimate to check whether the actuation channel is nominal. In this setting, nominal operation results in an estimated mean does not deviate significantly from the postulated mean used by the controller to implement the control law. For the scalar case, as seen in Section 3.4, this corresponds to the operator designing a safe operation region that is a 1D line centred around the mean with edge lengths equal to the $\delta$ as defined

in Section 3.4. If the ML estimator remains within this region, then the operator accepts $H_0$. However, for the multidimensional communication channel the operator determines a safe operation region that is a hypercube, centred around $\mathbf{M}$ with edge lengths determined by $\mathbf{L} \in S_+^m$. The structure of the lengths is such that $\mathbf{L} = \text{diag}(\delta_1, \delta_2, \ldots, \delta_m)$ to account for the different detection thresholds $\{\delta_i\}_{i=1}^m$ for each dimension of the actuation channel. The resulting safe operation region is given by

$$\mathscr{C}(\mathbf{M}, \mathbf{L}) = \left\{ \widehat{\mathbf{M}}_{ML} \in \mathbb{M}^m : -\mathbf{L} \preceq \widehat{\mathbf{M}}_{ML} - \mathbf{M} \preceq \mathbf{L} \right\}. \tag{5.16}$$

In this setting, an attack is declared at time step $k \in \mathbb{N}$ if $\widehat{\mathbf{M}}_{ML} \notin \mathscr{C}(\mathbf{M}, \mathbf{L})$. Otherwise, normal operation of the system continues and the operator continues monitoring the packet losses by updating its estimate $\widehat{\mathbf{M}}_k$ at time step $k$.

Note that the operator does not incorporate a monitoring performance metric in the cost function; instead, the packet loss monitoring procedure operates concurrent to the system operation but independently of the controller. In view of this, the attack construction is concerned with two performance metrics: the cost increase induced by the attack on the performance of the controller and satisfying that the calculated average of the packet losses induced by the attack conforms to the safe region defined by (5.16). When the attacker is considering an IID attack construction they slightly alter the safe operation region hypercube before incorporating it into their detection constraint. Namely, attack using an IID attack construction considers the following safe operation region as their detection constraint

$$\mathscr{C}^{\epsilon}(\mathbf{M}, \mathbf{L}) = \left\{ \widehat{\mathbf{M}}_{ML} \in \mathbb{M}^m : -\epsilon\mathbf{L} \preceq \widehat{\mathbf{M}}_{ML} - \mathbf{M} \preceq \epsilon\mathbf{L} \right\}, \tag{5.17}$$

where $\epsilon \in [0, 1]$ is a tuning parameter for the attack that trades-off the aggressiveness of the attack with the probability of detection of the attack. Specifically, the larger the value of $\epsilon$ the smaller the cost increase that will be caused by the IID attack however, there will also be a smaller probability of the attack being detected. Naturally, if an $\epsilon$ is chosen such that $\epsilon > 1$ then the detection hypercube greater than the safe operation

hypercube, similarly, if $\epsilon = 0$ then the detection hypercube becomes a single point centered at $\mathbf{M}$. A bound for the probability of detection is presented within Section 5.8, and in doing so informs the operator in the decision of setting the $\delta_i$ and informs the attack of the choice of $\epsilon$. This discussion of probability of detection is delayed such that we are able to discuss the probability of detection of the *optimal* stealthy attack. Naturally, the attacker may choose to use a diagonal matrix $\boldsymbol{\epsilon} \succ 0$ where they can decide upon the the trade-off between detection and cost increase within each channel, however, it is shown later that this is a trivial extension of the optimal attack construction. When considering the non-stationary processes for an attack the region (5.17) is generalised further to a time varying mean. This is discussed further in Section 5.7.

## 5.5 IID Attack Construction

Recall that the UDP-like protocol error trajectory given in (5.11b) depends on the mean of the control variable for the attacker, while the TCP-like protocol does not depend on the mean of the control variable (5.11a). For that reason, the derivation is presented separately for each protocol.

### 5.5.1 UDP-like Protocol

The optimal attack strategy for the UDP-like protocol is the solution to the optimisation problem

$$\max_{\overline{\Upsilon}^{\alpha}} \quad J_A\left(\mathscr{A}_k, \overline{\Upsilon}^{\alpha}\right), \tag{5.18a}$$

$$\text{s.t.} \quad \mathbf{M}^{\alpha} \in \mathscr{C}^{\epsilon}\left(\mathbf{M}, \mathbf{L}\right), \tag{5.18b}$$

where the constraint in the optimisation comes from the hypothesis test that the operator is performing (5.17). Note that the maximisation aims to increase the cost incurred by the controller as a result of the packet losses induced by the attack, while the constraint aims to keep the attack within the stealthy attack region. Additionally, the maximisation

in (5.18) and the minimisation of the control law in (5.9) differ in that $\mathbf{M}^{\alpha} \neq \mathbf{M}$. In the UDP-like setting the information set $\mathscr{A}_k$ does not have access to the previous realisations of packet losses for estimation, specifically, $\mathscr{I}_k = \mathscr{G}_k$ in (5.6). Using Lemma 1 from [20] and (5.12) yields the equivalent cost function given by

$$J_A^*\left(\mathscr{A}_k, \overline{\Upsilon}^{\alpha}\right) = X_k^{\mathsf{T}}\left(\mathbf{Q} + \Omega_p\right) X_k + \operatorname{tr}\left(\Omega_l \Sigma_{\mathcal{W}}\right) + \max_{\overline{\Upsilon}^{\alpha}} \Big\{ \mathcal{U}_k^{*\mathsf{T}}(\mathscr{G}_k) \overline{\Upsilon}^{\alpha} \Big( 2\Omega_{gp} X_k + \Big( \Omega_g \overline{\Upsilon}^{\alpha} + \Psi + (\mathbf{I} \odot \Omega_g) \left( \mathbf{I} - \overline{\Upsilon}^{\alpha} \right) \Big) \mathcal{U}_k^*(\mathscr{G}_k) \Big) \Big\}, \quad (5.19)$$

where the maximisation is subject to $\mathbf{M}^{\alpha} \in \mathscr{C}^{\epsilon}\left(\mathbf{M}, \mathbf{L}\right)$. For the sake of presentation clarity, it is assumed that all actuators for the system share a single communication channel, as in [59]. This simplifies the attack construction while displaying the same properties of the attack construction as in the general case i.e. where in the detection region (5.17) the maximums occur whilst simplifying the region itself. That being the case $\overline{\Upsilon}^{\alpha}$ is a diagonal matrix with equal entries, and therefore, $\overline{\Upsilon}^{\alpha} = \alpha \mathbf{I}$ where $\alpha \in [0, 1]$ is the control variable of the attacker and $\alpha \mathbf{I} \in \mathscr{C}^{\epsilon}\left(\mathbf{M}, \mathbf{L}\right)$. Similarly, the safe operation region $\mathscr{C}\left(\mathbf{M}, \mathbf{L}\right)$ is simplified, in this case to the interval

$$\mathscr{C}\left(\mu, \delta\right) = \left\{ \widehat{\mu} \in [0, 1] : -\delta \geq \widehat{\mu}_{ML} - \mu \geq \delta \right\}, \quad (5.20)$$

where $\delta \in [0, 1]$ denotes the detection threshold set by the operator. This simplification of the safe operation region then in turn results in a simplification of the detection constraint. This region becomes

$$\mathscr{C}^{\epsilon}\left(\mu, \delta\right) = \mathscr{C}'\left(\mu, \delta\right) = \left\{ \alpha \in [0, 1] : -\delta\epsilon \geq \alpha - \mu \geq \delta\epsilon \right\}. \quad (5.21)$$

Within this simplified setting, the attack strategy is characterised by the attack design parameter $\alpha$. In view of this, substituting $\alpha$ as the control variable in (5.19) simplifies the

optimisation problem to

$$J_A^*\left(\mathscr{A}_k, \overline{\Upsilon}^\alpha\right) = X_k^\mathsf{T}\left(\mathbf{Q}+\Omega_p\right)X_k + \operatorname{tr}\left(\Sigma_{\mathcal{W}}\Omega_l\right) + \max_{\alpha\in\mathscr{C}^\epsilon(\mu,\delta)}\left\{\mathcal{U}_k(\mathscr{G}_k)^\mathsf{T}\alpha\left(\alpha\Omega_g+(1-\alpha)\left(\mathbf{I}\odot\Omega_g\right)+\Psi-2\mathbf{G}(\mathscr{G}_k)\right)\mathcal{U}_k(\mathscr{G}_k)\right\}. \quad (5.22)$$

Note that the first two terms are constants that do not depend on $\alpha$. Therefore, it is sufficient to maximise the last term. Substituting $-\mathbf{G}^{-1}(\mathscr{G}_k)\,\Omega_{gp}X_k$ for $\mathcal{U}_k(\mathscr{G}_k)$ lets us write the term inside the maximisation as

$$f(\alpha) \triangleq X_k^\mathsf{T}\Omega_{gp}^\mathsf{T}\mathbf{G}^{-1}(\mathscr{G}_k)\,\alpha\left(\alpha\Omega_g+(1-\alpha)(\mathbf{I}\odot\Omega_g)+\Psi-2\mathbf{G}(\mathscr{G}_k)\right)\mathbf{G}^{-1}(\mathscr{G}_k)\,\Omega_{gp}X_k. \quad (5.23)$$

Note that (5.23) is quadratic in $\alpha$. Therefore, the function (5.23) is concave, convex, or linear in $\alpha$ depending on the system parameters. The attacker has no control over the convexity of the cost function used for the attack construction. However, the information set available to the attacker determines the convexity of the cost function, and therefore, the attacker is able to construct the optimal attack by solving (5.23) for any system parameters. In the following lemma we show that for the convex and linear systems the optimal attack construction is equivalent.

**Lemma 11.** *Let (5.23) be convex or linear in $\alpha$ over $\mathscr{C}^\epsilon(\mu,\delta)$. Then the maximum of this function is given by*

$$\max\{f(\alpha)\} = \max\left\{f(\min\{\mathscr{C}^\epsilon(\mu,\delta)\}), f(\max\{\mathscr{C}^\epsilon(\mu,\delta)\})\right\}. \quad (5.24)$$

*Proof.* Assume there is a maximum of (5.23) such that $\alpha \in \operatorname{Int}\{\mathscr{C}^\epsilon(\mu,\delta)\}$, we prove by contradiction that this is false, and therefore, the maximum is on the boundary of $\mathscr{C}^\epsilon(\mu,\delta)$. By the definition of convexity, for $\delta > 0$ it holds that

$$f(a) \geq \max\{f(a+\epsilon\delta), f(a-\epsilon\delta)\}, \quad (5.25)$$

$$f(a) \geq tf(a+\epsilon\delta) + \ (1-t)f(a-\epsilon\delta). \quad (5.26)$$

It follows that $f(a)$ is greater than any point of the line connecting $f(a+\epsilon\delta)$ and $f(a-\epsilon\delta))$ however, this breaks the convexity assumption of (5.23), and therefore, the maximum is on the boundary. This concludes the proof. □

When the function is concave there is a third maximising case. This is the case for which the global maximum of the function exists within the interval $\mathscr{C}^{\epsilon}(\mu,\delta)$. The following lemma captures this notion.

**Lemma 12.** *Let (5.23) be concave in $\alpha$ over $\mathscr{C}^{\epsilon}(\mu,\delta)$. Then the maximum of the function is given by*

$$\max\{f(\alpha)\} = \max\left\{f(\min\{\mathscr{C}^{\epsilon}(\mu,\delta)\}), f(\max\{\mathscr{C}^{\epsilon}(\mu,\delta)\}), f(\mathbb{1}_{\mathscr{C}^{\epsilon}(\mu,\delta)}\alpha_{\max})\right\}, \quad (5.27)$$

*where $\mathbb{1}_{\mathscr{B}}$ denotes the indicator function over the set $\mathscr{B}$.*

*Proof.* The proof has been moved to Appendix C.1.

Note that the $\alpha_{max}$ (defined in Appendix C.7) attack construction provides a globally optimal performance for the attacker from within the safe operation region. In fact, it also provides a lower probability of attack detection as it allows the attacker to operate away from the boundary condition of $\mathscr{C}^{\epsilon}(\mathbf{M},\mathbf{L})$.

The following lemma highlights that an attack that minimises the cost of the operator is not achieved by setting $\alpha = 1$. We show below that the optimal attack construction does not necessarily imply increasing the number of packet losses incurred by the operator. Indeed, there exists system parameters for which the optimal attack entails increasing the number of actuations. Whilst this might not be implementable in all attack scenarios, it is feasible to envision settings in which the attacker has full control of the actuation channel and can set the packet loss statistics at will. The following lemma captures this notion, namely, that the performance of the operator does not necessarily improve with the average number of received packets. This reiterates that the operator assumes a mean packet loss, and in doing so, creates an opportunity for the attacker to exploit the channel. Although this is not necessarily surprising, given that the operator has designed the optimal control

law about a given point it is a divergence from the traditional DoS attacks. Namely, DoS attacks that exclusively reduces the number of packets that successfully reach the end of the communication channel.

**Lemma 13.** *For any choice of system parameters it holds that*

$$\min_{\alpha\in[0,1)} f(a) \leq \min\left\{f(1), f(\mu)\right\}, \tag{5.28}$$

*where $f$ is defined in (5.23).*

*Proof.* Setting the first derivative of (5.23) equal to zero, and substituting in $\alpha = 1$ yields

$$f'(1) = \mathcal{U}_k(\mathcal{G}_k)^{*\mathsf{T}}\left(2\left(\mathbf{I}-\overline{\Upsilon}\right)\Omega_g - \Psi - \left(3\mathbf{I}-2\overline{\Upsilon}\right)(\mathbf{I}\odot\Omega_g)\right)\mathcal{U}_k^*(\mathcal{G}_k). \tag{5.29}$$

For this to be a minimising solution $\Psi = 2\left(\mathbf{I}-\overline{\Upsilon}\right)\Omega_g - \left(3\mathbf{I}-2\overline{\Upsilon}\right)(\mathbf{I}\odot\Omega_g)$. Due to $\Psi$ being a diagonal matrix and the structure of $\Omega_g$ it is only possible for this equality to hold in a system with $\mathbf{A}=\mathbf{0}$ and diagonal matrix $\mathbf{B}$. In this scenario $\Omega_g = (\mathbf{I}\odot\Omega_g)$ results in $\Psi = -(\mathbf{I}\odot\Omega_g)$. By assumption we have that $\Psi \succ 0$, but it is shown in Lemma 14 that $(\mathbf{I}\odot\Omega_g) \succ 0$ which is a contradiction. Therefore, $f'(\alpha=1)\neq 0$ and thus $\alpha = 1$ is not a minimising solution. Substituting $\alpha\mathbf{I} = \mu\mathbf{I} = \overline{\Upsilon}$ into the first derivative of (5.23) results in

$$\begin{aligned} f'(\alpha) =& \mathcal{U}_k(\mathcal{G}_k)^{*\mathsf{T}}\left(2\overline{\Upsilon}\Omega_g + \left(\mathbf{I}-2\overline{\Upsilon}\right)(\mathbf{I}\odot\Omega_g) + \Psi - 2\mathbf{G}(\mathcal{G}_k)\right)\mathcal{U}_k(\mathcal{G}_k)^* \\ =& -X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathcal{G}_k)\left(\Psi + (\mathbf{I}\odot\Omega_g)\right)\mathbf{G}^{-1}(\mathcal{G}_k)\,\Omega_{gp}X_k. \end{aligned} \tag{5.30}$$

This is not equal to 0 due to $\Psi, (\mathbf{I}\odot\Omega_g) \succ 0$. In view of this, (5.30) is strictly negative and not a minimising solution. This concludes the proof. □

**Theorem 9.** *Let $\mathcal{A}_k = \left\{\mathbf{A}, \mathbf{B}, \Sigma_W, \overline{\Upsilon}, \Omega, \Psi, \mathcal{G}_k\right\}$ be the information set available to construct the attack, then the optimal mean packet loss probability for an IID attack on a*

*control system that is communicating with a UDP-like protocol is given by*

$$\alpha^*_{\text{UDP}} = \max\left\{ f\left(\min\{\mathscr{C}^\epsilon(\mu,\delta)\}\right), f\left(\max\{\mathscr{C}^\epsilon(\mu,\delta)\}\right), f\left(\mathbb{1}_{\mathscr{C}^\epsilon(\mu,\delta)}\alpha_{\max}\right)\right\}, \quad (5.31)$$

*where*

$$f(a) \triangleq X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathscr{G}_k)\, a\left(a\Omega_g + (1-a)\left(\mathbf{I}\odot\Omega_g\right) + \Psi - 2\mathbf{G}(\mathscr{G}_k)\right)\mathbf{G}^{-1}(\mathscr{G}_k)\,\Omega_{gp}X_k \quad (5.32)$$

*Proof.* The result follows from the application of Lemma 11 for the convex and linear cases, Lemma 12 for the concave case, and by noticing that the set of solutions for the convex and linear cases is a subset of of the set of solutions of the concave case. This concludes the proof. □

### 5.5.2 TCP-like Protocol

The optimal attack strategy for the TCP-like protocol is the solution to the optimisation problem

$$\max_{\overline{\Upsilon}^\alpha} \quad J_A\left(\mathscr{A}_k, \overline{\Upsilon}^\alpha\right), \quad (5.33a)$$

$$\text{s.t.} \quad \mathbf{M}^\alpha \in \mathscr{C}^\epsilon(\mathbf{M},\mathbf{L}). \quad (5.33b)$$

Note that in this case, the information set $\mathscr{A}_k$ contains the realisations of the packet losses as given in $\mathscr{F}_k$. For that reason, the optimisation problem differs from that in (5.18) in that the cost function exhibits a different structure induced by the conditioning on the previous packet loss realisations. Substituting in the optimal control law for the TCP-like protocol (5.12) yields

$$J^*(\mathscr{A}_k) = X_k^{\mathsf{T}}\left(\mathbf{Q}+\Omega_p\right)X_k + \operatorname{tr}\left(\Omega_l\Sigma_{\mathcal{W}}\right) + \max_{\overline{\Upsilon}^\alpha}\left\{X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathscr{F}_k)\,\overline{\Upsilon}^\alpha\left(\Omega_g\overline{\Upsilon}^\alpha + \Psi - 2\mathbf{G}(\mathscr{F}_k)\right)\mathbf{G}^{-1}(\mathscr{F}_k)\,\Omega_{gp}X_k\right\}, \quad (5.34)$$

where the maximisation is subject to $\mathbf{M}^{\alpha} \in \mathscr{C}^{\epsilon}(\mathbf{M}, \mathbf{L})$. As with the UDP-like protocol attack construction it is assumed, without loss of generality, that all actuators share a single communication channel [59]. Therefore, $\overline{\Upsilon}^{\alpha} = \alpha \mathbf{I}$. Noting that the first two terms in (5.34) do not depend on $\overline{\Upsilon}^{\alpha}$ and that $\mathbf{G}(\mathscr{F}_k) = \left(\Omega_g \overline{\Upsilon} + \Psi\right)$, as shown in [20] and Chapter 4, then the term inside the maximisation is rewritten as

$$g(\alpha) \triangleq -X_k^{\mathsf{T}} \Omega_{gp}^{\mathsf{T}} \mathbf{G}^{-1}(\mathscr{F}_k)\, \alpha \left(\Omega_g \left(2\overline{\Upsilon} - \alpha \mathbf{I}\right) + \Psi\right) \mathbf{G}^{-1}(\mathscr{F}_k)\, \Omega_{gp} X_k. \tag{5.35}$$

Differentiating (5.35) results in

$$g'(\alpha) = -X_k^{\mathsf{T}} \Omega_{gp}^{\mathsf{T}} \mathbf{G}^{-1}(\mathscr{F}_k) \left(\Omega_g \left(2\overline{\Upsilon} - 2\alpha \mathbf{I}\right) + \Psi\right) \mathbf{G}^{-1}(\mathscr{F}_k)\, \Omega_{gp} X_k, \tag{5.36}$$

$$g''(\alpha) = 2X_k^{\mathsf{T}} \Omega_{gp}^{\mathsf{T}} \mathbf{G}^{-1}(\mathscr{F}_k)\, \Omega_g \mathbf{G}^{-1}(\mathscr{F}_k)\, \Omega_{gp} X_k. \tag{5.37}$$

**Lemma 14.** *Let the pair* $(\mathbf{A}, \mathbf{B})$ *be reachable and the state penalty matrix* $\Omega$ *be positive definite. Then since* $X_k \neq \mathbf{0}$ *almost surely, the function defined by (5.35) is convex in* $\alpha$ *over* $\mathscr{C}^{\epsilon}(\mu, \delta)$.

*Proof.* It follows from (5.37) that if $\Omega_g \succ 0$ and $X_k \neq \mathbf{0}$ then (5.37) is strictly greater than zero. Therefore, (5.35) is convex in $\alpha$ over $\mathscr{C}^{\epsilon}(\mu, \delta)$. It is shown in [30, p.225, 10.31(c)] that when $\operatorname{rank}(\Gamma) = \max\{Nn, Nm\}$ and $\Omega \succ 0$ then it follows that $\Omega_g \succ 0$. Since $(\mathbf{A}, \mathbf{B})$ is a reachable pair then $\operatorname{rank}\left[\mathbf{B}, \mathbf{AB}, \ldots, \mathbf{A}^{N-1}\mathbf{B}\right] = n$. Therefore, due to the triangular structure of $\Gamma$ we have that $\operatorname{rank}(\Gamma) = Nn$. Under these assumptions it follows that provided $m \leq n$ (5.37) is convex in $\alpha$ over $\mathscr{C}^{\epsilon}(\mu, \delta)$. This concludes the proof. □

**Theorem 10.** *It is shown in Lemma 14 that for a system operating a TCP-like protocol,*

$$g(\alpha) \triangleq -X_k^{\mathsf{T}} \Omega_{gp}^{\mathsf{T}} \mathbf{G}^{-1}(\mathscr{F}_k)\, \alpha \left(\Omega_g \left(2\overline{\Upsilon} - \alpha \mathbf{I}\right) + \Psi\right) \mathbf{G}^{-1}(\mathscr{F}_k)\, \Omega_{gp} X_k$$

*is convex. Therefore, the optimal choice of* $\alpha$ *is known to be on the boundary as shown in Lemma 13.*

$$\alpha^*_{\text{TCP}} = \max\left\{ g\left(\min\{\mathscr{C}^{\epsilon}(\mu,\delta)\}\right), g\left(\max\{\mathscr{C}^{\epsilon}(\mu,\delta)\}\right)\right\}.$$

Note that due to the convexity of (5.35), the solution of (5.36) results in the minimising value of $\alpha$, which interestingly is not $\alpha\mathbf{I} = \overline{\Upsilon}$, or $\alpha = 1$, but instead is given by

$$\alpha_{\min} = \frac{1}{2} h^{-1}_{\text{TCP}} \left( X_k^{\mathsf{T}} \Omega_{gp}^{\mathsf{T}} \mathbf{G}^{-1}(\mathscr{G}_k) \left( 2\Omega_g \overline{\Upsilon} + \Psi \right) \mathbf{G}^{-1}(\mathscr{G}_k)\, \Omega_{gp} X_k \right), \tag{5.38}$$

where $h_{\text{TCP}} = X_k^{\mathsf{T}} \Omega_{gp}^{\mathsf{T}} \mathbf{G}^{-1}(\mathscr{F}_k)\, \Omega_g \mathbf{G}^{-1}(\mathscr{F}_k)\, \Omega_{gp} X_k > 0$. When the TCP-like protocol without detection constraints is considered, additional insight can be obtained by analysing the attack construction

$$g(1) = X_k^{\mathsf{T}} \Omega_{gp}^{\mathsf{T}} \mathbf{G}^{-1}(\mathscr{F}_k) \left( \Omega_g \left( \mathbf{I} - 2\overline{\Upsilon} \right) - \Psi \right) \mathbf{G}^{-1}(\mathscr{F}_k)\, \Omega_{gp} X_k, \tag{5.39}$$

$$g(0) = 0. \tag{5.40}$$

From (5.39), if $\Omega_g \left( \mathbf{I} - 2\overline{\Upsilon} \right) \succ \Psi$ the maximising value of $\alpha$ is 1 or 0. The $\Omega_g \left( \mathbf{I} - 2\overline{\Upsilon} \right)$ term is the state penalty matrix $\Omega$ weighted by the reachability of the system and the packet loss probability, i.e. $\left( \mathbf{I} - \overline{\Upsilon} \right)$. The terms in (5.39) capture the average impact of actuation in the cost reduction with respect to the input penalty matrix $\Psi$. Therefore, the optimal attack is 1 when the average cost increase per actuation is greater than the average penalty induced by the actuation. As a result, for a system with a high probability of packet loss that penalises state error more than actuation, the optimal attack strategy is to allow perfect communication, i.e. all packets are received by the plant. Additionally, for $\overline{\Upsilon} \succ \frac{1}{2}\mathbf{I}$ , the optimal attack strategy is always 0. That being the case, for a system with a low probability of packet loss the detection criteria of the operator reduces to a one-sided test. Namely, the movement of the ML estimator in only one direction will cause a cost increase. Therefore, an attack will only cause a cost increase in one direction and that direction should be the only one monitored.

## 5.6 Cost Increase Analysis

In this section we evaluate the cost increase induced by the optimal IID attack by comparing the expected cost when an attack is present to the expected cost when no attack is present, i.e. $\mathbb{E}\left[J_A^*(\mathscr{A}_k)\right] - \mathbb{E}\left[J^*(\mathscr{J}_k)\right]$. In particular, we study the expected cost increase of the three attack strategies separately. Namely, each of the cases seen within Theorem 9. The analysis is carried out for the unconstrained case $\mathscr{C}^\epsilon(\mu, \delta) = [0, 1)$, i.e. the extreme cases of the average attack packet drop. Note that there is no loss of generality as the case with detection constraints can be analysed following the same approach with the appropriate scaling.

### 5.6.1 UDP-like Cost Analysis

**Attack performance when $\alpha^* \to 0$.** We first analyse the case when the attacker losses all the packets and induces the cost

$$\mathbb{E}\left[J_A^0(\mathscr{A}_k)\right] \triangleq \lim_{\alpha^* \to 0} \mathbb{E}\left[J_A(\mathscr{A}_k)\right]. \tag{5.41}$$

The expected cost when there is an attack is given by

$$\mathbb{E}\left[J_A^0(\mathscr{A}_k)\right] = \operatorname{tr}\left(\Sigma_X\left(\mathbf{Q} + \Omega_p\right) + \Sigma_{\mathcal{W}}\Omega_l\right) + \max\{f(\alpha)\}. \tag{5.42}$$

Since (5.23) is continuous in $\alpha$ we have that $\alpha^* \to 0$ implies $f(\alpha^*) \to 0$, and therefore, the cost increase is

$$\mathbb{E}\left[J_A^0(\mathscr{A}_k)\right] - \mathbb{E}\left[J^*(\mathcal{G}_k)\right] = X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathscr{G}_k)\,\overline{\Upsilon}\Omega_{gp}X_k > 0. \tag{5.43}$$

Note that the $\alpha^* \to 0$ attack strategy forces the system into open loop, and therefore, the expected cost increase coincides with the expected cost reduction introduced by the controller when there is no attack present in the communication channel.

**Attack performance when $\alpha^* = 1$.** In this case, the attacker allows successful reception of all packets, i.e. the actuation communication channel is perfect. Surprisingly, there exist systems for which the cost increase, given by

$$\mathbb{E}\left[J_A^1(\mathscr{A}_k)\right] \triangleq \mathbb{E}\left[J_A(\mathscr{A}_k)\right]\Big|_{\alpha^*=1}, \tag{5.44}$$

is positive despite the fact that the communication channel of the operator improves. Evaluation of (5.23) with perfect communication results in

$$\begin{aligned}\mathbb{E}\left[J^1(\mathscr{A}_k)\right] = &\operatorname{tr}\left(\Sigma_X\left(\mathbf{Q}+\Omega_p\right)+\Sigma_{\mathcal{W}}\Omega_l\right)\\ &+X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathscr{G}_k)\left(\mathbf{I}-2\overline{\Upsilon}\right)\left(\Omega_g-(\mathbf{I}\odot\Omega_g)\right)\mathbf{G}^{-1}(\mathscr{G}_k)\,\Omega_{gp}X_k\\ &-X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathscr{G}_k)\left((\mathbf{I}\odot\Omega_g)+\Psi\right)\mathbf{G}^{-1}(\mathscr{G}_k)\,\Omega_{gp}X_k.\end{aligned} \tag{5.45}$$

Unlike the $\alpha^* \to 0$ strategy, the $\alpha^* = 1$ construction does not guarantee an increase in cost for every system. In fact, the cost only increases when

$$\begin{aligned}&X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathscr{G}_k)\left(\mathbf{I}-2\overline{\Upsilon}\right)\left(\Omega_g-(\mathbf{I}\odot\Omega_g)\right)\mathbf{G}^{-1}(\mathscr{G}_k)\,\Omega_{gp}X_k\\ &\qquad\geq X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathscr{G}_k)\left((\mathbf{I}\odot\Omega_g)+\Psi\right)\mathbf{G}^{-1}(\mathscr{G}_k)\,\Omega_{gp}X_k>0,\\ &X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathscr{G}_k)\left(\Omega_g+\Psi\right)\mathbf{G}^{-1}(\mathscr{G}_k)\,\Omega_{gp}X_k\\ &\qquad\geq 2X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathscr{G}_k)\,\mathbf{G}\left(\mathscr{G}_k\right)\mathbf{G}^{-1}(\mathscr{G}_k)\,\Omega_{gp}X_k.\end{aligned} \tag{5.46}$$

Where in the second line the terms simplified to highlight the trade-off that decides this change in the attack outcome. Specifically if the quadratic terms are removed it shows that

$$\Omega_g+\Psi \succeq 2\mathbf{G}\left(\mathscr{G}_k\right) \succ 0 \tag{5.47}$$

$$2\left(\Omega_g+\Psi\right) \preceq \mathbf{G}^{-1}\left(\mathscr{G}_k\right) \tag{5.48}$$

Interestingly this relates the eigenvalues of the nominal system, the system with perfect communication, to the eigenvalues of the UDP-like controlled system. This relation shows

that for this particular attack to be viable to gain matrix of the UDP-like controlled system must be at least twice as large as the perfectly controlled system. Note that this is a condition for this particular attack to be viable and not a condition for the UDP-like control strategy to be optimal over the nominal control strategy. However, all variables that determine (5.46) are system parameters known by the attacker, and therefore, the attacker decides the optimal attack strategy accordingly. The expected cost increase is

$$\mathbb{E}\left[J_A^1(\mathscr{A}_k)\right] - \mathbb{E}\left[J^*(\mathscr{G}_k)\right] = X_k^\mathsf{T}\Omega_{gp}^\mathsf{T}\mathbf{G}^{-1}(\mathscr{G}_k)\left(\Omega_g + \Psi\right)\mathbf{G}^{-1}(\mathscr{G}_k)\,\Omega_{gp}X_k + \left(\overline{\Upsilon} - 2\mathbf{I}\right)X_k^\mathsf{T}\Omega_{gp}^\mathsf{T}\mathbf{G}^{-1}(\mathscr{G}_k)\,\Omega_{gp}X_k. \quad (5.49)$$

**Attacker performance when $\alpha^* = \mathbb{1}_{\mathscr{C}^\epsilon(\mu,\delta)}\alpha_{\max}$.** We tackle next the introduction of a general detection constraint. In this case, the expected cost for the attacker is

$$\mathbb{E}\left[J^{\alpha_{\max}}(\mathscr{A}_k)\right] \triangleq \mathbb{E}\left[J_A(\mathscr{A}_k)\right]\Big|_{\alpha^*=\alpha_{\max}} = \operatorname{tr}\left(\Sigma_X\left(\mathbf{Q}+\Omega_p\right) + \Sigma_{\mathcal{W}}\Omega_l\right) + f(\alpha_{\max}). \quad (5.50)$$

Algebraic manipulation of $f(\alpha_{\max})$ and substituting (C.7) yields

$$f(\alpha_{\max}) = \frac{h_{\text{UDP}}^{-1}}{4}\left(X_k^\mathsf{T}\Omega_{gp}^\mathsf{T}\mathbf{G}^{-1}(\mathscr{G}_k)\left(2\mathbf{G}(\mathscr{G}_k) - \Psi - (\mathbf{I}\odot\Omega_g)\right)\mathbf{G}^{-1}(\mathscr{G}_k)\,\Omega_{gp}X_k\right)^2, \quad (5.51)$$

where $h_{\text{TCP}} = X_k^\mathsf{T}\Omega_{gp}^\mathsf{T}\mathbf{G}^{-1}(\mathscr{F}_k)\,\Omega_g\mathbf{G}^{-1}(\mathscr{F}_k)\,\Omega_{gp}X_k$ and the inequality comes from the fact that $f$ is concave when $\alpha_{\max}$ is a feasible optimal attack strategy. The resulting cost increase is

$$\mathbb{E}\left[J^{\alpha_{\max}}(\mathscr{A}_k)\right] - J^*(\mathscr{G}_k) = X_k^\mathsf{T}\Omega_{gp}^\mathsf{T}\mathbf{G}^{-1}(\mathscr{G}_k)\,\overline{\Upsilon}\Omega_{gp}X_k + \frac{1}{4}h_{\text{UDP}}^{-1}\left(X_k^\mathsf{T}\Omega_{gp}^\mathsf{T}\mathbf{G}^{-1}(\mathscr{G}_k)\left(2\mathbf{G}(\mathscr{G}_k) - \Psi - (\mathbf{I}\odot\Omega_g)\right)\mathbf{G}^{-1}(\mathscr{G}_k)\,\Omega_{gp}X_k\right)^2 > 0. \quad (5.52)$$

Note that the inequality is strict, i.e. the attack guarantees a performance loss of the operator. As mentioned previously this attack strategy is only feasible when $\alpha_{\max} \in \mathscr{C}^\epsilon(\mu,\delta)$ and (5.23) is concave. Additionally, it can be seen that $\mathbb{E}\left[J^0(\mathscr{A}_k)\right] - \mathbb{E}\left[J^*(\mathscr{G}_k)\right]$ is a subset of the cost increase induced by the $\alpha^* = \mathbb{1}_{\mathscr{C}^\epsilon(\mu,\delta)}\alpha_{\max}$ strategy.

### 5.6.2 TCP-like Cost Analysis

The cost increase analysis for TCP-like protocols contains only two attack strategies. The analysis is again performed on the $\mathscr{C}^{\epsilon}(\mu, \delta) = [0, 1)$ interval.

**Attacker performance when $\alpha^* \to 0$.** For the attack construction that forces the system into open loop, the expected cost is given by

$$\mathbb{E}\left[J^0(\mathscr{A}_k)\right] = \operatorname{tr}\left(\Sigma_X\left(\mathbf{Q} + \Omega_p\right) + \Sigma_{\mathcal{W}}\Omega_l\right) + \lim_{\alpha^* \to 0} g(\alpha^*). \tag{5.53}$$

Since (5.40) is continuous in $\alpha$, we have that $\alpha^* \to 0$ implies $g(\alpha^*) \to 0$. Therefore, the expected cost increase is

$$\mathbb{E}\left[J^0(\mathscr{A}_k)\right] - \mathbb{E}\left[J^*\left(\mathscr{F}_k\right)\right] = X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathscr{F}_k)\,\overline{\Upsilon}\Omega_{gp}X_k > 0. \tag{5.54}$$

As with the UDP-like protocol, by implementing the $\alpha^* \to 0$ attack strategy the attacker forces the system into open loop and the cost increase is equal to the cost reduction expected by the operator. Note that the cost increase for the TCP-like protocol and the UDP-like protocol under the $\alpha^* \to 0$ strategy differ only in the $\mathbf{G}_{\mathscr{J}_k}$ term designed by the controller.

**Attacker performance when $\alpha^* = 1$.** In the TCP-like case, the attack that provides a perfect communication channel induces an expected cost given by

$$\mathbb{E}\left[J^1(\mathscr{A}_k)\right] = \operatorname{tr}\left(\Sigma_X\left(\mathbf{Q} + \Omega_p\right) + \Sigma_{\mathcal{W}}\Omega_l\right) + g(1). \tag{5.55}$$

Therefore, it follows form (5.39) that the expected cost increase induced by the $\alpha^* = 1$ strategy is

$$\begin{aligned}\mathbb{E}\left[J^1(\mathscr{A}_k)\right] - \mathbb{E}\left[J^*(\mathscr{F}_k)\right] = &\underbrace{X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathscr{F}_k)\left(\Omega_g\left(\mathbf{I} - 2\overline{\Upsilon}\right) - \Psi\right)\mathbf{G}^{-1}(\mathscr{F}_k)\,\Omega_{gp}X_k}_{>0} \\ &+ \underbrace{X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}(\mathscr{F}_k)\,\overline{\Upsilon}\Omega_{gp}X_k}_{\mathbb{E}[J^0(\mathscr{A}_k)] - \mathbb{E}[J^*(\mathscr{F}_k)]},\end{aligned} \tag{5.56}$$

where the first term is strictly positive following the assumption that the $\alpha^* = 1$ attack construction is optimal (5.39). Therefore, $\alpha* = 1$ is strictly greater than the $\alpha^* \to 0$ attack strategy only when $\Omega_g \left(\mathbf{I} - 2\overline{\Upsilon}\right) \succ \Psi$, which is the condition needed for the $\alpha^* = 1$ construction to be optimal.

## 5.7 Non-Stationary Random attacks

The plant given in (4.1) is Markovian, and therefore, it seems reasonable to assume that the attacker should be able to exploit the memory of the system in the construction of the attack. In that sense, the IID attack construction does not provide sufficient flexibility to incorporate the time dependency between consecutive packet losses. Motivated by this insight, we investigate the extension of random attacks to non-IID settings. Specifically, we consider the case in which the statistics of the attack are non-stationary. The resulting non-stationary attack construction extends the IID attack construction to an attack that corrupts a system with independent actuator channels. As in the IID case, the aim of the attacker is to increase the cost function while remaining in the safe operation region by adjusting the value of $\mathbf{M}^\alpha$. Specifically, the attack construction is no longer restricted to a constant $\mathbf{M}^\alpha$, i.e. $\mathbf{M}_k^\alpha \triangleq \mathbb{E}[\mathbf{V}_k^\alpha]$ for $k \in \mathbb{N}$. The derivation of the non-stationary attack construction is equivalent to the IID attack construction up to (5.19). Namely, the point at which the previous attack construction is reduced to a scalar. The reason for the necessity of a different derivation stems from the non-stationarity that induces $\overline{\Upsilon}^\alpha \neq \alpha\mathbf{I}$ since $\mathbf{M}_k^\alpha \neq \mathbf{M}_{k+1}^\alpha$ for all $k$. This attack is implemented on a multidimensional channel and not the scalar channel in the previous derivation, and therefore, considers a more general attack construction setting.

### 5.7.1 TCP-like Non-Stationary Attack

We first consider the non-stationary attack construction for the TCP-like protocol. Notice that for the non-stationary construction maximising (5.19) is equivalent to maximising

$$\begin{aligned} f\left(\overline{\Upsilon}^{\alpha}\right) &= \mathcal{U}_k^{*\mathsf{T}}(\mathscr{F}_k)\overline{\Upsilon}^{\alpha}\Big(\Omega_g\overline{\Upsilon}^{\alpha} + \Psi + (\mathbf{I}\odot\Omega_g)\left(\mathbf{I} - \overline{\Upsilon}^{\alpha}\right) - 2\mathbf{G}(\mathscr{G}_k)\Big)\mathcal{U}_k^{*}(\mathscr{F}_k) \\ &= \operatorname{tr}\Big(\overline{\Upsilon}^{\alpha}\Big((\Omega_g - (\mathbf{I}\odot\Omega_g))\overline{\Upsilon}^{\alpha} + (\mathbf{I}\odot\Omega_g) + \Psi - 2\mathbf{G}(\mathscr{F}_k)\Big)\mathcal{U}_k^{*}(\mathscr{F}_k)\mathcal{U}_k^{*\mathsf{T}}(\mathscr{F}_k)\Big)\,. \end{aligned}$$

Substituting $\mathbf{G}(\mathscr{F}_k)$ allows the optimal attack strategy for the TCP-like protocol to be posed as a quadratic optimisation problem (QP). The resulting construction is

$$\begin{aligned} \max_{\overline{\Upsilon}^{\alpha}} \quad & \operatorname{tr}\left(\left[\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha} - \overline{\Upsilon}^{\alpha}\left(2\overline{\Upsilon}\Omega_g + \Psi\right)\right]\mathcal{U}_k^{*}(\mathscr{F}_k)\mathcal{U}_k^{*\mathsf{T}}(\mathscr{F}_k)\right), \\ \text{s.t.} \quad & \mathbf{M}_k^{\alpha} \in \mathscr{C}^{\epsilon}(\mathbf{M},\mathbf{L}) \qquad \text{for } k \in \mathbb{N}. \end{aligned} \tag{5.57}$$

It should be stated that the above constraint on the attack is in fact equivalent to the constraint imposed on the IID attack construction. However, due to the fact that the IID construction has fewer degrees of freedom, namely it is fixed in time, the constraint simplifies to the region shown in (5.17). Note that the set of IID attack strategies is therefore a subset of the strategies considered in the non-stationary optimisation domain. Additionally, note that the optimisation in (5.57) is constrained by the hypercube $\mathscr{C}^{\epsilon}(\mathbf{M},\mathbf{L})$. Therefore, if IID is indeed the optimal attack structure then the proposed non-stationary attack construction coincides with the strategy presented in the previous section. If however, the cost induced by the non-stationary attack is greater than that induced by $\alpha\mathbf{I}$ then it follows that memory in the attack yields larger cost increases while satisfying the same detection constraints. It should be noted that the detection constraint for the IID scenario is much more restrictive that the non-stationary attack. Note that in the TCP-like scenario all three of the terms $\Omega_g$, $\Psi$, and $\mathcal{U}_k^{*}(\mathscr{F}_k)\mathcal{U}_k^{*\mathsf{T}}(\mathscr{F}_k)$ are positive or positive semidefinite. Both TCP-like and the following UDP-like QP formulations can be modified to include IID attacks on multidimensional channels provided that the additional constraint $\mathbf{M}_k^{\alpha} = \mathbf{M}_{k+1}^{\alpha}$ for all $k$ is included.

Note that (5.57) is a QP problem, and therefore, a solution exists and it can be computed numerically. However, we can find an analytic solution for our case. It is shown below that for the TCP-like protocol the attack is strictly convex in all attack variables. This implies that the analysis in the previous sections extend to not only a multidimensional communication channel but to a non-stationary attack within a multidimensional communication channel. Specifically, the optimal solution of the IID attack construction is shown to be a subset of the optimal non-stationary attack. The objective function of non-stationary TCP-like protocol attack, as seen in (5.57), is equivalent to

$$\begin{aligned} &\max_{\overline{\Upsilon}^{\alpha}} \left\{ \operatorname{tr}\left( \left[ \overline{\Upsilon}^{\alpha} \Omega_g \overline{\Upsilon}^{\alpha} - \overline{\Upsilon}^{\alpha} \left( 2\overline{\Upsilon} \Omega_g + \Psi \right) \right] \mathcal{U}_k^*(\mathscr{F}_k) \mathcal{U}_k^{*\mathsf{T}}(\mathscr{F}_k) \right) \right\}, \\ &\text{s.t.} \qquad \mathbf{M}_k^{\alpha} \in \mathscr{C}^{\epsilon}(\mathbf{M}, \mathbf{L}) \qquad \text{for } k \in \mathbb{N}. \end{aligned} \tag{5.58}$$

The following lemma characterises the almost sure convexity of the optimisation problem in (5.58).

**Lemma 15.** *The maximisation defined in (5.58) is convex in* $\overline{\Upsilon}^{\alpha}$.

*Proof.* The proof is moved to Appendix C.2.

**Corollary 6.** *There exists a global minimum of the function (5.58) that is defined as*

$$\overline{\Upsilon}^{\alpha}_{\min} = \frac{1}{2} \left( \mathbf{I} \odot \Omega_g^{-1} \left[ \left( 2\overline{\Upsilon} \Omega_g + \Psi \right) \mathcal{U}_k^*(\mathscr{F}_k) \mathcal{U}_k^{*\mathsf{T}}(\mathscr{F}_k) \right] \right) \left( \mathbf{I} \odot \left[ \mathcal{U}_k^*(\mathscr{F}_k) \mathcal{U}_k^{*\mathsf{T}}(\mathscr{F}_k) \right] \right)^{-1}. \tag{5.59}$$

*This is not equal to operator's postulate IID variable* $\overline{\Upsilon}$.

*Proof.* The proof is moved to Appendix C.3.

From Lemma 15 it follows that in order to maximise (5.58) the optimal stealthy non-stationary attack is characterised by a $\overline{\Upsilon}^{\alpha}$ on the boundary of $\mathscr{C}^{\epsilon}(\mathbf{M}, \mathbf{L})$. This leads to the following theorem.

**Theorem 11.** *The optimal stealthy attack for a control system communicating with a TCP-like protocol is defined as*

$$\max_{\overline{\Upsilon}^{\alpha}}\{\mathcal{J}\left(\overline{\Upsilon}^{\alpha}\right)\}=\max_{\overline{\Upsilon}^{\beta}}\left\{\mathcal{J}\left(\overline{\Upsilon}+\overline{\Upsilon}^{\beta}\right)\right\}. \tag{5.60}$$

*Proof.* From Lemma 15 it follows that the maximising stealthy attack solution of the cost will be on the boundary of the detection region $\mathscr{C}\left(\mathbf{M},\mathbf{L}\right)$. Specifically, the maximising $\overline{\Upsilon}^{\alpha}$ is

$$\overline{\Upsilon}^{\alpha}_{\max}=\max_{\overline{\Upsilon}^{\beta}}\left\{\mathcal{J}\left(\overline{\Upsilon}+\overline{\Upsilon}^{\beta}\right)\right\}, \tag{5.61}$$

where $\overline{\Upsilon}^{\beta}$ is defined as $\overline{\Upsilon}^{\beta}=\boldsymbol{\beta}\left(\mathbf{I}\otimes\epsilon\mathbf{L}\right)$ and $\boldsymbol{\beta}\in\mathbb{M}^{Nm}$ is defined as

$$\boldsymbol{\beta}=\begin{pmatrix}\beta_1 & 0 & \dots & 0\\ 0 & \beta_2 & \dots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \dots & \beta_{Nm}\end{pmatrix}, \tag{5.62}$$

where $\beta_i\in\{-1,1\}$ are the variables to be maximised over. This concludes the proof. □

This analytical solution has simplified the optimal attack problem from a QP problem to the problem of evaluating a function at $2Nm$ points and taking the maximum of them all. This has greatly reduced the complexity and computational efficiency of the optimal attack construction.

**Remark 5.** *As mentioned in Section 5.4 the attacker can substitute the scalar $\epsilon$ for a matrix $\boldsymbol{\epsilon}$. In doing so the optimisation becomes*

$$\overline{\Upsilon}^{\alpha}_{\max}=\max_{\boldsymbol{\beta}}\left\{\mathcal{J}\left(\overline{\Upsilon}+\overline{\Upsilon}^{\beta}\right)\right\}, \tag{5.63}$$

*where*

$$\overline{\Upsilon}^{\beta} = \boldsymbol{\beta}\left(\mathbf{I} \otimes \boldsymbol{\epsilon}\mathbf{L}\right) \tag{5.64}$$

*and* $\boldsymbol{\epsilon} \in [0,1]^m$ *is a diagonal penalty matrix for the stealth of the attack.*

The above remark gives the attack a much higher degree of freedom in designing the attack. However, in doing so creates additional decision problems. Namely, the attack now has another $m-1$ parameters that require tuning to give a desired trade-off between cost increase and probability of detection. For the following we assume $\boldsymbol{\epsilon} = \epsilon\mathbf{I}$ for ease of reading.

For a multidimensional channel in which the attacker wishes to perform an IID attack, the attacker simply adapts the $\overline{\Upsilon}^{\beta}$ such that

$$\overline{\Upsilon}^{\beta} = \mathbf{I} \otimes \mathbf{M}^{\alpha} \tag{5.65}$$

$$= \left(\mathbf{I} \otimes \left(\mathbf{M} + \boldsymbol{\beta}\epsilon\mathbf{L}\right)\right). \tag{5.66}$$

In this case $\boldsymbol{\beta}$ is an $m \times m$ matrix instead of an $Nm \times Nm$ matrix. Note that this implies

$$\mathbf{M}^{\alpha} = \mathbf{M} + \boldsymbol{\beta}\epsilon\mathbf{L}. \tag{5.67}$$

The computing complexity of (11) is reduced greatly by the simplification to a stationary attack. However, as mentioned above, by restricting the possible configurations of $\overline{\Upsilon}^{\alpha}$ the attacker does not guarantee the most damaging stealthy attack construction. Note that the scalar IID attack corresponds to two possible attack configurations of the multichannel non-stationary attack. Similarly, the stationary multichannel attack corresponds to $2m$ possible configuration of the possible $2Nm$ configurations of the multichannel non-stationary attack.

A graphical depiction of the optimisation region for a 2 dimensional communication channel for an IID attack is shown in Fig.5.1.

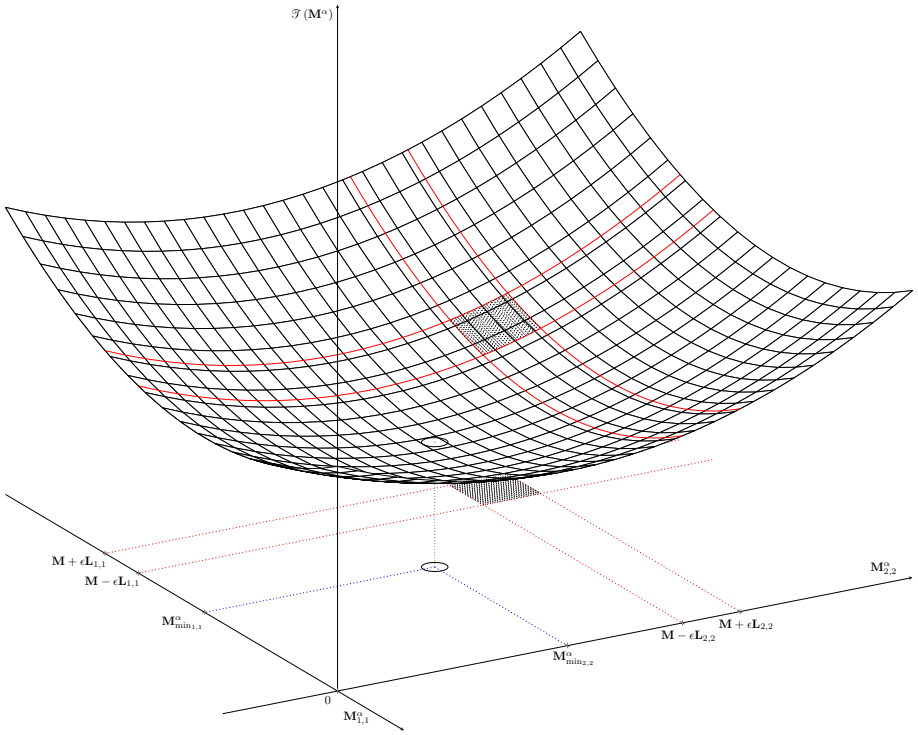


Fig. 5.1 Graphical interpretation of the Matrix channel attack optimisation.

### 5.7.2 UDP-like Non-Stationary Attack

Unlike the TCP-like attack optimisation, the convexity/concavity of the UDP-like attack optimisation problem is undetermined. As with the scalar case, the solution of the attack strategy for the UDP-like protocol is more complex. Performing the same analysis for the UDP-like system results in a similar QP formulation given by

$$\begin{aligned} \max_{\overline{\Upsilon}^\alpha} \quad & \operatorname{tr}\left(\left[\overline{\Upsilon}^\alpha \Omega_H \overline{\Upsilon}^\alpha - \overline{\Upsilon}^\alpha \left((\mathbf{I} \odot \Omega_g) + \Psi + 2\overline{\Upsilon}\Omega_H\right)\right] \mathcal{U}_k^*(\mathscr{G}_k)\mathcal{U}_k^{*\mathsf{T}}(\mathscr{G}_k)\right), \\ \text{s.t.} \quad & \mathbf{M}_k^\alpha \in \mathscr{C}^\epsilon(\mathbf{M}, \mathbf{L}) \qquad \text{for } k \in \mathbb{N}. \end{aligned} \tag{5.68}$$

As with the TCP-like non-stationary optimisation, note that the detection region is once again equivalent to (5.16) i.e. the shrinking hypercube the operator uses for detection. As mentioned above the convexity/concavity of the UDP-like attack optimisation problem is undetermined. This leads us to the following Lemma.

**Lemma 16.** *The objective function of the optimisation problem*

$$\begin{aligned} \max_{\overline{\Upsilon}^{\alpha}} \quad & \operatorname{tr}\left(\left[\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha} - \overline{\Upsilon}^{\alpha}\left((\mathbf{I}\odot\Omega_g) + \Psi + 2\overline{\Upsilon}\Omega_H\right)\right]\mathcal{U}_k^*(\mathcal{G}_k)\mathcal{U}_k^{*\mathsf{T}}(\mathcal{G}_k)\right), \\ s.t. \quad & \mathbf{M}_k^{\alpha} \in \mathscr{C}^{\epsilon}(\mathbf{M},\mathbf{L}) \qquad \text{for } k \in \mathbb{N}, \end{aligned} \tag{5.69}$$

*is neither convex nor concave in* $\overline{\Upsilon}^{\alpha}$ *and the second derivative is equal to* $\mathbb{0}$.

*Proof.* The proof is moved to Appendix C.4.

## 5.8 Probability of Detection

The above sections have shown that for the TCP-like protocol the optimal attack strategy is to operate on the boundary of the detection region. For the following section we consider the probability that the realisation of the random process corresponding to the packet losses exits the detection region. This is known as the probability of detection. Additionally, we restrict ourself to considering th IID attack. This does not mean this section only considers the scalar communication channel, only that $\mathbf{M}^{\alpha}$ is fixed and not time varying. Note that for this section we are considering a realisation of a sequence of random variables, *not* the realisation of a single random variable. Therefore, we are actually calculated the probability that a Binomially distributed sequence differs too far from the expected mean of a binomial distribution. Note that this is in fact a two sided statement. Initially, we consider the probability of false alarm rate. Specifically, for the system described in this chapter we are considering the probability of the following event

$$\theta = \widehat{\mathbf{M}}_{ML} \notin \mathscr{C}(\mathbf{M},\mathbf{L}). \tag{5.70}$$

Due to the definition of the hypercube $\mathscr{C}(\mathbf{M}, \mathbf{L})$ there are two possible events that allow the event (5.70) to occur. Namely, the events

$$\theta_1 = \widehat{\mathbf{M}}_{ML} - \mathbf{M} \succeq \mathbf{L} \tag{5.71}$$

$$\theta_2 = \widehat{\mathbf{M}}_{ML} - \mathbf{M} \preceq -\mathbf{L}. \tag{5.72}$$

The probabilities of these events occurring is defined as

$$\mathbb{P}[\theta_1] = \mathbb{P}\left[\sum_{i=1}^{k} \mathbf{V}_i > k(\mathbf{M} + \mathbf{L})\right], \tag{5.73a}$$

$$\mathbb{P}[\theta_2] = \mathbb{P}\left[\sum_{i=1}^{k} \mathbf{V}_i < k(\mathbf{M} - \mathbf{L})\right]. \tag{5.73b}$$

It should be noted that the above probabilities are both in matrix form. Namely, each channel within the actuation communication channel with have its own individual probability.

Now that we have defined the above events we can introduce the concept of probability of false alarm and the probability of detection. The probability of false alarm is the probability of either of these events occurring given that the system is under nominal conditions. This is defined as

$$\mathbb{P}_F = \mathbb{P}[\theta_1 | \mathbf{M} = \mathbf{M}] + \mathbb{P}[\theta_2 | \mathbf{M} = \mathbf{M}] \tag{5.74}$$

Similarly the probability of detection is defined as the probability of either of these events occurring given that the system is under attack. This is defined as

$$\mathbb{P}_D = \mathbb{P}[\theta_1 | \mathbf{M} = \mathbf{M}^\alpha] + \mathbb{P}[\theta_2 | \mathbf{M} = \mathbf{M}^\alpha] \tag{5.75}$$

Initially we consider the probability of false alarm. Within (5.73) the probabilities shown are that of the Binomial distribution, and therefore, have closed form expressions. Additionally, due to the fact that the probability of false alarm is two sided, it is expressed as the union of these probabilities. Due to the fact that these events are independent their

union is equivalent to the sum of the probabilities. Therefore

$$\mathbb{P}_F = \mathbb{P}\left[\sum_{i=1}^{k} \mathbf{V}_i > k\left(\mathbf{M}+\mathbf{L}\right)\middle|\, \mathbf{M}=\mathbf{M}\right] + \mathbb{P}\left[\sum_{i=1}^{k} \mathbf{V}_i < k\left(\mathbf{M}-\mathbf{L}\right)\middle|\, \mathbf{M}=\mathbf{M}\right] \tag{5.76}$$

$$= \sum_{i=1}^{\lceil k(\mathbf{M}-\mathbf{L})\rceil} \begin{pmatrix} k \\ i \end{pmatrix} \mathbf{M}^i \left(\mathbf{I}-\mathbf{M}\right)^{k-i} + \sum_{i=\lfloor k(\mathbf{M}+\mathbf{L})\rfloor}^{k} \begin{pmatrix} k \\ i \end{pmatrix} \mathbf{M}^i \left(\mathbf{I}-\mathbf{M}\right)^{k-i}. \tag{5.77}$$

The above expression is exact. It conveys the exact probability of false alarm for the operator under nominal conditions. Additionally, due to the fact that this is a Binomial distribution the probabilities are symmetric, so the above is able to be simplified to

$$\mathbb{P}_F = 2 \sum_{i=1}^{\lceil k(\mathbf{M}-\mathbf{L})\rceil} \begin{pmatrix} k \\ i \end{pmatrix} \mathbf{M}^i \left(\mathbf{I}-\mathbf{M}\right)^{k-i}. \tag{5.78}$$

The probability of detection is equivalent to the probability of the binomial sequence leaving an *unsymmetrical* region. This is represented as

$$\mathbb{P}_D = \mathbb{P}_D^1 + \mathbb{P}_D^2 \tag{5.79}$$

$$= \mathbb{P}\left[\sum_{i=1}^{k} \mathbf{V}_i^A > k\left(\mathbf{M}+\mathbf{L}\right)\right] + \mathbb{P}\left[\sum_{i=1}^{k} \mathbf{V}_i^A < k\left(\mathbf{M}-\mathbf{L}\right)\right] \tag{5.80}$$

$$= \sum_{i=1}^{\lceil k(\mathbf{M}-\mathbf{L})\rceil} \begin{pmatrix} k \\ i \end{pmatrix} \mathbf{M}^{\alpha^i} \left(\mathbf{I}-\mathbf{M}^{\alpha}\right)^{k-i} + \sum_{i=\lfloor k(\mathbf{M}+\mathbf{L})\rfloor}^{k} \begin{pmatrix} k \\ i \end{pmatrix} \mathbf{M}^{\alpha^i} \left(\mathbf{I}-\mathbf{M}^{\alpha}\right)^{k-i}, \tag{5.81}$$

where we have defined the probabilities $\mathbb{P}_D^1 = \mathbb{P}\left[\theta_1 | \, \mathbf{M}=\mathbf{M}^{\alpha}\right]$ and $\mathbb{P}_D^2 = \mathbb{P}\left[\theta_2 | \, \mathbf{M}=\mathbf{M}^{\alpha}\right]$. Note that these probabilities are not symmetric i.e. $\mathbb{P}_D^1 \neq \mathbb{P}_D^2$. In the case of probability of false alarm the mean of the sequence lay in the centre of the hypercube between $k\left(\mathbf{M}-\mathbf{L}\right)$ and $k\left(\mathbf{M}+\mathbf{L}\right)$. However, in the case of probability of detection the mean of the true sequence does not lie in the centre of this hypercube.

Within (5.81) we have presented the exact probabilities of detection. These expressions give little insight into how these probabilities behave. To that end, we bound the probabilities to gain further insight. Note that we are considering the sum of $k$ IID

Bernoulli random variables. Therefore, we define

$$Z_k = \sum_{i=1}^{k} \mathbf{V}_i^A. \tag{5.82}$$

where $Z_k$ is the sum of $k$ IID Bernoulli variables. This is known as a Binomially distributed random variable. We first compute the probability of detection that relates to realisations of sequences that lie above the $k\left(\mathbf{M}+\mathbf{L}\right)$ region. Namely, the sequences corresponding the first right hand side term within (5.79) i.e. the probability defined as $\mathbb{P}_D^1$.

The following our derivation follows along the lines of [14]. However, it should be noted that we perform a parallelised version of the derivation in [14]. Namely, we simultaneously derive the probability of detection for every communication channel within the multidimensional actuation channel. As shown in [14], the probability of a sum of IID variables exceeding a value is upper bounded by

$$\mathbb{P}\left[Z_k \geq \mathbf{T}\right] \leq \frac{\mathbb{E}\left[e^{\lambda Z_k}\right]}{e^{\lambda \mathbf{T}}}, \tag{5.83}$$

where $\lambda \in S_+^m$ is a diagonal matrix of positive real values and $\mathbf{T} \in S_{++}^m$ is a diagonal matrix that which in our case is equal to $\lfloor k\left(\mathbf{M}+\mathbf{L}\right)\rfloor$. The numerator of the fraction is the moment generating function of $Z_k$. Since (5.83) holds for any $\lambda \succ \mathbb{0}$ it follows that the operator may wish to minimise the upper bound. This is a natural step for the operator to take as the left hand side is independent of $\lambda$ and therefore, minimising the right hand side results in the tightest bound that the operator can achieve for this inequality. Which leads to the following theorem

With that in mind we define the logarithm of the numerator as the following function

$$\Psi_{Z_k}\left(\lambda\right) = \log\left(\mathbb{E}\left[e^{\lambda Z_k}\right]\right). \tag{5.84}$$

The minimum of that function is defined in [14] as the solution of

$$\Psi_{Z_k}^*\left(\mathbf{T}\right) = \sup_{\lambda \succ \mathbb{0}} \left(\lambda \mathbf{T} - \Psi_{Z_k}\left(\lambda\right)\right). \tag{5.85}$$

It is also shown in [14] that the above minimisation is able to be extended to negative values of $\lambda$. This result follows from the convexity of the exponential function and Jenson's inequality. Therefore, the above function can be extended to

$$\Psi^*_{Z_k}(\mathbf{T}) = \sup_{\lambda \in \mathbb{M}^m} \left(\lambda \mathbf{T} - \Psi_{Z_k}(\lambda)\right), \tag{5.86}$$

where we still impose the restriction of $\lambda$ being a diagonal matrix. The above derivation has resulted in a parallelisation of Chernoff's inequality [14]. Namely,

$$\mathbb{P}\left[Z_k \geq \mathbf{T}\right] \leq e^{-\Psi^*_{Z_k}(\mathbf{T})}. \tag{5.87}$$

The above is able to be simplified further. Note that we are considering the sum of IID variables, and therefore,

$$\begin{aligned} \Psi_{Z_k}(\lambda) &= \log\left(\mathbb{E}\left[e^{\lambda \sum_{i=1}^{k} V_i^A}\right]\right) && (5.88)\\ &= \log\left(\prod_{i=1}^{k} \mathbb{E}\left[e^{\lambda V_i^A}\right]\right) && (5.89)\\ &= k\Psi_{V_k^A}(\lambda). && (5.90) \end{aligned}$$

Given the above relation, it follows from (5.86) that

$$\Psi^*_{Z_k}(\mathbf{T}) \quad = k\Psi^*_{V_k^A}\left(\frac{\mathbf{T}}{k}\right). \tag{5.91}$$

Exploiting the fact that the variables are IID within the probability of detection yields

$$\mathbb{P}\left[Z_k \geq \mathbf{T}\right] \leq e^{-k\Psi^*_{V_k^A}\left(\frac{\mathbf{T}}{k}\right)}. \tag{5.92}$$

The upper bound presented can not be solved for the minimum of $\Psi_{V_k^A}$ in its current form. However, the case when $Z_k$ is centered means that $\Psi^*_{Z_k}$ is continuously differentiable. This then allows a closed form expression of the minimum to be calculated. Due to the fact that we can perform linear transformations of our sum of random variables, we are able

to perform a linear shifting of the variable $Z_k$ such that it is centred around $\mathbb{0}$. This is achieved by letting $T_k = Z_k - k\mathbf{M}^{\alpha}$ and substituting into (5.86).

$$\Psi^{*}_{Z_k}(\mathbf{T}) \quad = \lambda_{\mathbf{T}}\mathbf{T} - \Psi_{Z_k}(\lambda_{\mathbf{T}}), \tag{5.93}$$

where $\lambda_{\mathbf{T}}$ is such that

$$\frac{\partial \Psi_{Z_k}(\lambda_{\mathbf{T}})}{\partial \lambda} = \mathbf{T}. \tag{5.94}$$

From the properties of the function it follows that

$$\lambda_{\mathbf{T}} = \left(\frac{\partial \Psi_{Z_k}}{\partial \lambda}\right)^{-1}(\mathbf{T}), \tag{5.95}$$

where we have slightly abused notation in order to show the order of steps taken to obtain the equality. Namely, the function is differentiated, set equal to $\mathbf{T}$ and then rearranged to find $\lambda_{\mathbf{T}}$. Which leads to the following theorem .

**Theorem 12.** *The minimising value of $\lambda$ for the function*

$$\Psi_{T_k}(\lambda) = \log\left(\mathbb{E}\left[e^{\lambda Z_k}\right]\right). \tag{5.96}$$

*For a centered sequence of Bernoulli random variables is*

$$\lambda_{\mathbf{T}} = \log\left(\left(\frac{\mathbf{T}}{k} + \mathbf{M}^{\alpha}\right)(\mathbf{I} - \mathbf{M}^{\alpha})\left(\mathbf{I} - \frac{\mathbf{T}}{k} - \mathbf{M}^{\alpha}\right)^{-1}(\mathbf{M}^{\alpha})^{-1}\right). \tag{5.97}$$

*Proof.* The proof is moved to Appendix C.5.

From Theorem 12 we have a closed form expression of $\lambda_{\mathbf{T}}$. Therefore, we are able to express the minimum of $\Psi^{*}_{T_k}$. Which leads to the following theorem

**Theorem 13.** *The minimising value of* $\lambda_{\mathbf{T}}$ *results in the following probability of detection bound*

$$\mathbb{P}_D \leq e^{-k\mathcal{D}\left(\frac{\lfloor k(\mathbf{M}+\mathbf{L})\rfloor}{k}\|\mathbf{M}^{\alpha}\right)} + e^{-k\mathcal{D}\left(\frac{\lceil k(\mathbf{M}-\mathbf{L})\rceil}{k}\|\mathbf{M}^{\alpha}\right)}. \tag{5.98}$$

*Proof.* The proof is moved to Appendix C.6.

**Corollary 7.** *It follows from Theorem 13 that for an* $\epsilon \neq 1$ *i.e.* $\mathbf{M}^{\alpha} \neq \mathbf{M} \pm \mathbf{L}$ *the probability of detection tends to* 0 *as* $k \to \infty$ *Specifically,*

$$\mathbb{P}_D \xrightarrow[k\to\infty]{} 0 \tag{5.99}$$

*Proof.* The proof follows from the fact that for a fixed constant $c > 0$ it is known that

$$e^{-kc} \xrightarrow[k\to\infty]{} 0. \tag{5.100}$$

It result follows from the non-negativity of the KL divergence and that it is non-zero for any two distributions that are not identical. This concludes the proof. □

**Remark 6.** *It should be noted that due to the equality within the probability of detection if* $\epsilon = 1$ *then as* $k \to \infty$ *the probability of detection tends to* 1*.*

Through use of Theorem 13 the probability of false alarm is also bounded. The probability of false alarm is bounded as

$$\begin{aligned} \mathbb{P}_D &\leq e^{-k\mathcal{D}\left(\frac{\lfloor k(\mathbf{M}+\mathbf{L})\rfloor}{k}\|\mathbf{M}\right)} + e^{-k\mathcal{D}\left(\frac{\lceil k(\mathbf{M}-\mathbf{L})\rceil}{k}\|\mathbf{M}\right)} && (5.101)\\ &= 2e^{-k\mathcal{D}\left(\frac{\lfloor k(\mathbf{M}+\mathbf{L})\rfloor}{k}\|\mathbf{M}\right)}, && (5.102) \end{aligned}$$

where the second line follows from the symmetry hypercube when placed at the centre of the distribution around $\mathbf{M}$.

## 5.9 Chapter Conclusion

In the above we characterise the optimal IID attack construction for UDP-like and TCP-like systems with multidimensional packet loss actuation communication channels. The attack is constructed as a DoS attacks over the actuation communication channel. The attack is also derived under the assumption that the operator monitors the state of the communication channel. It is shown that the optimal hypothesis test is governed by the calculated average packet loss. We have also shown that the optimal attack strategy does not always increase the number of packet losses within a given channel. In fact, we characterise the effect of the system parameters over the solution structure and show that three different scenarios emerge for which the attack strategy is different. Interestingly, the attacker only needs knowledge of $\Omega_g$, $\Psi$ , and $\mathbf{M}$ to decide the optimal strategy, unless the system operates with a UDP-like protocol and the function (5.23) is concave, in which case all system parameters must be known. The attacker does not however, require knowledge of the current control system state, or the operators measurements. For all cases, the cost increase of the optimal IID construction has been characterised and analysed. We have also shown that the IID attack construction is not optimal by proposing an achievability scheme that constructs attacks with non-stationary statistics.

Within Chapter 8 it is shown numerically that the proposed non-stationary attack outperforms the IID attack in most settings although at the expense of a slight increase in computational complexity. This is surprising as information-theoretic arguments in similar settings suggest that IID attacks are indeed the most damaging from a communication point of view. The combination of Chapter 4 and Chapter 5 have given the optimal decision for the operator and the attacker, respectively for a multidimensional packet loss communication channel.

# Chapter 6

# Stochastic Linear Control Systems with Noisy Communication Channels

## 6.1 Introduction

In the following chapter we study a control system that communicates over two communication channels and derive the optimal cost in this setting. This is the same process as followed in Chapter 4. As before, there are two communication channels that correspond to the two communication links between the controller and the plant. Namely, the sensory communication channel, that goes from the plant sensors to the controller and the actuation communication channel, that goes from the controller to the plant actuators. However, unlike Chapter 4 the communication channels within this, and the following chapter, are Additive White Gaussian Noise (AWGN) communication channels. This is as opposed to the Bernoulli packet loss communication channels considered within Chapter 4 and 5. Both of these AWGN communication channels are imperfect and corrupt the message signals with IID additive Gaussian noise. The message signals within each communication channel are the system state information and the actuation signal, for the sensory, and the actuation communication channel, respectively. This is a more general model than the Bernoulli packet loss communication channels presented in Chapters 4 and 5.

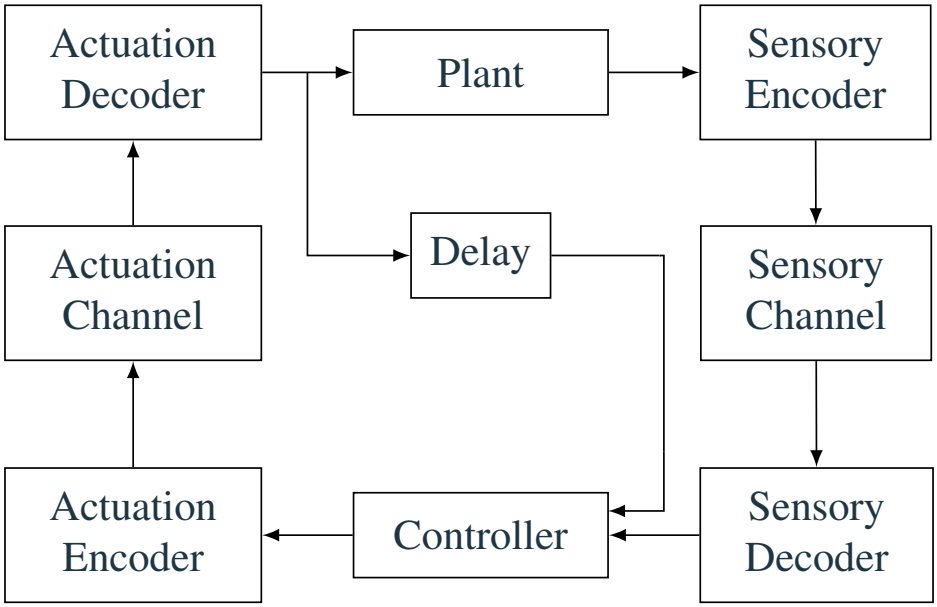


Fig. 6.1 Implementation of the perfect auxiliary channel within the system model.

Following this model construction we derive the optimal control cost for a control system that communicates over two separate multidimensional communication channels. Due to the construction of the communication channels, there is an increase in the errors within the system. Therefore, in doing this construction, we explicitly characterise the cost of communication within each channel.

In the same way that within Chapter 4 two different communication protocols are implemented in an effort to counter the effect of imperfect communication. The following chapter derives the optimal cost for three separate system models. Initially, the system is developed with access to an additional *perfect* auxiliary communication channel. This *perfect* auxiliary communication channel scenario corresponds to a control system that transmits the realisation of the actuation signal that enters the plant back to the controller. This system model is depicted in Fig. 6.1. We derive the optimal cost for controlling this system over the communication channels. Following this, the auxiliary communication channel is removed and the optimal control cost is once again re-derived. The model of a control system with no auxiliary channel is depicted in Fig. 6.2. After the control costs

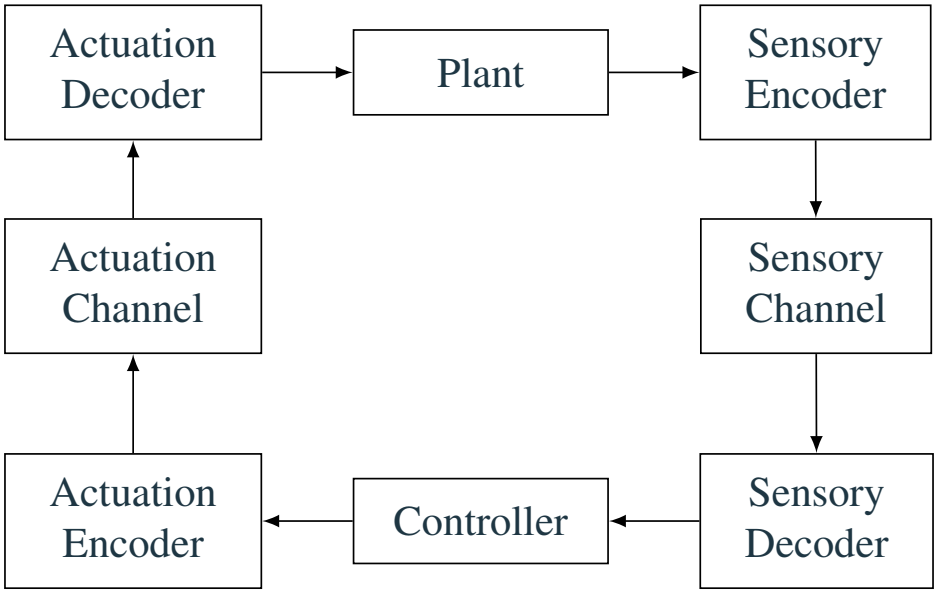


Fig. 6.2 Implementation of the the control system with no auxiliary channel.

are derived we show that the resulting cost of controlling a system optimally with no auxiliary channel is strictly larger than the first system model i.e. the system depicted in Fig. 6.1. For the third and final system model, the auxiliary channel is reintroduced, but this time the communication channel is *imperfect* and is in fact modelled as a third AWGN channel. This system model is depicted in Fig. 6.3. Following the derivation of each of the optimal control costs for each system model we analyse the difference in cost between all three system. By a perfect communication channel we refer to the communication channel that replicates the channel input at the output without altering the signal; in contrast, an imperfect communication channel produces a signal at the output via a random transformation of the input. Following this construction we characterisation the cost difference between all three control systems. Specifically, by not monitoring the realisation of the actuation variable the expected LQG cost of this system necessarily increases. This is starkly reminiscent of the differences caused by the acknowledgement signal seen in Chapters 4 and 5. Namely, the cost difference between the UDP-like and the TCP-like protocols.

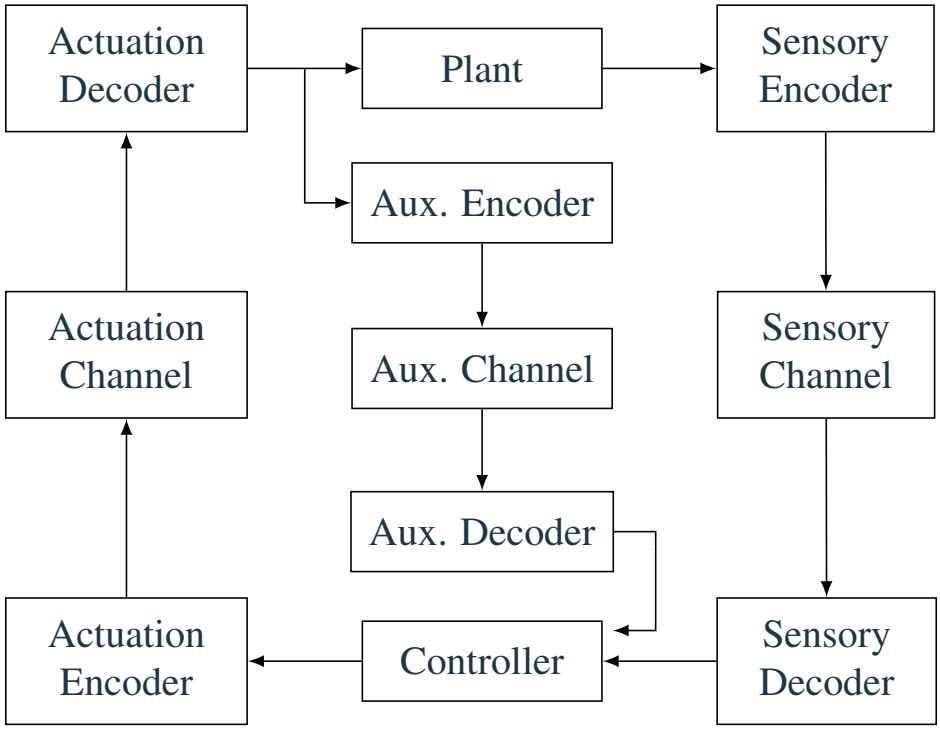


Fig. 6.3 Implementation of the imperfect auxiliary channel within the control system.

## 6.2 Perfect Communication Channel System Model

We begin by describing the standard state space system model studied in this chapter. Much like in the previous chapters, we consider a standard LTI state space system. Namely, a discrete time state space model, defined as

$$X_{k+1} = \mathbf{F}X_k + \mathbf{G}U_k + W_k, \tag{6.1a}$$

where $\mathbf{F} \in \mathbb{R}^{n\times n}$ is the dynamics matrix; $X_k \in \mathbb{R}^n$ describes the state of the plant at time step $k \in \mathbb{N}$; $X_0 \in \mathbb{R}^n$ is the initial state of the plant and is modelled as a vector of Gaussian random variables with mean $\mathbf{0} \in \mathbb{R}^n$ and covariance matrix $\Sigma_X \in S^n_{++}$; $\mathbf{G} \in \mathbb{R}^{n\times m}$ is the control matrix; $U_k \in \mathbb{R}^m$ is the vector of control inputs at time step $k$; and $W_k \in \mathbb{R}^n$ is the process noise used modelled as a vector of Gaussian random variables with mean $\mathbf{0} \in \mathbb{R}^n$ and covariance matrix $\Sigma_W \in S^n_{++}$. In addition to this we adopt the a standard sensory

model

$$Y_k = \mathbf{H}X_k + V'_k, \tag{6.1b}$$

where $Y_k \in \mathbb{R}^q$ is the received sensor signal at time step $k \in \mathbb{N}$; $\mathbf{H} \in \mathbb{R}^{q\times n}$ is the linearised sensor matrix; $V'_k \in \mathbb{R}^q$ is the nominal sensor noise used to capture the effect of sensor error caused by linearisation of the $\mathbf{H}$ matrix, this noise variable has mean $\mathbf{0} \in \mathbb{R}^m$ and covariance matrix $\Sigma_{V'} \in S^m_{++}$.

### 6.2.1 Optimal Control with Perfect Communication

The objective of optimal control is to minimise a cost function of the control systems' states and inputs by deciding on the sequence of control inputs. To give consideration to control laws that are implementable, we restrict the analysis to causal control laws. In our setting this boils down to the set of causal joint distributions. Note that by considering the set of random transformations we generalise the set of causal deterministic functions. Specifically, the set of causal joint distributions contains the set of causal deterministic functions. These causal deterministic functions are represented by probability distributions that concentrate all of their probability into a single mathematical point, and therefore, sampling of these single mass point distributions returns the same value. This means that if a causal deterministic control law is in fact the global optimal control law, then the resultant globally minimising family of casual joint distributions is also a causal deterministic function of the states. This causal set is defined as

$$^{\mathcal{O}}\mathcal{U} = \left\{ \mathcal{P}_{U_0,\dots,U_N|Y_0,\dots,Y_N} : \mathcal{P}_{U^N||Y^N} = \prod_{i=0}^{N} \mathbb{P}\left(U_i|U^{i-1}, Y^i\right) \right\}, \tag{6.2}$$

where the upper index on random variables indicates that the random variable contains all previous random variables, i.e. $U^i = \{U_0, \dots, U_i\}$ and $\mathcal{P}_{U_0,\dots,U_N|Y_0,\dots,Y_N}$ represents the family of joint distributions on $\{U_0, \dots, U_N\}$ given the random variables $\{Y_0, \dots, Y_N\}$. Naturally, the definition of (6.2) is interpreted as the set of all distributions over $\{U_0, \dots, U_N\}$ such

that for every $k$ the distribution of $U_k$ depends only on the previous random variables $U^{k-1}$ and $Y^k$.

When minimising a given cost function over this family of distributions the operator selects the optimal family of joint distributions. Therefore, when the control law is particularised with a realisation of $Y_k$, at a given time $k$, the operator is left with a particular distribution that depends only on the previous distributions. This distribution is then sampled to give the control signal for the current time instance.

Note that in our setting the plant model considered is a Gauss-Markov model. Therefore, only the most recent measurement of the state is required for obtaining optimality guarantees. This implies that the optimal distribution is of the form of a feedback controller. Additionally, due to the assumptions previously mentioned on the plant, such as Gauss-Markov modelling and IID noise statistics, the optimal control strategy results in the set of causal deterministic *functions*. The optimal set of functions is a well known result in control theory. The expected value of a LQG cost function is adopted as the cost function to be analysed. It is known that with perfect communication the optimal control cost is obtained by solving an Algebraic Riccati equation [21]. This result condensed into a theorem and is reported below for convenience.

**Theorem 14.** *Consider the state space system,*

$$X_{k+1} = \mathbf{F}X_k + \mathbf{G}U_k + W_k, \tag{6.3a}$$

$$Y_k = X_k. \tag{6.3b}$$

*The optimal control cost is*

$$\begin{aligned} J^* &= \min_{\mathcal{P}_{U_0,\dots,U_N|Y_0,\dots,Y_N} \in \mathcal{U}} \left\{ \limsup_{N\to\infty} \frac{1}{N} \mathbb{E}\left[ \sum_{k=0}^{N-1} X_k^{\mathsf{T}} \mathbf{Q}_X X_k + U_k^{\mathsf{T}} \mathbf{Q}_U U_k \right] \right\} \\ &= \mathbb{E}\left[ W^{\mathsf{T}} \mathbf{P} W \right] \\ &= \operatorname{tr}\left( \mathbf{P} \Sigma_W \right), \end{aligned} \tag{6.4}$$

*where* $\mathbf{Q}_X \in S_+^n$ *is the state penalty matrix;* $\mathbf{Q}_U \in S_{++}^m$ *is the input penalty matrix;* $N \in \mathbb{N}$ *is the time horizon;* $\mathcal{P}_{U_0,\dots,U_N|Y_0,\dots,Y_N}$ *is the joint distribution of all control inputs over the horizon,* $N$*; and the set* $\mathcal{U}$ *is as defined in (6.2). The optimal control law is*

$$U_k^* = -\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)^{-1}\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{F}X_k = -\mathbf{K}X_k, \tag{6.5}$$

*where* $\mathbf{K} \in \mathbb{M}^{m\times n}$ *is the controller gain and* $\mathbf{P} \in \mathbb{M}^n$ *is the steady state solution of the Riccatti equation defined by*

$$\mathbf{P} = \mathbf{F}^\mathsf{T}\left(\mathbf{P} - \mathbf{P}\mathbf{G}\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)^{-1}\mathbf{G}^\mathsf{T}\mathbf{P}\right)\mathbf{F} + \mathbf{Q}_X. \tag{6.6}$$

It should also be noted that in the perfect communication scenario the sensory matrix $\mathbf{H}$ is set to the identity. For more information on results like these see [7]. Additionally, the methodology is switched to the DP approach. The choice to switch to MPC for Chapters 4 and 5 is made to reveal additional insights into the nature of the controller and attack design. However, for our purposes, this and the following chapter obtain no additional insight through the MPC approach and remain in the DP format.

## 6.3 Imperfect Channel Construction

In the following we introduce the communication channels on the above system. A commonly used channel is the Additive White Gaussian Noise Channel (AWGN). We adopt the AWGN channel for the system model.

Two imperfect communication channels are constructed. One channel from the plant sensors to the controller, termed the sensory communication channel, and another from the controller to the plant actuators termed the actuation communication channel. To combat the randomness of the channels, we adopt a classical communications framework that introduces encoding and decoding blocks at the input and the output of the channel, respectively. In that manner, the communication errors introduced by the channel are arbitrarily reduced provided the communication rate is below the capacity of the

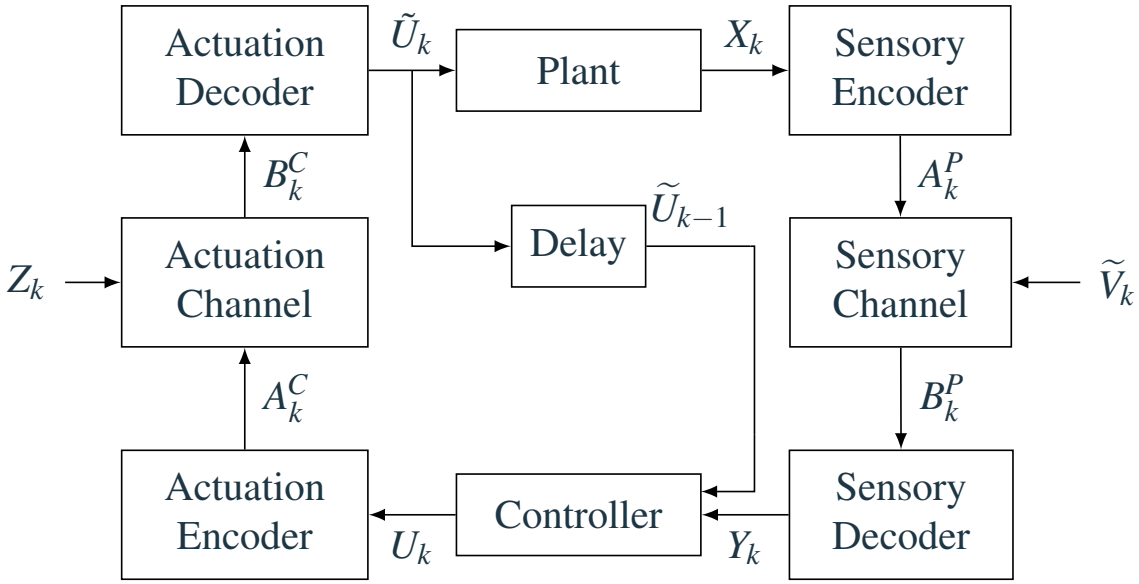


Fig. 6.4 Communication channel implementation within a control system, where the additional lines represent the transmission of the variable $\widetilde{U}_k$ over the perfect auxiliary communication channel.

channel [60]. The implementation of the channels within the control system setting is depicted in Fig. 6.4. It should be noted that in addition to the imperfect communication channels, the actuation and the sensory communication channels, we also initially include a perfect communication channel that transmits the realisation of the variable $\widetilde{U}_k$ back to the controller. This channel is initially assumed perfect in an attempt to characterise the impact of the actuation and sensory channel in isolation. Later on the assumption that this auxiliary channel is a perfect communication channel is dropped. Specifically, the perfect auxiliary communication channel is dropped and the result is generalised to include an imperfect auxiliary communication channel.

A communication system is described by three objects: the input alphabet, the channel, and the output alphabet. As mentioned above, the communication channels we adopt are AWGN channels. Additionally, the encoders and decoders used are probabilistic encoders and decoders. In doing so we generalise deterministic encoders which are modelled as Dirac measures. These Dirac measures allow us to establish equivalence to modelling the encoders and decoders as deterministic functions, this is much in the same way as

the deterministic control laws are chosen. That being the case, the encoders, channel, and the decoders are all modelled as stochastic kernels [71]. In order to define these two communication channels explicitly the following information sets are defined

$$\mathscr{P}_k^E \triangleq \left\{ X_k, A_{k-1}^P, B_{k-1}^P, \widetilde{U}_{k-1}, B_{k-1}^C \mathscr{P}_{k-1}^E \right\}, \tag{6.7a}$$

$$\mathscr{P}_k^D \triangleq \left\{ B_k^P, Y_{k-1}, U_{k-1}, \widetilde{U}_{k-1}, \mathscr{P}_{k-1}^D \right\}, \tag{6.7b}$$

$$\mathscr{C}_k^E \triangleq \left\{ Y_k, B_k^P, U_k, A_{k-1}^C, B_{k-1}^C, \widetilde{U}_{k-1}, \mathscr{C}_{k-1}^E \right\}, \tag{6.7c}$$

$$\mathscr{C}_k^D \triangleq \left\{ B_k^C, \widetilde{U}_{k-1}, \mathscr{C}_{k-1}^D \right\}, \tag{6.7d}$$

where $\mathscr{P}_k^E$ is the information set available to the sensory channel encoder at time $k$; $\mathscr{P}_k^D$ is the information set available to the sensory channel decoder at time $k$; $\mathscr{C}_k^E$ is the information set available to the actuation channel encoder at time $k$; $\mathscr{C}_k^D$ is the information set available to the actuation channel decoder at time $k$; $A_k^P \in \mathbb{R}^n$is the random variable corresponding to the sensory communication channel encoder outputs at time $k$; $B_k^P \in \mathbb{R}^n$is the random variable corresponding to the sensory communication channel decoder inputs at time $k$; $A_k^C \in \mathbb{R}^m$ is the random variable corresponding to the actuation communication channel encoder outputs at time $k$; $B_k^C \in \mathbb{R}^m$is the random variable corresponding to the actuation communication channel decoder inputs at time $k$; and $\widetilde{U}_k \in \mathbb{R}^m$ is the actuation communication channel decoder output which is the corrupted control signal, $U_k$. It should be noted that the both of the encoders have access to the previous communication channel output. This is required in order for communication to occur in a channel with bounded errors, as shown in [71]. Specifically, this assumption is required for communication to occur within a channel governing the communication of an unstable dynamics matrix. Therefore, for a stable dynamics matrix $\mathbf{F}$ it is possible for bounded error within the channel even when the variables $B_k^P$ and $B_k^C$ are dropped from the information sets $\mathscr{P}_k^E$ and $\mathscr{C}_k^E$, respectively. Additionally, as seen in (6.7), the decoder on each side of the control system has access to a subset of the information that the encoder on the same side has

access to. Namely,

$$\mathscr{P}_k^E \supset \mathscr{C}_k^D, \tag{6.8}$$

$$\mathscr{C}_k^E \supset \mathscr{P}_k^D. \tag{6.9}$$

This is a result of the causality within the system in conjunction with *perfect* information exchange between objects on each side of the communication channels. By this statement it is meant that the controller is co-located with the actuation channel encoder and the sensory channel decoder. Similarly, the plant is co-located with the sensory channel encoder and the actuation channel decoder. Given the emphasis we have placed on the causality of this system we define the information pattern of all the random variables. This is defined as

$$X_0, A_0^P, B_0^P, Y_0, U_0, A_0^C, B_0^C, \tilde{U}_0, X_1, \ldots, X_{N-1}, A_{N-1}, B_{N-1}, Y_{N-1}, U_{N-1}, A_{N-1}^C, B_{N-1}^C, \tilde{U}_{N-1} \tag{6.10}$$

This time ordering is equivalent with a clockwise movement around Fig. 6.4. With the above definitions in place it allows the following objects to be defined.

### 6.3.1 Encoders

The information available to the encoder on the sensory channel side is the current state measurement in addition to all previous states, sensory channel inputs, and sensory channel outputs. This collection of variables is known as the information set $\mathscr{P}_k^E$, as stated above. Therefore, due to the utilisation of probabilistic encoders the sensory channel encoder is the stochastic kernel

$$\mathcal{P}\left(A_k^P | X_k, B_{k-1}^P, \tilde{U}_{k-1}, A_{k-1}^P, \mathscr{P}_{k-1}^E\right). \tag{6.11a}$$

The deterministic sensory channel encoder is defined as the mapping

$$\psi^P\left(X_k\right) : X_k \to A_k^P \tag{6.11b}$$

The actuation channel encoder has access to the current system measurement and sensory channel output in addition to all previous measurements and sensory channel outputs. Therefore, the actuation channel encoder is the stochastic kernel

$$\mathcal{P}\left(A_k^C | Y_k, B_k^P, U_k, \tilde{U}_{k-1}, A_{k-1}^C, B_{k-1}^C, \mathscr{C}_{k-1}^E\right). \tag{6.12a}$$

The deterministic actuation channel encoder is defined as the random mapping

$$\psi^C\left(X_k\right) : U_k \to A_k^C \tag{6.12b}$$

These definitions encompasses all *causal* random and *causal* deterministic mappings.

### 6.3.2 Decoders

The decoder for the sensory communication channel has access to the current channel output as well as all previous system measurements. This is defined in (6.7) as the information set $\mathscr{P}_k^D$. The sensory channel decoder is the stochastic kernel,

$$\mathcal{P}\left(Y_k | B_k^P, Y_{k-1}, U_{k-1}, \tilde{U}_{k-1}, \mathscr{P}_{k-1}^D\right). \tag{6.13a}$$

The deterministic sensory channel decoder is therefore, defined as the random mapping

$$\varphi^P\left(B_k^P\right) : B_k^P \to Y_k. \tag{6.13b}$$

The decoder on the actuation communication channel has access to the current actuation channel output in addition to all previous actuation channel outputs and control inputs. This collection is known as the information set $\mathscr{P}_k^D$. Therefore, the actuation channel decoder is the stochastic kernel,

$$\mathcal{P}\left(\tilde{U}_k | B_k^C, \tilde{U}_{k-1}, \mathscr{C}_{k-1}^D\right). \tag{6.14a}$$

This deterministic decoder is therefore defined as the random mapping

$$\varphi^C\left(B_k^C\right) : B_k^C \to \widetilde{U}_k. \tag{6.14b}$$

With the definitions of the encoders and decoders made the only object left is the channel itself.

### 6.3.3 Channels

The channel is the mathematical model of how randomness is introduced to the input signal at the output of the channel. A discrete channel is defined to be a system consisting of an input alphabet $\mathscr{A}$, an output alphabet $\mathscr{B}$, and a probability transition matrix $\mathcal{P}_{Y|X}$ that express the probability of observing a given output symbol $y \in \mathscr{B}$ for a given input symbol $x \in \mathscr{A}$. The channels defined to be the random mapping from the input alphabet, $\mathscr{A}$, to the output alphabet, $\mathscr{B}$. The channel is said to be memoryless if the probability distribution of the output depends only on the input at that time instance and is conditionally independent of previous channel inputs and outputs. Therefore a memoryless channel, $\mathcal{P}_{Y|X}^N$, is defined as a channel that gives a sequence of outputs, $Y = (y_1, y_2, \ldots, y_N) \in \mathscr{B}^n$, from the corresponding set of inputs, $X = (x_1, x_2, \ldots, x_N) \in \mathscr{A}^n$. The transition probabilities are defined as

$$\mathcal{P}_{Y|X}^N = \prod_{i=1}^{N} \mathbb{P}\left(y_i|x_i\right), \tag{6.15}$$

where the upper index implies $N$ channel uses. A stationary memoryless channel refers to a channel where each channel use is independent from all previous and all future channel uses. All channels from this point are assumed to be stationary memoryless channels. In fact, as mentioned we adopt the use of AWGN channels, which are both stationary and memoryless. There are two communication channels within the system model, and therefore, two channels to be defined. Specifically, the sensory channel which is defined as $\mathcal{P}_{B^P|A^P}^N$ and the actuation channel which is defined as $\mathcal{P}_{B^C|A^C}^N$.

### 6.3.4 Communication Channel

With the above definitions we now describe the entirety of the communication channel. Specifically, it can be summarised as a nesting of the above functions. The sensory communication channel is expressed as the deterministic mapping

$$\mathcal{P}^r_{Y_k|X_k} = \psi^P \left( \varphi^P \left( \mathbf{H} X_k + V'_k \right) + \widetilde{V}_k \right), \tag{6.16a}$$

where $\widetilde{V}_k$ is the additive Gaussian noise introduced from the sensory channel with mean $\mathbf{0} \in \mathbb{R}^q$ and covariance matrix $\Sigma_{\widetilde{V}} \in S^q_{++}$. The actuation communication channel is similarly represented as

$$\mathcal{P}^r_{\widetilde{U}_k|U_k} = \psi^C \left( \varphi^C \left( U_k \right) + Z_k \right) \tag{6.16b}$$

where $Z_k$ is the additive Gaussian noise introduced from the actuation channel with mean $\mathbf{0} \in \mathbb{R}^m$ and covariance matrix $\Sigma_Z \in S^m_{++}$.

## 6.4 Imperfect Communication Channel System Model

We now introduce noise into the measurements of the state and into the actuation signal. To that end, the updated control system model is defined as

$$X_{k+1} = \mathbf{F} X_k + \mathbf{G} \widetilde{U}_k + W_k, \tag{6.17a}$$

$$\widetilde{U}_k = U_k + Z_k, \tag{6.17b}$$

$$Y_k = \mathbf{H} X_k + V_k, \tag{6.17c}$$

$$V_k = \widetilde{V}_k + V'_k, \tag{6.17d}$$

where $V_k \in \mathbb{R}^n$ is the transformed sensory noise, modelling the combined effect of the sensor linearisation error and the sensory channel noise, modelled as a vector of Gaussian random variables with mean $\mathbf{0} \in \mathbb{R}^m$ and covariance matrix $\Sigma_V \in S^m_{++}$. The noise introduced into

these variables is a result of the communication channels they are transmitted across. Due to the statistics of the actuation channel, it follows that $\mathbb{E}\left[\widetilde{U}_k\right] = U_k$. This system model is able to be re-arranged such that

$$X_{k+1} = \mathbf{F}X_k + \mathbf{G}U_k + \widetilde{W}_k, \tag{6.18a}$$

$$\widetilde{W}_k = \mathbf{G}Z_k + W_k, \tag{6.18b}$$

where $\widetilde{W}_k$ is a zero mean random variable with covariance $\Sigma_{\widetilde{W}} \in S^n_{++}$.

### 6.4.1 Optimal Control with Imperfect Communication

where it follows that in designing the optimal family of causal joint distributions $\mathcal{P}_{U_0,\dots,U_N|Y_0,\dots,Y_N} \in \mathcal{U}$ the operator also designs the optimal family of causal joint distributions $\mathcal{P}_{\widetilde{U}_0,\dots,\widetilde{U}_N}$.

In order to fully asses the control system with imperfect communication channels the system must be recast slightly in order to invoke Theorem 14. This follows a similar process as shown in [71]. Namely, the optimal cost function is represented as a sum of the optimal control cost and the cost of communication over each of the communication channels. First, the system must be able to be represented as a *fully observed* state space model in $\widehat{X}_k$; where $\widehat{X}_k \in \mathbb{R}^n$ is the operators estimate of the state variable at time $k$. Once this is achieved the Riccati optimal control result can be implemented by substituting the variable $\widehat{X}_k$ for $X_k$. To that end, the predicted state estimation error and the predicted error for the control signal is defined as

$$E^X_k\left(\mathscr{P}^D_k\right) = X_k - \widehat{X}_k\left(\mathscr{P}^D_k\right), \tag{6.19a}$$

$$E^U_k = \widetilde{U}_k - U_k, \tag{6.19b}$$

where $\widehat{X}_k\left(\mathscr{P}^D_k\right) = \mathbb{E}\left[X_k|\mathscr{P}^D_k\right]$. Note that the error on the actuation channel is not a function of the information set. This is a choice made to emphasise the fact that there is no estimation done on the plant side of the control system. Namely, whatever the realisation of the signal $\widetilde{U}_k$ that is received at the plant enters the system unaltered. This

is due to the fact control systems only perform estimation within the controller and not at the plant. Given that $X_k = \widehat{X}_k\left(\mathscr{P}_k^D\right) + E_k^X\left(\mathscr{P}_k^D\right)$ and $\widetilde{U}_k = U_k + E_k^U$, the system prediction at time $k$ for the time step $k+1$ is

$$\begin{aligned}
\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) &= \mathbb{E}\left[X_{k+1}\middle|\mathscr{P}_k^D\right] \\
&= \mathbb{E}\left[\mathbf{F}X_k + \mathbf{G}\widetilde{U}_k + W_k\middle|\mathscr{P}_k^D\right] \\
&= \mathbb{E}\left[\mathbf{F}\left(\widehat{X}_k\left(\mathscr{P}_k^D\right) + E_k^X\left(\mathscr{P}_k^D\right)\right) + \mathbf{G}\left(U_k + E_K^U\right) + W_k\middle|\mathscr{P}_k^D\right] \\
&= \mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{W}_k\left(\mathscr{P}_k^D\right),
\end{aligned} \tag{6.20}$$

where $\overline{W}_k\left(\mathscr{P}_k^D\right) \in \mathbb{R}^n$ is defined as

$$\overline{W}_k\left(\mathscr{P}_k^D\right) = \mathbb{E}\left[\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right) + \mathbf{G}E_k^U + W_k\middle|\mathscr{P}_k^D\right]. \tag{6.21}$$

This fully observed state space system can be improved upon if the system is updated with the new information that the sensors provide. The observation model is defined as

$$Y_k = \mathbf{H}X_k + V_k. \tag{6.22}$$

Therefore the updated state estimate $\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right)$, is defined as

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) = \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) + \mathbf{L}_k\left(Y_k - \mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)\right), \tag{6.23}$$

where $\mathbf{L}_k \in \mathbb{M}^{n\times q}$ is the optimal Kalman filter gain at time $k$. This representation of the updated state estimate is able to be recast into a fully observed state space system. This leads to the following theorem.

**Theorem 15.** *For an observable pair,* $(\mathbf{F}, \mathbf{G})$ *the updated state estimate*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) = \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) + \mathbf{L}_k\left(Y_k - \mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)\right), \tag{6.24}$$

*is equivalent to the fully observed state space system,*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{6.25a}$$

$$\widehat{Y}_{k}=\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{6.25b}$$

*where* $\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right)$ *is defined as*

$$\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right)=\mathbf{G}E_{k}^{U}+\mathbf{L}_{k}\left(\mathbf{H}\left(\mathbf{F}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right)+W_{k}\right)+V_{k+1}\right), \tag{6.26}$$

*and* $\mathbf{L}_k$ *is the optimal Kalman filter gain at time step* $k$*.*

*Proof.* The proof is moved to Appendix. D.1.

The above theorem groups all of the randomness of the control systems into a single variable. Namely, the process noise of a new state variable. In doing so the new system is fully observed. To invoke Theorem 14, all of the random variables within (6.25) must be uncorrelated with one another. Which leads to the following Lemma

**Lemma 17.** *All of the variables within* $\overline{\overline{W}}_k$ *are uncorrelated.*

*Proof.* The proof is moved to Appendix D.2.

When considering the optimal cost (6.4) the expectation is slightly modified to account for the noisy channels. This expectation must be taken with respect to the joint measure

$$\begin{aligned}\mathbb{P}\left(X^{N},A^{P^{N-1}},B^{P^{N-1}},Y^{N-1},U^{N-1},\widetilde{U}^{N-1}\right)=&\\ \prod_{k=0}^{N-1}\Big\{\mathbb{P}\left(X_{k+1}|X_{k},\widetilde{U}_{k}\right)&\mathbb{P}\left(A_{k}^{P}|X_{k},B_{k-1}^{P},\widetilde{U}_{k-1},A_{k-1}^{P},\mathscr{P}_{k-1}\right)\mathbb{P}\left(B_{k}^{P}|A_{k}^{p}\right)\\ \times\mathbb{P}\left(Y_{k}|B_{k}^{P},Y_{k-1},U_{k-1},\widetilde{U}_{k-1},\mathscr{P}_{k-1}^{D}\right)&\mathbb{P}\left(U_{k}|U_{k-1},Y_{k}\right)\mathbb{P}\left(B_{k}^{C}|A_{k}^{C}\right)\\ \times\mathbb{P}\left(A_{k}^{C}|Y_{k},B_{k}^{P},U_{k},\widetilde{U}_{k-1},A_{k-1}^{C},\mathscr{C}_{k-1}\right)&\mathbb{P}\left(\widetilde{U}_{k}|B_{k}^{C},\widetilde{U}_{k-1},\mathscr{C}_{k-1}^{D}\right)\Big\}\mathbb{P}(X_{0}).\end{aligned} \tag{6.27}$$

Although initially complicated (6.27) is able to be broken down into the individual contributions from the overall control system. Each term within the product begins with the random transformation in the plant and moves clockwise around the system depicted

in Figure 6.4. For example, $\mathbb{P}\Big(X_{k+1}|X_k,\widetilde{U}_k\Big)$ describes the transformation from once state to the next given the input into the state; then $\mathbb{P}\Big(A_k^P|X_k,B_{k\text{-}1}^P,\widetilde{U}_{k\text{-}1},A_{k\text{-}1}^P,\mathscr{P}_{k\text{-}1}\Big)$ describes the random process of drawing the variable $A_k^P$ given the information at that point; following on to $\mathbb{P}\Big(B_k^P|A_k^p\Big)$ which then describes the transformation within the sensory channel, an so on through the system. This separability between all of the random transformations is possible only due to the independency assumptions on the random variables from one another. The above clearly shows exactly how the expectation over these random variables is executed, i.e. sequentially.

Due to the introduction of the communication channels there are additional stochastic kernels that are introduced into the expectation. Specifically, the kernels (6.11), (6.13), and the stochastic kernels of the communication channels. Therefore, the cost of the partially observed system is

$$J^*=\min_{\mathcal{P}_{U_0,\dots,U_N|Y_0,\dots,Y_N}\in\mathcal{U}}\left\{\limsup_{N\to\infty}\frac{1}{N}\left(\mathbb{E}\left[\sum_{k=0}^{N}X_k^{\mathsf{T}}\mathbf{Q}_XX_k+\widetilde{U}_k^{\mathsf{T}}\mathbf{Q}_U\widetilde{U}_k\right]\right)\right\} \tag{6.28}$$

$$\begin{aligned}=\min_{\mathcal{P}_{U_0,\dots,U_N|Y_0,\dots,Y_N}\in\mathcal{U}}\Bigg\{\limsup_{N\to\infty}\frac{1}{N}\Bigg(&\sum_{k=0}^{N}\mathbb{E}\left[\widehat{X}_k^{\mathsf{T}}\Big(\mathscr{P}_k^D\Big)\mathbf{Q}_X\widehat{X}_k\Big(\mathscr{P}_k^D\Big)+U_k^{\mathsf{T}}\mathbf{Q}_UU_k\right]\\&+\mathbb{E}\left[E_k^X\Big(\mathscr{P}_k^D\Big)\mathbf{Q}_XE_k^X\Big(\mathscr{P}_k^D\Big)\right]+\mathbb{E}\left[E_k^{U^{\mathsf{T}}}\mathbf{Q}_UE_k^U\right]\Bigg)\Bigg\}\end{aligned} \tag{6.29}$$

$$\begin{aligned}=\min_{\mathcal{P}_{U_0,\dots,U_N|Y_0,\dots,Y_N}\in\mathcal{U}}\Bigg\{\limsup_{N\to\infty}\frac{1}{N}\Bigg(&\sum_{k=0}^{N}\mathbb{E}\left[\widehat{X}_k^{\mathsf{T}}\Big(\mathscr{P}_k^D\Big)\mathbf{Q}_X\widehat{X}_k\Big(\mathscr{P}_k^D\Big)+U_k^{\mathsf{T}}\mathbf{Q}_UU_k\right]\Bigg)\Bigg\}\\&+\limsup_{N\to\infty}\frac{1}{N}\left(\sum_{k=0}^{N}\mathbb{E}\left[E_k^X\Big(\mathscr{P}_k^D\Big)\mathbf{Q}_XE_k^X\Big(\mathscr{P}_k^D\Big)\right]+\mathbb{E}\left[E_k^{U^{\mathsf{T}}}\mathbf{Q}_UE_k^U\right]\right).\end{aligned} \tag{6.30}$$

where the substitution of (6.19) is made and due to the uncorrelated nature of the errors $\mathbb{E}\left[E_k^X\mathbf{Q}E_k^U\right]=0$. Additionally, it should be noted that due to the no dual effect property [71] the errors are unaffected by the optimal control choice and are removed from the minimisation. The first term of (6.30) is of the correct form to invoke Theorem 14, with a change of variables. Therefore, the optimal linear control law for the new state variable is

$$U_k^*=-\mathbf{K}\widehat{X}_k\Big(\mathscr{P}_k^D\Big), \tag{6.31}$$

with associated optimal cost,

$$\operatorname{tr}\left(P\Sigma_{\overline{\overline{W}}}\right), \tag{6.32}$$

where $\mathbf{K}$ is defined as the optimal gain matrix according to (6.5). It is assumed that the error covariances converge. Specifically the covariances

$$\begin{aligned}
\Sigma_{E_k^U} &= \mathbb{E}\left[E_{k+1}^U {E_{k+1}^U}^{\mathsf{T}} \middle| \mathscr{P}_{k+1}^D\right] \\
&= \Sigma_Z = \Sigma_{E^U}, \\
\Sigma_{E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right)} &= \mathbb{E}\left[E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right)E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right)^{\mathsf{T}} \middle| \mathscr{P}_{k+1}^D\right] \\
&= \widetilde{\mathbf{L}}_k\left(\mathbf{F}\Sigma_{E_k^X\left(\mathscr{P}_k^D\right)}\mathbf{F}^{\mathsf{T}} + \Sigma_W\right)\widetilde{\mathbf{L}}_k^{\mathsf{T}} + \mathbf{L}_k\Sigma_V\mathbf{L}_k^{\mathsf{T}},
\end{aligned} \tag{6.33}$$

are assumed to have converged to their solutions, where $\widetilde{\mathbf{L}}_k = (\mathbf{I} - \mathbf{L}_k\mathbf{H})$. This assumption is reasonable given that the Kalman filter gain $\mathbf{L}_k$ is designed such that the error covariances converge, the same assumption is made in [71]. Additionally the Kalman filter gain $\mathbf{L}_k$ is also assumed to have converged to its steady state value $\mathbf{L}$. These steady state covariance matrices are defined such that

$$\begin{aligned}
\Sigma_{E^U} &= \Sigma_{E^U} = \Sigma_Z, \\
\Sigma_{E^X} &= \widetilde{\mathbf{L}}\left(\mathbf{F}\Sigma_{E^X}\mathbf{F}^{\mathsf{T}} + \Sigma_W\right)\widetilde{\mathbf{L}}^{\mathsf{T}} + \mathbf{L}\Sigma_V\mathbf{L}^{\mathsf{T}}.
\end{aligned} \tag{6.34}$$

Note that the error covariance matrix of each channel does not depend on the error covariance of the other channel, showing a separation quality between the two channels.

With these results in mind the optimal system cost is written as

$$
\begin{aligned}
J^* &= \operatorname{tr}\left(\mathbf{P}\Sigma_{\overline{\overline{W}}}\right) + \operatorname{tr}\left(\mathbf{Q}_X\Sigma_{E^X}\right) + \operatorname{tr}\left(\mathbf{Q}_U\Sigma_{E^U}\right) && (6.35)\\
&= \operatorname{tr}\left(\mathbf{P}\mathbb{E}\left[\overline{\overline{W}}_k\,\overline{\overline{W}}_k^{\mathsf{T}}\right]\right) + \operatorname{tr}\left(\mathbf{Q}_X\Sigma_{E^X}\right) + \operatorname{tr}\left(\mathbf{Q}_U\Sigma_{E^U}\right) && (6.36)\\
&= \operatorname{tr}\left(\mathbf{P}\mathbb{E}\left[\left(\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right) + \widetilde{W}_k - E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right)\right)\left(\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right) + \widetilde{W}_k - E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right)\right)^{\mathsf{T}}\right]\right)\\
&\qquad + \operatorname{tr}\left(\mathbf{Q}_X\Sigma_{E^X}\right) + \operatorname{tr}\left(\mathbf{Q}_U\Sigma_{E^U}\right) && (6.37)\\
&= \operatorname{tr}\left(\mathbf{P}\left(\mathbf{F}\Sigma_{E^X}\mathbf{F}^{\mathsf{T}} + \mathbf{G}\Sigma_{E^U}\mathbf{G}^{\mathsf{T}} + \Sigma_W - \Sigma_{E^X}\right)\right) + \operatorname{tr}\left(\mathbf{Q}_X\Sigma_{E^X}\right) + \operatorname{tr}\left(\mathbf{Q}_U\Sigma_{E^U}\right) && (6.38)\\
&= \operatorname{tr}\left(\mathbf{P}\Sigma_W\right) + \operatorname{tr}\left(\left(\mathbf{F}^{\mathsf{T}}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^X}\right) + \operatorname{tr}\left(\left(\mathbf{G}^{\mathsf{T}}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{E^U}\right), && (6.39)
\end{aligned}
$$

where in line (6.37) the relation (D.22) is substituted for $\overline{\overline{W}}_k$. It is seen in (6.39) that the cost function for a system operating over a noisy communication channel is split into three additive terms. Specifically, the cost is represented as the cost of controlling the system optimally with perfect communication, with two additional terms relating to the cost incurred by communicating in each communication channel. This result is an extension from the formulation in [71] to a system with both channels experiencing noisy additive terms. These results extend [50] to a system with additive noise on the sensory channel in addition to generalising the communication channel model to include a decoder and an encoder within the communication channel structure.

## 6.5 Imperfect Communication Channel Model without an Auxiliary Channel

In the following we assume that the sensory channel decoder does not have access to the realisation of the plant input. This is due to the removal of the perfect auxiliary communication channel within the system architecture. This is shown visually in Fig. 6.5. This small change in system operation leads to a drastic change in error statistics. Removal of this auxiliary communication channel causes the state estimation error to depend not only on the sensory communication channel statistics but also the actuation communication

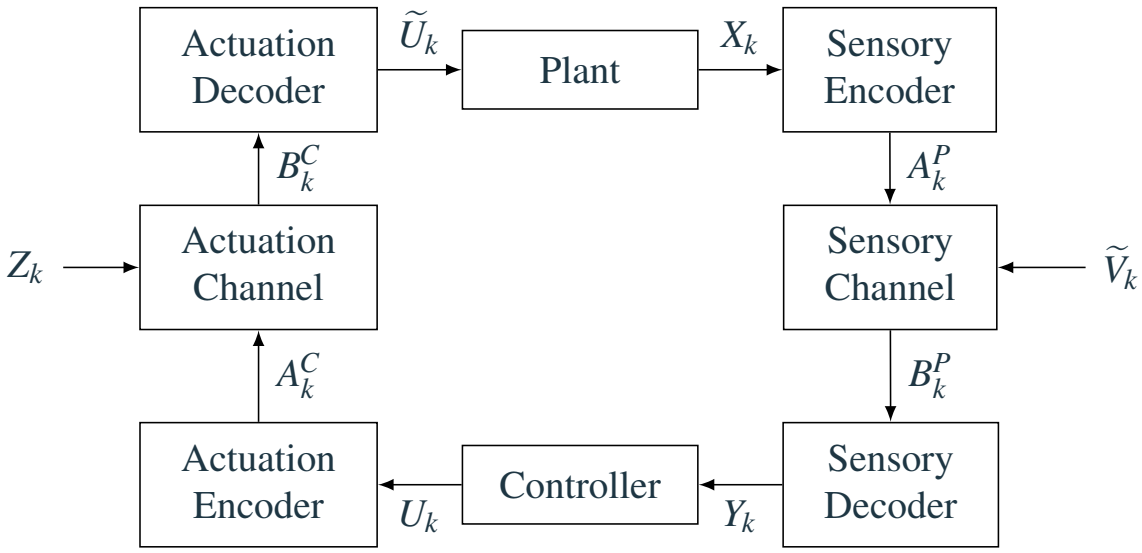


Fig. 6.5 Communication channel implementation within a control system, where there is no transmission of the variable $\widetilde{U}_k$ over an auxiliary communication channel.

channel statistics. This is due to the fact that the operator is unable to remove the effect of the unknown noise within the state estimate. This error is however lessened through use of the Kalman filter. But this effect still propagates through to the final LQG cost, causing an increase from the cost that includes the perfect auxiliary communication channel.

The information sets within (6.7) are re-defined to account for the restricted information available. Noting the difference in access to the $\widetilde{U}_k$ variable from the previous yields the following information sets

$$\mathscr{P}_k^E = \left\{ X_k, A_{k-1}^P, B_{k-1}^P, \widetilde{U}_{k-1}, \mathscr{P}_{k-1}^E \right\}, \tag{6.40a}$$

$$\mathscr{P}_k^D = \left\{ B_k^P, Y_k, U_{k-1}, \mathscr{P}_{k-1}^D \right\}, \tag{6.40b}$$

$$\mathscr{C}_k^E = \left\{ Y_k, B_k^P, U_k, \mathscr{C}_{k-1}^E \right\}, \tag{6.40c}$$

$$\mathscr{C}_k^D = \left\{ B_k^C, \widetilde{U}_{k-1}, \mathscr{C}_{k-1}^D \right\}. \tag{6.40d}$$

Note the absence of the $\widetilde{U}_k$ variable combined with the presence of the uncorrupted input $U_k$ in the controller side information sets. Inclusion of this term ensures that the

separation of optimal control and estimation remains, i.e. there is no dual effect from the control law choice.

The system modelling and channel construction follows the same structure as in Section 6.4.1.

### 6.5.1 Optimal Control without Auxiliary Channel

In order to assess the impact of the auxiliary communication channel, an expected LQG cost function is adopted. For this system model the cost definition is

$$J = \limsup_{N\to\infty} \frac{1}{N}\mathbb{E}\left[\sum_{k=0}^{N-1} X_k^{\mathsf{T}}\mathbf{Q}_X X_k + \widetilde{U}_k^{\mathsf{T}}\mathbf{Q}_U\widetilde{U}_k\right]. \tag{6.41}$$

Note that, as before, in the cost function the variable $\widetilde{U}_k$ is used and not the uncorrupted input signal $U_k$. This is due to the fact that the noisy actuation signal is the signal that enters the plant and not the uncorrupted signal $U_k$. The optimal cost function for this system is defined as

$$J^* = \min_{\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N}\in\mathcal{U}} \left\{\limsup_{N\to\infty} \frac{1}{N}\mathbb{E}\left[\sum_{k=0}^{N-1} X_k^{\mathsf{T}}\mathbf{Q}_X X_k + \widetilde{U}_k^{\mathsf{T}}\mathbf{Q}_U\widetilde{U}_k\right]\right\}, \tag{6.42}$$

where as before the operator designs the optimal joint distributions $\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N} \in \mathcal{U}$ such that they are contained within the causal set of joint distributions (6.2). The above is identical to that which used in section (6.4.1), however, it should be noted that the distribution of the operators measurements $Y_k$ for (6.42) are different due to the lack of information about the random variable $\widetilde{U}_k$. This results in a strictly larger cost for non-zero covariance matrices $\Sigma_{\widetilde{V}}$ and $\Sigma_Z$.

Following the same procedure as in Section 6.4.1 and a similar procedure as in [71], the cost function is represented as a sum of the optimal control cost and the cost of communication over each of the communication channels. The system must be able to be represented as a fully observed state space model in $\widehat{X}_k$. Once this is achieved the Riccati optimal control result is implemented with substitution of the variable $\widehat{X}_k$ for $X_k$. To that

end, the predicted state estimation error and the predicted error for the control signal is defined as

$$E_k^X\left(\mathscr{P}_k^D\right) = X_k - \widehat{X}_k\left(\mathscr{P}_k^D\right), \tag{6.43a}$$

$$E_k^U = \widetilde{U}_k - U_k. \tag{6.43b}$$

Given that $X_k = \widehat{X}_k\left(\mathscr{P}_k^D\right) + E_k^X\left(\mathscr{P}_k^D\right)$ and $\widetilde{U}_k = U_k + E_k^U$, the fully observed system is written as

$$\begin{aligned}
\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) &= \mathbb{E}\left[X_{k+1}\middle|\mathscr{P}_k^D\right] \\
&= \mathbb{E}\left[\mathbf{F}X_k + \mathbf{G}\widetilde{U}_k + W_k\middle|\mathscr{P}_k^D\right] \\
&= \mathbb{E}\left[\mathbf{F}\left(\widehat{X}_k\left(\mathscr{P}_k^D\right) + E_k^X\left(\mathscr{P}_k^D\right)\right) + \mathbf{G}\left(U_k + E_K^U\right) + W_k\middle|\mathscr{P}_k^D\right] \\
&= \mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{W}_k\left(\mathscr{P}_k^D\right),
\end{aligned} \tag{6.44}$$

where $\overline{W}_k\left(\mathscr{P}_k^D\right) \in \mathbb{R}^n$ is defined as

$$\overline{W}_k\left(\mathscr{P}_k^D\right) = \mathbb{E}\left[\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right) + \mathbf{G}E_k^U + W_k\middle|\mathscr{P}_k^D\right]. \tag{6.45}$$

As before the observation model continues to be

$$Y_k = \mathbf{H}X_k + V_k. \tag{6.46}$$

As before this representation is improved on if the system is updated with the new information that the sensors provide. Specifically, the updated state estimate $\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right)$ defined as

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) = \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) + \mathbf{L}_k\left(Y_k - \mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)\right). \tag{6.47}$$

We are able to cast the problem as a state space system with perfect observation. This leads to the following theorem.

**Theorem 16.** *The updated state estimate,*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_k\left(Y_k-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)\right), \tag{6.48}$$

*is equivalent to the state space system*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_k+\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{6.49a}$$

$$\widehat{Y}_k=\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{6.49b}$$

*where* $\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right)$ *is defined as*

$$\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right)=\mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}E_{k}^{U}+W_k\right)+\mathbf{L}_kV_{k+1}, \tag{6.50}$$

*and* $\mathbf{L}_k$ *is the optimal Kalman filter gain at time step* $k$*.*

*Proof.* The proof is moved to Appendix D.3.

The above theorem, groups all of the randomness into a single variable. Namely, the process noise of the new state variable. In doing so the new state variable is fully observed. To invoke Theorem 14, all of the random variables within (6.49) must be uncorrelated. To that end, the actuation error is

$$E_{k}^{U}=\widetilde{U}_k-U_k=Z_k. \tag{6.51}$$

Therefore, the actuation error $E_{k}^{U}$ is independent of the control law $U_k$. By definition the actuation noise $Z_k$ is independent of all other random variables. Therefore, the actuation error $E_{k}^{U}$ is also independent of the predicted state estimation error $E_{k+1}^{X}\left(\mathscr{P}_{k}^{D}\right)$ and the plant noise $W_k$ for all $k$. Similar to the actuation error, $W_k$ and $V_k$ are by definition

independent of all other random variables. The predicted estimation error is

$$
\begin{aligned}
E_{k+1}^{X}\left(\mathscr{P}_k^D\right) &= X_{k+1} - \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) && (6.52)\\
&= \left(\mathbf{F}X_k + \mathbf{G}U_k + \widetilde{W}_k\right) - \left(\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{W}_k\left(\mathscr{P}_k^D\right)\right) && (6.53)\\
&= \mathbf{F}\left(E_k^X\left(\mathscr{P}_k^D\right) - \mathbb{E}\left[\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right)\middle|\mathscr{P}_k^D\right]\right)\\
&\qquad + \mathbf{G}\left(E_k^U - \mathbb{E}\left[E_k^U\middle|\mathscr{P}_k^D\right]\right) + \left(W_k - \mathbb{E}\left[W_k\middle|\mathscr{P}_k^D\right]\right) && (6.54)\\
&= \mathbf{F}E_k^X\left(\mathscr{P}_k^D\right) + \mathbf{G}E_k^U + W_k. && (6.55)
\end{aligned}
$$

The state error prediction is independent from the actuation error as shown above. Additionally, as shown in [71], the prediction estimate is independent from the plant noise, $W_k$. Naturally, when the controller has access to additional information, the performance of the estimate is improved, and results in

$$
\begin{aligned}
E_{k+1}^{X}\left(\mathscr{P}_{k+1}^D\right) &= X_{k+1} - \widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right)\\
&= \mathbf{F}X_k + \mathbf{G}U_k + \widetilde{W}_k - \left(\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{\overline{W}}_k\left(\mathscr{P}_k^D\right)\right)\\
&= \mathbf{F}E_k^X\left(\mathscr{P}_k^D\right) + \widetilde{W}_k - \overline{\overline{W}}_k\left(\mathscr{P}_k^D\right) && (6.56)\\
&= \left(\mathbf{I} - \mathbf{L}_k\mathbf{H}\right)\left(\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right) + \mathbf{G}E_k^U + W_k\right) - \mathbf{L}_k V_{k+1}. && (6.57)
\end{aligned}
$$

As shown in [71], the state estimation error is uncorrelated with the process noise $W_k$. However, linear combinations of independent random variables are random variables. Therefore, the results presented in [71] hold and the state estimation error is uncorrelated with all other random variables, provided they are independent from one another, which as shown above holds in our setting. To see this explicitly note that (6.57) can be rewritten as

$$
E_{k+1}^{X}\left(\mathscr{P}_{k+1}^D\right) = \widetilde{\mathbf{F}}E_k^X\left(\mathscr{P}_k^D\right) + \widetilde{\overline{W}}_k,
$$

where $\widetilde{\mathbf{F}} = (\mathbf{I} - \mathbf{L}_k\mathbf{H})\,\mathbf{F}$ and

$$\widetilde{\widetilde{W}}_k = (\mathbf{I} - \mathbf{L}_k\mathbf{H})\left(\mathbf{G}E_k^U + W_k\right) + \mathbf{L}_k V_{k+1}.$$

This means, the updated error $E_k^X\left(\mathscr{P}_k^D\right)$ is uncorrelated with all other random variables.

When considering the optimal cost given by (6.42) the expectation is slightly modified to account for the noisy channels. This expectation must be executed with respect to the joint distribution

$$\begin{aligned}
&\mathbb{P}\left(X^N, A^{P^{N-1}}, B^{P^{N-1}}, Y^{N-1}, U^{N-1}, \widetilde{U}^{N-1}\right) = \\
&\quad \prod_{k=0}^{N-1} \Big\{ \mathbb{P}\left(X_{k+1}|X_k, \widetilde{U}_k\right)\mathbb{P}\left(A_k^P|X_k, B_{k-1}^P, \widetilde{U}_{k-1}, A_{k-1}^P, \mathscr{P}_{k-1}\right)\mathbb{P}\left(B_k^P|A_k^p\right) \\
&\quad \times \mathbb{P}\left(Y_k|B_k^P, Y_{k-1}, U_{k-1}, \mathscr{P}_{k-1}^D\right)\mathbb{P}\left(U_k|U_{k-1}, Y_k\right)\mathbb{P}\left(A_k^C|Y_k, B_k^P, U_k, A_{k-1}^C, \mathscr{C}_{k-1}\right) \\
&\quad \times \mathbb{P}\left(B_k^C|A_k^C\right)\mathbb{P}\left(\widetilde{U}_k|B_k^C, \widetilde{U}_{k-1}, \mathscr{C}_{k-1}^D\right)\Big\}\,\mathbb{P}(X_0).
\end{aligned} \tag{6.58}$$

Due to the introduction of the communication channels there are additional stochastic kernels that are introduced into the expectation. Therefore, the cost of the partially observed system is

$$J^* = \min_{\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N} \in \mathscr{U}} \left\{ \limsup_{N\to\infty} \frac{1}{N}\mathbb{E}\left[\sum_{k=0}^{N-1} X_k^{\mathsf{T}}\mathbf{Q}_X X_k + \widetilde{U}_k^{\mathsf{T}}\mathbf{Q}_U\widetilde{U}_k\right]\right\}, \tag{6.59}$$

$$\begin{aligned}
&= \min_{\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N} \in \mathscr{U}} \left\{ \limsup_{N\to\infty} \frac{1}{N}\left(\sum_{k=0}^{N} \mathbb{E}\left[\widehat{X}_k^{\mathsf{T}}\left(\mathscr{P}_k^D\right)\mathbf{Q}_X\widehat{X}_k\left(\mathscr{P}_k^D\right) + U_k^{\mathsf{T}}\mathbf{Q}_U U_k\right]\right)\right\} \\
&\qquad + \limsup_{N\to\infty} \frac{1}{N}\left(\sum_{k=0}^{N} \mathbb{E}\left[E_k^X\left(\mathscr{P}_k^D\right)\mathbf{Q}_X E_k^X\left(\mathscr{P}_k^D\right)\right] + \mathbb{E}\left[{E_k^U}^{\mathsf{T}}\mathbf{Q}_U E_k^U\right]\right),
\end{aligned} \tag{6.60}$$

where the substitution of (6.43) is made and due to the uncorrelated nature of the errors $\mathbb{E}\left[E_k^X\mathbf{Q}E_k^U\right] = 0$. The first term of (6.60) is of the correct form to invoke Theorem 14 with a change of variables. Therefore, the optimal linear control law for the new state variable is

$$U_k^* = -\mathbf{K}\widehat{X}_k\left(\mathscr{P}_k^D\right), \tag{6.61}$$

with associated optimal cost,

$$\operatorname{tr}\left(P\Sigma_{\overline{\overline{W}}}\right), \tag{6.62}$$

where $\mathbf{K}$ is defined as the optimal gain matrix according to (6.5). It is assumed that the error covariances converge to the fixed values, specifically the covariances

$$\begin{aligned}\Sigma_{E_k^U} &= \mathbb{E}\left[{E_{k+1}^U}^{\mathsf{T}} E_{k+1}^U \middle| \mathscr{P}_{k+1}^D\right] \\ &= \Sigma_Z = \Sigma_{E^U}, \qquad (6.63)\\ \Sigma_{E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right)} &= \mathbb{E}\left[E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right)^{\mathsf{T}} E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right) \middle| \mathscr{P}_{k+1}^D\right] \\ &= \widetilde{\mathbf{L}}_k^{\mathsf{T}}\left(\mathbf{F}^{\mathsf{T}}\Sigma_{E_k^X\left(\mathscr{P}_k^D\right)}\mathbf{F} + \mathbf{G}^{\mathsf{T}}\Sigma_{E^U}\mathbf{G} + \Sigma_W\right)\widetilde{\mathbf{L}}_k + \mathbf{L}_k\Sigma_V\mathbf{L}_k^{\mathsf{T}}, \qquad (6.64)\end{aligned}$$

where $\widetilde{\mathbf{L}}_k = (\mathbf{I} - \mathbf{L}_k\mathbf{H})$, are assumed to have converged to their solutions. Additionally, the Kalman filter gain $\mathbf{L}_k$ is also assumed to have converged to its steady state value $\mathbf{L}$. These steady state covariance matrices are defined such that

$$\begin{aligned}\Sigma_{E^U} &= \Sigma_{E^U}, \\ \Sigma_{E^X} &= \widetilde{\mathbf{L}}^{\mathsf{T}}\left(\mathbf{F}^{\mathsf{T}}\Sigma_{E^X}\mathbf{F} + \mathbf{G}^{\mathsf{T}}\Sigma_{E^U}\mathbf{G} + \Sigma_W\right)\widetilde{\mathbf{L}} + \mathbf{L}\Sigma_V\mathbf{L}^{\mathsf{T}}. \qquad (6.65)\end{aligned}$$

Under this assumption, the optimal system cost is

$$\begin{aligned}J &= \operatorname{tr}\left(\mathbf{P}\Sigma_{\overline{\overline{W}}}\right) + \operatorname{tr}\left(\mathbf{Q}_X\Sigma_{E^X}\right) + \operatorname{tr}\left(\mathbf{Q}_U\Sigma_{E^U}\right) \qquad (6.66)\\ &= \operatorname{tr}\left(\mathbf{P}\mathbb{E}\left[\overline{\overline{W}}_k\ \overline{\overline{W}}_k^{\mathsf{T}}\right]\right) + \operatorname{tr}\left(\mathbf{Q}_X\Sigma_{E^X}\right) + \operatorname{tr}\left(\mathbf{Q}_U\Sigma_{E^U}\right) \qquad (6.67)\\ &= \operatorname{tr}\left(\mathbf{P}\mathbb{E}\left[\left(\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right) + \widetilde{W}_k - E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right)\right)\left(\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right) + \widetilde{W}_k - E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right)\right)^{\mathsf{T}}\right]\right) \\ &\qquad + \operatorname{tr}\left(\mathbf{Q}_X\Sigma_{E^X}\right) + \operatorname{tr}\left(\mathbf{Q}_U\Sigma_{E^U}\right) \qquad (6.68)\\ &= \operatorname{tr}\left(\mathbf{P}\left(\mathbf{F}\Sigma_{E^X}\mathbf{F}^{\mathsf{T}} + \mathbf{G}\Sigma_{E^U}\mathbf{G}^{\mathsf{T}} + \Sigma_W - \Sigma_{E^X}\right)\right) + \operatorname{tr}\left(\mathbf{Q}_X\Sigma_{E^X}\right) + \operatorname{tr}\left(\mathbf{Q}_U\Sigma_{E^U}\right) \qquad (6.69)\\ &= \operatorname{tr}\left(\mathbf{P}\Sigma_W\right) + \operatorname{tr}\left(\left(\mathbf{F}^{\mathsf{T}}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^X}\right) + \operatorname{tr}\left(\left(\mathbf{G}^{\mathsf{T}}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{E^U}\right), \qquad (6.70)\end{aligned}$$

where in (6.68) the relation (6.56) is substituted for $\overline{\overline{W}}_k$. It is seen in (6.70) that the cost function for a system operating over a noisy communication channel is split into three additive terms. As before these three terms correspond to the cost of optimal control, communication over the sensory channel, and communication over the actuation channel. However, each of these terms represent different quantities. Specifically, the error covariances in each channel have different statistics, and therefore, converge to different values. It will be shown in Section 6.7 that the cost of the system without the acknowledgment link is strictly greater than the cost of the system with the link, provided the communication channel introduces noise.

## 6.6 Imperfect Communication Channel with an Imperfect Auxiliary Channel

In the following the operator implements the auxiliary communication channel as seen in the first system model (Fig 6.4). However, unlike the first system model the operator implements an imperfect channel for the auxiliary channel. This decision is made to generalise the system architecture further. In this way it is shown that this is the middle case of the two previous system derivations. Namely, if the noise within the auxiliary channel is below a threshold then the operator successfully reduces the error in the estimate and is able to reduce the overall system cost. However, if the noise in this auxiliary channel is above this threshold then the operator is best disregarding the additional information and acting as though there is no auxiliary channel. This threshold value is quantified in the cost difference section. The system model is depicted in Fig 6.6.

The information sets of the system once again require redefinition.

$$\mathscr{P}_k^E = \left\{ X_k, A_{k-1}^P, B_{k-1}^P, \widetilde{U}_{k-1}, \mathscr{P}_{k-1}^E \right\}, \tag{6.71a}$$

$$\mathscr{P}_k^D = \left\{ B_k^P, Y_{k-1}, U_{k-1}, \widetilde{\widetilde{U}}_{k-1}, \mathscr{P}_{k-1}^D \right\}, \tag{6.71b}$$

$$\mathscr{C}_k^E = \left\{ Y_k, B_k^P, U_k, A_{k-1}^C, B_{k-1}^C, \widetilde{\widetilde{U}}_{k-1}, \mathscr{C}_{k-1}^E \right\}, \tag{6.71c}$$

$$\mathscr{C}_k^D = \left\{ B_k^C, \widetilde{U}_{k-1}, \mathscr{C}_{k-1}^D \right\}, \tag{6.71d}$$

where $\widetilde{\widetilde{U}}_k$ is the random variable at the output of the imperfect auxiliary communication channel. Note that due to the inclusion of $U_k$ within $\mathscr{P}_k^D$ there is still separation of optimal control and estimation, i.e. as in Section 6.4.1 there is no dual effect from the control law choice. The system modelling and channel construction is the same as before however there is now an additional imperfect communication channel.

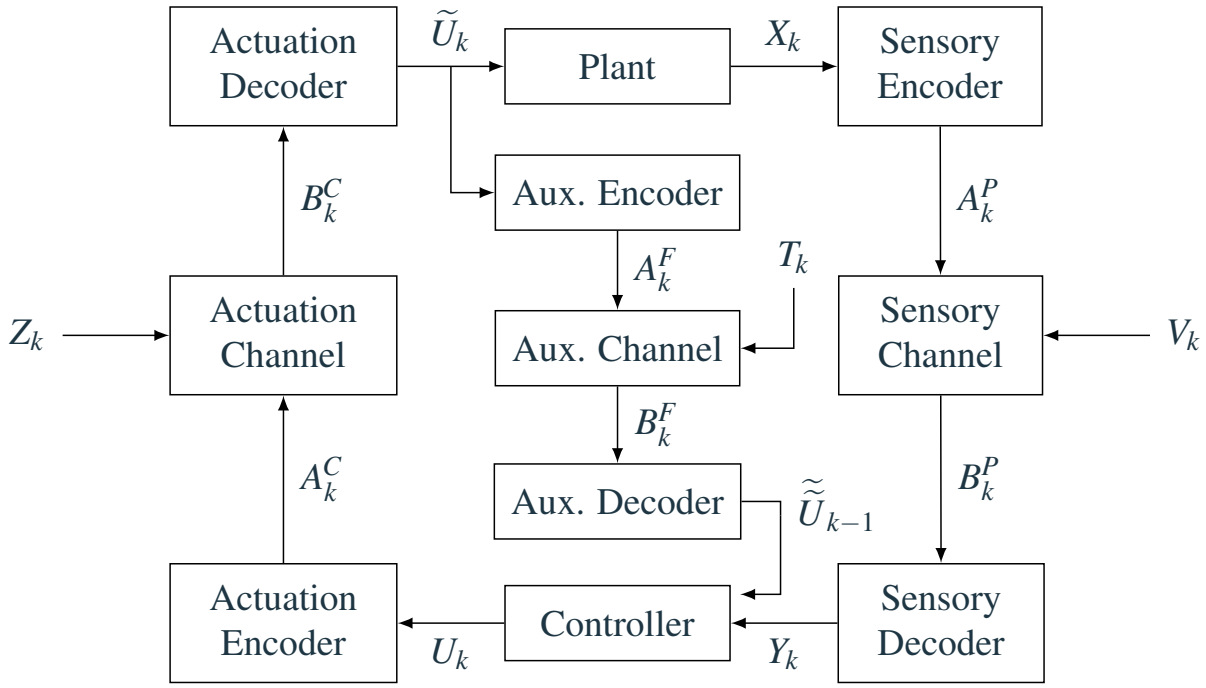


Fig. 6.6 Communication channel implementation within a control system, where the the variable $\widetilde{U}_k$ is transmitted over an imperfect auxiliary communication channel.

### 6.6.1 Optimal Control with Imperfect Auxiliary Channel

In order to assess the impact of the imperfect auxiliary communication channel, the expected value of a LQG cost function is once again adopted. For this system model it is defined as

$$J = \limsup_{N\to\infty} \frac{1}{N}\mathbb{E}\left[\sum_{k=0}^{N-1} X_k^{\mathsf{T}}\mathbf{Q}_X X_k + \widetilde{U}_k^{\mathsf{T}}\mathbf{Q}_U\widetilde{U}_k\right]. \tag{6.72}$$

Once again the cost function includes the variable $\widetilde{U}_k$ and not the uncorrupted input signal $U_k$ or the variable $\widetilde{\widetilde{U}}_k$. This is due to the fact that the noisy actuation signal is still the signal that enters the plant. The optimal cost function for this system is therefore defined as

$$J^* = \min_{\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N}\in\mathscr{U}} \left\{\limsup_{N\to\infty} \frac{1}{N}\mathbb{E}\left[\sum_{k=0}^{N-1} X_k^{\mathsf{T}}\mathbf{Q}_X X_k + \widetilde{U}_k^{\mathsf{T}}\mathbf{Q}_U\widetilde{U}_k\right]\right\}, \tag{6.73}$$

where as before the operator designs the optimal joint distributions $\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N} \in \mathscr{U}$ such that they are contained within the causal set of joint distributions (6.2). The above is identical to that which defined within (6.4.1) and (6.42), however, once again the distribution of the operators measurements $Y_k$ for (6.73) are different to both of the previous derivations due the noisy information about the random variable $\widetilde{U}_k$.

**Theorem 17.** *The updated state estimate*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) = \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) + \mathbf{L}_k\left(Y_k - \mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)\right), \tag{6.74}$$

*is equivalent to the state space system*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) = \mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{\overline{W}}_k\left(\mathscr{P}_k^D\right), \tag{6.75a}$$

$$\widehat{Y}_k = \widehat{X}_k\left(\mathscr{P}_k^D\right), \tag{6.75b}$$

*where* $\overline{\overline{W}}_k\left(\mathscr{P}_k^D\right)$ *is defined as*

$$\overline{\overline{W}}_k\left(\mathscr{P}_k^D\right) = \mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right) + \mathbf{G}T_k + W_k\right) + \mathbf{L}_k V_{k+1}, \tag{6.76}$$

*and* $T_k$ *is the zero mean AWGN introduced by the imperfect auxiliary communication channel with covariance* $\Sigma_T$*.*

*Proof.* The proof is moved to Appendix D.4.

Proving that the process noise of the above state space system is uncorrelated is a trivial extension of Lemma 17. Specifically because the process noise produced from Theorem 17 is identical to the process noise within Lemma 17 with the addition of an IID vectorial Gaussian variable. Therefore, all of the variables within (6.76) are uncorrelated.

Before proceeding with the optimal cost first the updated sensor error is defined

$$\begin{aligned} E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right) &= X_{k+1} - \widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) \\ &= \mathbf{F}X_k + \mathbf{G}U_k + \widetilde{W}_k - \left(\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{\overline{W}}_k\left(\mathscr{P}_k^D\right)\right) \\ &= \mathbf{F}E_k^X\left(\mathscr{P}_k^D\right) + \widetilde{W}_k - \overline{\overline{W}}_k\left(\mathscr{P}_k^D\right). \end{aligned} \tag{6.77}$$

The optimal cost of the partially observed system is defined as

$$J^* = \min_{\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N} \in \mathcal{U}} \left\{ \limsup_{N\to\infty} \frac{1}{N}\mathbb{E}\left[\sum_{k=0}^{N-1} X_k^{\mathsf{T}}\mathbf{Q}_X X_k + \widetilde{U}_k^{\mathsf{T}}\mathbf{Q}_U\widetilde{U}_k\right]\right\}, \tag{6.78}$$

$$\begin{aligned} = \min_{\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N} \in \mathcal{U}} \Bigg\{ \limsup_{N\to\infty} \frac{1}{N} \Bigg( &\sum_{k=0}^{N} \mathbb{E}\left[\widehat{X}_k^{\mathsf{T}}\left(\mathscr{P}_k^D\right)\mathbf{Q}_X\widehat{X}_k\left(\mathscr{P}_k^D\right) + U_k^{\mathsf{T}}\mathbf{Q}_U U_k\right] \\ &+ \mathbb{E}\left[E_k^X\left(\mathscr{P}_k^D\right)\mathbf{Q}_X E_k^X\left(\mathscr{P}_k^D\right)\right] + \mathbb{E}\left[{E_k^U}^{\mathsf{T}}\mathbf{Q}_U E_k^U\right]\Bigg)\Bigg\}. \end{aligned} \tag{6.79}$$

where the substitution of (6.75) is made and due to the uncorrelated nature of the errors it holds that $\mathbb{E}\left[E_k^X\mathbf{Q}E_k^U\right] = 0$. The first term of (6.79) is of the correct form to invoke Theorem 14 with a change of variables. Therefore, the optimal linear control law for the

new control system is

$$U_k^* = -\mathbf{K}\widehat{X}_k\left(\mathscr{P}_k^D\right), \tag{6.80}$$

with associated optimal cost

$$\mathrm{tr}\left(\mathbf{P}\Sigma_{\overline{\overline{W}}}\right), \tag{6.81}$$

where the optimal gain is independent of the system, and therefore, $\mathbf{K}$ is defined as the optimal gain matrix according to (6.5). It is assumed that the error covariances converge to the fixed values, specifically the time varying covariances,

$$\begin{aligned}
\Sigma_{E_k^U} &= \mathbb{E}\left[{E_{k+1}^U}^{\mathsf{T}} E_{k+1}^U \middle| \mathscr{P}_{k+1}^D\right] \\
&= \Sigma_Z = \Sigma_{E^U}, \\
\Sigma_{E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right)} &= \mathbb{E}\left[E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right)^{\mathsf{T}} E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right) \middle| \mathscr{P}_{k+1}^D\right] \\
&= \widetilde{\mathbf{L}}_k^{\mathsf{T}}\left(\mathbf{F}^{\mathsf{T}}\Sigma_{E_k^X\left(\mathscr{P}_k^D\right)}\mathbf{F} + \mathbf{G}^{\mathsf{T}}\Sigma_T\mathbf{G} + \Sigma_W\right)\widetilde{\mathbf{L}}_k + \mathbf{L}_k\Sigma_V\mathbf{L}_k^{\mathsf{T}}
\end{aligned} \tag{6.82}$$

where the terms $\widetilde{\mathbf{L}}_k = (\mathbf{I} - \mathbf{L}_k\mathbf{H})$ are assumed to have converged to their solutions. Additionally, the Kalman filter gain $\mathbf{L}_k$ is also assumed to have converged to its steady state value $\mathbf{L}$. This is the same assumption as is made in the previous sections. These steady state covariance matrices are defined such that

$$\begin{aligned}
\Sigma_{E^U} &= \Sigma_{E^U}, \\
\Sigma_{E^X} &= \widetilde{\mathbf{L}}^{\mathsf{T}}\left(\mathbf{F}^{\mathsf{T}}\Sigma_{E^X}\mathbf{F} + \mathbf{G}^{\mathsf{T}}\Sigma_T\mathbf{G} + \Sigma_W\right)\widetilde{\mathbf{L}} + \mathbf{L}\Sigma_V\mathbf{L}^{\mathsf{T}}.
\end{aligned} \tag{6.83}$$

Under this assumption, the optimal system cost is written as

$$
\begin{aligned}
J^* &= \operatorname{tr}\left(\mathbf{P}\Sigma_{\overline{\overline{W}}}\right) + \operatorname{tr}\left(\mathbf{Q}_X\Sigma_{E^X}\right) + \operatorname{tr}\left(\mathbf{Q}_U\Sigma_{E^U}\right) && (6.84)\\
&= \operatorname{tr}\left(\mathbf{P}\mathbb{E}\left[\overline{\overline{W}}_k\,\overline{\overline{W}}_k^{\mathsf{T}}\right]\right) + \operatorname{tr}\left(\mathbf{Q}_X\Sigma_{E^X}\right) + \operatorname{tr}\left(\mathbf{Q}_U\Sigma_{E^U}\right) && (6.85)\\
&= \operatorname{tr}\left(\mathbf{P}\mathbb{E}\left[\left(\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right) + \widetilde{W}_k - E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right)\right)\left(\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right) + \widetilde{W}_k - E_{k+1}^X\left(\mathscr{P}_{k+1}^D\right)\right)^{\mathsf{T}}\right]\right)\\
&\qquad + \operatorname{tr}\left(\mathbf{Q}_X\Sigma_{E^X}\right) + \operatorname{tr}\left(\mathbf{Q}_U\Sigma_{E^U}\right) && (6.86)\\
&= \operatorname{tr}\left(\mathbf{P}\left(\mathbf{F}\Sigma_{E^X}\mathbf{F}^{\mathsf{T}} + \mathbf{G}\Sigma_{E^U}\mathbf{G}^{\mathsf{T}} + \Sigma_W - \Sigma_{E^X}\right)\right) + \operatorname{tr}\left(\mathbf{Q}_X\Sigma_{E^X}\right) + \operatorname{tr}\left(\mathbf{Q}_U\Sigma_{E^U}\right) && (6.87)\\
&= \underbrace{\operatorname{tr}\left(\mathbf{P}\Sigma_W\right)}_{1} + \underbrace{\operatorname{tr}\left(\left(\mathbf{F}^{\mathsf{T}}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^X}\right)}_{2} + \underbrace{\operatorname{tr}\left(\left(\mathbf{G}^{\mathsf{T}}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{E^U}\right)}_{3}, && (6.88)
\end{aligned}
$$

where in line (6.86) the relation (6.77) is substituted for $\overline{\overline{W}}_k$. It is seen in (6.88) that the cost function for a system operating over a noisy communication channel is split into three additive terms. As before, these three terms correspond to the cost of optimal control, communication over the sensory channel, and communication over the actuation channel. However, as with the previous cases each of these communication costs represent different values.

## 6.7 Cost Difference with Communication Channels

The cost difference between each of the three system models is quantified below. Initially, it is shown that the cost difference between the systems described in Theorem 15 and Theorem 16 is strictly positive. Specifically, it is shown that the cost of the system is strictly increased by not employing the use of the perfect auxiliary communication channel. In the following derivations we characterise the conditions for the noisy auxiliary channel cost as described within Theorem 17 to outperform the system without an auxiliary channel. Additionally, it should be noted that the system with an imperfect auxiliary communication channel only matches the cost of the system with a perfect auxiliary communication channel when the covariance of the noise of the imperfect auxiliary communication channel is the zero matrix. Namely, $\Sigma_T = \mathbb{0}$.

In order to continue without confusion we define each of the sensory covariance matrices with differing labels. The error covariance for the control system with a perfect auxiliary communication channel is

$$\begin{aligned}\Sigma_{E^P_{k+1}\left(\mathscr{P}^D_{k+1}\right)} &= \mathbb{E}\left[E^P_{k+1}\left(\mathscr{P}^D_{k+1}\right)E^P_{k+1}\left(\mathscr{P}^D_{k+1}\right)^{\mathsf{T}}\middle|\mathscr{P}^D_{k+1}\right]\\ &= \widetilde{\mathbf{L}}_k\left(\mathbf{F}\Sigma_{E^P_k\left(\mathscr{P}^D_k\right)}\mathbf{F}^{\mathsf{T}}+\Sigma_W\right)\widetilde{\mathbf{L}}_k^{\mathsf{T}}+\mathbf{L}_k\Sigma_V\mathbf{L}_k^{\mathsf{T}}.\end{aligned} \tag{6.89}$$

This time varying error covariance describes the error term in Theorem 15. Similarly, the error covariance for the control system with an imperfect auxiliary communication channel is

$$\begin{aligned}\Sigma_{E^I_{k+1}\left(\mathscr{P}^D_{k+1}\right)} &= \mathbb{E}\left[E^I_{k+1}\left(\mathscr{P}^D_{k+1}\right)E^I_{k+1}\left(\mathscr{P}^D_{k+1}\right)^{\mathsf{T}}\middle|\mathscr{P}^D_{k+1}\right]\\ &= \widetilde{\mathbf{L}}_k\left(\mathbf{F}\Sigma_{E^I_k\left(\mathscr{P}^D_k\right)}\mathbf{F}^{\mathsf{T}}+\mathbf{G}\Sigma_T\mathbf{G}^{\mathsf{T}}+\Sigma_W\right)\widetilde{\mathbf{L}}_k^{\mathsf{T}}+\mathbf{L}_k\Sigma_V\mathbf{L}_k^{\mathsf{T}}.\end{aligned} \tag{6.90}$$

This time varying error covariance describes the error term in Theorem 17. Lastly, the error covariance for the control system with no auxiliary communication channel is

$$\begin{aligned}\Sigma_{E^N_{k+1}\left(\mathscr{P}^D_{k+1}\right)} &= \mathbb{E}\left[E^N_{k+1}\left(\mathscr{P}^D_{k+1}\right)E^N_{k+1}\left(\mathscr{P}^D_{k+1}\right)^{\mathsf{T}}\middle|\mathscr{P}^D_{k+1}\right]\\ &= \widetilde{\mathbf{L}}_k\left(\mathbf{F}\Sigma_{E^N_k\left(\mathscr{P}^D_k\right)}\mathbf{F}^{\mathsf{T}}+\mathbf{G}\Sigma_{E^U}\mathbf{G}^{\mathsf{T}}+\Sigma_W\right)\widetilde{\mathbf{L}}_k^{\mathsf{T}}+\mathbf{L}_k\Sigma_V\mathbf{L}_k^{\mathsf{T}}.\end{aligned} \tag{6.91}$$

This time varying error covariance describes the error term in Theorem 16. Naturally, the limit of the covariance matrices are defined as

$$\Sigma_{E^P} = \widetilde{\mathbf{L}}\left(\mathbf{F}\Sigma_{E^P}\mathbf{F}^{\mathsf{T}}+\Sigma_W\right)\widetilde{\mathbf{L}}^{\mathsf{T}}+\mathbf{L}\Sigma_V\mathbf{L}^{\mathsf{T}}, \tag{6.92}$$

$$\Sigma_{E^I} = \widetilde{\mathbf{L}}\left(\mathbf{F}\Sigma_{E^I}\mathbf{F}^{\mathsf{T}}+\mathbf{G}\Sigma_T\mathbf{G}^{\mathsf{T}}+\Sigma_W\right)\widetilde{\mathbf{L}}^{\mathsf{T}}+\mathbf{L}\Sigma_V\mathbf{L}^{\mathsf{T}}, \tag{6.93}$$

$$\Sigma_{E^N} = \widetilde{\mathbf{L}}\left(\mathbf{F}\Sigma_{E^N}\mathbf{F}^{\mathsf{T}}+\mathbf{G}\Sigma_{E^U}\mathbf{G}^{\mathsf{T}}+\Sigma_W\right)\widetilde{\mathbf{L}}^{\mathsf{T}}+\mathbf{L}\Sigma_V\mathbf{L}^{\mathsf{T}}, \tag{6.94}$$

respectively. With these definitions made the respective optimal costs are characterised. In doing so we explicitly show the differences between terms

$$J_P^* = \operatorname{tr}\left(\mathbf{P}\Sigma_W\right) + \operatorname{tr}\left(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^P}\right) + \operatorname{tr}\left(\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{E^U}\right), \quad (6.95)$$

$$J_I^* = \operatorname{tr}\left(\mathbf{P}\Sigma_W\right) + \operatorname{tr}\left(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^I}\right) + \operatorname{tr}\left(\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{E^U}\right), \quad (6.96)$$

$$J_N^* = \operatorname{tr}\left(\mathbf{P}\Sigma_W\right) + \operatorname{tr}\left(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^N}\right) + \operatorname{tr}\left(\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{E^U}\right). \quad (6.97)$$

It follows from this characterisation that the difference between system costs can be described in terms of the limits of the error covariances. With that knowledge we define the following function

$$f_k\left(\mathbf{A}\right) = \sum_{i=0}^{k}\left(\widetilde{\mathbf{L}}_{k-i}\mathbf{F}\right)^i \widetilde{\mathbf{L}}_{k-i}\mathbf{G}\mathbf{A}\mathbf{G}^\mathsf{T}\widetilde{\mathbf{L}}_{k-i}^\mathsf{T}\left(\widetilde{\mathbf{L}}_{k-i}\mathbf{F}\right)^{i^\mathsf{T}}, \quad (6.98)$$

where $f_k\left(\mathbf{A}\right)$ is the parametric mapping $f_k\left(\mathbf{A}\right) : \mathbb{M}^m \to \mathbb{M}^n$ with parameter $\mathbf{A} \in \mathbb{M}^m$. The above function captures the effect of the the error introduced by the presence or the lack of the presence of the auxiliary channel. To see this note that

$$\Sigma_{E_{k+1}^P\left(\mathscr{P}_{k+1}^D\right)} = \widetilde{\mathbf{L}}_k\left(\mathbf{F}\Sigma_{E_k^X\left(\mathscr{P}_k^D\right)}\mathbf{F}^\mathsf{T} + \Sigma_W\right)\widetilde{\mathbf{L}}_k^\mathsf{T} + \mathbf{L}_k\Sigma_V\mathbf{L}_k^\mathsf{T} + f_k\left(\mathbb{0}\right), \quad (6.99)$$

$$\Sigma_{E_{k+1}^I\left(\mathscr{P}_{k+1}^D\right)} = \widetilde{\mathbf{L}}_k\left(\mathbf{F}\Sigma_{E_k^X\left(\mathscr{P}_k^D\right)}\mathbf{F}^\mathsf{T} + \Sigma_W\right)\widetilde{\mathbf{L}}_k^\mathsf{T} + \mathbf{L}_k\Sigma_V\mathbf{L}_k^\mathsf{T} + f_k\left(\Sigma_T\right), \quad (6.100)$$

$$\Sigma_{E_{k+1}^N\left(\mathscr{P}_{k+1}^D\right)} = \widetilde{\mathbf{L}}_k\left(\mathbf{F}\Sigma_{E_k^X\left(\mathscr{P}_k^D\right)}\mathbf{F}^\mathsf{T} + \Sigma_W\right)\widetilde{\mathbf{L}}_k^\mathsf{T} + \mathbf{L}_k\Sigma_V\mathbf{L}_k^\mathsf{T} + f_k\left(\Sigma_{E^U}\right). \quad (6.101)$$

Note the equivalence in all terms with the exception of the functional term defined in (6.98). Additionally, we denote by $f_\infty\left(\mathbf{A}\right)$ as the limit value of the function. We term this value the limit value and not the converged value. This is due to the fact our analysis does not pertain to the conditions under which this function converges. It follows from the standard Kalman filter that this function necessarily converges under certain conditions, namely, with perfect communication there are many results for this convergence. This is due to the fact that with no communication error the above function is equivalent to a standard Kalman filter. However, we do not explore the conditions under which this convergence

remains in this thesis. It is seen in Chapter 8 that this function does converge for real values on a real control system. Therefore, the limit values of the error covariances are defined as

$$\Sigma_{E^P} = \widetilde{\mathbf{L}} \left( \mathbf{F} \Sigma_{E^X} \mathbf{F}^\mathsf{T} + \Sigma_W \right) \widetilde{\mathbf{L}}^\mathsf{T} + \mathbf{L} \Sigma_V \mathbf{L}^\mathsf{T} + f_\infty \left( \mathbb{0} \right), \tag{6.102a}$$

$$\Sigma_{E^I} = \widetilde{\mathbf{L}} \left( \mathbf{F} \Sigma_{E^X} \mathbf{F}^\mathsf{T} + \Sigma_W \right) \widetilde{\mathbf{L}}^\mathsf{T} + \mathbf{L}_k \Sigma_V \mathbf{L}^\mathsf{T} + f_\infty \left( \Sigma_T \right), \tag{6.102b}$$

$$\Sigma_{E^N} = \widetilde{\mathbf{L}} \left( \mathbf{F} \Sigma_{E^X} \mathbf{F}^\mathsf{T} + \Sigma_W \right) \widetilde{\mathbf{L}}^\mathsf{T} + \mathbf{L} \Sigma_V \mathbf{L}^\mathsf{T} + f_\infty \left( \Sigma_{E^U} \right). \tag{6.102c}$$

Therefore, the analysis of the function $f_k(\mathbf{A})$ results in the analysis of cost differences between the system designs. This leads to the following theorem.

**Theorem 18.** *The cost difference between the system without an auxiliary communication channel and the system with is strictly positive for any system with noise on the actuation communication channel. Namely*

$$J_N^* \geq J_P^* \tag{6.103}$$

*with equality if and only if*

$$\Sigma_Z = \mathbb{0}. \tag{6.104}$$

*Proof.* We define the cost difference between the two systems is defined as

$$J_{\Delta(N,P)}^* = J_N^* - J_P^* \tag{6.105}$$

$$= \operatorname{tr} \left( \left( \mathbf{F}^\mathsf{T} \mathbf{P} \mathbf{F} - \mathbf{P} + \mathbf{Q}_X \right) \Sigma_{E^N} \right) - \operatorname{tr} \left( \left( \mathbf{F}^\mathsf{T} \mathbf{P} \mathbf{F} - \mathbf{P} + \mathbf{Q}_X \right) \Sigma_{E^P} \right). \tag{6.106}$$

Note that $\mathbf{P}$ is independent of the system architecture. This is a direct result of the no dual effect [71]. Manipulation of this relation results in

$$\begin{aligned} J_{\Delta(N,P)}^* &= \operatorname{tr} \left( \left( \mathbf{F}^\mathsf{T} \mathbf{P} \mathbf{F} - \mathbf{P} + \mathbf{Q}_X \right) \left( f_\infty \left( \Sigma_{E^U} \right) - f_\infty \left( \mathbb{0} \right) \right) \right) \\ &= \operatorname{tr} \left( \left( \mathbf{F}^\mathsf{T} \mathbf{P} \mathbf{F} - \mathbf{P} + \mathbf{Q}_X \right) \left( f_\infty \left( \Sigma_{E^U} \right) - \mathbb{0} \right) \right). \end{aligned} \tag{6.107}$$

The term $\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X$ is strictly positive definite as it is the solution of the ARE, and therefore, the positivity of (6.107) is solely determined by the relation $f_\infty(\Sigma_{E^U}) - \mathbb{0}$. However, $\Sigma_{E^U} = \Sigma_Z$. Therefore, this term is positive for all non-zero $\Sigma_Z$ and it holds that

$$\begin{aligned} J^*_{\Delta(N,P)} &= J^*_N - J^*_I \geq 0, \\ J^*_N &\geq J^*_P, \end{aligned} \tag{6.108}$$

with equality if and only if $\Sigma_Z = \mathbb{0}$. This concludes the proof. □

**Theorem 19.** *Let the auxiliary channel be such that*

$$\Sigma_Z \succ \Sigma_T. \tag{6.109}$$

*Then*

$$J^*_N > J^*_I. \tag{6.110}$$

*Proof.* We define the cost difference between the two systems is defined as

$$J^*_{\Delta(N,I)} = J^*_N - J^*_I \tag{6.111}$$

$$= \operatorname{tr}\left(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^N}\right) - \operatorname{tr}\left(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^I}\right). \tag{6.112}$$

Substitution of the relations in (6.102) yields

$$J^*_{\Delta(N,I)} = \operatorname{tr}\left(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\left(f_\infty(\Sigma_{E^U}) - f_\infty(\Sigma_T)\right)\right). \tag{6.113}$$

The positivity of this term is determined by the term $f_\infty(\Sigma_{E^U}) - f_\infty(\Sigma_T)$. However, $\Sigma_{E^U} = \Sigma_Z$ and by assumption, $\Sigma_Z \succ \Sigma_T$. Due to the quadratic nature of the function $f_k$ the equivalence between these costs only occurs when $\Sigma_Z = \Sigma_T$, otherwise, this term is positive

and it holds that

$$J^*_{\Delta(N,I)} = J^*_N - J^*_I > 0,$$
$$J^*_N > J^*_I. \tag{6.114}$$

Additionally, this inequality is reversed for the case $\Sigma_Z \prec \Sigma_T$. In this case the operator disregards any additional information provided by the noisy auxiliary channel and the optimal control cost is equal to $J^*_N$. This concludes the proof. □

The above theorem shows an auxiliary channel only improves performance if the operator guarantees that the auxiliary communication channel has a better Signal to Noise Ratio (SNR) than the actuation communication channel. Under this assumption the cost function of the imperfect auxiliary channel system is strictly less than the no auxiliary channel system cost. This highlights the usefulness of the auxiliary communication channel for systems where communication in one direction is more reliable that the other. For example, systems with communication channels that send information from the plant to the controller with a higher SNR than the actuation communication channel, necessarily decrease the system cost by implementing an auxiliary communication channel.

**Theorem 20.** *Let the auxiliary channel be such that*

$$\Sigma_Z \succeq \Sigma_T. \tag{6.115}$$

*Then*

$$J^*_N = J^*_I = J^*_P, \tag{6.116}$$

*if and only if*

$$\Sigma_Z \equiv \mathbb{0}. \tag{6.117}$$

*Proof.* It follows from Theorem 18 that the costs $J_N^*$ and $J_P^*$ are only equivalent when there is no actuation communication channel noise. i.e. $\Sigma_Z = \mathbb{0}$. Additionally, Theorem 19 states that in order for the cost $J_I^*$ to be greater than or equal to $J_N^*$ it must hold that $\Sigma_Z \succeq \Sigma_T$. However, both of these covariance matrices are a member of the set $S_{++}^m$. Therefore, if $\Sigma_Z = \mathbb{0}$ it must also hold that either $\Sigma_T = \mathbb{0}$ in which case $J_I^* = J_P^*$ or the imperfect communication architecture is not viable in which case $J_I^* = J_N^* = J_P^*$. This concludes the proof. □

The above shows that all three system models are only equivalent in the case of a system with a perfect actuation communication channel. All other AWGN channels necessarily invoke a cost difference between the three communication channels. To that end, the following theorem summarises the cost difference between the three system models.

**Theorem 21.** *Let the auxiliary channel be such that*

$$\Sigma_Z \succeq \Sigma_T. \tag{6.118}$$

*Then*

$$J_N^* \geq J_I^* \geq J_P^*. \tag{6.119}$$

*With equality in the upper bound when $\Sigma_Z = \Sigma_T$ and equality in the lower bound only when $\Sigma_T = \mathbb{0}$.*

*Proof.* The inequality in the upper bounds follows directly from Theorem 19. The lower bound follows as a result of Theorem 20. This concludes the proof. □

The above theorem shows that provided that the auxiliary communication channel is viable, then the system with an imperfect auxiliary communication channel has an optimal control system cost that is bounded by the other two. The usefulness of Theorem 21 follows from the interpretation that the imperfect auxiliary channel characterises a Pareto front of optimal control between the two other system models. By this it is meant that for

any imperfect auxiliary channel that has a higher SNR that the actuation communication channel the optimal control cost will be proportional to the covariance of $\Sigma_T$. Therefore, the operator is able to perform a communication cost allocation optimisation problem much like in Chapter 4. However, in contrast to Chapter 4 the operator optimises over the eigenmodes of the covariance matrix $\Sigma_T$, discussion of this further is seen within Chapter 9.

## 6.8 Chapter Conclusion

In the above, we have derived the resultant optimal cost for an operator of a control system that communicates over a vectorial AWGN communication channel. This has been done for multiple system structures. We also show that there is a differing cost for each of these system designs. Namely, by not monitoring the realisations of the noise in the actuation channel the operator necessarily experiences an additional estimation error increase and therefore, an additional associated control cost.

It should be noted that the system designs considered are starkly reminiscent of the UDP-like/TCP-like system designs seen within Chapter 3 - 5. Namely, the auxiliary communication channel is the AWGN generalisation of the perfect acknowledgement link seen within these chapters. When considering this interpretation, the results of Section 6.7 have stark similarity to those seen within Chapter 4.

This chapter concludes the optimal decision for the operators. Specifically, this chapter has shown the optimal choice of control law for an operator that controls a system over two AWGN communication channels. However, the operator also monitors these channels and performs a hypothesis test on each. Discussion of hypothesis test is within Chapter 7.

# Chapter 7

# Optimal Stealthy Data-Injection Attacks in Control Systems

## 7.1 Introduction

The optimal control law for the operator of a system with AWGN communication channels is studied in Chapter 6. In this chapter, we turn our attention to the attacker. The attacker, as in Chapter 5, has two objectives: to maximise the expected cost of the system and to remain undetected. This second objective is modelled as a detection constraint in the objective function of the attacker. The communication channels of a control system are constructed in Chapter 6. Therein they are modelled as AWGN communication channels.

Due to this fact the following attack implementation changes from the attack construction in Chapter 5. Namely, the attacker uses a Gaussian random variable as their control variable. Specifically, the attacker injects an additive Gaussian noise stream. As seen in [34], additive Gaussian noise is an optimal attack strategy in terms of increasing cost whilst minimising probability of detection for a linear IID system. This result follows from the work in [61] Therein, the authors conclude that Gaussian noise is the worst case additive noise for wireless networks, this is an extension of the already known result that Gaussian additive noise is the worst case noise for point-to-point communications. Therefore, we adopt additive Gaussian noise for the attack model in an attempt to characterise the worst

case attack scenario for the operator. Additionally, were the attacker to implement a DoS attack upon this system construction it would be detected trivially. This is due to the fact that the communication channel is assumed to be communicating perfect with respect to packet drops but imperfectly with respect to additive Gaussian noise.

The attack is also assumed to be zero mean. This is due to the fact that, as mentioned in Chapter 6, it is the Nash equilibrium between the operator and the attacker. To see this, imagine the following *game*. Again we use the term *game* in a descriptive sense and not as the mathematical concept. A *turn* of the following game is arbitrarily long and does not necessarily correspond to a time instance of the control system. The operator takes their *turn* first, they note that there is no attack, and therefore, perform the optimal control strategy as laid out in Chapter 6. During this period of time the control system functions nominally. The attacker on their turn injects a non-zero mean Gaussian signal. After which the operator is able to estimate the mean of the injected signal. Therefore, the operator can then counter this injected signal in their transmitted signals. At which point the control system has reverted back to a scenario of a zero mean attack variable, with a change of variables. Namely, the operator has offset the attacker's non-zero mean Gaussian random variable such that it is transformed into a zero mean Gaussian random variable. The attacker is then able to detect this offset in after an arbitrary passage of time. Following which the attacker may then change the mean of the random injection signal again. This move and counter move between the attacker and the operator is able to go on indefinitely. Therefore, we consider zero mean strategies, this strategy is a saddle-point between the two *players*.

As mentioned above the attacker is constrained such that the attacked communication channel statistics cannot significantly differ from the nominal communication channel statistics. This is modelled in the following chapter through use of the KL-divergence. The reason for choice of the KL-divergence in section 7.2. Therefore, the attacker has control over the design of the covariance matrix of the attack variable and intends to use this design to maximise the cost of the operator such that the KL-divergence does not exceed a specified level.

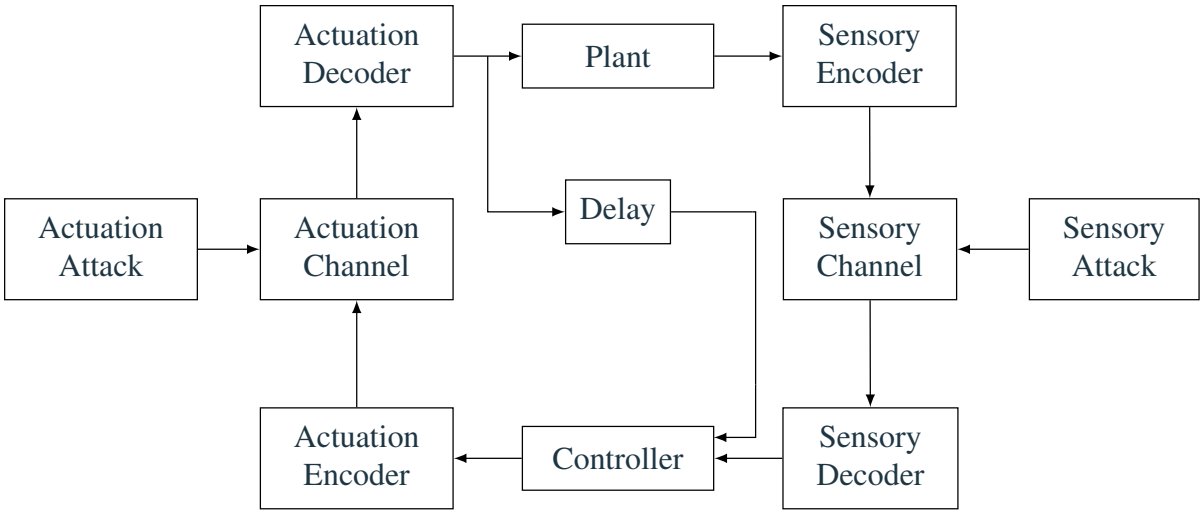


Fig. 7.1 System diagram of the control system whilst undergoing a data injection attack.

In the following chapter we characterise the cost increase caused by any data-injection attack on the AWGN communication channels for each of the three system architectures presented in Chapter 6. Due to the introduction of the attacker the system models presented in Chapter 6 are altered. We consider the attack construction on each system in the same order as in Chapter 6 for ease of reading. Initially, we consider the system with a *perfect* auxiliary communication channel. The system with a *perfect* auxiliary communication channel during a data injection attack is depicted in Fig. 7.1. Note the introduction of each of the attacker vectors in each communication channel. Following this attack construction and analysis we switch to the system with no auxiliary communication channel. This system under attack is depicted in Fig. 7.2. Finally, we then consider the attack upon a system with the *imperfect* auxiliary communication channel. This system model is depicted in Fig. 7.3. Note that due to the introduction of a third AWGN channel the attacker has access to a third attack vector. Following each of the attack construction we then proceed to derive the optimal attack statistics for the injected signal for each of the communication channels, respectively. Specifically, for a scalar communication channel we provide an exact solution for given detection constraints and we also provide a lower

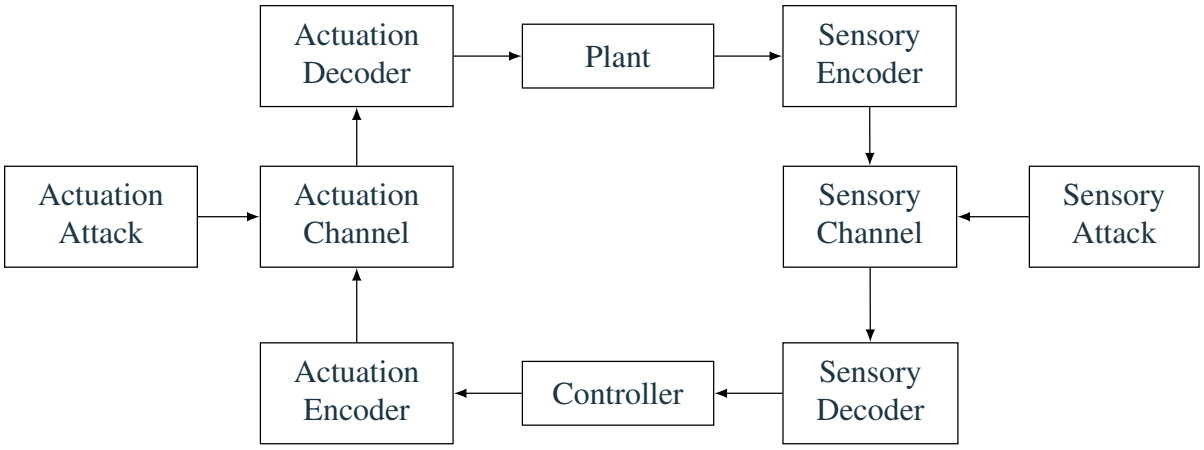


Fig. 7.2 System diagram of the control system whilst undergoing a data injection attack.

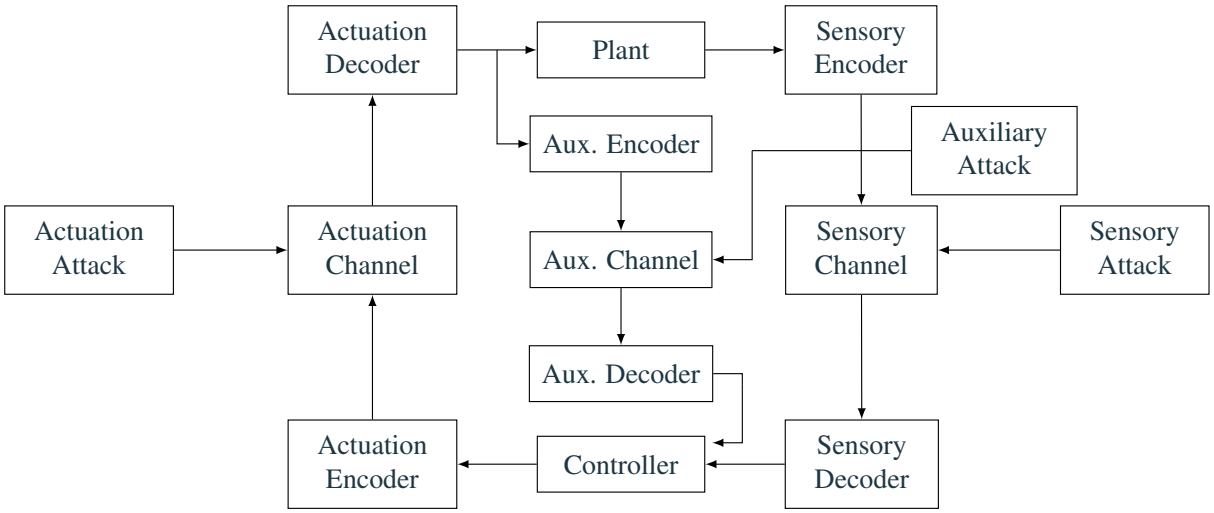


Fig. 7.3 System diagram of the control system whilst undergoing a data injection attack.

bound for the optimal covariance matrix of the injected signal for the vectorial channel case.

## 7.2 Communication Channel Monitoring and Attack Detection

As in previous chapters, when there is the possibility of an attack being present within a system the operator employs a detection regime. In this chapter there are no packet drops to be monitored, instead the operator must monitor the realisations of an AWGN channel and accept a hypothesis test region with this information. Namely, the outcome of the following hypothesis test is decided by the realisation of the variables within each of the communication channels

$$H_0 : \text{There is no attack present,} \tag{7.1a}$$

$$H_1 : \text{There is an attack present.} \tag{7.1b}$$

The operator performs the optimal control law as defined in (6.31). For the systems defined in Chapter 6, three communication channels are already defined. These are the sensory communication channel $\mathcal{P}^N_{B^P|A^P}$, the actuation communication channel $\mathcal{P}^N_{B^C|A^C}$ and the auxiliary communication channel $\mathcal{P}^N_{B^F|A^F}$ where $A^F_k$ and $B^F_k$ are the auxiliary communication channel input and output symbols, respectively. The upper indexing is used to refer to the auxiliary *feedback* channel, to not get it confused with the attack vector within the auxiliary communication channel defined below. These communication channels are henceforth termed the nominal communication channels. These correspond to the communication channels of a system with no data-injection attack present. Furthermore, we introduce three additional communication channels. A communication channel corresponding to each of the previous communication channels when a data injection attack is implemented. These are defined as the attacked sensory communication channel $\mathcal{Q}^N_{B^P|A^P}$, the attacked actuation communication channel $\mathcal{Q}^N_{B^C|A^C}$, and the attacked auxiliary communication channel $\mathcal{Q}^N_{B^F|A^F}$. These new communication channels are all AWGN communication channels.

The KL-divergence is implemented as a detection constraint. The KL-divergence is a measure between two distributions. Additionally, the KL-divergence is equivalent to he ML test. Namely, for IID data minimising the KL-divergence is equivalent to maximising the ML estimator. The KL-divergence between two distributions $P = \{p_i\}_{p_i \in \mathscr{P}}$ and $Q = \{q_i\}_{q_i \in \mathscr{Q}}$ is defined as

$$\mathcal{D}\left(P \parallel Q\right) \triangleq \sum_{i=1}^{M} p_i \log\left(\frac{p_i}{q_i}\right), \tag{7.2}$$

where the convention $0 \log(\frac{0}{0}) = 0$ is assumed. From (7.2) it follows that $\mathcal{D}\left(P \parallel Q\right) = 0$ if and only if $Q = P$. With this in mind the operator conducts the following hypothesis tests

$$H_0^P : \mathcal{D}\left(\mathcal{Q}^N_{B^P|A^P} \parallel \mathcal{P}^N_{B^P|A^P}\right) \leq \delta_1, \tag{7.3a}$$
$$H_1^P : \mathcal{D}\left(\mathcal{Q}^N_{B^P|A^P} \parallel \mathcal{P}^N_{B^P|A^P}\right) > \delta_1. \tag{7.3b}$$

for the sensory communication channel,

$$H_0^C : \mathcal{D}\left(\mathcal{Q}^N_{B^C|A^C} \parallel \mathcal{P}^N_{B^C|A^C}\right) \leq \delta_2, \tag{7.4a}$$
$$H_1^C : \mathcal{D}\left(\mathcal{Q}^N_{B^C|A^C} \parallel \mathcal{P}^N_{B^C|A^C}\right) > \delta_2. \tag{7.4b}$$

for the actuation communication channel, and

$$H_0^F : \mathcal{D}\left(\mathcal{Q}^N_{B^F|A^F} \parallel \mathcal{P}^N_{B^F|A^F}\right) \leq \delta_3, \tag{7.5a}$$
$$H_1^F : \mathcal{D}\left(\mathcal{Q}^N_{B^F|A^F} \parallel \mathcal{P}^N_{B^F|A^F}\right) > \delta_3. \tag{7.5b}$$

for the auxiliary communication channel. The presence of $N$ within the upper index of each distribution indicates that this is the KL-divergence of the *joint* distribution over the entire horizon length $N$. This horizon length is set by the operator and is arbitrary. This hypothesis test construction implies that the operator is conducting a single hypothesis test at the end of the horizon length $N$, and not sequentially. This forces the attacker to

remain stealthy not only at every time step during the attack but also at the end when the operator has access to all of the information possible. This means the following attack derivations are the highly restricted by their detection constraint, however, any attacks derived using this detection constraint are also undetectable by any other less restrictive test, such as a sequential test. It should be noted that the above is a slight abuse of notation. Namely, the above KL-divergences have taken families of distributions as inputs and not distributions. Specifically, the families $\mathcal{Q}^N_{B^P|A^P}$, $\mathcal{Q}^N_{B^C|A^C}$, $\mathcal{Q}^N_{B^F|A^F}$, $\mathcal{P}^N_{B^P|A^P}$, $\mathcal{P}^N_{B^C|A^C}$, and $\mathcal{P}^N_{B^F|A^F}$. Therefore, each of the above hypothesis tests are actually performing the below calculation

$$\mathbb{E}_{A^D}\left[\mathcal{D}\left(\mathcal{Q}^N_{B^D|A^D=a^D} \parallel \mathcal{P}^N_{B^D|A^D=a^D}\right)\right], \tag{7.6}$$

where $A^D$ and $B^D$ are dummy channel input and output channel variables. However, due the fact that we are dealing with AWGN channels it follows for the actuation channel that

$$\begin{aligned}\mathcal{P}_{B^C} &= A^C_i + Z_i,\\ \mathcal{Q}_{B^C} &= A^C_i + Z_i + A^U_i.\end{aligned} \tag{7.7}$$

The above readily translates to the other two channels. Additionally due to the above each of the channel distributions are a linear translation of one another. Therefore, the KL-divergence is not altered and the above hypothesis test are in fact

$$H^P_0 : \mathcal{D}\left(\mathcal{P}_{\mathcal{Y}+\mathcal{A}^X} \parallel \mathcal{P}_{\mathcal{Y}}\right) \leq \delta_1, \tag{7.8a}$$

$$H^P_1 : \mathcal{D}\left(\mathcal{P}_{\mathcal{Y}+\mathcal{A}^X} \parallel \mathcal{P}_{\mathcal{Y}}\right) > \delta_1, \tag{7.8b}$$

for the sensory communication channel,

$$H^C_0 : \mathcal{D}\left(\mathcal{P}_{\mathcal{Z}+\mathcal{A}^U} \parallel \mathcal{P}_{\mathcal{Z}}\right) \leq \delta_2, \tag{7.9a}$$

$$H^C_1 : \mathcal{D}\left(\mathcal{P}_{\mathcal{Z}+\mathcal{A}^U} \parallel \mathcal{P}_{\mathcal{Z}}\right) > \delta_2, \tag{7.9b}$$

for the actuation communication channel, and

$$H_0^F : \mathcal{D}\left(\mathcal{P}_{\mathscr{T}+\mathscr{A}^A} \parallel \mathcal{P}_{\mathscr{T}}\right) \leq \delta_3, \tag{7.10a}$$

$$H_1^F : \mathcal{D}\left(\mathcal{P}_{\mathscr{T}+\mathscr{A}^A} \parallel \mathcal{P}_{\mathscr{T}}\right) > \delta_3, \tag{7.10b}$$

where, as in Chapters 4 and 5, the calligraphic font represents the stacked version of a vector. Explicitly written, these variables are defined as

$$\begin{gathered}
\mathscr{V} = \begin{pmatrix} V_0 \\ V_1 \\ \vdots \\ V_N \end{pmatrix}, \quad \mathscr{Z} = \begin{pmatrix} Z_0 \\ Z_1 \\ \vdots \\ Z_N \end{pmatrix}, \quad \mathscr{T} = \begin{pmatrix} T_0 \\ T_1 \\ \vdots \\ T_N \end{pmatrix}, \\
\mathscr{A}^X = \begin{pmatrix} A_0^X \\ A_1^X \\ \vdots \\ A_N^X \end{pmatrix}, \quad \mathscr{A}^U = \begin{pmatrix} A_0^U \\ A_1^U \\ \vdots \\ A_N^U \end{pmatrix}, \quad \mathscr{A}^A = \begin{pmatrix} A_0^A \\ A_1^A \\ \vdots \\ A_N^A \end{pmatrix}.
\end{gathered} \tag{7.11}$$

Naturally, due to the nature of the input variables within the KL-divergences the upper index of $N$ is implicitly included within the vectors structure. From these definitions it follows that (7.1) is equivalent to

$$H_0 : H_0^F \cap H_0^C \cap H_0^P, \tag{7.12a}$$

$$H_1 : H_1^F \cup H_1^C \cup H_1^P, \tag{7.12b}$$

where through a slight abuse of notation it is seen that if any of the three hypothesis test result in the alternate outcome the operator declares an attack on the control system. Namely, for there to be no attack declared the operator must decide that there is no attack on any of the communication channels present.

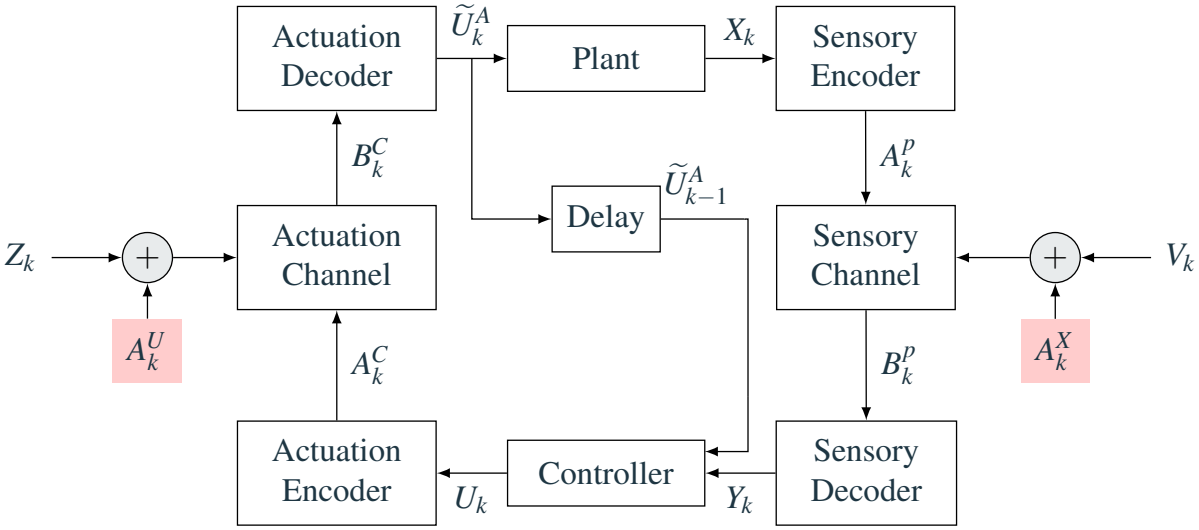


Fig. 7.4 Attack implementation on both communication channels implemented in a control system, where there is transmission of the variable $\widetilde{U}_k$ over a perfect auxiliary communication channel.

## 7.3 Attack Construction with Perfect Auxiliary Communication Channel

Initially, the attack is implemented upon the system that incorporates a perfect auxiliary communication channel within the system architecture. Note that for this system, due to the fact that there is no noise on the auxiliary communication channel the operator is able to set $\delta_3 = 0$. For any imperfect channel this choice of $\delta$ is poor, as any finite sequence of Gaussian variables would cause a non-zero KL-divergence with probability 1. However, due to this being a perfect communication channel this is not an issue, and therefore, the attacker is not able to perform any attack on the auxiliary communication channel without being detected. With this in mind, we introduce the optimisation function of the attacker.

This is defined as

$$J_A^* = \max_{\{\mathcal{Q}_{BC|AC}^N, \mathcal{Q}_{BP|AP}^N\}} J^* \tag{7.13}$$

$$\begin{aligned} J_A^* = \max_{\{\mathcal{Q}_{BC|AC}^N, \mathcal{Q}_{BP|AP}^N\}} & \left\{ \min_{\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N} \in \mathcal{U}} \left\{ \limsup_{N\to\infty} \frac{1}{N} \mathbb{E}\left[ \sum_{k=0}^{N-1} X_k^{\mathsf{T}} \mathbf{Q}_X X_k + \widetilde{U}_k^{A\mathsf{T}} \mathbf{Q}_U \widetilde{U}_k^A \right] \right\} \right\}, \\ \text{s.t. } & \mathcal{D}\left(\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U} \parallel \mathcal{P}_{\mathscr{Z}}\right) \leq \delta_1 \ , \quad \text{and} \quad \mathcal{D}\left(\mathcal{P}_{\mathscr{Y}+\mathscr{A}^X} \parallel \mathcal{P}_{\mathscr{Y}}\right) \leq \delta_2, \end{aligned} \tag{7.14}$$

where $\delta_i \in \mathbb{R}$ is a tuning parameter set by the system operator and $\widetilde{U}_k^A \in R^m$ represents the optimal control law at time $k$ that has been corrupted by the nominal actuation communication channel and the actuation communication channel data injection attack. Namely, the optimal control law corrupted by the attacked communication channel. The $\delta_i$ variables relate to the trade-off between false alarm rate and probability of detection. The communication channels considered are all AWGN communication channels, therefore, (7.14) is equivalent to

$$\begin{aligned} J_A^* = \max_{\{\Sigma_{A^U} \in S_+^m, \Sigma_{A^X} \in S_+^n\}} & \left\{ \min_{\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N} \in \mathcal{U}} \left\{ \limsup_{N\to\infty} \frac{1}{N} \mathbb{E}\left[ \sum_{k=0}^{N-1} X_k^{\mathsf{T}} \mathbf{Q}_X X_k + \widetilde{U}_k^{A\mathsf{T}} \mathbf{Q}_U \widetilde{U}_k^A \right] \right\} \right\}, \\ \text{s.t. } & \mathcal{D}\left(\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U} \parallel \mathcal{P}_{\mathscr{Z}}\right) \leq \delta_1 \ , \quad \text{and} \quad \mathcal{D}\left(\mathcal{P}_{\mathscr{Y}+\mathscr{A}^X} \parallel \mathcal{P}_{\mathscr{Y}}\right) \leq \delta_2, \end{aligned} \tag{7.15}$$

where $\Sigma_{A^U}$ is the covariance matrix the random variable injected into the actuation communication channel and $\Sigma_{A^X}$ is the covariance matrix of the zero mean random variable that is injected into the sensory communication channel. These injected random variables are defined as the IID Gaussian variable $A_k^U \in \mathbb{R}^m$ with mean $\mathbf{0} \in \mathbb{R}^m$ and covariance $\Sigma_{A^U}$ for the actuation channel attack and $A_k^X \in \mathbb{R}^m$ as the IID Gaussian variable with mean $\mathbf{0} \in \mathbb{R}^m$ and covariance $\Sigma_{A^X}$ for the sensory channel attack. The system model must be modified to account for the inclusion of the data injection attack

variables

$$X_{k+1} = \mathbf{F}X_k + \mathbf{G}\widetilde{U}_k^A + W_k, \tag{7.16a}$$

$$\widetilde{U}_k^A = U_k + Z_k + A_k^U, \tag{7.16b}$$

$$Y_k = \mathbf{H}X_k + V_k + A_k^X. \tag{7.16c}$$

Note that this state space system is equivalently represented as

$$X_{k+1} = \mathbf{F}X_k + \mathbf{G}U_k + \widetilde{W}_k^A, \tag{7.17}$$

$$\widetilde{W}_k^A = \mathbf{G}E_k^U + \mathbf{G}A_k + W_k. \tag{7.18}$$

All new terms are additive Gaussian variables that are independent from all other random variables within the Gauss-Markov model as previously seen in the control system model in (6.17).

Due to the introduction of the data injection attack, the information sets defined in (6.7) require updating in order to include the new variables. These are re-defined as

$$\mathscr{P}_k^E = \left\{X_k, A_{k-1}^P, B_{k-1}^P, \widetilde{U}_{k-1}^A, \mathscr{P}_{k-1}^E\right\}, \tag{7.19a}$$

$$\mathscr{P}_k^D = \left\{B_k^P, Y_{k-1}, U_{k-1}, \widetilde{U}_{k-1}^A, \mathscr{P}_{k-1}^D\right\}, \tag{7.19b}$$

$$\mathscr{C}_k^E = \left\{Y_k, B_k^P, U_k, A_{k-1}^C, B_{k-1}^C, \widetilde{U}_{k-1}^A, \mathscr{C}_{k-1}^E\right\}, \tag{7.19c}$$

$$\mathscr{C}_k^D = \left\{B_k^C, \widetilde{U}_{k-1}^A, \mathscr{C}_{k-1}^D\right\}. \tag{7.19d}$$

Note that these information sets are the attacker's and not the operators. This is due to the fact that the attack knows that the additional variables are present whereas the operator does not and instead performs the hypothesis detection detailed above. Due to the fact that a linear combination of Gaussian variables are still a Gaussian variables the previous results from Section 6.4.1 hold and the resultant cost of the system is

$$J^* = \operatorname{tr}\left(\mathbf{P}\Sigma_W\right) + \operatorname{tr}\left(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^{X^A}}\right) + \operatorname{tr}\left(\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{E^{U^A}}\right), \tag{7.20}$$

where due to the presence of the attack, both of the communication channel error covariances $\Sigma_{E^X}$ and $\Sigma_{E^U}$ now depend on $\Sigma_{A^X}$ and $\Sigma_{A^U}$. These new communication channels error are $\Sigma_{E^{X^A}} \in S_+^n$ and $\Sigma_{E^{U^A}} \in S_+^m$, respectively. Therefore, the objective of the attacker becomes

$$\begin{aligned} J_A^* = \max_{\{\Sigma_{A^U} \in S_+^m, \Sigma_{A^X} \in S_+^n\}} & \Big\{ \operatorname{tr}\left(\mathbf{P}\Sigma_W\right) + \operatorname{tr}\left(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^{X^A}}\right) \\ & \qquad + \operatorname{tr}\left(\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{E^{U^A}}\right)\Big\}, \\ \text{s.t. } & \mathcal{D}\left(\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U} \parallel \mathcal{P}_{\mathscr{Z}}\right) \leq \delta_1 \ , \quad \text{and} \quad \mathcal{D}\left(\mathcal{P}_{\mathscr{Y}+\mathscr{A}^X} \parallel \mathcal{P}_{\mathscr{Y}}\right) \leq \delta_2, \end{aligned} \tag{7.21}$$

Although correct, the above form is not particularly useful for an operator or an attacker. Specifically, in (7.21) the operator has no obvious interpretation of how damaging an attack is, nor does an attacker have a tractable optimisation problem. However, if a similar methodology as before is followed it is revealed how the data injection attack effects each of these error covariances, and therefore, the cost. Namely, in the below we show that the above error covariances can be split into the nominal cost terms plus the additional induced attack cost. With that in mind, the errors in each communication channel are defined as

$$E_k^{X^A}\left(\mathscr{P}_k^D\right) = X_k - \widehat{X}_k\left(\mathscr{P}_k^D\right), \tag{7.22a}$$

$$\begin{aligned} E_k^{U^A} &= \widetilde{U}_k^A - U_k \\ &= E_k^U + A_k^U. \end{aligned} \tag{7.22b}$$

Note that, the actuation communication channel error is equivalent to the actuation error in the nominal case with the addition of the error induced by the actuation communication channel attack variable $A_k^U$. The sensory error is not as simple as the actuation error. This is because the error in the sensory communication channel is time varying. Initially, we

deal with the predicted state estimate of the system, this is defined as

$$\begin{aligned}
\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) &= \mathbb{E}\left[X_{k+1}\middle|\mathscr{P}_k^D\right] && (7.23)\\
&= \mathbb{E}\left[\mathbf{F}X_k + \mathbf{G}\tilde{U}_k^A + W_k\middle|\mathscr{P}_k^D\right] && (7.24)\\
&= \mathbb{E}\left[\mathbf{F}\left(\widehat{X}_k\left(\mathscr{P}_k^D\right) + E_k^{X^A}\left(\mathscr{P}_k^D\right)\right) + \mathbf{G}\left(U_k + E_k^U + A_k^U\right) + W_k\middle|\mathscr{P}_k^D\right] && (7.25)\\
&= \mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \mathbb{E}\left[\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}\left(Z_k + A_k^U\right) + W_k\middle|\mathscr{P}_k^D\right] && (7.26)\\
&= \mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{W}_k^A\left(\mathscr{P}_k^D\right), && (7.27)
\end{aligned}$$

where we define $\overline{W}_k^A\left(\mathscr{P}_k^D\right)$ as

$$\overline{W}_k^A\left(\mathscr{P}_k^D\right) = \mathbb{E}\left[\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}\left(E_k^U + A_k^U\right) + W_k\middle|\mathscr{P}_k^D\right]. \tag{7.28}$$

As discussed in Chapter 6, the predicted state estimate is not the state variable that the operator controls the system through. The operator improves their estimates of the states through use of system measurements. To that end, we recast the updated state estimate into a state space system model. This leads to the following theorem.

**Theorem 22.** *The updated state estimate of the system under attack*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) = \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) + \mathbf{L}_k\left(Y_k - \mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)\right), \tag{7.29}$$

*is equivalent to the state space system given by*

$$\begin{aligned}
\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) &= \mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{\overline{W}}_k^A\left(\mathscr{P}_k^D\right), && (7.30a)\\
\widehat{Y}_k &= \widehat{X}_k\left(\mathscr{P}_k^D\right), && (7.30b)
\end{aligned}$$

*where* $\overline{\overline{W}}_k^A\left(\mathscr{P}_k^D\right)$ *is defined as*

$$\overline{\overline{W}}_k^A\left(\mathscr{P}_k^D\right) = \mathbf{G}E_k^{U^A} + \mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + W_k\right) + \mathbf{L}_k\left(V_{k+1} + A_{k+1}^X\right), \tag{7.31}$$

*and* $\mathbf{L}_k$ *is the optimal Kalman filter gain at time step* $k$*, as defined in Theorem 15.*

*Proof.* The proof is moved to Appendix E.1.

The system is in the form of a fully observed state space model. However, in order to employ the result of Theorem 14 the errors must be uncorrelated. This brings us to the next Lemma.

**Lemma 18.** *All variables in* $\overline{\overline{W}}_k^A\left(\mathscr{P}_k^D\right)$ *are uncorrelated.*

*Proof.* The proof is moved to Appendix E.2

It is evident from (E.25) and (E.14), that the error terms include the relevant attack variable within each error term. As seen in (7.21), the cost induced by the data injection attack depends on the covariances of both of the attacked communication channels. With this in mind, and the derivations above, we delve into an in depth description of these error covariances. The error covariance of the actuation communication channel is

$$\begin{aligned}
\Sigma_{E_{k+1}^{U^A}} &= \mathbb{E}\left[E_{k+1}^{U^A} E_{k+1}^{U^A\mathsf{T}} | \mathscr{C}_k^D\right] && (7.32)\\
&= \mathbb{E}\left[\left(E_{k+1}^{U} + A_{k+1}^{U}\right)\left(E_{k+1}^{U} + A_{k+1}^{U}\right)^{\mathsf{T}} | \mathscr{C}_k^D\right] && (7.33)\\
&= \mathbb{E}\left[E_{k+1}^{U} E_{k+1}^{U\mathsf{T}} + A_{k+1}^{U} A_{k+1}^{U\mathsf{T}} | \mathscr{C}_k^D\right] && (7.34)\\
&= \Sigma_{E^U} + \Sigma_{A^U}. && (7.35)
\end{aligned}$$

This error covariance is equivalent to the nominal communication error (6.19b) with the addition of the data injection attack covariance $\Sigma_{A^U}$. Additionally, the error covariance of the actuation communication channel is a constant, and therefore, as before

$$\Sigma_{E_{k+1|\mathscr{C}_k}^{U^A}} = \Sigma_{E_{k|\mathscr{C}_k}^{U^A}} = \Sigma_{E^{U^A}} = \Sigma_{E^U} + \Sigma_{A^U}. \tag{7.36}$$

Due to this fact, throughout the rest of the derivations the time indexing on the actuation error covariance is dropped for notation simplicity. Following a similar process for the

updated state estimation error covariance

$$\Sigma_{E_{k+1}^{X^A}\left(\mathscr{P}_{k+1}^{D}\right)} = \mathbb{E}\left[E_{k+1}^{X^A}\left(\mathscr{P}_{k+1}^{D}\right)^{\mathsf{T}} E_{k+1}^{X^A}\left(\mathscr{P}_{k+1}^{D}\right)\middle|\mathscr{P}_{k+1}^{D}\right] \tag{7.37}$$

$$= \mathbb{E}\left[\left(\widetilde{\mathbf{L}}_k\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^{D}\right)+W_k\right)-\mathbf{L}_k\left(A_{k+1}^{X}+V_{k+1}\right)\right)\right.$$
$$\left.\times\left(\widetilde{\mathbf{L}}_k\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^{D}\right)+W_k\right)-\mathbf{L}_k\left(A_{k+1}^{X}+V_{k+1}\right)\right)^{\mathsf{T}}\middle|\mathscr{P}_{k+1}^{D}\right] \tag{7.38}$$

$$= \mathbb{E}\left[\widetilde{\mathbf{L}}_k\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^{D}\right)E_k^{X^A}\left(\mathscr{P}_k^{D}\right)^{\mathsf{T}}\mathbf{F}^{\mathsf{T}}+W_kW_k^{\mathsf{T}}\right)\widetilde{\mathbf{L}}_k^{\mathsf{T}}\right.$$
$$\left.+\mathbf{L}_k\left(A_{k+1}^{X}A_{k+1}^{X\,\mathsf{T}}+V_{k+1}V_{k+1}^{\mathsf{T}}\right)\mathbf{L}_k^{\mathsf{T}}\middle|\mathscr{P}_k^{D}\right] \tag{7.39}$$

$$= \widetilde{\mathbf{L}}_k\left(\mathbf{F}\Sigma_{E_k^{X^A}\left(\mathscr{P}_k^{D}\right)}\mathbf{F}^{\mathsf{T}}+\Sigma_W\right)\widetilde{\mathbf{L}}_k^{\mathsf{T}}+\mathbf{L}_k\left(\Sigma_{A^X}+\Sigma_V\right)\mathbf{L}_k^{\mathsf{T}}. \tag{7.40}$$

As in [71], it is assumed that the error covariance $\Sigma_{E_k^X}$ converges to the fixed value $\widetilde{\Sigma}_{E^X}$. The converged value of the state error covariance is defined as the solution to (7.40) when the Kalman filter gain has converged to the steady state value $\mathbf{L}$. The resulting error covariance is

$$\Sigma_{E^{X^A}} = \widetilde{\mathbf{L}}\left(\mathbf{F}\Sigma_{E^{X^A}}\mathbf{F}^{\mathsf{T}}+\Sigma_W\right)\widetilde{\mathbf{L}}^{\mathsf{T}}+\mathbf{L}\left(\Sigma_{A^X}+\Sigma_V\right)\mathbf{L}^{\mathsf{T}}. \tag{7.41}$$

Additionally, (7.41) is equivalent to the nominal error covariance plus the additional error induced by the attack. To see this note that

$$\Sigma_{E^{X^A}} = \Sigma_{E^X} + g_\infty\left(\Sigma_{A^X}\right), \tag{7.42}$$

where $\Sigma_{E^X}$ is the nominal limit value of the system error, as seen in (D.23), and

$$g_k\left(\mathbf{A}\right) = \sum_{i=0}^{k}\left(\widetilde{\mathbf{L}}_{k-i}\mathbf{F}\right)^i\mathbf{L}_{k-i}\mathbf{A}\mathbf{L}_{k-i}^{\mathsf{T}}\left(\widetilde{\mathbf{L}}_{k-i}\mathbf{F}\right)^{i^{\mathsf{T}}}. \tag{7.43}$$

Additionally, we slightly abuse notation and denote $g_\infty\left(\mathbf{A}\right)$ as the value of $k$ such that this function has reach a limit. For simplicity we define the variable $\widetilde{\Sigma}_{A^X}$ as this limit value of the above function i.e. $g_\infty\left(\Sigma_{A^X}\right)$. Note that once again, we term these the limit values, and not the converged values. The updated state estimate error covariance during

an attack is

$$\Sigma_{E^XA} = \Sigma_{E^X} + \widetilde{\Sigma}_{A^X}. \tag{7.44}$$

Naturally, the matrix $\widetilde{\Sigma}_{A^X}$ is wholly characterised by the variable $\Sigma_{A^X}$. Revisiting the system cost (7.21) it is seen that

$$\begin{aligned} J_A^* = &\max_{\{\Sigma_{A^U}\in S_+^m, \Sigma_{A^X}\in S_+^n\}} \Big\{ \mathrm{tr}\left(\mathbf{P}\Sigma_W\right) + \mathrm{tr}\left(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^XA}\right) \\ &\qquad + \mathrm{tr}\left(\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{E^UA}\right)\Big\} \qquad (7.45) \\ = &\max_{\{\Sigma_{A^U}\in S_+^m, \Sigma_{A^X}\in S_+^n\}} \Big\{ \mathrm{tr}\left(\mathbf{P}\Sigma_W\right) + \mathrm{tr}\left(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^XA}\right) \\ &\qquad + \mathrm{tr}\left(\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{E^U}\right) + \mathrm{tr}\left(\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{A^U}\right)\Big\} \qquad (7.46) \\ = &\max_{\{\Sigma_{A^U}\in S_+^m, \Sigma_{A^X}\in S_+^n\}} \Big\{ \mathrm{tr}\left(\mathbf{P}\Sigma_W\right) + \mathrm{tr}\left(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^X}\right) \\ &\qquad + \mathrm{tr}\left(\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{E^U}\right) + \mathrm{tr}\left(\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{A^U}\right) \\ &\qquad + \mathrm{tr}\Big(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\widetilde{\Sigma}_{A^X}\Big)\Big\}. \qquad (7.47) \end{aligned}$$

Remarkably, the above optimal control cost whilst under attack is represented as the previous optimal control cost with noisy communication channels, plus two additional terms that depend on the attack variable statistics. Specifically, the matrices $\Sigma_{A^U}$ and $\widetilde{\Sigma}_{A^X}$. Therefore, the optimisation of the attacker has been reduced to compute the optimisation problem

$$\begin{aligned} J_A^* = &\max_{\{\Sigma_{A^U}, \Sigma_{A^X}\}} \Big\{ \mathrm{tr}\Big(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\widetilde{\Sigma}_{A^X} + \left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{A^U}\Big)\Big\}, \\ &\text{s.t. } \mathcal{D}\left(\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U} \parallel \mathcal{P}_{\mathscr{Z}}\right) \leq \delta_1 \ , \quad \text{and} \quad \mathcal{D}\left(\mathcal{P}_{\mathscr{Y}+\mathscr{A}^X} \parallel \mathcal{P}_{\mathscr{Y}}\right) \leq \delta_2. \end{aligned} \tag{7.48}$$

Note that all of the terms within the maximisation are either positive or non-negative definite. In the following section we provide analytic bounds for the solution of this optimisation problem and provide the exact solution in a simplified system setting.

## 7.4 Attack Analysis with Perfect Auxiliary Communication Channel

As is seen in (7.48), the covariance matrix $\Sigma_{A^U} \in S_+^m$ and the matrix $\widetilde{\Sigma}_{A^X} \in S_+^n$ are both non-negative definite matrices. Therefore, given that all other terms are also either non-negative or positive definite, the optimisation of (7.48) becomes maximising $\Sigma_{A^U}$ and $\Sigma_{A^X}$ subject to the KL-divergence constraints. The KL-divergence, as seen in (7.2), is equivalently defined as [25],

$$\mathcal{D}\left(\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U} \parallel \mathcal{P}_{\mathscr{Z}}\right) = \int_{\Omega} \mathcal{P}_{\mathscr{Z}+\mathscr{A}^U} \log\left(\frac{\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U}}{\mathcal{P}_{\mathscr{Z}}}\right) d\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U}, \tag{7.49}$$

where $\Omega$ is the entire probability space. The communication channels being considered are AWGN communication channels. Therefore, with substitution of the relevant covariance matrices, the KL-divergence between these two communication channels is simplified to [69]

$$\mathcal{D}\left(\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U} \parallel \mathcal{P}_{\mathscr{Z}}\right) = \frac{1}{2}\mathrm{tr}\left(\Sigma_{\mathcal{P}_{\mathscr{Z}}}^{-1}\Sigma_{\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U}}\right) - \frac{1}{2}m + \frac{1}{2}\log\left(\frac{|\Sigma_{\mathcal{P}_{\mathscr{Z}}}|}{\left|\Sigma_{\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U}}\right|}\right). \tag{7.50}$$

The sequence of variables is stationary, additionally, the covariance matrices of the communication channels are known and presented in Section 7.3. Therefore, the KL-divergence is simplified to

$$\begin{aligned}
\mathcal{D}\left(\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U} \parallel \mathcal{P}_{\mathscr{Z}}\right) &= \frac{1}{2}\left(\mathrm{tr}\left(\Sigma_Z^{-1}\left(\Sigma_Z + \Sigma_{A^U}\right)\right) - m + \log\left(\frac{|\Sigma_Z|}{|\Sigma_Z + \Sigma_{A^U}|}\right)\right) && (7.51)\\
&= \frac{1}{2}\left(\mathrm{tr}\left(\Sigma_Z^{-1}\Sigma_{A^U} + \mathbf{I}\right) - m + \log\left(\frac{|\Sigma_Z|}{|\Sigma_Z + \Sigma_{A^U}|}\right)\right) && (7.52)\\
&= \frac{1}{2}\left(\mathrm{tr}\left(\Sigma_Z^{-1}\Sigma_{A^U}\right) + \log\left(\frac{|\Sigma_Z|}{|\Sigma_Z + \Sigma_{A^U}|}\right)\right) && (7.53)\\
&= \frac{1}{2}\mathrm{tr}\left(\Sigma_Z^{-1}\Sigma_{A^U}\right) + \frac{1}{2}\log\left(\frac{|\Sigma_Z|}{|\Sigma_Z|\left|\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right|}\right) && (7.54)\\
&= \frac{1}{2}\Big(\mathrm{tr}\left(\Sigma_Z^{-1}\Sigma_{A^U}\right) - \log\left|\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right|\Big). && (7.55)
\end{aligned}$$

The secondary KL-divergence constraint is simplified to an equivalent definition

$$\mathcal{D}\left(\mathcal{P}_{\mathcal{Y}+\mathcal{A}^X} \parallel \mathcal{P}_{\mathcal{Y}}\right) = \frac{1}{2}\Big(\mathrm{tr}\left(\Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right) - \log\Big|\mathbf{I} + \Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\Big|\Big). \tag{7.56}$$

In order to solve the optimisation problem the following Lagrangian is constructed

$$\begin{aligned}\mathscr{L} = \mathrm{tr}\Big(\Big(\mathbf{F}^{\mathsf{T}}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\Big)\widetilde{\Sigma}_{A^X} + \Big(\mathbf{G}^{\mathsf{T}}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\Big)\Sigma_{A^U}\Big) \\ + \frac{\lambda_1}{2}\left(\mathrm{tr}\left(\Sigma_Z^{-1}\Sigma_{A^U}\right) - \log\left|\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right| - 2\delta_1\right) \\ + \frac{\lambda_2}{2}\left(\mathrm{tr}\left(\Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right) - \log\left|\mathbf{I} + \Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right| - 2\delta_2\right).\end{aligned} \tag{7.57}$$

In order to perform the derivatives of the Lagrangian seen in (7.57), the following Lemma is introduced.

**Lemma 19.** *The derivative of*

$$f\left(\mathbf{A}\right) = \mathrm{tr}\left(\mathbf{B}\mathbf{A}\right) + \alpha\left(\mathrm{tr}\left(\mathbf{C}^{-1}\mathbf{A}\right) - \log\left|\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right| - \beta\right), \tag{7.58}$$

*with respect to the matrix* $\mathbf{A} \in S_+^n$ *is*

$$\begin{aligned}\frac{\partial f\left(\mathbf{A}\right)}{\partial \mathbf{A}} = \mathbf{B} + \mathbf{B}^{\mathsf{T}} + 2\alpha\mathbf{C}^{-1} - \alpha\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1}\mathbf{C}^{-1} - \alpha\mathbf{C}^{-1}\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1} \\ -\mathbf{I} \odot \left[\mathbf{B} + \alpha\mathbf{C}^{-1} - \alpha\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1}\mathbf{C}^{-1}\right],\end{aligned} \tag{7.59}$$

*where* $\odot$ *is the Hadamard product and* $\mathbf{I} \odot (\cdot) = diag(\cdot)$.

*Proof.* The proof is moved to Appendix E.3.

As a result of Lemma 19, the first derivatives of the Lagrangian are

$$\begin{aligned}\frac{\partial \mathscr{L}}{\partial \Sigma_{A^U}} = \left(\mathbf{G}^{\mathsf{T}}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right) + \left(\mathbf{G}^{\mathsf{T}}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)^{\mathsf{T}} + \lambda_1\Sigma_Z^{-1} \\ - \frac{\lambda_1}{2}\left[\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right]^{-1}\Sigma_Z^{-1} - \frac{\lambda_1}{2}\Sigma_Z^{-1}\left[\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right]^{-1} \\ -\mathbf{I} \odot \left[\left(\mathbf{G}^{\mathsf{T}}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right) + \frac{\lambda_1}{2}\Sigma_Z^{-1} - \frac{\lambda_1}{2}\left[\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right]^{-1}\Sigma_Z^{-1}\right],\end{aligned} \tag{7.60}$$

for the derivative with respect to the actuation covariance derivative and

$$\begin{aligned}\frac{\partial \mathscr{L}}{\partial \widetilde{\Sigma}_{A^X}} = &\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right) + \left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)^\mathsf{T} + \lambda_2 \Sigma_V^{-1} \\ &- \frac{\lambda_2}{2}\left[\mathbf{I} + \Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right]^{-1}\Sigma_V^{-1} - \frac{\lambda_2}{2}\Sigma_V^{-1}\left[\mathbf{I} + \Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right]^{-1} \\ &- \mathbf{I} \odot \left[\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right) + \frac{\lambda_2}{2}\Sigma_V^{-1} - \frac{\lambda_2}{2}\left[\mathbf{I} + \Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right]^{-1}\Sigma_V^{-1}\right], \quad (7.61)\end{aligned}$$

for the derivative with respect to the sensory covariance matrix attack. Next the attacker must set these derivatives equal to $\mathbb{0}$ and solve for each respective variable. Although (7.60) and (7.61) look complicated, the process of solving them is simplified using the following lemma.

**Lemma 20.** *It is to be shown that solving*

$$\begin{aligned}\mathbb{0} = \; &\mathbf{B} + \mathbf{B}^\mathsf{T} + 2\alpha\mathbf{C}^{-1} - \alpha\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1}\mathbf{C}^{-1} - \alpha\mathbf{C}^{-1}\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1} \\ &- \mathbf{I} \odot \left[\mathbf{B} + \alpha\mathbf{C}^{-1} - \alpha\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1}\mathbf{C}^{-1}\right], \quad (7.62)\end{aligned}$$

*is equivalent to solving*

$$2\mathbf{B} + 2\alpha\mathbf{C}^{-1} - 2\alpha\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1}\mathbf{C}^{-1} = \mathbb{0}. \quad (7.63)$$

*Proof.* The proof is moved to Appendix E.4.

Through use of Lemma 20 (7.60) is rearranged to give

$$\frac{2}{\lambda_1}\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right) + \Sigma_Z^{-1} = \left[\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right]^{-1}\Sigma_Z^{-1} \quad (7.64)$$

$$\begin{aligned}\frac{2}{\lambda_1}\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right) + \Sigma_Z^{-1} &= \left[\Sigma_Z^{-1}\left(\Sigma_Z + \Sigma_{A^U}\right)\right]^{-1}\Sigma_Z^{-1} && (7.65)\\ &= \left[\Sigma_Z + \Sigma_{A^U}\right]^{-1}\Sigma_Z\,\Sigma_Z^{-1} && (7.66)\\ &= \left[\Sigma_Z + \Sigma_{A^U}\right]^{-1}. && (7.67)\end{aligned}$$

Solving the above for $\Sigma_{A^U}$ gives

$$\mathbf{I} = \left[\frac{2}{\lambda_1}\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right) + \Sigma_Z^{-1}\right][\Sigma_Z + \Sigma_{A^U}] \tag{7.68}$$

$$\Sigma_{A^U} = \left[\frac{2}{\lambda_1}\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right) + \Sigma_Z^{-1}\right]^{-1} - \Sigma_Z \tag{7.69}$$

$$\Sigma_{A^U} = \left[\frac{2}{\lambda_1}\Delta^{P^U} + \Sigma_Z^{-1}\right]^{-1} - \Sigma_Z \tag{7.70}$$

$$\Sigma_{A^U} = \Sigma_Z\left[\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + \mathbf{I}\right]^{-1} - \Sigma_Z, \tag{7.71}$$

where $\Delta^{P^U} = \mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U$. Following a similar procedure for (7.61) yields

$$\frac{2}{\lambda_2}\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right) + \Sigma_V^{-1} = \left[\mathbf{I} + \Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right]^{-1}\Sigma_V^{-1} \tag{7.72}$$

$$\frac{2}{\lambda_2}\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right) + \Sigma_V^{-1} = \left[\left(\Sigma_V^{-1}\right)\left(\Sigma_V + \widetilde{\Sigma}_{A^X}\right)\right]^{-1}\Sigma_V^{-1} \tag{7.73}$$

$$= \left[\Sigma_V + \widetilde{\Sigma}_{A^X}\right]^{-1}\Sigma_V\Sigma_V^{-1} \tag{7.74}$$

$$= \left[\Sigma_V + \widetilde{\Sigma}_{A^X}\right]^{-1}. \tag{7.75}$$

Solving for $\widetilde{\Sigma}_{A^X}$ gives

$$\mathbf{I} = \left[\frac{2}{\lambda_2}\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right) + \Sigma_V^{-1}\right]\left[\Sigma_V + \widetilde{\Sigma}_{A^X}\right] \tag{7.76}$$

$$\widetilde{\Sigma}_{A^X} = \left[\frac{2}{\lambda_2}\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right) + \Sigma_V^{-1}\right]^{-1} - \Sigma_V \tag{7.77}$$

$$\widetilde{\Sigma}_{A^X} = \left[\frac{2}{\lambda_2}\Delta^{P^X} + \Sigma_V^{-1}\right]^{-1} - \Sigma_V, \tag{7.78}$$

where $\Delta^{P^X} = \left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)$. This gives the solution of the first two derivatives of (7.57). Performing the derivative of (7.57) with respect to each of the variables, $\lambda_1$ and $\lambda_2$, gives

$$\frac{\partial\mathscr{L}}{\partial\lambda_1} = \frac{1}{2}\mathrm{tr}\left(\Sigma_Z^{-1}\Sigma_{A^U}\right) - \frac{1}{2}\log\left(\left|\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right|\right) - \delta_1, \tag{7.79}$$

and

$$\frac{\partial \mathscr{L}}{\partial \lambda_2} = \frac{1}{2}\mathrm{tr}\left(\Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right) - \frac{1}{2}\log\left(\left|\mathbf{I} + \Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right|\right) - \delta_2, \tag{7.80}$$

respectively. Note that the derivatives of the Lagrangian in (7.57) with respect to the $\lambda_i$ variables only depends on the KL-divergence constraint. This is to be expected as these are the constraints of the Lagrangian. Initially, (7.79) is to be solved and then the solution of (7.80) follows trivially due to the similarities between them. Setting the derivative of (7.79) equal to $\mathbb{0}$ yields

$$\begin{aligned}\delta_1 = \frac{1}{2}\mathrm{tr}\left(\Sigma_Z^{-1}\left(\Sigma_Z\left[\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + \mathbf{I}\right]^{-1} - \Sigma_Z\right)\right) \\ -\frac{1}{2}\log\left|\mathbf{I} + \Sigma_Z^{-1}\left(\Sigma_Z\left[\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + \mathbf{I}\right]^{-1} - \Sigma_Z\right)\right|,\end{aligned} \tag{7.81}$$

$$\delta_1 + \frac{m}{2} = \frac{1}{2}\mathrm{tr}\left(\left[\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + \mathbf{I}\right]^{-1}\right) - \frac{1}{2}\log\left|\left[\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + \mathbf{I}\right]^{-1}\right|. \tag{7.82}$$

With all $\lambda_1$ terms grouped onto one side it allows further simplification. Taking exponentials of both sides yields

$$e^{2\delta_1+m} = e^{\left[\mathrm{tr}\left(\left[\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z+\mathbf{I}\right]^{-1}\right)-\log\left|\left[\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z+\mathbf{I}\right]^{-1}\right|\right]}, \tag{7.83}$$

$$e^{2\delta_1+m} = \left|\left[\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + \mathbf{I}\right]\right| e^{\mathrm{tr}\left(\left[\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z+\mathbf{I}\right]^{-1}\right)}. \tag{7.84}$$

Through use of [30, 10.62] the exponential on the right hand side of the above is lower bounded as follows

$$\left|\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + \mathbf{I}\right| e^{\mathrm{tr}\left(\left[\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z+\mathbf{I}\right]^{-1}\right)} \geq \left|\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + \mathbf{I}\right| \frac{\left|\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + 2\mathbf{I}\right|}{\left|\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + \mathbf{I}\right|} \tag{7.85}$$

$$\left|\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + \mathbf{I}\right| e^{\mathrm{tr}\left(\left[\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z+\mathbf{I}\right]^{-1}\right)} \geq \left|\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + 2\mathbf{I}\right| \geq \left|\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z\right| + \left|2\mathbf{I}\right|, \tag{7.86}$$

where in (7.86) the lower bound [30, 10.59(c)] is used to lower bound the determinant sum. Therefore, (7.84) is rearranged to give,

$$e^{2\delta_1+m} \geq \left|\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z\right| + \left|2\mathbf{I}\right| \tag{7.87}$$

$$\left|\Sigma_Z^{-1}\right| e^{2\delta_1+m} - \left|2\Sigma_Z^{-1}\right| \geq \left|\frac{2}{\lambda_1}\Delta^{P^U}\right| \tag{7.88}$$

$$\left|\Sigma_Z^{-1}\Delta^{P^{-1}}\right| \left(e^{2\delta_1+m} - 2^m\right) \geq \left|\frac{2}{\lambda_1}\mathbf{I}\right| \tag{7.89}$$

$$\sqrt[m]{\left|\Sigma_Z^{-1}\Delta^{P^{U^{-1}}}\right| \left(e^{2\delta_1+m} - 2^m\right)} \geq \frac{2}{\lambda_1}. \tag{7.90}$$

Note that (7.79) and (7.80) are equivalent with a substitution of variables. Therefore, the bound on $\lambda_2$ is

$$\sqrt[m]{\left|\Sigma_V^{-1}\Delta^{P^{X^{-1}}}\right| \left(e^{2\delta_2+m} - 2^m\right)} \geq \frac{2}{\lambda_2}. \tag{7.91}$$

Substituting the bound in (7.90) for $\frac{2}{\lambda_1}$ back into the critical points of $\Sigma_{A^U}$, namely (7.71), gives the following bound for the optimal stealthy attack

$$\Sigma_{A^U} = \Sigma_Z \left[\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + \mathbf{I}\right]^{-1} - \Sigma_Z \tag{7.92}$$

$$\Sigma_{A^U} \geq \Sigma_Z \left[\sqrt[m]{\left|\Sigma_Z^{-1}\Delta^{P^{U^{-1}}}\right| \left(e^{2\delta_1+m} - 2^m\right)}\Delta^{P^U}\Sigma_Z + \mathbf{I}\right]^{-1} - \Sigma_Z. \tag{7.93}$$

This gives a lower bound on the optimal attack strategy for the actuator attack communication channel. Similarly, for the sensory communication channel the lower bound on the optimal attack is

$$\widetilde{\Sigma}_{A^X} \geq \Sigma_V \left[\sqrt[m]{\left|\Sigma_V^{-1}\Delta^{P^{X^{-1}}}\right| \left(e^{2\delta_1+m} - 2^m\right)}\Delta^{P^X}\Sigma_V + \mathbf{I}\right]^{-1} - \Sigma_V. \tag{7.94}$$

The inequalities (7.93) and (7.94) are lower bounds on the attack strategy for the actuation and the sensory communication channel for a multidimensional Gaussian data injection attack, respectively. As seen in (7.93) and (7.94) there is a separation between

the optimal attack on each communication channel. Specifically, due to the disconnect between optimal attacks, the optimisation of each attack can be considered separately. So, an attacker that only has access to a single communication channel employs the same attack strategy on a given communication channel as an attacker with access to both communication channels.

### 7.4.1 Single actuator System

As mentioned above, the lower bound presented is for a multidimensional Gaussian data injection attack with $m$ actuators and $q$ sensors. If, however, the system is reduced to a single actuator, or sensor, the optimal attack construction, for each respective communication channel, is able to be solved exactly. The reduction of the system is such that $U_k \in \mathbb{R}$, and $m = 1$ for the optimal solution for the actuation communication channel attack. The reduction of the system for the sensory communication channel attack is such that $Y_k \in \mathbb{R}$, and $q = 1$ for the optimal solution. Note that, due to the separation between the attacks, the optimal attack for each communication channel is still be solved separately. Specifically, a system with a single actuator but multiple states is able to have the exact solution for the actuator communication channel attack whilst simultaneously being applicable for the multidimensional attack lower bound on the sensory communication channel. To that end the optimal attack solution for both communication channels is derived for scalar communication channels and the *mix and match*, nature of the attacks developed follows. The derivation of the optimal attack solution for the scalar actuation communication channel is identical to the derived bound until (7.84). Therefore, beginning with (7.84) we have that

$$e^{2\delta_1+m} = \left|\left[\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + \mathbf{I}\right]\right| e^{\operatorname{tr}\left(\left[\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z+\mathbf{I}\right]^{-1}\right)}, \tag{7.95}$$

$$e^{2\delta_1+1} = \left(\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + 1\right) e^{\left(\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z+1\right)^{-1}}, \tag{7.96}$$

$$-\frac{1}{e^{2\delta_1+1}} = -\left(\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + 1\right)^{-1} e^{-\left(\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z+1\right)^{-1}}. \tag{7.97}$$

At this stage, the right hand side is of the form $xe^x$. Therefore, (7.97) is simplified through use of the Lambert W-function [62]. Applying this function to both sides yields

$$-\frac{1}{e^{2\delta_1+1}} = -\left(\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + 1\right)^{-1} e^{-\left(\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z+1\right)^{-1}} \tag{7.98}$$

$$W\left(-\frac{1}{e^{2\delta_1+1}}\right) = -\left(\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + 1\right)^{-1}, \tag{7.99}$$

where $W_{-1}(\cdot)$ is the $-1$ branch of the Lambert W-function and is defined as the inverse function of $y = xe^x$, as seen in [62, Sec. 2]. Re-arranging this gives

$$-\frac{1}{W_{-1}\left(-\frac{1}{e^{2\delta_1+1}}\right)} = \frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + 1 \tag{7.100}$$

$$-\frac{1}{\Delta^{P^U}\Sigma_Z} - \frac{1}{\Delta^{P^U}\Sigma_Z\, W_{-1}\left(-\frac{1}{e^{2\delta_1+1}}\right)} = \frac{2}{\lambda_1} \tag{7.101}$$

Substituting this solution back into the stationary point, as seen in (7.71), yields

$$\Sigma_{A^U} = \Sigma_Z\left(\frac{2}{\lambda_1}\Delta^{P^U}\Sigma_Z + 1\right)^{-1} - \Sigma_Z \tag{7.102}$$

$$\Sigma_{A^U} = \Sigma_Z\left[-\frac{1}{W_{-1}\left(-\frac{1}{e^{2\delta_1+1}}\right)}\right]^{-1} - \Sigma_Z \tag{7.103}$$

$$\Sigma_{A^U} = -\Sigma_Z\, W_{-1}\left(-\frac{1}{e^{2\delta_1+1}}\right) - \Sigma_Z. \tag{7.104}$$

As before, performing the same process for the sensory communication channel with $Y_k \in \mathbb{R}$ and $q = 1$ yields the optimal sensory communication channel data injection attack solution

$$\widetilde{\Sigma}_{A^X} = -\Sigma_V\, W_{-1}\left(-\frac{1}{e^{2\delta_2+1}}\right) - \Sigma_V. \tag{7.105}$$

Note that, if $\delta_i$ is set to 0 then the optimal attack in this scenario is to construct a covariance matrix that is the zero matrix. Meaning that with $\delta_i$ set to 0 the optimal attack is to perform no attack, or put another way, no stealthy attack exists. This is as to be

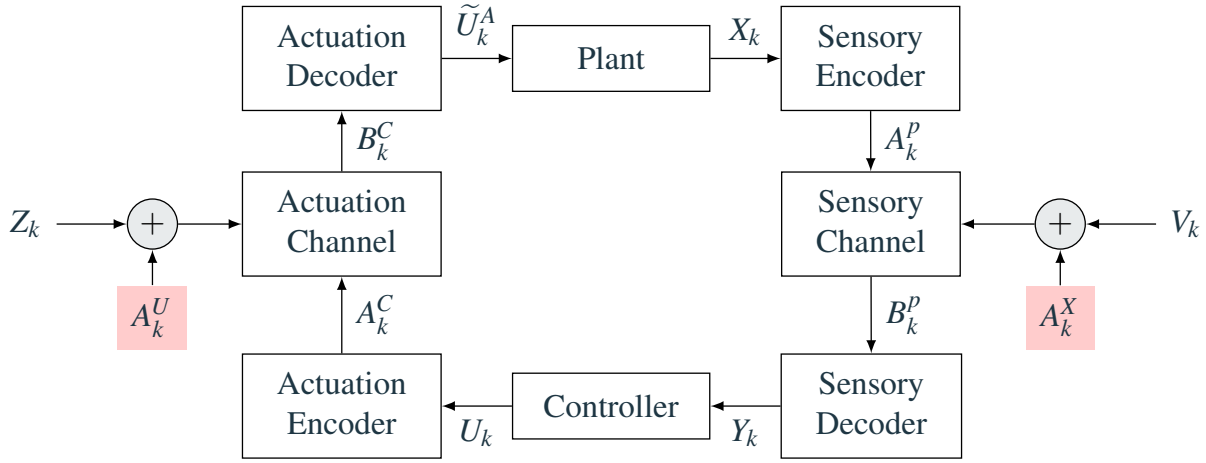


Fig. 7.5 Attack implementation on communication channels implemented in a control system, where there is no transmission of the variable $\widetilde{U}_k$ over an auxiliary communication channel.

expected due to the nature of the KL-divergence. Due to the separation between the two attack constructions in each respective communication channel, any combination of these attack constructions are applicable for the corresponding system. Namely, a system with a single actuator but multiple sensors can employ the optimal solution on the actuation channel while utilising the sensory channel bound for the optimal data injection attack and vice-versa.

## 7.5 Attack Construction Without an Auxiliary Channel

The attack construction must be re-worked for the scenario without the auxiliary communication channel. This section studies the effect of not employing an auxiliary communication channel for estimation. Specifically, this section informs the operator of the increased damage an attack can cause through not monitoring the actuation communication channel. Note that in this case there is no auxiliary communication channel, and therefore, the attacker once again can perform no attack without being instantly detected. This can be thought of again the operator setting $\delta_3 = 0$. However, the communication channel $\mathcal{P}^N_{B^F|A^F}$

is a perfect erasure communication channel. Specifically, every channel output is the zero vector, with probability 1, for every given channel input.

As before in order achieve their objective, the attacker injects two zero mean Gaussian random variables. One into each of the communication channels. This is implemented as seen in Fig. 7.5. Similarly to before, the attacker is constrained such that the attacked communication channel statistics cannot drastically differ from the nominal communication channel statistics. Specifically, this is modelled through use of the KL-divergence. With the above laid out, it follows that the only difference in the system model from Section 7.3 is the choice of not utilising an auxiliary communication channel.

For the system with no auxiliary communication channel the optimisation function of the attacker is expressed as

$$J_A^* = \max_{\{\mathcal{Q}_{BC|AC}^N, \mathcal{Q}_{BP|AP}^N\}} \{J^*\} \tag{7.106}$$

$$\begin{aligned} J_A^* = \max_{\{\mathcal{Q}_{BC|AC}^N, \mathcal{Q}_{BP|AP}^N\}} & \left\{ \min_{\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N} \in \mathscr{U}} \left\{ \limsup_{N\to\infty} \frac{1}{N} \mathbb{E}\left[ \sum_{k=0}^{N-1} X_k^{\mathsf{T}} \mathbf{Q}_X X_k + \widetilde{U}_k^{A\mathsf{T}} \mathbf{Q}_U \widetilde{U}_k^A \right] \right\} \right\}, \\ & \text{s.t. } \mathcal{D}\left(\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U} \parallel \mathcal{P}_{\mathscr{Z}}\right) \leq \delta_1 \ , \quad \text{and} \quad \mathcal{D}\left(\mathcal{P}_{\mathscr{Y}+\mathscr{A}^X} \parallel \mathcal{P}_{\mathscr{Y}}\right) \leq \delta_2. \end{aligned} \tag{7.107}$$

This is of the same form as (7.14) due to the fact that the objective of the attacker and constraints remain the same, only the system structure has change. Specifically, what each of the variables within (7.107) represent changes. The injected signals, as before, are zero mean Gaussian variables $A_k^U \in \mathbb{R}^m$ and $A_k^X \in \mathbb{R}^q$. The communication channels considered are all AWGN communication channels, therefore, (7.107) is equivalent to

$$\begin{aligned} J_A^* = \max_{\{\Sigma_{A^U} \in S_+^m, \Sigma_{A^X} \in S_+^n\}} & \left\{ \min_{\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N} \in \mathscr{U}} \left\{ \limsup_{N\to\infty} \frac{1}{N} \mathbb{E}\left[ \sum_{k=0}^{N-1} X_k^{\mathsf{T}} \mathbf{Q}_X X_k + \widetilde{U}_k^{A\mathsf{T}} \mathbf{Q}_U \widetilde{U}_k^A \right] \right\} \right\}, \\ & \text{s.t. } \mathcal{D}\left(\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U} \parallel \mathcal{P}_{\mathscr{Z}}\right) \leq \delta_1 \ , \quad \text{and} \quad \mathcal{D}\left(\mathcal{P}_{\mathscr{Y}+\mathscr{A}^X} \parallel \mathcal{P}_{\mathscr{Y}}\right) \leq \delta_2, \end{aligned} \tag{7.108}$$

The system model remains as in (7.16), with the inclusion of the data injection attack variables

$$X_{k+1} = \mathbf{F}X_k + \mathbf{G}\widetilde{U}_k^A + W_k, \tag{7.109a}$$

$$\widetilde{U}_k^A = U_k + Z_k + A_k^U, \tag{7.109b}$$

$$Y_k = \mathbf{H}X_k + V_k + A_k^X. \tag{7.109c}$$

As before, the state space system is equivalently represented as

$$X_{k+1} = \mathbf{F}X_k + \mathbf{G}U_k + \widetilde{W}_k^A, \tag{7.110}$$

$$\widetilde{W}_k^A = \mathbf{G}E_k^U + \mathbf{G}A_k + W_k. \tag{7.111}$$

All new terms are additive Gaussian variables that are independent from all other random variables within the Gauss-Markov model previously seen in (6.17).

The information sets defined in (7.19) require updating in order to account for the lack of the auxiliary communication channel. These new information sets are similar to those defined in (6.40). Indeed, they are defined as

$$\mathscr{P}_k^E = \left\{X_k, A_{k-1}^P, B_{k-1}^P, \widetilde{U}_{k-1}^A \mathscr{P}_{k-1}^E\right\}, \tag{7.112a}$$

$$\mathscr{P}_k^D = \left\{B_k^P, Y_{k-1}, U_{k-1}, \mathscr{P}_{k-1}^D\right\}, \tag{7.112b}$$

$$\mathscr{C}_k^E = \left\{Y_k, B_k^P, U_k, B_{k-1}^C, \widetilde{U}_{k-1}^A, \mathscr{C}_{k-1}^E\right\}, \tag{7.112c}$$

$$\mathscr{C}_k^D = \left\{B_k^C, \widetilde{U}_{k-1}^A, \mathscr{C}_{k-1}^D\right\}. \tag{7.112d}$$

Due to the fact that linear combinations of independent Gaussian variables are still a Gaussian variables the previous results from Section 6.4.1 hold and the resultant cost of the system is

$$J^* = \operatorname{tr}\left(\mathbf{P}\Sigma_W\right) + \operatorname{tr}\left(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^{X^A}}\right) + \operatorname{tr}\left(\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{E^{U^A}}\right), \tag{7.113}$$

where, due to the presence of the attack, both of the communication channel error covariances $\Sigma_{E^X}$ and $\Sigma_{E^U}$, now depend on $\Sigma_{A^X}$ and $\Sigma_{A^U}$. It should be noted that these error covariances are not equivalent to those defined in Section 7.3, or any in Chapter 6 due to the lack of information about the variable $\widetilde{U}_k^A$ and the inclusion of the attack. The objective of the attacker is therefore recast as

$$\begin{aligned} J_A^* = \max_{\{\Sigma_{A^U} \in S_+^m, \Sigma_{A^X} \in S_+^n\}} & \Big\{ \operatorname{tr}\left(\mathbf{P}\Sigma_W\right) + \operatorname{tr}\left(\left(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^{X^A}}\right) \\ & + \operatorname{tr}\left(\left(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{E^{U^A}}\right)\Big\}, \\ \text{s.t. } & \mathcal{D}\left(\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U} \parallel \mathcal{P}_{\mathscr{Z}}\right) \leq \delta_1 \ , \quad \text{and} \quad \mathcal{D}\left(\mathcal{P}_{\mathscr{Y}+\mathscr{A}^X} \parallel \mathcal{P}_{\mathscr{Y}}\right) \leq \delta_2. \end{aligned} \tag{7.114}$$

If a similar methodology as before is followed it is revealed how the data injection attack effects each of these error covariances, and therefore, the cost. Namely, in the below we show that the above error covariances are able to be split into the nominal cost terms plus the additional induced attack cost. Due to the lack of information about the actuation communication channel realisation it is seen that much like in the control case the cost is strictly increases by not monitoring the actuation communication channel. To that end, the error terms in each communication channel are defined as

$$E_k^{X^A}\left(\mathscr{P}_k^D\right) = X_k - \widehat{X}_k\left(\mathscr{P}_k^D\right), \tag{7.115a}$$

$$E_k^{U^A} = \widetilde{U}_k^A - U_k, \tag{7.115b}$$

$$= E_k^U + A_k^U. \tag{7.115c}$$

The actuation communication channel error is equivalent to the actuation error in Section 7.3. The cost increase by not employing an auxiliary communication channel comes directly from the sensory communication channel error. This is similar to that seen in

Section 6.5. To that end the predicted state estimate of the system is defined as

$$\begin{aligned}
\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) &= \mathbb{E}\left[X_{k+1}\middle|\mathscr{P}_k^D\right] && (7.116)\\
&= \mathbb{E}\left[\mathbf{F}X_k + \mathbf{G}\tilde{U}_k^A + W_k\middle|\mathscr{P}_k^D\right] && (7.117)\\
&= \mathbb{E}\left[\mathbf{F}\left(\widehat{X}_k\left(\mathscr{P}_k^D\right) + E_k^{X^A}\left(\mathscr{P}_k^D\right)\right) + \mathbf{G}\left(U_k + E_k^U + A_k^U\right) + W_k\middle|\mathscr{P}_k^D\right] && (7.118)\\
&= \mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \mathbb{E}\left[\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}\left(Z_k + A_k^U\right) + W_k\middle|\mathscr{P}_k^D\right] && (7.119)\\
&= \mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{W}_k^A\left(\mathscr{P}_k^D\right), && (7.120)
\end{aligned}$$

where

$$\overline{W}_k^A\left(\mathscr{P}_k^D\right) = \mathbb{E}\left[\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}\left(E_k^U + A_k^U\right) + W_k\middle|\mathscr{P}_k^D\right]. \tag{7.121}$$

Interestingly, the predicted state estimate is equivalent to the predicted state estimate for the system with a perfect auxiliary communication channel even during an attack. It is only when the error is updated that the differences are explicit. With that in mind we once again recast the updated state estimation into a state space system model.

**Theorem 23.** *The updated state estimate of the system under attack*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) = \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) + \mathbf{L}_k\left(Y_k - \mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)\right), \tag{7.122}$$

*is equivalent to the state space system*

$$\begin{aligned}
\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) &= \mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{\overline{W}}_k^A\left(\mathscr{P}_k^D\right), && (7.123a)\\
\widehat{Y}_k &= \widehat{X}_k\left(\mathscr{P}_k^D\right), && (7.123b)
\end{aligned}$$

*where* $\overline{\overline{W}}_k^A\left(\mathscr{P}_k^D\right)$ *is defined as*

$$\overline{\overline{W}}_k^A\left(\mathscr{P}_k^D\right) = \mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}E_k^{U^A} + W_k\right) + \mathbf{L}_k\left(V_{k+1} + A_{k+1}^X\right), \tag{7.124}$$

*and* $\mathbf{L}_k$ *is the optimal Kalman filter gain at time step* $k$*, as defined in Theorem 16.*

*Proof.* The proof is moved to Appendix E.5.

As seen in the previous section $E_{k+1}^{U}$ is independent of all other random variables. Additionally, the actuation communication channel attack variable $A_{k+1}^{U}$ is defined as independent of all other random variables. Therefore, the actuation error when under attack, (7.115c), is independent of the predicted state estimation error and the plant noise. This is the same as in Section 7.3. The predicted state estimation error is defined as

$$
\begin{aligned}
E_{k+1}^{X^A}\left(\mathscr{P}_k^D\right) &= X_{k+1} - \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) && (7.125)\\
&= \mathbf{F}X_k + \mathbf{G}U_k + \widetilde{W}_k^A - \left(\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{W}_k^A\left(\mathscr{P}_k^D\right)\right) && (7.126)\\
&= \mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}A_k^U + \widetilde{W}_k - \overline{W}_k^A\left(\mathscr{P}_k^D\right) && (7.127)\\
&= \mathbf{F}\left(E_k^{X^A}\left(\mathscr{P}_k^D\right) - \mathbb{E}\left[E_k^{X^A}\left(\mathscr{P}_k^D\right)\middle|\mathscr{P}_k^D\right]\right) + \mathbf{G}\left(A_k^U - \mathbb{E}\left[A_k^U\middle|\mathscr{P}_k^D\right]\right) + W_k\\
&\qquad + \mathbf{G}\left(E_k^U - \mathbb{E}\left[E_k^U\middle|\mathscr{P}_k^D\right]\right) && (7.128)\\
&= \mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}A_k^U + \mathbf{G}E_k^U + W_k. && (7.129)
\end{aligned}
$$

Note that the actuation communication channel attack only effects the *predicted* state error. This is due to the fact that this data injection attack actually enters the system whereas the sensory communication channel attack only effects the measurements of the states. However, without the auxiliary communication channel this estimation error propagates through to the updated state estimation error. With that in mind the updated state estimate is

$$
\begin{aligned}
E_{k+1}^{X^A}\left(\mathscr{P}_{k+1}^D\right) &= X_{k+1} - \widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) && (7.130)\\
&= \mathbf{F}X_k + \mathbf{G}U_k + \widetilde{W}_k^A - \left(\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{\overline{W}}_k^A\left(\mathscr{P}_k^D\right)\right) && (7.131)\\
&= \mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \widetilde{W}_k^A - \overline{\overline{W}}_k^A\left(\mathscr{P}_k^D\right) && (7.132)\\
&= \mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}A_k^U + \mathbf{G}E_k^U + W_k - \mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}E_k^{U^A} + W_k\right)\\
&\qquad - \mathbf{L}_k\left(V_{k+1} + A_{k+1}^X\right) && (7.133)\\
&= \widetilde{\mathbf{L}}_k\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}A_k^U + \mathbf{G}E_k^U + W_k\right) - \mathbf{L}_k\left(A_{k+1}^X + V_{k+1}\right). && (7.134)
\end{aligned}
$$

It is evident from (7.134) and (7.115c) that the error terms include the relevant attack variable within each error term. In fact, the updated state estimate error includes both attack variables. As seen in (7.114), the cost induced by the optimal attack depends on the covariances of both of the communication channels. Given that the error terms both depend on the attack variables the error covariances undoubtedly also depend on the attack variable statistics. To that end the covariance of the actuation communication channel is

$$\Sigma_{E^{UA}_{k+1}} = \mathbb{E}\left[E^{UA}_{k+1} {E^{UA}_{k+1}}^{\mathsf{T}} | \mathscr{P}^D_k\right] \tag{7.135}$$

$$= \mathbb{E}\left[\left(E^U_{k+1} + A^U_{k+1}\right)\left(E^U_{k+1} + A^U_{k+1}\right)^{\mathsf{T}} | \mathscr{P}^D_k\right] \tag{7.136}$$

$$= \mathbb{E}\left[E^U_{k+1} {E^U_{k+1}}^{\mathsf{T}} + A^U_{k+1} {A^U_{k+1}}^{\mathsf{T}} | \mathscr{C}^D_k\right] \tag{7.137}$$

$$= \Sigma_{E^U} + \Sigma_{A^U}. \tag{7.138}$$

As before, the error covariance of the actuation communication channel is a constant, and therefore

$$\Sigma_{E^{UA}_{k+1}\left(\mathscr{P}^D_k\right)} = \Sigma_{E^{UA}_{k}\left(\mathscr{P}^D_k\right)} = \Sigma_{E^{UA}} = \Sigma_{E^U} + \Sigma_{A^U}. \tag{7.139}$$

Following a similar process for the updated state estimation error covariance

$$\Sigma_{E^{XA}_{k+1}\left(\mathscr{P}^D_{k+1}\right)} = \mathbb{E}\left[E^{XA}_{k+1}\left(\mathscr{P}^D_{k+1}\right)^{\mathsf{T}} E^{XA}_{k+1}\left(\mathscr{P}^D_{k+1}\right) \middle| \mathscr{P}^D_{k+1}\right] \tag{7.140}$$

$$\begin{aligned} &= \mathbb{E}\Big[\left(\widetilde{\mathbf{L}}_k\left(\mathbf{F}E^{XA}_k\left(\mathscr{P}^D_k\right) + \mathbf{G}A^U_k + \mathbf{G}E^U_k + W_k\right) - \mathbf{L}_k\left(A^X_{k+1} + V_{k+1}\right)\right) \\ &\quad \times\left(\widetilde{\mathbf{L}}_k\left(\mathbf{F}E^{XA}_k\left(\mathscr{P}^D_k\right) + \mathbf{G}A^U_k + \mathbf{G}E^U_k + W_k\right) - \mathbf{L}_k\left(A^X_{k+1} + V_{k+1}\right)\right)^{\mathsf{T}} \middle| \mathscr{P}^D_{k+1}\Big] \\ &= \mathbb{E}\Big[\widetilde{\mathbf{L}}_k\left(\mathbf{F}E^{XA}_k {E^{XA}_k}^{\mathsf{T}}\mathbf{F}^{\mathsf{T}} + \mathbf{G}E^U_k {E^U_k}^{\mathsf{T}}\mathbf{G}^{\mathsf{T}}\right)\widetilde{\mathbf{L}}_k^{\mathsf{T}} \\ &\qquad + \widetilde{\mathbf{L}}_k\left(\mathbf{G}A^U_k {A^U_k}^{\mathsf{T}}\mathbf{G}^{\mathsf{T}} + W_k {W_k}^{\mathsf{T}}\right)\widetilde{\mathbf{L}}_k^{\mathsf{T}} \\ &\qquad\qquad + \mathbf{L}_k\left(A^X_{k+1} {A^X_{k+1}}^{\mathsf{T}} + V_{k+1}V^{\mathsf{T}}_{k+1}\right)\mathbf{L}_k^{\mathsf{T}} \middle| \mathscr{P}^D_k\Big] \end{aligned} \tag{7.141}$$

$$= \widetilde{\mathbf{L}}_k\Big(\mathbf{F}\Sigma_{E^{XA}_k\left(\mathscr{P}^D_k\right)}\mathbf{F}^{\mathsf{T}} + \mathbf{G}\left(\Sigma_{E^U} + \Sigma_{A^U}\right)\mathbf{G}^{\mathsf{T}} + \Sigma_W\Big)\widetilde{\mathbf{L}}_k^{\mathsf{T}} \tag{7.142}$$

$$+ \mathbf{L}_k\left(\Sigma_{A^X} + \Sigma_V\right)\mathbf{L}_k^{\mathsf{T}}. \tag{7.143}$$

As in [71] it is assumed that the error covariance $\Sigma_{E_k^X}$ converges to the value $\widetilde{\Sigma}_{E^X}$. The limit value of the state error covariance is defined as the steady state solution to (7.143) when the Kalman filter gain has converged to the value $\mathbf{L}$. Namely, it is defined as

$$\Sigma_{E^{XA}} = \widetilde{\mathbf{L}} \left( \mathbf{F} \Sigma_{E^{XA}} \mathbf{F}^{\mathsf{T}} + \mathbf{G} \left( \Sigma_{E^U} + \Sigma_{A^U} \right) \mathbf{G}^{\mathsf{T}} + \Sigma_W \right) \widetilde{\mathbf{L}}^{\mathsf{T}} + \mathbf{L} \left( \Sigma_{A^X} + \Sigma_V \right) \mathbf{L}^{\mathsf{T}}. \quad (7.144)$$

Additionally, (7.144) is equivalent to

$$\Sigma_{E^{XA}} = \Sigma_{E^X} + f_\infty \left( \Sigma_{A^U} \right) + g_\infty \left( \Sigma_{A^X} \right), \quad (7.145)$$

where the functions are as defined in (6.98) and (7.43), respectively. Additionally, $\Sigma_{E^X}$ is the limit value of the nominal system error, as seen in (D.23). We denote these limit vales as $\widetilde{\Sigma}_{A^U} = f_\infty \left( \Sigma_{A^U} \right)$ and $\widetilde{\Sigma}_{A^X} = g_\infty \left( \Sigma_{A^U} \right)$. These variables are wholly characterised by their respective covariance matrices $\Sigma_{A^U}$ and $\Sigma_{A^X}$. Revisiting the system cost, (7.114), it is known that

$$\begin{aligned} J_A^* = & \max_{\{\Sigma_{A^U} \in S_+^m, \Sigma_{A^X} \in S_+^n\}} \Big\{ \operatorname{tr} \left( \mathbf{P} \Sigma_W \right) + \operatorname{tr} \left( \left( \mathbf{F}^{\mathsf{T}} \mathbf{P} \mathbf{F} - \mathbf{P} + \mathbf{Q}_X \right) \Sigma_{E^{XA}} \right) \\ & + \operatorname{tr} \left( \left( \mathbf{G}^{\mathsf{T}} \mathbf{P} \mathbf{G} + \mathbf{Q}_U \right) \Sigma_{E^{UA}} \right) \Big\} \quad (7.146) \\ = & \max_{\{\Sigma_{A^U} \in S_+^m, \Sigma_{A^X} \in S_+^n\}} \Big\{ \operatorname{tr} \left( \mathbf{P} \Sigma_W \right) + \operatorname{tr} \Big( \Big( \mathbf{F}^{\mathsf{T}} \mathbf{P} \mathbf{F} - \mathbf{P} + \mathbf{Q}_X \Big) \Sigma_{E^{XA}} \Big) \\ & + \operatorname{tr} \Big( \Big( \mathbf{G}^{\mathsf{T}} \mathbf{P} \mathbf{G} + \mathbf{Q}_U \Big) \Sigma_{E^U} \Big) + \operatorname{tr} \Big( \Big( \mathbf{G}^{\mathsf{T}} \mathbf{P} \mathbf{G} + \mathbf{Q}_U \Big) \Sigma_{A^U} \Big) \Big\} \quad (7.147) \\ = & \max_{\{\Sigma_{A^U} \in S_+^m, \Sigma_{A^X} \in S_+^n\}} \Big\{ \operatorname{tr} \left( \mathbf{P} \Sigma_W \right) + \operatorname{tr} \Big( \Big( \mathbf{F}^{\mathsf{T}} \mathbf{P} \mathbf{F} - \mathbf{P} + \mathbf{Q}_X \Big) \Sigma_{E^X} \Big) \\ & + \operatorname{tr} \Big( \Big( \mathbf{G}^{\mathsf{T}} \mathbf{P} \mathbf{G} + \mathbf{Q}_U \Big) \Sigma_{E^U} \Big) + \operatorname{tr} \Big( \Big( \mathbf{G}^{\mathsf{T}} \mathbf{P} \mathbf{G} + \mathbf{Q}_U \Big) \Sigma_{A^U} \Big) \\ & + \operatorname{tr} \Big( \Big( \mathbf{F}^{\mathsf{T}} \mathbf{P} \mathbf{F} - \mathbf{P} + \mathbf{Q}_X \Big) \Big( \widetilde{\Sigma}_{A^X} + \widetilde{\Sigma}_{A^U} \Big) \Big) \Big\}. \quad (7.148) \end{aligned}$$

The above optimal control cost whilst under attack is represented as the attacked optimal control seen within Section 7.3 plus an additional term that depends on the covariance of $A_k^U$. This additional term is a direct result of not monitoring the actuation communication channel. This additional term is the error induced into the updated state estimate by not monitoring the actuation communication channel. Specifically, the operator is not able to

know exactly which input has entered the plant and therefore necessarily has an additional error in their updated state estimate. The optimisation of the attacker has been reduced to computing the optimisation problem

$$\begin{aligned}\max_{\{\Sigma_{A^U}\in S_+^m,\Sigma_{A^X}\in S_+^n\}} &\left\{\mathrm{tr}\Big(\Big(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F}-\mathbf{P}+\mathbf{Q}_X\Big)\Big(\widetilde{\Sigma}_{A^U}+\widetilde{\Sigma}_{A^X}\Big)+\Big(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G}+\mathbf{Q}_U\Big)\Sigma_{A^U}\Big)\right\},\\ \text{s.t. } \mathcal{D}\left(\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U}\parallel\mathcal{P}_{\mathscr{Z}}\right)\leq\delta_1 \quad &\text{and} \quad \mathcal{D}\left(\mathcal{P}_{\mathscr{Y}+\mathscr{A}^X}\parallel\mathcal{P}_{\mathscr{Y}}\right)\leq\delta_2.\end{aligned} \tag{7.149}$$

Note that all of the terms within the maximisation are either positive or non-negative definite. In the following section we provide analytic bounds for the solution of this optimisation problem and provide the exact solution in a simplified system setting.

## 7.6 Attack Analysis with no Auxiliary Channel

The optimal attack for the system lacking an auxiliary communication channel is different from the result derived within Section 7.4. This is seen through the fact that the induced cost depends on an additional parameter, namely, $\widetilde{\Sigma}_{A^U}$. The detection constraints however, remain the same as before. The simplified KL Divergence constraints are restated for ease of reading

$$\mathcal{D}\left(\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U}\parallel\mathcal{P}_{\mathscr{Z}}\right)=\frac{1}{2}\Big(\mathrm{tr}\left(\Sigma_Z^{-1}\Sigma_{A^U}\right)-\log\left|\mathbf{I}+\Sigma_Z^{-1}\Sigma_{A^U}\right|\Big), \tag{7.150a}$$

$$\mathcal{D}\left(\mathcal{P}_{\mathscr{Y}+\mathscr{A}^X}\parallel\mathcal{P}_{\mathscr{Y}}\right)=\frac{1}{2}\Big(\mathrm{tr}\left(\Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right)-\log\left|\mathbf{I}+\Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right|\Big). \tag{7.150b}$$

With the above constraints stated, it allows for the definition of the Lagrangian that corresponds to the system with no auxiliary communication channel. This is defined as

$$\begin{aligned}\mathscr{L}=&\,\mathrm{tr}\Big(\Big(\mathbf{F}^\mathsf{T}\mathbf{P}\mathbf{F}-\mathbf{P}+\mathbf{Q}_X\Big)\Big(\widetilde{\Sigma}_{A^X}+\widetilde{\Sigma}_{A^U}\Big)+\Big(\mathbf{G}^\mathsf{T}\mathbf{P}\mathbf{G}+\mathbf{Q}_U\Big)\Sigma_{A^U}\Big)\\ &+\frac{\lambda_1}{2}\left(\mathrm{tr}\left(\Sigma_Z^{-1}\Sigma_{A^U}\right)-\log\left|\mathbf{I}+\Sigma_Z^{-1}\Sigma_{A^U}\right|-2\delta_1\right)\\ &+\frac{\lambda_2}{2}\left(\mathrm{tr}\left(\Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right)-\log\left|\mathbf{I}+\Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right|-2\delta_2\right).\end{aligned} \tag{7.151}$$

Utilising the substitutions from the previous analysis section highlights where the differences between these two attack strategies arise

$$\begin{aligned}\mathscr{L} = \operatorname{tr}\left(\Delta^{PX}\widetilde{\Sigma}_{A^X} + \Delta^{P^U}\Sigma_{A^U} + \Delta^{PX}\widetilde{\Sigma}_{A^U}\right) + \frac{\lambda_1}{2}\left(\operatorname{tr}\left(\Sigma_Z^{-1}\Sigma_{A^U}\right) - \log\left|\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right| - 2\delta_1\right) \\ + \frac{\lambda_2}{2}\left(\operatorname{tr}\left(\Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right) - \log\left|\mathbf{I} + \Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right| - 2\delta_2\right).\end{aligned} \tag{7.152}$$

In the above the differences arise from the additional $\Delta^{PX}\widetilde{\Sigma}_{A^U}$ term. Due to the fact that there are no changes to the KL divergence constraints, or indeed any change to the terms that depends on $\widetilde{\Sigma}_{A^X}$, three derivatives remain the same. Specifically, the two derivatives of (7.152) with respect to each of the variables $\lambda_1$ and $\lambda_2$ defined as

$$\frac{\partial\mathscr{L}}{\partial\lambda_1} = \frac{1}{2}\operatorname{tr}\left(\Sigma_Z^{-1}\Sigma_{A^U}\right) - \frac{1}{2}\log\left(\left|\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right|\right) - \delta_1, \tag{7.153}$$

and

$$\frac{\partial\mathscr{L}}{\partial\lambda_2} = \frac{1}{2}\operatorname{tr}\left(\Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right) - \frac{1}{2}\log\left(\left|\mathbf{I} + \Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right|\right) - \delta_2, \tag{7.154}$$

respectively. Additionally, the Lagrangian derivative with respect to the attack statistic $\widetilde{\Sigma}_{A^X}$ remains as

$$\widetilde{\Sigma}_{A^X} = \left[\frac{2}{\lambda_2}\Delta^{PX} + \Sigma_V^{-1}\right]^{-1} - \Sigma_V, \tag{7.155}$$

when this derivative of the Lagrangian is set equal to $\mathbb{0}$ and rearranged. Furthermore, due to the separation between the attack construction for each communication channel the attack strategy on the sensory communication channel remains as seen in Section 7.4. Namely, the lower bound on the sensory communication channel remains as

$$\widetilde{\Sigma}_{A^X} \geq \Sigma_V\left[\sqrt[m]{\left|\Sigma_V^{-1}\Delta^{PX^{-1}}\right|(e^{2\delta_1+m} - 2^m)}\Delta^{PX}\Sigma_V + \mathbf{I}\right]^{-1} - \Sigma_V, \tag{7.156}$$

and the optimal solution of the system with a scalar $Y_k$ is

$$\widetilde{\Sigma}_{A^X} = -\Sigma_V \; W_{-1}\left(-\frac{1}{e^{2\delta_2+1}}\right) - \Sigma_V. \tag{7.157}$$

With the above results given all that remains is the derivation of the optimal attack for the actuation channel. The first thing to be tackled is the derivative of the Lagrangian with respect to $\Sigma_{A^U}$. With that in mind, from Lemma 19 all of the functions derivatives are known other that the term $\text{tr}\left(\Delta^{P^X}\widetilde{\Sigma}_{A^U}\right)$. Specifically, the derivative is

$$\begin{aligned}\frac{\partial \mathscr{L}}{\partial \Sigma_{A^U}} = 2\Delta^{P^U} + \lambda_1\Sigma_Z^{-1} - \lambda_1\left[\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right]^{-1}\Sigma_Z^{-1} + \frac{\partial \text{tr}\left(\Delta^{P^X}\widetilde{\Sigma}_{A^U}\right)}{\Sigma_{A^U}} \\ -\mathbf{I}\odot\left[\Delta^{P^U} + \frac{\lambda_1}{2}\Sigma_Z^{-1} - \frac{\lambda_1}{2}\left[\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right]^{-1}\Sigma_Z^{-1}\right],\end{aligned} \tag{7.158}$$

Naturally, this derivative is non-trivial due to the fact that $\widetilde{\Sigma}_{A^U}$ is a function of $\Sigma_{A^U}$. However, it should be noted that all terms within $\widetilde{\Sigma}_{A^U}$ are linear in $\Sigma_{A^U}$. This allows for the following transformation

$$\text{tr}\left(\mathbf{A}\widetilde{\Sigma}_{A^U}\right) = \text{tr}\left(\mathbf{A} f_\infty\left(\Sigma_{A^U}\right)\right) \tag{7.159}$$

$$= \text{tr}\left(\mathbf{A}\left[\sum_{i=0}^{\infty}\left(\widetilde{\mathbf{L}}_{\infty\text{-}i}\mathbf{F}\right)^i \widetilde{\mathbf{L}}_{\infty\text{-}i}\mathbf{G}\Sigma_{A^U}\mathbf{G}^\mathsf{T}\widetilde{\mathbf{L}}_{\infty\text{-}i}^\mathsf{T}\left(\widetilde{\mathbf{L}}_{\infty\text{-}i}\mathbf{F}\right)^{i^\mathsf{T}}\right]\right) \tag{7.160}$$

$$= \text{tr}\left(\sum_{i=0}^{\infty}\mathbf{A}\left(\widetilde{\mathbf{L}}_{\infty\text{-}i}\mathbf{F}\right)^i \widetilde{\mathbf{L}}_{\infty\text{-}i}\mathbf{G}\Sigma_{A^U}\mathbf{G}^\mathsf{T}\widetilde{\mathbf{L}}_{\infty\text{-}i}^\mathsf{T}\left(\widetilde{\mathbf{L}}_{\infty\text{-}i}\mathbf{F}\right)^{i^\mathsf{T}}\right) \tag{7.161}$$

$$= \text{tr}\left(\sum_{i=0}^{\infty}\mathbf{G}^\mathsf{T}\widetilde{\mathbf{L}}_{\infty\text{-}i}^\mathsf{T}\left(\widetilde{\mathbf{L}}_{\infty\text{-}i}\mathbf{F}\right)^{i^\mathsf{T}}\mathbf{A}\left(\widetilde{\mathbf{L}}_{\infty\text{-}i}\mathbf{F}\right)^i \widetilde{\mathbf{L}}_{\infty\text{-}i}\mathbf{G}\Sigma_{A^U}\right) \tag{7.162}$$

$$= \text{tr}\left(h_\infty\left(\mathbf{A}\right)\Sigma_{A^U}\right), \tag{7.163}$$

where we slightly abuse notation to use $\infty$ to represent the time step at which the function $h_k\left(\Sigma_{A^U}\right)$ has converged to steady state. From the above definition the function $h_k\left(\mathbf{A}\right)$ is defined as

$$h_k\left(\mathbf{A}\right) = \sum_{i=0}^{k}\mathbf{G}^\mathsf{T}\widetilde{\mathbf{L}}_{k\text{-}i}^\mathsf{T}\left(\widetilde{\mathbf{L}}_{k\text{-}i}\mathbf{F}\right)^{i^\mathsf{T}}\mathbf{A}\left(\widetilde{\mathbf{L}}_{k\text{-}i}\mathbf{F}\right)^i \widetilde{\mathbf{L}}_{k\text{-}i}\mathbf{G}, \tag{7.164}$$

and is the mapping $h_k(\mathbf{A}) : \mathbb{M}^n \to \mathbb{M}^m$. Note that this summation is symmetric. With the transformation shown in (7.163) the derivative in (7.158) becomes

$$\begin{aligned}\frac{\partial \mathscr{L}}{\partial \Sigma_{A^U}} &= 2\Delta^{P^U} + \lambda_1 \Sigma_Z^{-1} - \lambda_1 \left[\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right]^{-1} \Sigma_Z^{-1} + \frac{\partial \mathrm{tr}\left(h_\infty\left(\Delta^{P^X}\right)\Sigma_{A^U}\right)}{\Sigma_{A^U}} \\ &\quad -\mathbf{I} \odot \left[\Delta^{P^U} + \frac{\lambda_1}{2}\Sigma_Z^{-1} - \frac{\lambda_1}{2}\left[\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right]^{-1}\Sigma_Z^{-1}\right], \qquad (7.165) \\ &= 2\Delta^{P^U} + \lambda_1 \Sigma_Z^{-1} - \lambda_1 \left[\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right]^{-1} \Sigma_Z^{-1} + 2h_\infty\left(\Delta^{P^X}\right) \\ &\quad -\mathbf{I} \odot \left[\Delta^{P^U} + h_\infty\left(\Delta^{P^X}\right) + \frac{\lambda_1}{2}\Sigma_Z^{-1} - \frac{\lambda_1}{2}\left[\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right]^{-1}\Sigma_Z^{-1}\right]. \qquad (7.166)\end{aligned}$$

As in the previous case the above is able to be simplified through use of Lemma 20. In doing so this yields

$$\begin{aligned}\frac{2}{\lambda_1}\left(\Delta^{P^U} + h_\infty\left(\Delta^{P^X}\right)\right) + \Sigma_Z^{-1} &= \left[\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right]^{-1}\Sigma_Z^{-1} \qquad (7.167) \\ \frac{2}{\lambda_1}\left(\Delta^{P^U} + h_\infty\left(\Delta^{P^X}\right)\right) + \Sigma_Z^{-1} &= \left[\left(\Sigma_Z^{-1}\right)\left(\Sigma_Z + \Sigma_{A^U}\right)\right]^{-1}\Sigma_Z^{-1}, \qquad (7.168) \\ &= \left[\Sigma_Z + \Sigma_{A^U}\right]^{-1}\Sigma_Z\Sigma_Z^{-1} \qquad (7.169) \\ &= \left[\Sigma_Z + \Sigma_{A^U}\right]^{-1}. \qquad (7.170)\end{aligned}$$

Solving the above for $\Sigma_{A^U}$ gives

$$\begin{aligned}\mathbf{I} &= \left[\frac{2}{\lambda_1}\left(\Delta^{P^U} + h_\infty\left(\Delta^{P^X}\right)\right) + \Sigma_Z^{-1}\right]\left[\Sigma_Z + \Sigma_{A^U}\right], \qquad (7.171) \\ \Sigma_{A^U} &= \left[\frac{2}{\lambda_1}\left(\Delta^{P^U} + h_\infty\left(\Delta^{P^X}\right)\right) + \Sigma_Z^{-1}\right]^{-1} - \Sigma_Z, \qquad (7.172) \\ \Sigma_{A^U} &= \left[\frac{2}{\lambda_1}\left(\Delta^{P^U} + h_\infty\left(\Delta^{P^X}\right)\right) + \Sigma_Z^{-1}\right]^{-1} - \Sigma_Z, \qquad (7.173) \\ \Sigma_{A^U} &= \Sigma_Z\left[\frac{2}{\lambda_1}\left(\Delta^{P^U} + h_\infty\left(\Delta^{P^X}\right)\right)\Sigma_Z + \mathbf{I}\right]^{-1} - \Sigma_Z, \qquad (7.174)\end{aligned}$$

Note that the above solution is identical to the solution in (7.71) with the substitution of $\Delta^{P^U}$ for the sum $\Delta^{P^U} + h_\infty\left(\Delta^{P^X}\right)$. Therefore, with that in mind, the previous results follow trivially. Namely, the lower bound on the optimal attack for the actuation

communication channel becomes

$$\Sigma_{A^U} \geq \Sigma_Z \left[ \sqrt[m]{\left|\Sigma_Z^{-1}\left(\Delta^{P^U} + h_\infty\left(\Delta^{P^X}\right)\right)\right|(e^{2\delta_1+m} - 2^m)}\left(\Delta^{P^U} + h_\infty\left(\Delta^{P^X}\right)\right)\Sigma_Z + \mathbf{I}\right]^{-1} - \Sigma_Z. \tag{7.175}$$

Similarly, the optimal solution for a system with a single actuator is

$$\Sigma_{A^U} = -\Sigma_Z \; W_{-1}\left(-\frac{1}{e^{2\delta_1+1}}\right) - \Sigma_Z. \tag{7.176}$$

Note that due to the replacement of $\Delta^{P^U}$ with the sum $\Delta^{P^U} + h_\infty\left(\Delta^{P^X}\right)$ the covariance is scaled with terms relating to both of the commination channels which necessarily creates a difference in attack structure for all $h_\infty\left(\Delta^{P^X}\right) \neq \mathbb{0}$. From the quadratic nature of the function $h_\infty(\cdot)$ and the structure of $\Delta^{P^X}$ we expect this term to be strictly positive for most use cases. Additionally, the solution with a single actuator is identical to the previous solution, as seen in (7.104). This shows that the optimal attack strategy is independent of the system structure, and only depends on the communication channel statistics, namely, $\Sigma_Z$. However, as seen in (7.175), the lower bound is changed.

One important point should be made here. Although the optimal attacks for each system structure are identical, the induced costs are not. This is due to the fact that the system with no auxiliary communication channel has an additional cost term associated with the attack variable that is non-negative definite. Meaning that for any non-zero attack variable the cost increase caused by the attack will be strictly grater than the cost of the system with a perfect auxiliary communication channel. Note that this statement holds irrespective of any cost differences prior to the attack implementation. Namely, it is already known that, from Theorem 18, the system without an auxiliary communication channel has a higher optimal cost under nominal conditions. In addition to this higher nominal operating cost, the system without an auxiliary communication channel has a cost function that is more sensitive to data injection attacks. This effect increases the cost associated with no auxiliary communication channel even further. Therefore, the presence

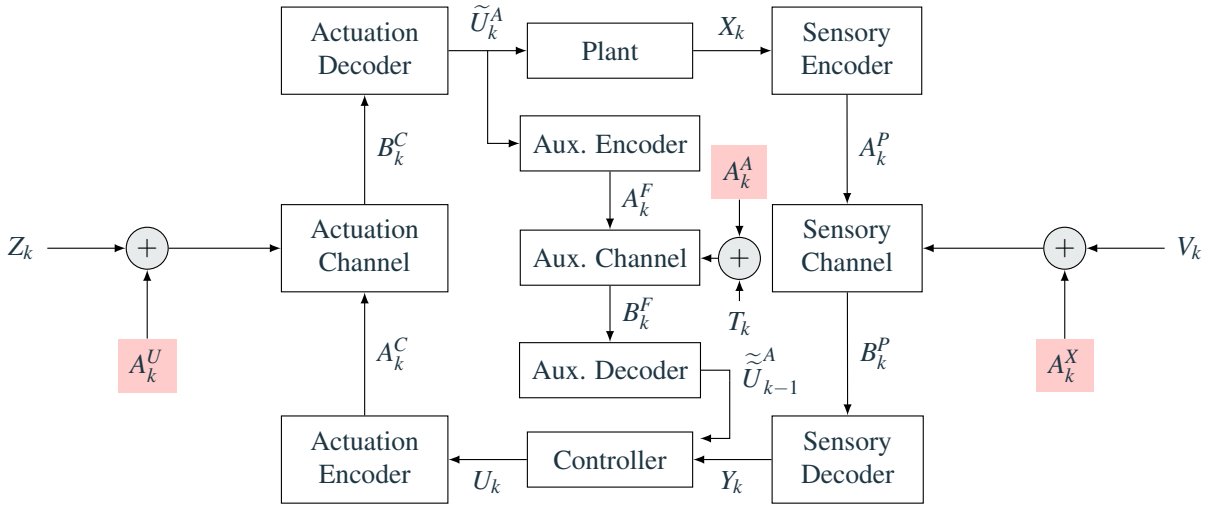


Fig. 7.6 Attack implementation on all communication channels implemented in a control system, where there is transmission of the variable $\widetilde{U}_k$ over imperfect auxiliary communication channel.

of an auxiliary communication channel not only reduces the control cost, but also acts as an attack mitigation tool. The following section discusses the attack construction for a system with an imperfect auxiliary communication channel.

## 7.7 Attack Construction with an Imperfect Auxiliary Channel

As is seen from Theorem 17 the effect of noise in the actuation communication channel is removed from the state estimate even with an imperfect auxiliary communication channel. This is achieved at the cost of introducing an additional error from the imperfect auxiliary communication channel. However, the introduction of an additional imperfect communication channel allows the possibility of another attack vector for the attacker. We denote this new attack vector $A_k^A$ and is once again an additive IID Gaussian variable with mean $\mathbf{0}$ and covariance $\Sigma_{A^A}$. This is depicted in Fig.7.6.

Due to the introduction of the additional attack vector the information sets require redefinition. The information sets of the system with an imperfect auxiliary communication

channel while under attack is defined as

$$\mathscr{P}_k^E = \left\{ X_k, A_{k-1}^P, B_{k-1}^P, \widetilde{U}_{k-1}^A, \mathscr{P}_{k-1}^E \right\}, \tag{7.177a}$$

$$\mathscr{P}_k^D = \left\{ B_k^P, Y_{k-1}, U_{k-1}, \widetilde{\widetilde{U}}_{k-1}^A, \mathscr{P}_{k-1}^D \right\}, \tag{7.177b}$$

$$\mathscr{C}_k^E = \left\{ Y_k, B_k^P, U_k, A_{k-1}^C, B_{k-1}^C, \widetilde{\widetilde{U}}_{k-1}^A, \mathscr{C}_{k-1}^E \right\}, \tag{7.177c}$$

$$\mathscr{C}_k^D = \left\{ B_k^C, \widetilde{U}_{k-1}^A, \mathscr{C}_{k-1}^D \right\}, \tag{7.177d}$$

where $\widetilde{\widetilde{U}}_k^A$ is the random variable at the output of the imperfect auxiliary communication channel under attack. Due to the inclusion of $U_k$ within $\mathscr{P}_k^D$ there is still separation of optimal control and estimation for the operator.

### 7.7.1 Optimal Control with Imperfect Auxiliary Channel while under Attack

In order to assess the impact of the attack within the system, the expected value of a LQG cost function is once again adopted. The LQG cost is defined as

$$J = \limsup_{N\to\infty} \frac{1}{N} \mathbb{E}\left[ \sum_{k=0}^{N-1} X_k^{\mathsf{T}} \mathbf{Q}_X X_k + \widetilde{U}_k^{A\mathsf{T}} \mathbf{Q}_U \widetilde{U}_k^A \right]. \tag{7.178}$$

Once again the cost function includes the variable $\widetilde{U}_k^A$ and not the uncorrupted input signal $U_k$ or the variable $\widetilde{\widetilde{U}}_k^A$. The optimal cost function for the operator of this system is defined as

$$J^* = \min_{\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N} \in \mathscr{U}} \left\{ \limsup_{N\to\infty} \frac{1}{N} \mathbb{E}\left[ \sum_{k=0}^{N-1} X_k^{\mathsf{T}} \mathbf{Q}_X X_k + \widetilde{U}_k^{A\mathsf{T}} \mathbf{Q}_U \widetilde{U}_k^A \right] \right\}. \tag{7.179}$$

From this point the attacker is able to define their objective. Namely the objective function of the attacker is defined as

$$J_A^* = \max_{\Sigma_{AX}, \Sigma_{AU}, \Sigma_{AA}} \left\{ \min_{\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N} \in \mathscr{U}} \left\{ \limsup_{N\to\infty} \frac{1}{N} \mathbb{E}\left[ \sum_{k=0}^{N-1} X_k^{\mathsf{T}} \mathbf{Q}_X X_k + \widetilde{U}_k^{A\mathsf{T}} \mathbf{Q}_U \widetilde{U}_k^A \right] \right\} \right\}. \tag{7.180}$$

Note the inclusion of the third attack variable $\Sigma_{A^A}$. As before, the operator minimisation is first simplified before the attacker performs their maximisation. Which leads to the following theorem.

**Theorem 24.** *The updated state estimate*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_k\left(Y_k-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)\right), \tag{7.181}$$

*is equivalent to the state space system,*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_k+\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right), \tag{7.182a}$$

$$\widehat{Y}_k=\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{7.182b}$$

*where* $\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right)$ *is defined as*

$$\overline{\overline{W}}^{A}\left(\mathscr{P}_{k}^{D}\right)=\mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_{k}^{X^A}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}\left(T_k+A_{k}^{A}\right)+W_k\right)+\mathbf{L}_k\left(V_{k+1}+A_{k+1}^{X}\right). \tag{7.183}$$

*Proof.* The proof is moved to Appendix E.6.

Proving that the process noise of the above state space system is uncorrelated is a trivial extension of previous results. Specifically, because the process noise produced from Theorem 17 is identical to the process noise within Lemma 17 with the addition of an IID vectorial Gaussian variable. Therefore, all of the variables within (E.67) are uncorrelated.

Before proceeding with the optimal cost first the updated sensor error is defined

$$\begin{aligned}E_{k+1}^{X^A}\left(\mathscr{P}_{k+1}^{D}\right)&=X_{k+1}-\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)\\&=\mathbf{F}X_k+\mathbf{G}U_k+\widetilde{W}_{k}^{A}-\left(\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_k+\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right)\right)\\&=\mathbf{F}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right)+\widetilde{W}_{k}^{A}-\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right).\end{aligned} \tag{7.184}$$

The optimal cost of the partially observed system is defined as

$$\begin{aligned} J_A^* &= \max_{\Sigma_{A^X}, \Sigma_{A^U}, \Sigma_{AA}} \left\{ \min_{\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N} \in \mathcal{U}} \left\{ \limsup_{N\to\infty} \frac{1}{N} \mathbb{E}\left[ \sum_{k=0}^{N-1} X_k^{\mathsf{T}} \mathbf{Q}_X X_k + \widetilde{U}_k^{A\mathsf{T}} \mathbf{Q}_U \widetilde{U}_k^A \right] \right\} \right\} \\ &= \max_{\Sigma_{A^X}, \Sigma_{A^U}, \Sigma_{AA}} \left\{ \min_{\mathcal{P}_{U_0,\ldots,U_N|Y_0,\ldots,Y_N} \in \mathcal{U}} \left\{ \limsup_{N\to\infty} \frac{1}{N} \left( \sum_{k=0}^{N} \mathbb{E}\left[ \widehat{X}_k^{\mathsf{T}} \mathbf{Q}_X \widehat{X}_k + U_k^{\mathsf{T}} \mathbf{Q}_U U_k \right] \right.\right.\right. \\ &\qquad \left.\left.\left. + \mathbb{E}\left[ E_k^{X^A}\left(\mathscr{P}_k^D\right) \mathbf{Q}_X E_k^{X^A}\left(\mathscr{P}_k^D\right) \right] + \mathbb{E}\left[ E_k^{U^A{}^{\mathsf{T}}} \mathbf{Q}_U E_k^{U^A} \right] \right) \right\} \right\}. \end{aligned} \tag{7.185}$$

The first term of (7.185) is of the correct form to invoke Theorem 14, with a change of variables. Therefore, the optimal linear control law for the new control system is

$$U_k^* = -\mathbf{K}\widehat{X}_k\left(\mathscr{P}_k^D\right), \tag{7.186}$$

with associated optimal cost

$$\operatorname{tr}\left(\mathbf{P}\Sigma_{\overline{\overline{W}}^A}\right), \tag{7.187}$$

where the optimal gain is independent of the system, and $\mathbf{K}$ is defined as the optimal gain matrix according to (6.5). It is assumed that the error covariances converge to the fixed values. Specifically the time varying covariances,

$$\Sigma_{E_k^{U^A}} = \mathbb{E}\left[ E_{k+1}^{U^A{}^{\mathsf{T}}} E_{k+1}^{U^A} \middle| \mathscr{P}_{k+1}^D \right] \tag{7.188}$$

$$= \Sigma_Z + \Sigma_{A^U} = \Sigma_{E^{U^A}}, \tag{7.189}$$

$$\Sigma_{E_{k+1}^{X^A}\left(\mathscr{P}_{k+1}^D\right)} = \mathbb{E}\left[ E_{k+1}^{X^A}\left(\mathscr{P}_{k+1}^D\right)^{\mathsf{T}} E_{k+1}^{X^A}\left(\mathscr{P}_{k+1}^D\right) \middle| \mathscr{P}_{k+1}^D \right] \tag{7.190}$$

$$\begin{aligned} &= \widetilde{\mathbf{L}}_k^{\mathsf{T}} \left( \mathbf{F}^{\mathsf{T}} \Sigma_{E_k^{X^A}\left(\mathscr{P}_k^D\right)} \mathbf{F} + \mathbf{G}^{\mathsf{T}} \left( \Sigma_T + \Sigma_{A^A} \right) \mathbf{G} + \Sigma_W \right) \widetilde{\mathbf{L}}_k \\ &\qquad + \mathbf{L}_k \left( \Sigma_V + \Sigma_{A^X} \right) \mathbf{L}_k^{\mathsf{T}}, \end{aligned} \tag{7.191}$$

are assumed to have converged to their solutions. Additionally, the Kalman filter gain $\mathbf{L}_k$ is also assumed to have converged to its steady state value $\mathbf{L}$. These steady state covariance

matrices are defined such that

$$\Sigma_{E^{U^A}} = \Sigma_{E^{U^A}} = \Sigma_{A^U} + \Sigma_Z, \tag{7.192}$$

$$\Sigma_{E^{X^A}} = \tilde{\mathbf{L}}^{\mathsf{T}} \left( \mathbf{F}^{\mathsf{T}} \Sigma_{E^{X^A}} \mathbf{F} + \mathbf{G}^{\mathsf{T}} \left( \Sigma_T + \Sigma_{A^A} \right) \mathbf{G} + \Sigma_W \right) \tilde{\mathbf{L}} + \mathbf{L} \left( \Sigma_V + \Sigma_{A^X} \right) \mathbf{L}^{\mathsf{T}}. \tag{7.193}$$

The above covariances are able to be split into additive terms that separate the covariance of the nominal system error from the additional induced attack error is

$$\begin{aligned} \Sigma_{E^{X^A}} = \tilde{\mathbf{L}}^{\mathsf{T}} \left( \mathbf{F}^{\mathsf{T}} \Sigma_{E^X} \mathbf{F} + \mathbf{G}^{\mathsf{T}} \Sigma_T \mathbf{G} + \Sigma_W \right) \tilde{\mathbf{L}} + \mathbf{L} \Sigma_V \mathbf{L}^{\mathsf{T}} + g_\infty \left( \Sigma_{A^X} \right) \\ + f_\infty \left( \Sigma_{A^A} \right), \end{aligned} \tag{7.194}$$

$$\Sigma_{E^{X^A}} = \Sigma_{E^X} + g_\infty \left( \Sigma_{A^X} \right) + f_\infty \left( \Sigma_{A^A} \right), \tag{7.195}$$

where, $f_k(\mathbf{A})$ and $g_k(\mathbf{A})$ are defined in (6.98) and (7.43), respectively. We define the following matrices

$$\widetilde{\Sigma}_{A^X} = g_\infty \left( \Sigma_{A^X} \right), \tag{7.196}$$

$$\widetilde{\Sigma}_{A^A} = f_\infty \left( \Sigma_{A^A} \right). \tag{7.197}$$

Naturally, the statistics of the variables $\widetilde{\Sigma}_{A^X}$ and $\widetilde{\Sigma}_{A^X}$ are wholly determined by the attack statistics $\Sigma_{A^X}$ and $\Sigma_{A^X}$, respectively. Under the assumption that all of the covariances

have converged, the optimal system cost is written as

$$J^* = \mathrm{tr}\left(\mathbf{P}\Sigma_{\overline{\overline{W}}^A}\right) + \mathrm{tr}\left(\mathbf{Q}_X\Sigma_{E^{X^A}}\right) + \mathrm{tr}\left(\mathbf{Q}_U\Sigma_{E^{A^U}}\right) \tag{7.198}$$

$$= \mathrm{tr}\left(\mathbf{P}\mathbb{E}\left[\overline{\overline{W}}_k^A\ \overline{\overline{W}}_k^{A\mathsf{T}}\right]\right) + \mathrm{tr}\left(\mathbf{Q}_X\Sigma_{E^{X^A}}\right) + \mathrm{tr}\left(\mathbf{Q}_U\Sigma_{E^{U^A}}\right) \tag{7.199}$$

$$= \mathrm{tr}\left(\mathbf{P}\mathbb{E}\left[\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \widetilde{W}_k^A - E_{k+1}^{X^A}\left(\mathscr{P}_{k+1}^D\right)\right)\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \widetilde{W}_k^A - E_{k+1}^{X^A}\left(\mathscr{P}_{k+1}^D\right)\right)^{\mathsf{T}}\right]\right)$$
$$+\mathrm{tr}\left(\mathbf{Q}_X\Sigma_{E^{X^A}}\right) + \mathrm{tr}\left(\mathbf{Q}_U\Sigma_{E^{U^A}}\right) \tag{7.200}$$

$$= \mathrm{tr}\left(\mathbf{P}\left(\mathbf{F}\Sigma_{E^{X^A}}\mathbf{F}^{\mathsf{T}} + \mathbf{G}\Sigma_{E^{U^A}}\mathbf{G}^{\mathsf{T}} + \Sigma_W - \Sigma_{E^{X^A}}\right)\right) + \mathrm{tr}\left(\mathbf{Q}_X\Sigma_{E^{X^A}}\right)$$
$$+\mathrm{tr}\left(\mathbf{Q}_U\Sigma_{E^{U^A}}\right) \tag{7.201}$$

$$= \mathrm{tr}\left(\mathbf{P}\Sigma_W\right) + \mathrm{tr}\left(\left(\mathbf{F}^{\mathsf{T}}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^{X^A}}\right)$$
$$+\mathrm{tr}\left(\left(\mathbf{G}^{\mathsf{T}}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{E^{U^A}}\right) \tag{7.202}$$

$$= \mathrm{tr}\left(\mathbf{P}\Sigma_W\right) + \mathrm{tr}\left(\left(\mathbf{F}^{\mathsf{T}}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\left(\Sigma_{E^X} + \widetilde{\Sigma}_{A^X} + \widetilde{\Sigma}_{A^A}\right)\right)$$
$$+\mathrm{tr}\left(\left(\mathbf{G}^{\mathsf{T}}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\left(\Sigma_{E^U} + \Sigma_{A^U}\right)\right) \tag{7.203}$$

$$= \mathrm{tr}\left(\mathbf{P}\Sigma_W\right) + \mathrm{tr}\left(\left(\mathbf{F}^{\mathsf{T}}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\Sigma_{E^X}\right) + \mathrm{tr}\left(\left(\mathbf{G}^{\mathsf{T}}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_Z\right)$$
$$+\mathrm{tr}\left(\left(\mathbf{G}^{\mathsf{T}}\mathbf{P}\mathbf{G} + \mathbf{Q}_U\right)\Sigma_{A^U}\right) + \mathrm{tr}\left(\left(\mathbf{F}^{\mathsf{T}}\mathbf{P}\mathbf{F} - \mathbf{P} + \mathbf{Q}_X\right)\left(\widetilde{\Sigma}_{A^X} + \widetilde{\Sigma}_{A^A}\right)\right), \tag{7.204}$$

where in line (7.200) the relation (7.184) is substituted for $\overline{\overline{W}}_k^A$. It is seen in (7.204) that the cost function for a system operating over a noisy auxiliary communication channel while experiencing a data injection attack is split into five additive terms. As before, these terms correspond to the cost of optimal control, communication over the sensory communication channel, communication over the actuation communication channel, the induced cost of attack in the actuation communication channel, and the cost of the attack in the sensory communication channel and the auxiliary communication channel.

The above optimal control cost whilst under attack is represented as the optimal control cost with an imperfect auxiliary communication communication channel, plus terms that depend on the covariance of the attack variables. Specifically, the matrices $\Sigma_{A^U}$, $\widetilde{\Sigma}_{A^A}$, and $\widetilde{\Sigma}_{A^X}$. Which leads to the following theorem.

**Theorem 25.** *For the system in Theorem 24 the cost increase under attack is given by*

$$\max_{\{\Sigma_{A^U},\Sigma_{A^X},\Sigma_{A^A}\}} \Big\{ \mathrm{tr}\Big(\big(\mathbf{F}^{\mathsf{T}}\mathbf{P}\mathbf{F}-\mathbf{P}+\mathbf{Q}_X\big)\big(\widetilde{\Sigma}_{A^A}+\widetilde{\Sigma}_{A^X}\big)+\big(\mathbf{G}^{\mathsf{T}}\mathbf{P}\mathbf{G}+\mathbf{Q}_U\big)\Sigma_{A^U}\Big)\Big\},$$
$$\text{s.t. } \mathcal{D}\left(\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U} \parallel \mathcal{P}_{\mathscr{Z}}\right) \le \delta_1 \ , \quad \text{and} \quad \mathcal{D}\left(\mathcal{P}_{\mathscr{Y}+\mathscr{A}^X} \parallel \mathcal{P}_{\mathscr{Y}}\right) \le \delta_2.$$
$$\text{and} \qquad \mathcal{D}\left(\mathcal{P}_{\mathscr{T}+\mathscr{A}^A} \parallel \mathcal{P}_{\mathscr{T}}\right) \le \delta_3. \tag{7.205}$$

## 7.8 Attack Analysis with an Imperfect Auxiliary Communication Channel

As is seen in Section 7.7, the system cost depends on the covariance matrices $\Sigma_{A^U}$, $\widetilde{\Sigma}_{A^A}$, and $\widetilde{\Sigma}_{A^X}$. The KL-divergences are each simplified, as before, to yield the following

$$\mathcal{D}\left(\mathcal{P}_{\mathscr{Z}+\mathscr{A}^U} \parallel \mathcal{P}_{\mathscr{Z}}\right) = \frac{1}{2}\Big(\mathrm{tr}\left(\Sigma_Z^{-1}\Sigma_{A^U}\right) - \log\left|\mathbf{I}+\Sigma_Z^{-1}\Sigma_{A^U}\right|\Big), \tag{7.206}$$
$$\mathcal{D}\left(\mathcal{P}_{\mathscr{Y}+\mathscr{A}^X} \parallel \mathcal{P}_{\mathscr{Y}}\right) = \frac{1}{2}\Big(\mathrm{tr}\left(\Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right) - \log\left|\mathbf{I}+\Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right|\Big), \tag{7.207}$$
$$\mathcal{D}\left(\mathcal{P}_{\mathscr{T}+\mathscr{A}^A} \parallel \mathcal{P}_{\mathscr{T}}\right) = \frac{1}{2}\Big(\mathrm{tr}\left(\Sigma_T^{-1}\widetilde{\Sigma}_{A^A}\right) - \log\left|\mathbf{I}+\Sigma_T^{-1}\widetilde{\Sigma}_{A^A}\right|\Big). \tag{7.208}$$

From this the Lagrangian is constructed as

$$\begin{aligned}\mathscr{L} = \mathrm{tr}\Big(\big(\mathbf{F}^{\mathsf{T}}\mathbf{P}\mathbf{F}-\mathbf{P}+\mathbf{Q}_X\big)\widetilde{\Sigma}_{A^X}+\big(\mathbf{G}^{\mathsf{T}}\mathbf{P}\mathbf{G}+\mathbf{Q}_U\big)\Sigma_{A^U}\Big) \\ +\frac{\lambda_1}{2}\left(\mathrm{tr}\left(\Sigma_Z^{-1}\Sigma_{A^U}\right)-\log\left|\mathbf{I}+\Sigma_Z^{-1}\Sigma_{A^U}\right|-2\delta_1\right) \\ +\frac{\lambda_2}{2}\left(\mathrm{tr}\left(\Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right)-\log\left|\mathbf{I}+\Sigma_V^{-1}\widetilde{\Sigma}_{A^X}\right|-2\delta_2\right) \\ +\frac{\lambda_3}{2}\left(\mathrm{tr}\left(\Sigma_T^{-1}\widetilde{\Sigma}_{A^A}\right)-\log\left|\mathbf{I}+\Sigma_T^{-1}\widetilde{\Sigma}_{A^A}\right|-2\delta_3\right).\end{aligned} \tag{7.209}$$

Note the inclusion of the third constraint variable $\lambda_3$. In order to perform the derivatives of the Lagrangian seen in (7.209), Lemma 19 is utilised. Note that Lemma 19 is still valid for the Lagrangian in (7.209), however, it does require the lemma to be invoked three times as opposed to twice in the previous derivation. Additionally, it should be pointed

out that the additional terms that within (7.209) do not depend on any of the other terms. Therefore, the first derivative with respect to $\Sigma_{A^U}$ and $\widetilde{\Sigma}_{A^X}$ remain unchanged from (7.60) and (7.61), respectively. Namely, once these derivatives are set to zero and rearranged they are

$$\Sigma_{A^U} = \Sigma_Z \left[ \frac{2}{\lambda_1} \Delta^{P^U} \Sigma_Z + \mathbf{I} \right]^{-1} - \Sigma_Z, \tag{7.210}$$

$$\widetilde{\Sigma}_{A^X} = \left[ \frac{2}{\lambda_2} \Delta^{P^X} + \Sigma_V^{-1} \right]^{-1} - \Sigma_V. \tag{7.211}$$

This gives the solution of the first two derivatives of (7.209). The third derivative with respect to $\widetilde{\Sigma}_{A^A}$ is calculated in the very same fashion, and therefore yields

$$\widetilde{\Sigma}_{A^A} = \left[ \frac{2}{\lambda_3} \Delta^{P^X} + \Sigma_T^{-1} \right]^{-1} - \Sigma_T. \tag{7.212}$$

Similarly the derivatives with respect to each of the $\lambda_i$ variables is defined as

$$\frac{\partial \mathscr{L}}{\partial \lambda_1} = \frac{1}{2} \mathrm{tr} \left( \Sigma_Z^{-1} \Sigma_{A^U} \right) - \frac{1}{2} \log \left( \left| \mathbf{I} + \Sigma_Z^{-1} \Sigma_{A^U} \right| \right) - \delta_1, \tag{7.213}$$

$$\frac{\partial \mathscr{L}}{\partial \lambda_2} = \frac{1}{2} \mathrm{tr} \left( \Sigma_V^{-1} \widetilde{\Sigma}_{A^X} \right) - \frac{1}{2} \log \left( \left| \mathbf{I} + \Sigma_V^{-1} \widetilde{\Sigma}_{A^X} \right| \right) - \delta_2, \tag{7.214}$$

$$\frac{\partial \mathscr{L}}{\partial \lambda_3} = \frac{1}{2} \mathrm{tr} \left( \Sigma_T^{-1} \widetilde{\Sigma}_{A^A} \right) - \frac{1}{2} \log \left( \left| \mathbf{I} + \Sigma_T^{-1} \widetilde{\Sigma}_{A^A} \right| \right) - \delta_3. \tag{7.215}$$

Due to the separation in the channels the optimal attack strategy remains as before for the sensory and the actuation communication channels. With a change of variables the results presented for each of the constraints is equivalent. Therefore, the lower bound on $\lambda_3$ is

$$\sqrt[m]{\left| \Sigma_T^{-1} \Delta^{P^{X^{-1}}} \right| (e^{2\delta_3 + m} - 2^m)} \geq \frac{2}{\lambda_3}. \tag{7.216}$$

Substituting the bound in (7.216) for $\frac{2}{\lambda_3}$ back into the critical points of $\Sigma_{A^A}$, namely (7.212), gives the following bound for the optimal stealthy attack

$$\widetilde{\Sigma}_{A^A} \geq \Sigma_T \left[ \sqrt[m]{\left| \Sigma_T^{-1} \Delta^{P^{X^{-1}}} \right| (e^{2\delta_3 + m} - 2^m)} \Delta^{P^X} \Sigma_T + \mathbf{I} \right]^{-1} - \Sigma_T. \tag{7.217}$$

Therefore the resulting bounds for all three attack variables are

$$\Sigma_{A^U} \geq \Sigma_Z \left[ \sqrt[m]{\left| \Sigma_Z^{-1} \Delta^{P^{U^{-1}}} \right| (e^{2\delta_1 + m} - 2^m) \Delta^{P^U} \Sigma_Z + \mathbf{I}} \right]^{-1} - \Sigma_Z, \tag{7.218a}$$

$$\widetilde{\Sigma}_{A^X} \geq \Sigma_V \left[ \sqrt[m]{\left| \Sigma_V^{-1} \Delta^{P^{X^{-1}}} \right| (e^{2\delta_2 + m} - 2^m) \Delta^{P^X} \Sigma_V + \mathbf{I}} \right]^{-1} - \Sigma_V, \tag{7.218b}$$

$$\widetilde{\Sigma}_{A^A} \geq \Sigma_T \left[ \sqrt[m]{\left| \Sigma_T^{-1} \Delta^{P^{X^{-1}}} \right| (e^{2\delta_3 + m} - 2^m) \Delta^{P^X} \Sigma_T + \mathbf{I}} \right]^{-1} - \Sigma_T, \tag{7.218c}$$

The inequalities in (7.218a), (7.218c), and (7.218b) are a lower bound on the attack strategy for the communication channels for a multidimensional Gaussian data injection attack in each communication channel. As seen in all three of these bounds there is a separation between the optimal attack on each communication channel. Specifically, due to the disconnect between optimal attacks, the optimisation of each attack is able to be considered separately. So, an attacker that only has access to a single communication channel employs the same attack strategy on a given communication channel as an attacker with access to all communication channels.

### 7.8.1 Single Actuator System

As before the optimal attack for each communication channel can be solved exactly. The reduction of the system is as before, namely, such that $U_k \in \mathbb{R}$ and $Y_k \in \mathbb{R}$. This is due to the fact that the dimensionality of the auxiliary communication channel is determined by the magnitude of $m$. Note that, as before, due to the separation between the attacks, the optimal attack for each communication channel is still solved separately. Due to this, the optimal attack for the actuation and sensory communication channel remain as before. The derivation remains identical to the previous derivations and it is found that the optimal attack on the auxiliary communication channel is

$$\widetilde{\Sigma}_{A^A} = -\Sigma_T \; W_{-1}\left( -\frac{1}{e^{2\delta_3 + 1}} \right) - \Sigma_T. \tag{7.219}$$

Due to the separation between the attack constructions in each communication channel, any combination of these attack constructions are applicable for the corresponding system.

It should be noted that due to the fact that the attack strategy on the actuation and sensory communication channel is identical to that in Section 7.4. If there is no attack performed on the auxiliary communication channel then the cost increase induced by the attack is identical to the cost induced by the perfect auxiliary communication channel attack. Additionally, this cost increase will be bounded inside of the cost increase by both of the previous attacks, provided that $\widetilde{\Sigma}_{A^U} \succ \widetilde{\Sigma}_{A^A}$. If $\delta_3$ is such that $\widetilde{\Sigma}_{A^A} \succ \widetilde{\Sigma}_{A^U}$ then the induced cost by the attack on the imperfect auxiliary communication channel is greater than both of the previous optimal attack constructions.

## 7.9 Chapter Conclusion

This chapter has fully characterised the Gaussian data-injection attack construction within a control system. Namely, we have given the solution of the optimal covariance matrix for a scalar communication channel, in addition to bounds for the optimal vectorial data-injection attack. In tandem with the derivation of the optimal attack characteristics we have explicitly stated the cost increase caused by an attack. Therefore, informing any operator of a system the degree of which an attack can damage a system through use of a data-injection attack within the communication channels.

It should be noted once again that the derivations provided are for an attacker with access to the system model and the nominal communication channel statistics and the hypothesis test and parameters therein. Access to this information is assumed in order to inform an operator of the worst case attack performance i.e. the attack that can cause the most damage. Therefore, any attack with access to less information will necessarily give a smaller cost increase, or be detected easier. Specifically, in informing the operator of the exact possible worst case cost increase the operator can calculate this for a given probability of detection. After which if the expected cost increase is within acceptable parameters the operator can consider the control system *safe* from data-injection attacks.

Where by *safe* it is meant that the system has an acceptable increase of expected cost during an undetectable attack, this is equivalent to 'acceptable losses'.

# Chapter 8

# Case Studies

In the following chapter we consider various case studies for each of the control systems designed and the associated attack strategies derived for those systems. Each case study section is constructed in the same manner as the respective chapters. Unless stated otherwise the numerical results are obtained by averaging over 1000 realisations of the process.

## 8.1 Deterministic DoS Attacks

The attack constructions derived in Chapter 3 cause a cost increase to the operators cost function whilst attempting to remain undetected. With this in mind the following section simulates each of the derived attack constructions. A scalar system is considered for all of this sections simulations. The following simulations are valid for any system, provided it is stable under the assumptions in [59]. Namely, assuming that it is ensured that $\overline{V} > 1 - \frac{1}{\prod_i |\lambda_i(\mathbf{A})|^2}$, where $\lambda_i(\mathbf{A})$ are the unstable eigenvalues of $\mathbf{A}$, the stability assumption holds. This result of stability is derived within [59].

All simulations in this section are performed on an unstable dynamics matrix, $\mathbf{A} = 1.1$, and with noise statistics, $\Sigma_W = 0.01$ and $\Sigma_Z = 0.01$. The operator assumes an actuator communication channel with an IID Bernoulli packet drop probability of $\overline{V} = 0.3$.

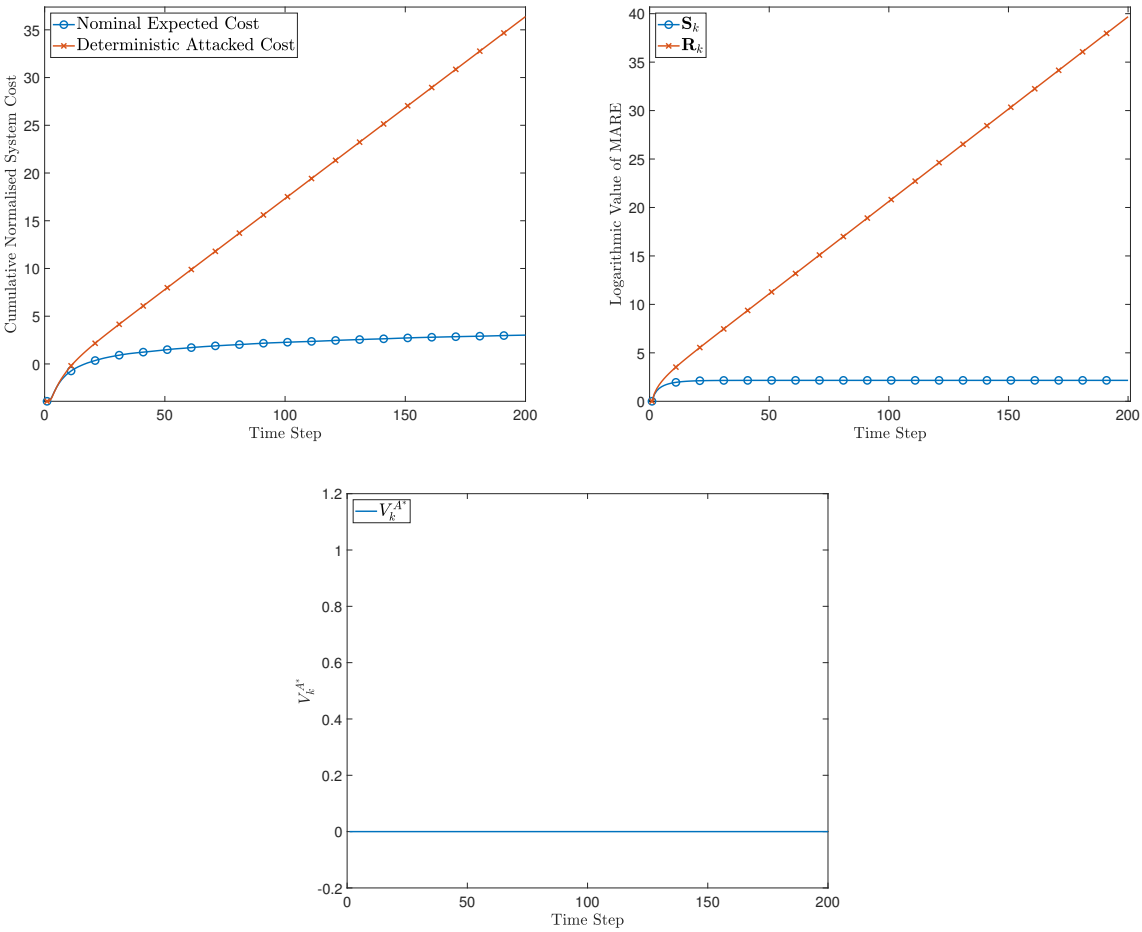


Fig. 8.1 Cost of the system with time-varying Gain under attack (green) and without (yellow), also the time evolution of the MAREs, in addition the optimal actuation choice, $V_k^{A^*}$.

### 8.1.1 Unconstrained Attack Construction

The first set of simulations relate to the optimal unconstrained attack, and due to the fact there are no constraints on attack detection, these attacks on the system drive it into the unstable region. Therefore, the system cost and the MARE values are represented in logarithmic scale, this is shown in Fig. 8.1. Note that the MARE of the attacker is equivalent to the MARE corresponding to a no actuation case for which the optimal sequence is indeed $\left\{V_i^{A^*}\right\}_{i=1}^{N} = 0$, where for these simulations $N = 200$, the length of the simulation. Namely, the condition (3.25) was never met in a single simulation over

the 1000 simulations used for the above plots in addition to this we have never seen this condition met in any simulations performed with the unconstrained attack. A shorter length could have been chosen for the this simulation due to the fact that the MARE $\mathbf{S}_k$ converges far earlier. However, we keep the longer end time to keep them consistent with the following simulations.

### 8.1.2 Constant Detection Constraint

When the attack with detection constraints is considered we see that the system remains stable for a time period proportional to the magnitude of $\Lambda$ and then reverts to the case without detection constraints. This is shown in Fig. 8.2, as it shows that the cost initially converges before growing exponentially. This behaviour is explained through Lemma 5. Namely, as time increases the detection term converges to zero, as a result of the optimal attack mimicking the random nature. It should also be noted that $J_N^{A^*} < J_N^*$ until the point at which the detection term converges when the attack construction reverts to the case without detection i.e. Fig. 8.1. A point of interest is that at the time instant the MARE corresponding to $\mathbf{R}_k$ intersects and surpasses $\mathbf{S}_\infty$, the cost of the system under attack also surpasses the operators expected cost for the secure system. Both of these facts are due to the fact that the detection term dominates the optimal choice of $V_k^A$. Therefore, if this construction produces a *perfect* representation of a Bernoulli random variable with $\overline{V} = 0.5$ then the attack derivation results in the sequence $V_k^A \to \{0, 1, 0, 1, 0, 1, ...\}$. This results in a realisation that is always below the average cost scenario presented in [59] as is seen in Fig. 8.2. The duration before switching into the unconstrained attack behaviour is shown to be proportional to $\Lambda$ explicitly in Fig. 8.3 and Fig. 8.4. Namely, the larger the constant $\Lambda$ term the longer the period of *perfect* realisations lasts. It is interesting to note that when the detection constraints are introduced the behaviour of the MARE changes drastically. The MARE term $\mathbf{R}_k$ is no longer a non-decreasing function, as is shown in Fig. 8.4, in fact it *bounces* off of $\mathbf{S}_\infty$ whenever it touches until the point at which the detection converges at which point it crosses and diverges. This behaviour corresponds to the condition that was previously never met in the unconstrained attack having an

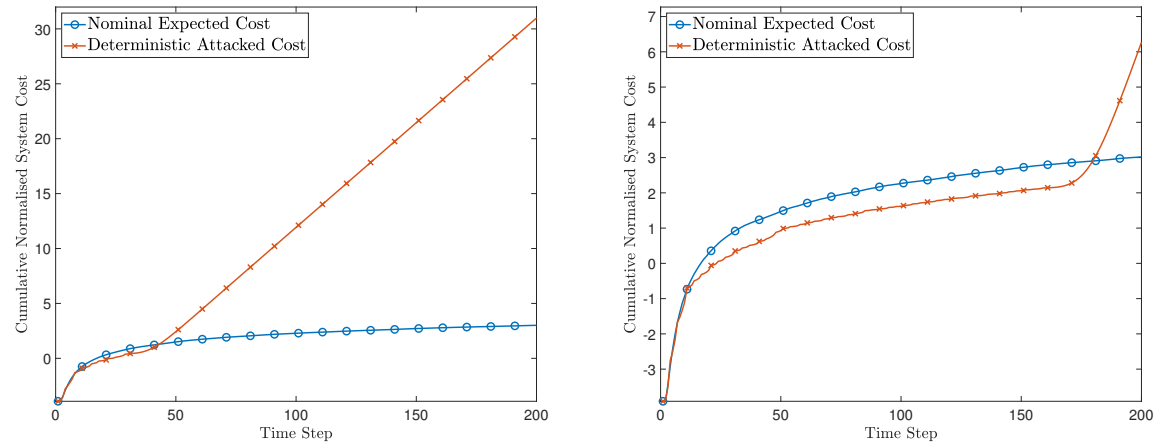


Fig. 8.2 Cost of the system when under attack (green) without (yellow) as a function of time for $\Lambda = 350, 2000$.

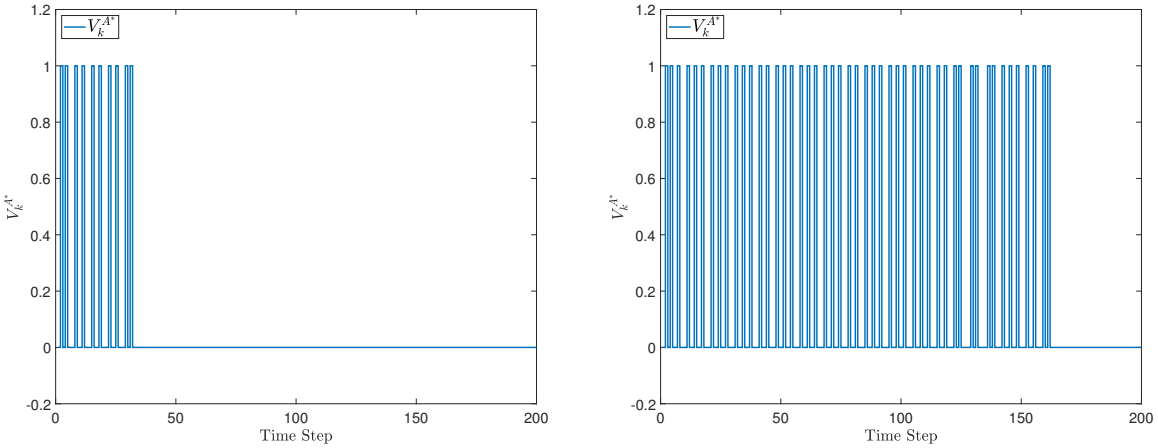


Fig. 8.3 Optimal actuation, $V_k^*$, for the attacker for $\Lambda = 350, 2000$.

influence on the attack. However, as mentioned above there is complete dominance of either the detection or optimal unconstrained attack term at any given time instant. This highlights the need for a reformulation of $\Lambda$ in order to keep the system stable while ensuring an increased cost for the operator.

### 8.1.3 Time Varying Detection Constraint

When considering the optimal time-varying attack, all of the shortcomings of the previous attack strategies are addressed. Namely, the expected cost is increased indefinitely, this

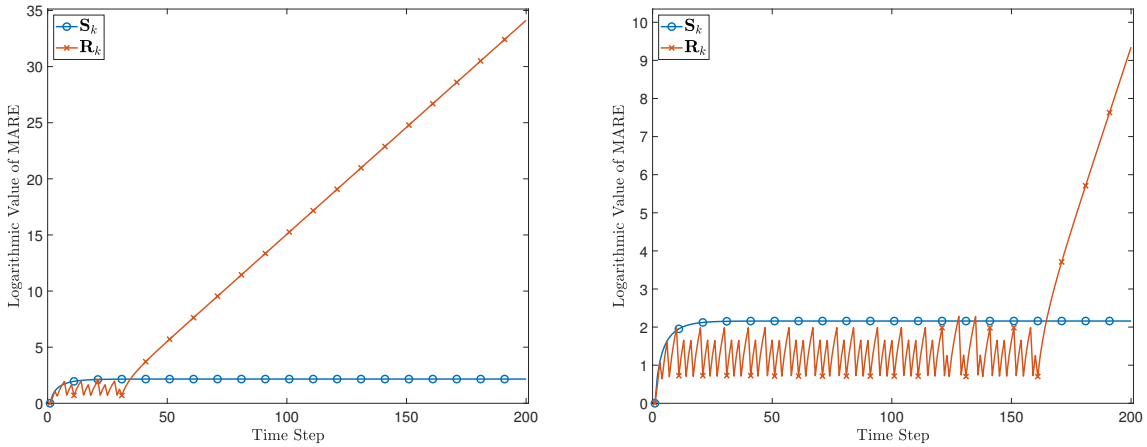


Fig. 8.4 The MARE values as a function of time for $\Lambda = 350, 2000$.

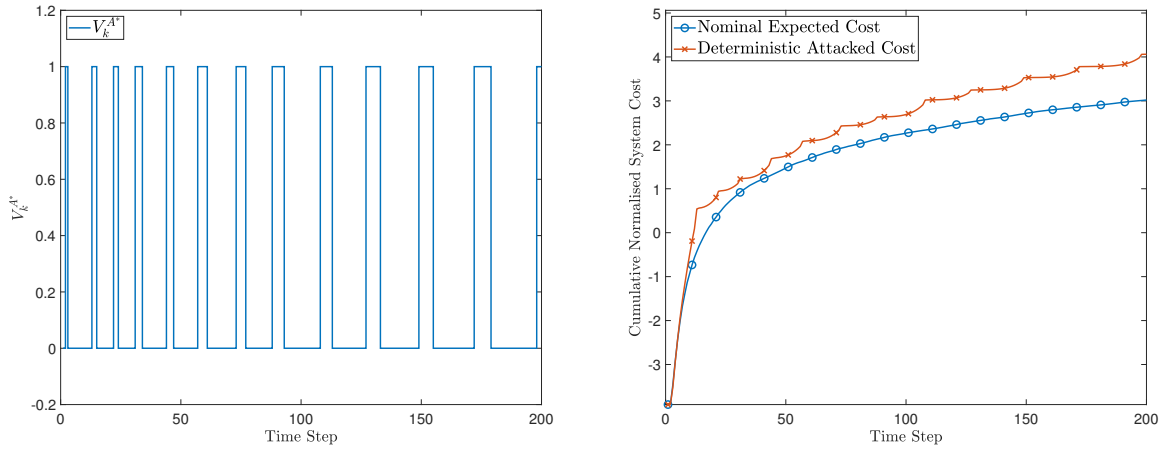


Fig. 8.5 The time varying detection attack.

happens in tandem with the attack remaining undetected. This behaviour becomes apparent in Fig. 8.5. Interestingly, this attack strategy results in an attack pattern that prioritises packet drops in succession. Namely, there are periods of all packet drops followed by periods of all packet transmission. Additionally, these periods grow in length as time goes on. This is as a result of the detection constraint. Specifically, due to the normalisation in the detection constraint it requires a longer period of time for the ML estimator to be moved the same amount as it would have been earlier on in the attack window.

## 8.2 Multichannel Packet Loss Control Case Studies

For the following case studies we conduct simulations for two separate systems. Namely, a single actuator system and a system with multiple actuators. This choice is made to highlight the properties control algorithms developed in Chapter 4.

### 8.2.1 Single Actuator System

The first system we consider is the inverted pendulum system as reported in [59]. The discrete time state space model of the pendulum is provided in [59] and reported here for convenience

$$\mathbf{A} = \begin{pmatrix} 1.001 & 0.005 & 0.000 & 0.000 \\ 0.35 & 1.001 & -0.135 & 0.000 \\ -0.001 & 0.000 & 1.001 & 0.005 \\ -0.375 & -0.001 & 0.590 & 1.001 \end{pmatrix}, \mathbf{B} = \begin{pmatrix} 0.001 \\ 0.540 \\ -0.002 \\ -1.066 \end{pmatrix}, \quad \Psi = 2\mathbf{I}_N, \tag{8.1a}$$

$$\Omega = \mathbf{I}_N \otimes \begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{8.1b}$$

the prediction horizon is $N = 80$. Note that this system has a single actuator, and therefore, there is no difference between the variables $\mu$ and $\overline{\Upsilon}$. Indeed, they are the same scalar multiplied by appropriately dimensioned identity matrices.

The analysis in Section 4.4 characterises the maximal cost difference between the two protocols. Namely, the TCP-like and the UDP-like protocols. Therein, the system is reduced to a scalar communication channel, similar to that seen in Chapter 3. In Chapter 4 the expected cost difference as a function of the packet transmission parameter, $\mu$, is

defined to be

$$J_{\Delta}^{*}\left(\overline{\Upsilon}\right) \triangleq J^{*}\left(\mathcal{G}_{k}\right) - J^{*}\left(\mathcal{F}_{k}\right). \tag{8.2}$$

In Theorem 3 it is shown that $J_{\Delta}^{*}\left(\overline{\Upsilon}\right)$ converges to 0 for a $\overline{\Upsilon}$ in the vicinity of either $\mathbf{I}$ or $\mathbf{0}$. The convergence of the cost difference in these limit cases is observed in Fig. 8.6. The limit cases of a $\overline{\Upsilon}$ in the vicinity of $\mathbf{I}$ or $\mathbf{0}$ correspond to deterministic cases. Note, these are the only cases for which the TCP-like and UDP-like information sets are equivalent, and therefore, the control laws are identical. Furthermore, in the limit case when $\overline{\Upsilon}$ is in the vicinity of $\mathbf{I}$ the control law for both protocols are also equivalent to a nominal LQG controller that does not account for packet loss in the actuation channel. It is seen in Figure 8.6 that the characterisation given in Section 4.4 corresponds to the observed behaviour. Specifically, there is a maximal point in the $[0, 1]$ region. This maximal point is highlighted with the vertical arrow, which corresponds to the maximal point $\overline{\Upsilon}^{D^*} = 0.0031$ as predicted by Theorem 5. Theorem 3 states that the TCP-like cost is strictly less than the UDP-like as is also seen in Fig. 8.6. Additionally, as seen in Corollary 3, for a given expected system cost $J^{*}\left(\mathcal{I}_{k}\right)$ the TCP-like protocol has a smaller channel transition probability, $\overline{\Upsilon}$. This is shown in Fig. 8.6.

The cost difference of the two protocols arises from different control laws. Table 8.1 shows the closed loop eigenvalues of the TCP-like and the UDP-like protocols. Where the closed loop gain $\mathbf{K}_{\mathcal{I}_k}$ is defined as the first $m$ by $n$ block of the matrix $\mathbf{G}_{\mathcal{I}_k}\Omega_{gp}$ . Additionally, the packet transmission variable is set at $\overline{\Upsilon} = 0.9\mathbf{I}$ for the calculation of the closed loop eigenvalues. As shown in Table 8.1, the TCP-like protocol has a conjugate pair of eigenvalues with a smaller complex component when compared to the UDP-like eigenvalues. This suggests the damping of the state response is lower for the UDP-like protocol than the TCP-like protocol. Additionally, the magnitude of the TCP complex-conjugate eigenvalues is closer to the origin, this points to faster decay in the response of these modes.

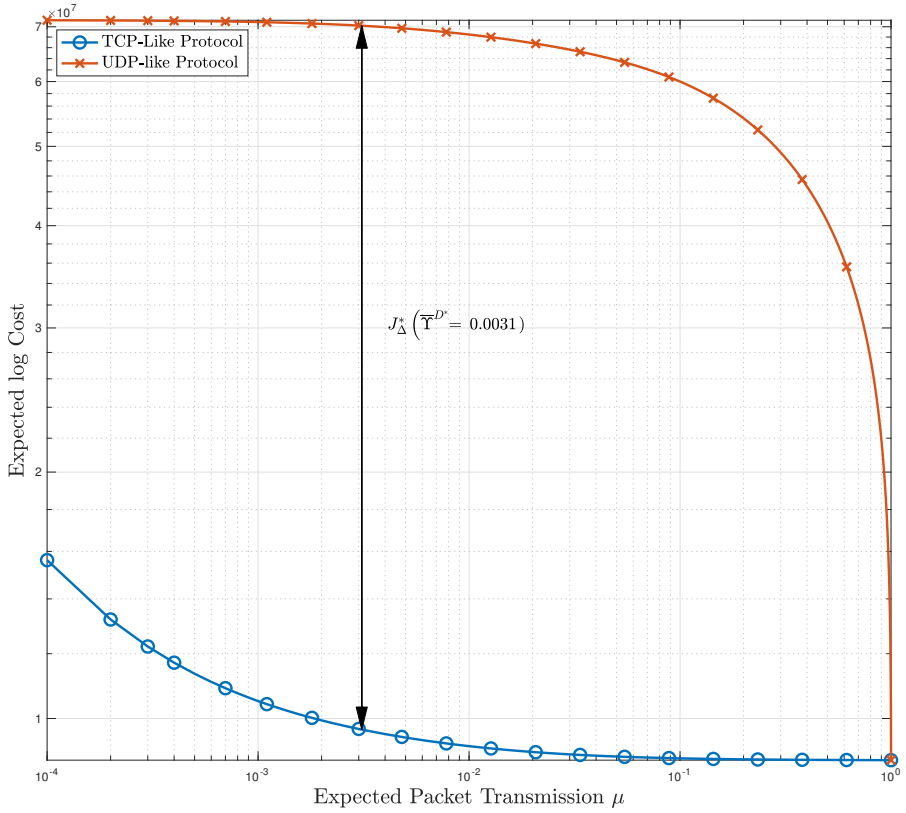


Fig. 8.6 Cost difference between the UDP-like TCP-like protocols operating on the inverted pendulum system described in [59] as a function of the channel packet packet transmission probability.

### 8.2.2 Multiple Actuator System

For the second case study we consider an arbitrary system with multiple actuators. This system is constructed as,

$$\mathbf{A} = \begin{pmatrix} 1.03 & 0.005 \\ 0.35 & 1.01 \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{8.3a}$$

$$\Psi = \mathbf{I}_N \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \Omega = \mathbf{I}_N \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{8.3b}$$

Table 8.1 Closed Loop Eigenvalues of (8.1)

| $\lambda_i(\mathbf{A} - \mathbf{B}\mathbf{K}_{\mathcal{J}_k})$ | TCP-like Eigenvalues | UDP-like Eigenvalues |
|---|---|---|
| $\lambda_1$ | $0.9497 + 0.0056i$ | $0.9907 + 0.0201i$ |
| $\lambda_2$ | $0.9497 - 0.0056i$ | $0.9907 - 0.0201i$ |
| $\lambda_3$ | $-0.1148$ | $0.9729$ |
| $\lambda_4$ | $0.9978$ | $0.9382$ |

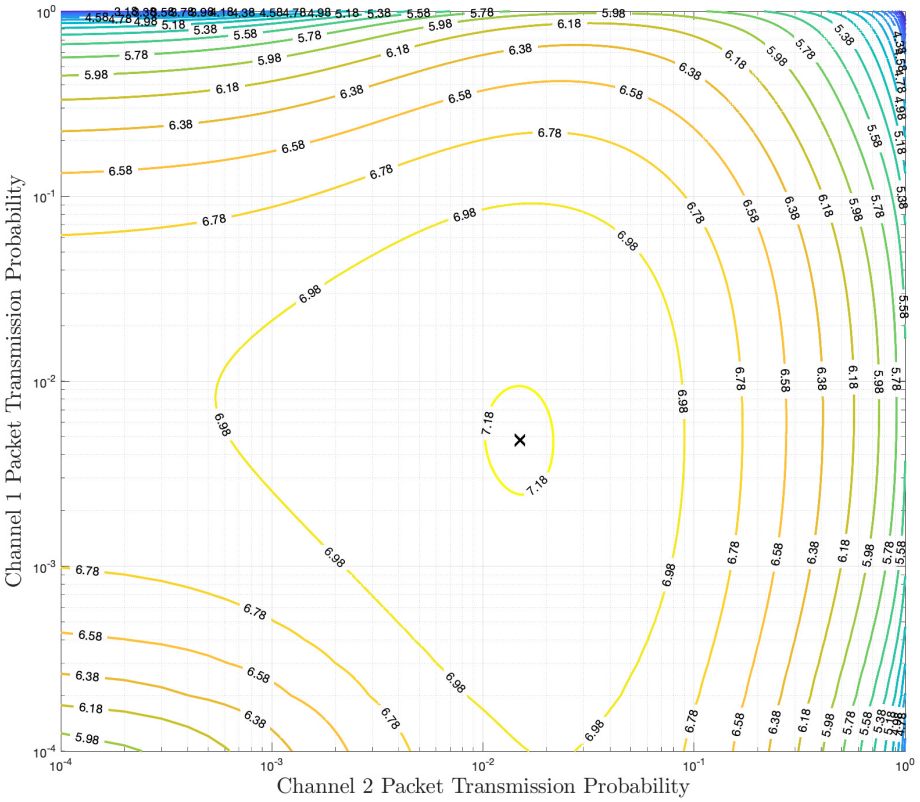


Fig. 8.7 The optimal cost difference between the UDP-like and the TCP-like protocols for the system (8.3) as a function of the channel packet packet transmission probabilities in both actuation channel dimensions.

and the prediction horizon is set to $N = 10$. The system in (8.3) has multiple actuators and thus is used to highlight the generality of our results. The expected cost difference, as seen in Fig. 8.7, shows existence of a maximal point despite the system having multiple actuators, as predicted by Theorem 5. This is marked with a black cross in Fig. 8.7.

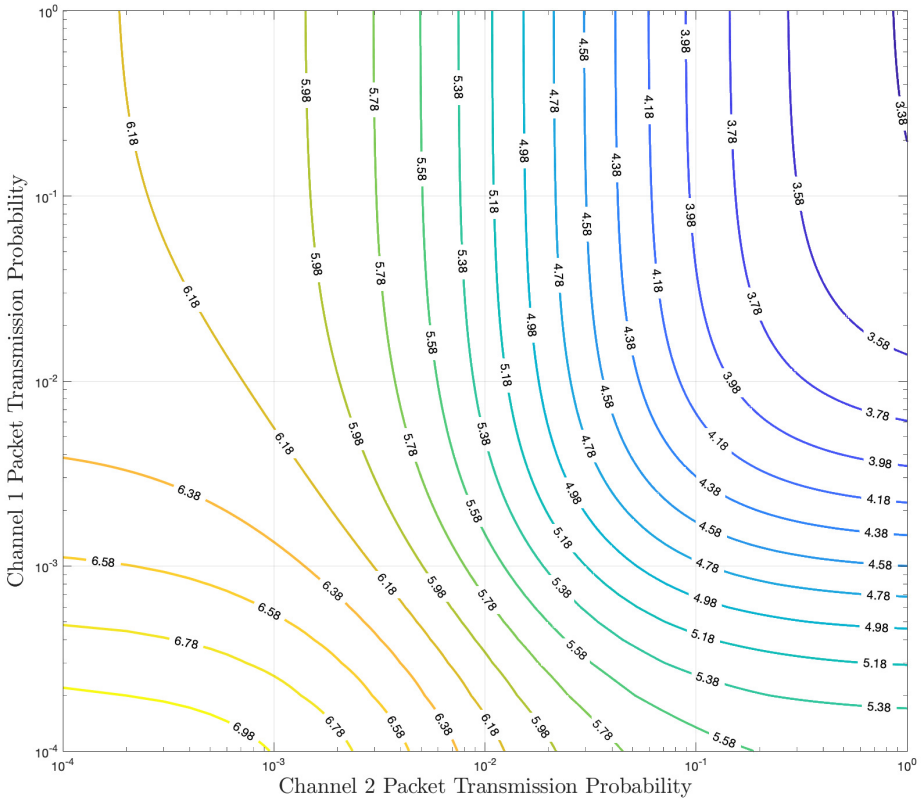


Fig. 8.8 Cost values for the TCP-like protocol operating on system (8.3) as a function of the channel packet packet transmission probabilities in both actuation channel dimensions.

This indicates that the results extend to multiple actuators. Fig. 8.7 shows that the cost difference is strictly positive when $\mathbf{M} \neq \mathbf{I}$ and $\mathbf{M} \neq \mathbf{0}$.

When considering the expected cost for this system, the presence of a second actuator means the expected cost is a function of multiple packet transmission variables. As a result, there are regions in $[0, 1] \times [0, 1]$ where the expected cost remains fixed for a range of values of $\mathbf{M}$. This behaviour is depicted in Fig. 8.8 and Fig. 8.9 for the TCP-like and UDP-like expected costs, respectively. As mentioned for the previous case study, the control laws developed in Section 4.3 are different for each protocol. As shown in Table 8.2, the UDP-like protocol has a complex conjugate pair of eigenvalues.

Table 8.2 Closed Loop Eigenvalues of (8.3)

| $\lambda_i(\mathbf{A}-\mathbf{B}\mathbf{K}_{\mathcal{J}_k})$ | TCP-like Eigenvalues | UDP-like Eigenvalues |
|---|---|---|
| $\lambda_1$ | $-0.1082$ | $0.4904+0.0312i$ |
| $\lambda_2$ | $-0.8938$ | $0.4904-0.0312i$ |

Note that for the purposes of calculating the eigenvalues in Table 8.2, the communication channel is not a scalar, in fact we set $\mathbf{M} = \left(\begin{smallmatrix} 0.7 & 0 \\ 0 & 0.01 \end{smallmatrix}\right)$. As with the pendulum case study it is seen that the TCP-like and the UDP-like control laws induce different behaviour in the state trajectories. It should be noted that the average state trajectories resemble a damped systems with minimal oscillations for both protocols. Although the UDP-like

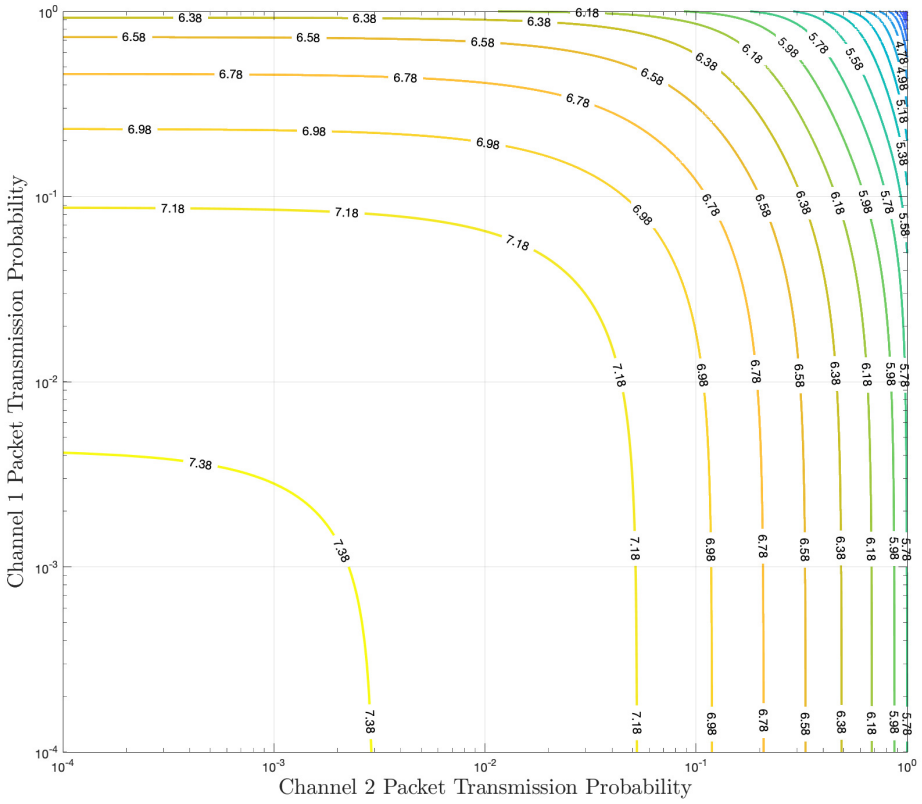


Fig. 8.9 Cost values for the UDP-like protocol operating on system (8.3) as a function of the channel packet packet transmission probabilities in both actuation channel dimensions.

response resembles a significantly less damped system. This is interesting given the real part of the TCP-like closed loop eigenvalues are negative and one of them approaches the maximum frequency for stable oscillations. We suggest that this behaviour despite the eigenvalues is a result of the fact that only a percentage of the actuations chosen make it through to the plant and that this limits the oscillating behaviour. In that vein, notice that the closed loop eigenvalues do not take into account the actuation channel statistics. Namely, we have presented the eigenvalues $\lambda_i(\mathbf{A} - \mathbf{B}\mathbf{K}_{\mathscr{g}_k})$ and not the averaged eigenvalues $\mathbb{E}\left[\lambda_i(\mathbf{A} - \mathbf{B}\mathbf{K}_{\mathscr{g}_k})\right] = \widehat{\lambda}_i(\mathbf{A} - \overline{\Upsilon}\mathbf{B}\mathbf{K}_{\mathscr{g}_k})$.

## 8.3 Random DoS Attacks

The following case studies focus upon a comparison between the IID attack construction and the non-stationary attack construction. This comparison is conducted over two communication channels for the same system. To that end, we use the same test system as in Section 8.2. Specifically, the multiple actuator system

$$\mathbf{A} = \begin{pmatrix} 1.03 & 0.005 \\ 0.35 & 1.01 \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{8.4a}$$

$$\Psi = \mathbf{I}_N \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \Omega = \mathbf{I}_N \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{8.4b}$$

and the prediction horizon is set to $N = 10$. The first simulation is performed over a scalar communication channel with $\mathbf{M} = 0.7\mathbf{I}$. The system is averaged over 1000 realisations and the state trajectories are shown in Fig. 8.10 for a system operating with a TCP-like protocol and the UDP-like protocol is depicted in Fig. 8.11. Interestingly, when under either of the attack constructions the UDP-like system trajectory, as seen in Fig. 8.11, displays a larger change from the nominal state trajectory when compared with TCP-like trajectory depicted in Fig. 8.10. Additionally, these plots show that the increase in cost attributed with both of the attack constructions stems from their ability to delay the convergence of the states to 0.

We also consider an additional channel model. For the second channel model we consider an $\mathbf{M} = \text{diag}\,(0.7, 0.01)$. Additionally, these simulations are obtained by averaging 1000 realisations of the state trajectories. By altering the communication channel model it is seen that the non-stationary attack has a larger increase from the nominal state trajectory when compared to the IID attack. This is seen in Fig. 8.12 for the TCP-like protocol and in Fig. 8.13 for the UDP-like protocol. As in the previous communication channel model, the system operating with a UDP-like protocol, as seen in Fig. 8.13, is more vulnerable to attacks than a system operating with a TCP-like protocol, as seen in Fig. 8.12.

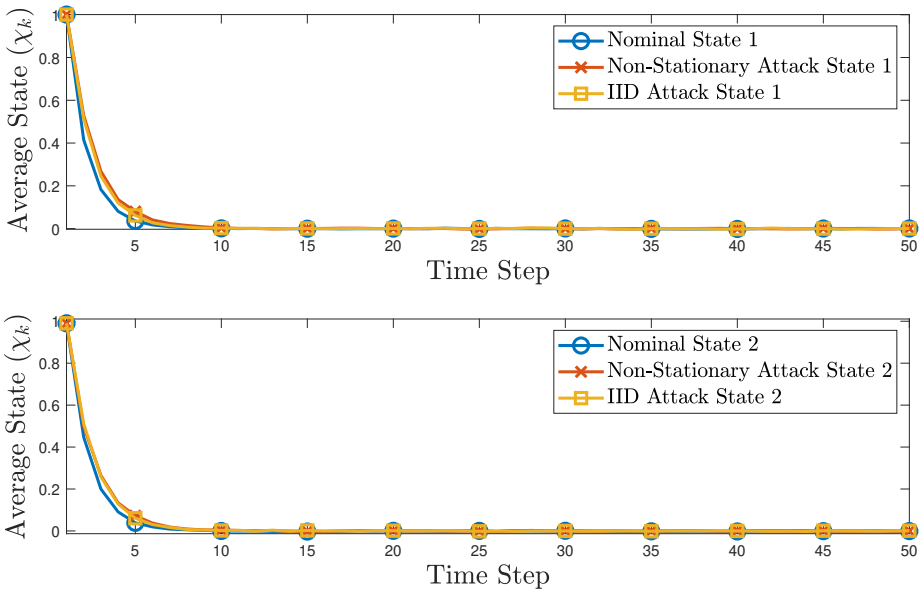


Fig. 8.10 System with TCP-like protocol with $\mathbf{A} = \left(\begin{smallmatrix} 1.03 & 0.005 \\ 0.35 & 0.5 \end{smallmatrix}\right)$, $\mathbf{M} = 0.7$, and $\delta = 0.1$.

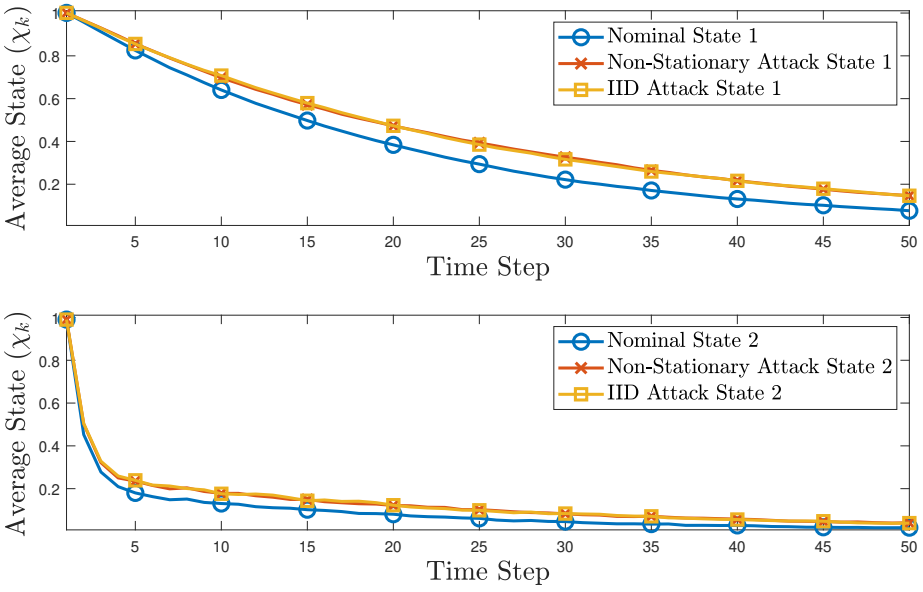


Fig. 8.11 System with UDP-like protocol with $\mathbf{A} = \left(\begin{smallmatrix} 1.03 & 0.005 \\ 0.35 & 0.5 \end{smallmatrix}\right)$, $\mathbf{M} = 0.7$, and $\delta = 0.1$.

In order to quantify this degradation of control performance we now consider the normalised LQG optimal costs of each of these simulations. The LQG cost for system utilising a UDP-like protocol with no attack present is 7.671. Interestingly, the LQG cost

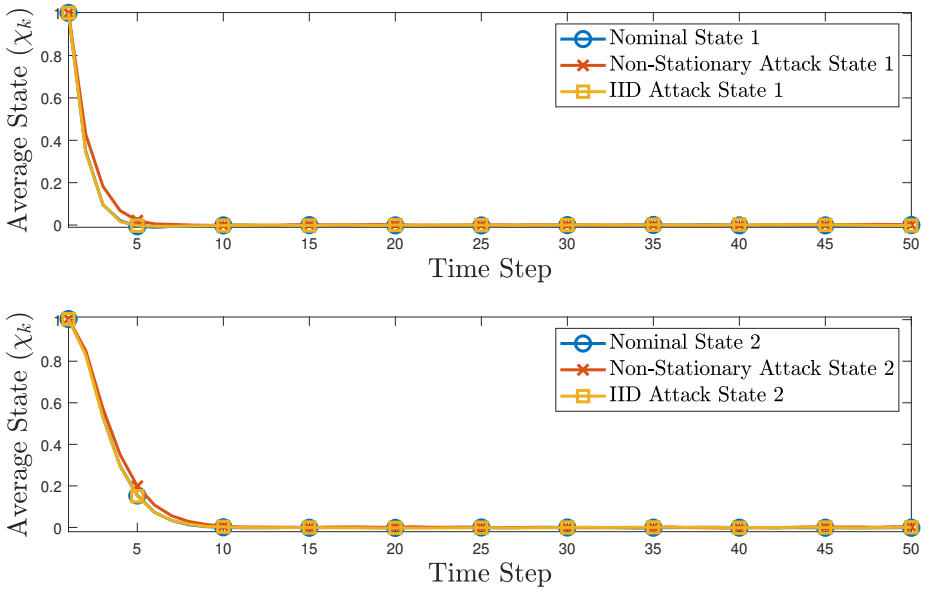


Fig. 8.12 System with TCP-like protocol with $\mathbf{A} = \left(\begin{smallmatrix} 1.03 & 0.005 \\ 0.35 & 0.5 \end{smallmatrix}\right)$, $\mathbf{M} = \left(\begin{smallmatrix} 0.7 & 0 \\ 0 & 0.01 \end{smallmatrix}\right)$, and $\mathbf{L} = 0.1\mathbf{I}$.

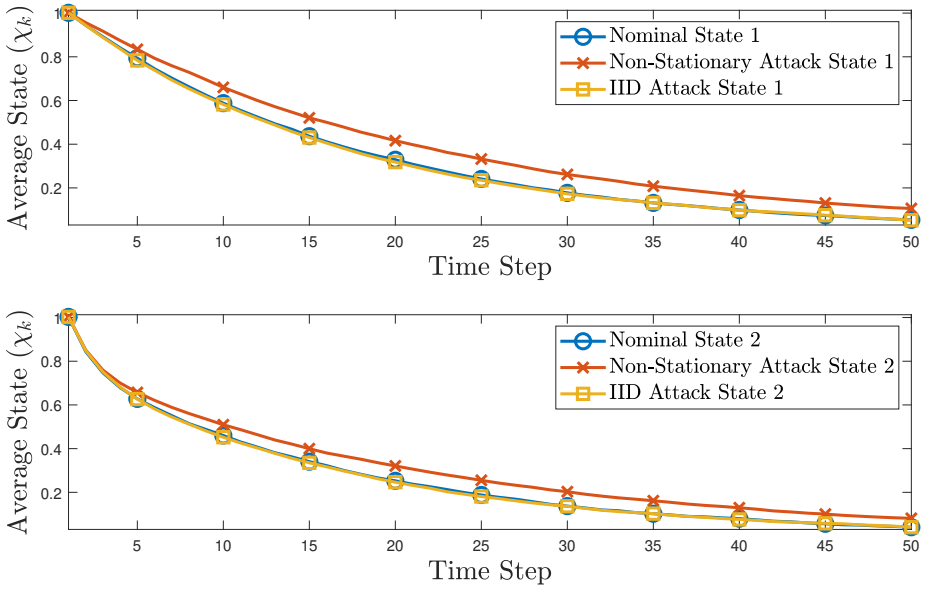


Fig. 8.13 System with UDP-like protocol with $\mathbf{A} = \left(\begin{smallmatrix} 1.03 & 0.005 \\ 0.35 & 0.5 \end{smallmatrix}\right)$, $\mathbf{M} = \left(\begin{smallmatrix} 0.7 & 0 \\ 0 & 0.01 \end{smallmatrix}\right)$, and $\mathbf{L} = 0.1\mathbf{I}$.

induced by the non-stationary attack on this same system is 18.217 while the terminal cost induced by the IID attack is 13.26. This suggests that UDP-like protocols are more

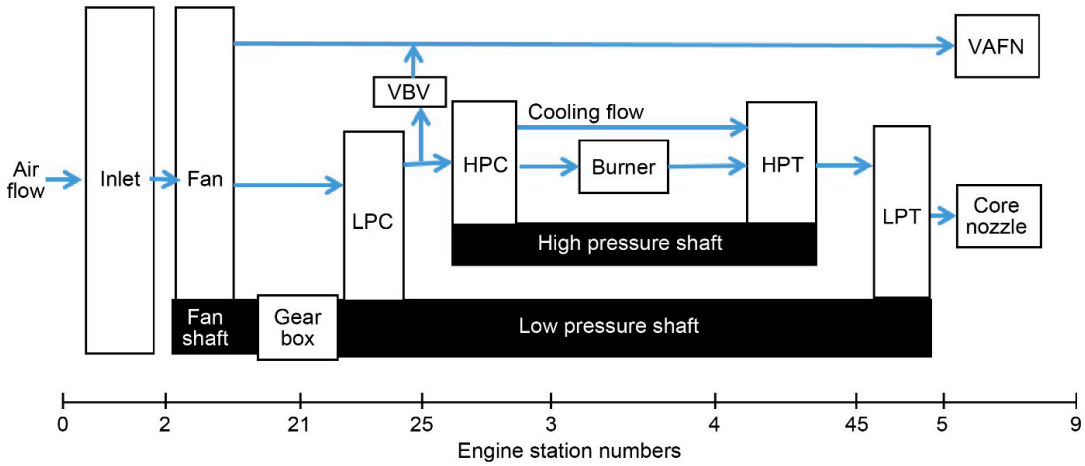


Fig. 8.14 System model of the Advanced Geared Turbo-Fan engine, the conceptual 30,000 lbf thrust class gas turbine engine containing high pressure, low pressure, and fan shafts

vulnerable to non-stationary attacks than to IID attacks. Surprisingly, for the TCP-like case the performance of the IID attack outperforms the non-stationary attack. Specifically, the average LQG cost induced by the IID attack is 8.689 whereas the averaged LQG cost induced by the non-stationary attack is 8.525. Admittedly, the difference is small and might be a result of evaluating the cost with a finite number of realisations, but the results seem to suggest that there is no significant advantage in implementing non-stationary attacks in TCP-like systems.

## 8.4 Advanced Geared Turbofan Engine

The simulations for the following two sections, the sections related to case studies for Chapters 6 and 7, are performed on the Advanced Geared Turbofan (AGTF) Engine [33]. Specifically, the simulations are performed on the linearised state space model of the AGTF engine. The system model of the AGTF engine is depicted in Fig. 8.14 and a short description of the system is as follows and is as described in [33]. The low pressure shaft and fan shaft are connected by a gearbox with a 3.1 to 1 gear ratio, which acts to increase fuel efficiency and reduce gas turbine noise. The low pressure shaft is powered by a low pressure turbine (LPT) and drives the fan and low pressure compressor (LPC). A Variable

Bleed Valve (VBV) improves the stall margin of the LPC by diverting air from the exit of the LPC to the engine bypass stream, effectively lowering the LPC exit pressure. The High Pressure Shaft (HPS) of the engine includes a high pressure compressor (HPC), a combustion chamber (Burner), and a high pressure turbine (HPT) in series. Flow moving through the HPS exits through a conventional nozzle, while engine bypass air (Cooling flow) exits through a Variable area fan Nozzle (VAFN). The presence of a VAFN has many advantages that include, but are not limited to, improved engine efficiency and noise reduction. More details on the AGTF30 engine are found within [33]. As mentioned above, the model used for the following simulations is the linearised state space model of the engine. The system models in Chapter 6 and Chapter 7 are for discrete time systems. Therefore, the linearised model of the AGTF engine is also discretised for the simulations. After discretisation we obtain the following state space model of the system.

$$\mathbf{A} = \begin{pmatrix} 0.6431 & 0.0913 \\ 0.0630 & 0.8199 \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} 658.1230 \\ 1380.6673 \end{pmatrix}, \tag{8.5a}$$

$$\mathbf{C} = \begin{pmatrix} 9.2316 & 0.0647 \\ 0.0119 & 0.0001 \\ 0.0130 & 0.0294 \\ -0.0643 & -0.0958 \\ 0.3226 & 0.0000 \\ 0.0000 & 1.0000 \\ -2.7960 & 0.7866 \\ 0.5432 & -1.2728 \end{pmatrix}, \quad \mathbf{D} = \begin{pmatrix} 2.4802 \\ -0.01607 \\ 136.6786 \\ 2601.3524 \\ 0.0000 \\ 0.0000 \\ 4503.7009 \\ 9347.3971 \end{pmatrix}, \quad \mathbf{Q}_X = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{Q}_U = 1, \tag{8.5b}$$

The above model is rounded to 4 decimal places, for ease of reading, however, the simulations below are calculated to 8 decimal places. Additionally, the process noise in the system has covariance $\Sigma_W = 1 \times 10^{-10}\mathbf{I}$. Note that the penalty matrices are set to the Identity matrix. This choice is made as our results do not pertain any particular plant

behaviour. Specifically, our results focus on the effect of the communication channels in a control system, and therefore, the choice of the $\mathbf{Q}_X$ and $\mathbf{Q}_U$ penalty matrices is not of particular interest. For more details on the AGTF engine please see [33].

## 8.5 Control Over Noisy Communication Channels

As mentioned above the simulations in this section are of the AGTF engine. The system model is seen in (8.5). Additionally, all of the following simulations are averages over 1000 iterations of the control system. The main focus of Chapter 6 pertains to the effect introducing the imperfect communication channels, and therein, the additional noise. To that end, we defined the nominal noise covariance matrices as

$$\Sigma_Z = 1 \times 10^{-8}\mathbf{I}_m, \quad \Sigma_V = 1 \times 10^{-8}\mathbf{I}_p, \quad \Sigma_T = 1 \times 10^{-9}\mathbf{I}_m. \tag{8.6}$$

Note that $\Sigma_Z \succ \Sigma_T$, and therefore, the results of Theorem 21 hold and the expected cost of the system with an imperfect auxiliary channel should be bounded between the other two system models. In fact, in Fig.8.15 the costs of the three separate systems are plotted over time. It is seen that, as predicted the cost of the system with an imperfect auxiliary channel is bounded between the perfect auxiliary channel and the no auxiliary channel systems. The costs are plotted in logarithmic scale, and therefore, the convergence seen corresponds to the bounded state stability as mentioned in Chapter 6. To see the differences in cost clearer, note Fig. 8.16. This plot shows the cost differences between the imperfect auxiliary channel and the perfect channel in addition to the difference between the system with no auxiliary channel and the perfect auxiliary channel system. Additionally, it is seen in Fig. 8.16 that the cost differences converge. This is a result of each of the respective costs converging, and therefore, the cost differences converge.

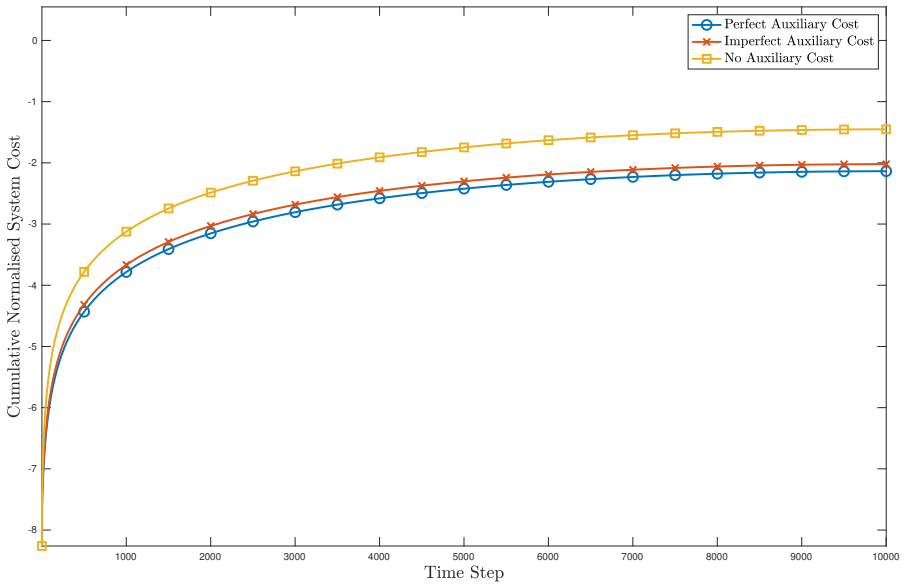


Fig. 8.15 Logarithm plot of the costs of each of the three system designs.

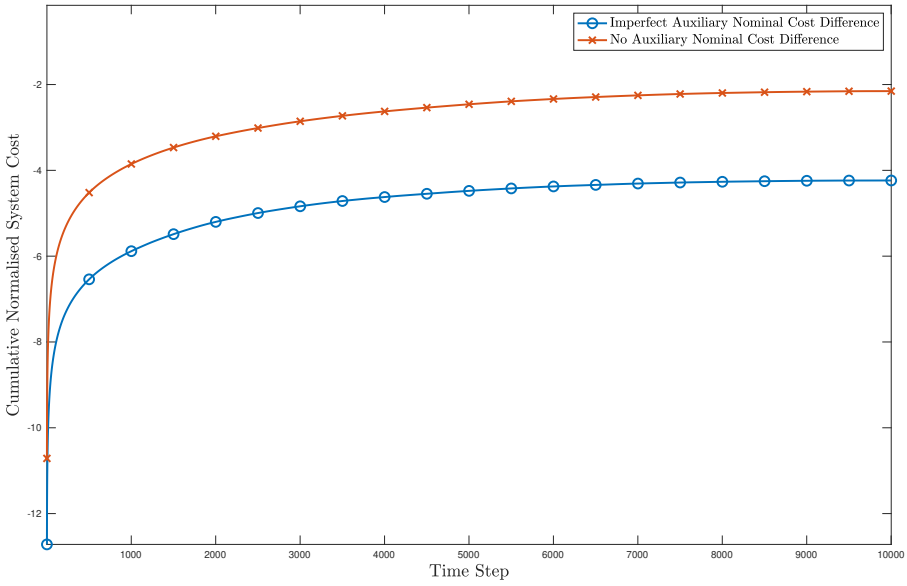


Fig. 8.16 Cost difference between the imperfect auxiliary communication channel and the perfect auxiliary channel and the cost difference between the no auxiliary channel and the perfect communication channel system.

## 8.6 Data Injection Attack Simulations

As in the previous section, the following simulations are performed on the AGTF engine. The state space model of this system is as defined in 8.5. Additionally, the operator of the system is the same as in the previous section. Namely, the nominal noise statistics are defined as

$$\Sigma_Z = 1 \times 10^{-8}\mathbf{I}_m, \quad \Sigma_V = 1 \times 10^{-8}\mathbf{I}_p, \quad \Sigma_T = 1 \times 10^{-9}\mathbf{I}_m. \tag{8.7}$$

Also, for this section, the operator is required to choose a value for $\delta$. For the below, unless otherwise stated, $\delta_1 = \delta_2 = \delta_3 = 4$. Due to the fact the fact that $m = 1$ for this system, the optimal attack values are known. Specifically, for the $\delta$ values set above it is known that the optimal value for the covariances of the signals injected into the actuation and the auxiliary communication channels are

$$\Sigma_{A^U} = 2.2977 \times 10^{-7}, \quad \Sigma_{A^A} = 2.2977 \times 10^{-8}. \tag{8.8}$$

For the system laid out above, the bound for the optimal attack on the sensory communication yields a matrix close to the zero matrix. However, if this matrix is scaled such that the KL divergence constraint is not exceeded, it results in a covariance matrix that achieves a KL divergence closer to the $\delta$ constraint while preserving the *weightings* in each eigenvalue of the lower bound optimal covariance matrix. For the following simulations

that scaled matrix is

$$\Sigma_{Ax}=\begin{pmatrix} 1.622\times10^{-13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 9.642\times10^{-8} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2.014\times10^{-9} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1.629\times10^{-10} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1.343\times10^{-10} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2.449\times10^{-12} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2.006\times10^{-11} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2.240\times10^{-12} \end{pmatrix}. \quad (8.9)$$

The above matrix is rounded to 4 significant figures for ease of reading. The above value of $\Sigma_{Ax}$ yields a KL divergence of 3.648. This value is well in the $\delta$ as set by the operator. It should be noted, that the optimal solutions, (8.8) and (8.8), result in a KL-divergence of 4 for each respective constraint.

The cost for the system with a perfect auxiliary communication channel is depicted in Fig. 8.17, which shows that the cost of the system is strictly increased throughout the attack. This cost is calculated as an average over 1000 simulations. Additionally, Fig. 8.18 shows the averaged state trajectories of the system. The plots in Fig. 8.18 shows the variance of the state trajectories of the system under nominal conditions and when the system is under attack. When considering the variance the trajectories presented are the Mean Squared Error of the realisations from the expected state trajectories. Note the smaller variance of the nominal state trajectories when compared to the attacked trajectories. This is as a result of attacker injecting noise into the system increasing the error but not altering the expected state trajectories.

When considering the system with no auxiliary communication channel many similarities are observed . For instance, as seen in Fig. 8.19 the averaged cost increases when there is an attack. However, this increase in cost is much larger than the increase in Fig 8.17.

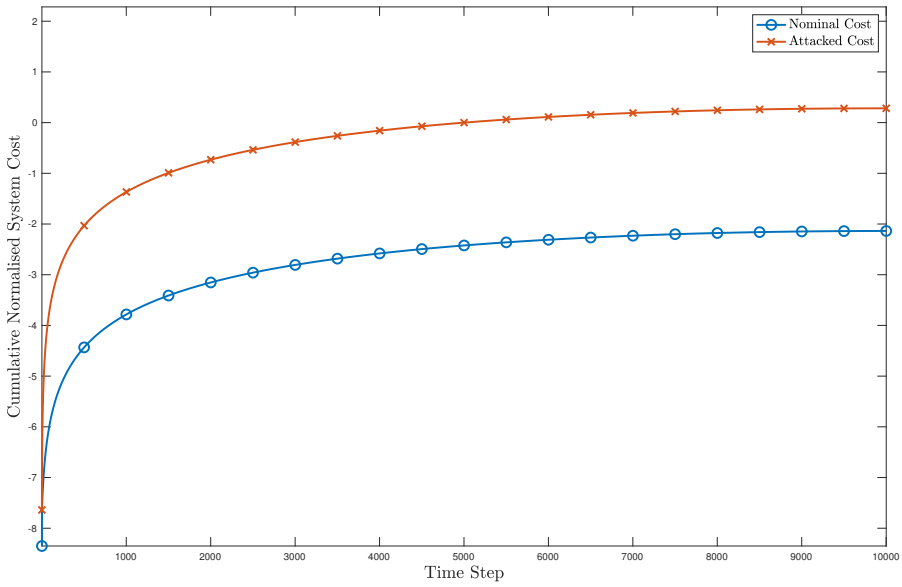


Fig. 8.17 Normalised log cost of the system with a perfect auxiliary communication channel both under nominal conditions and during the attack.

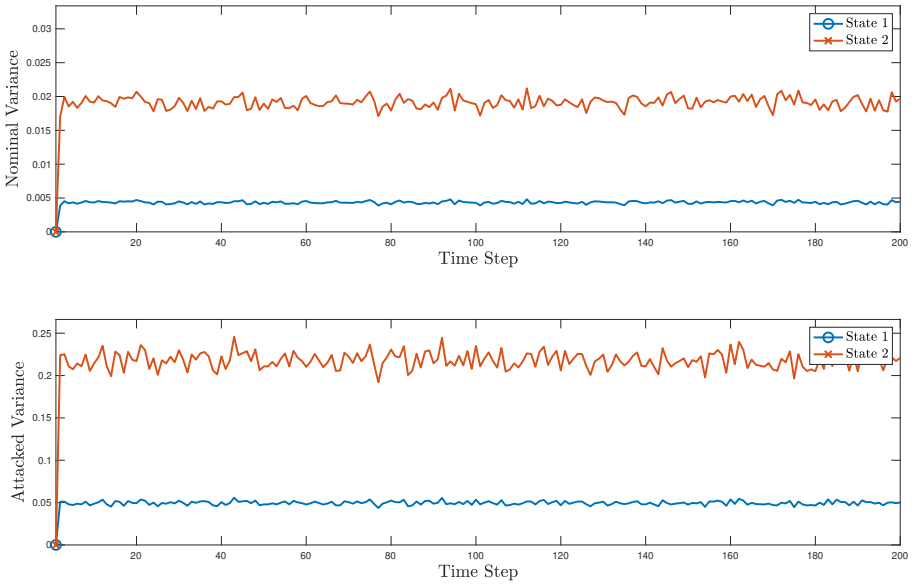


Fig. 8.18 Variance trajectories of the states of the system with a perfect auxiliary communication channel both under nominal conditions and during the attack.

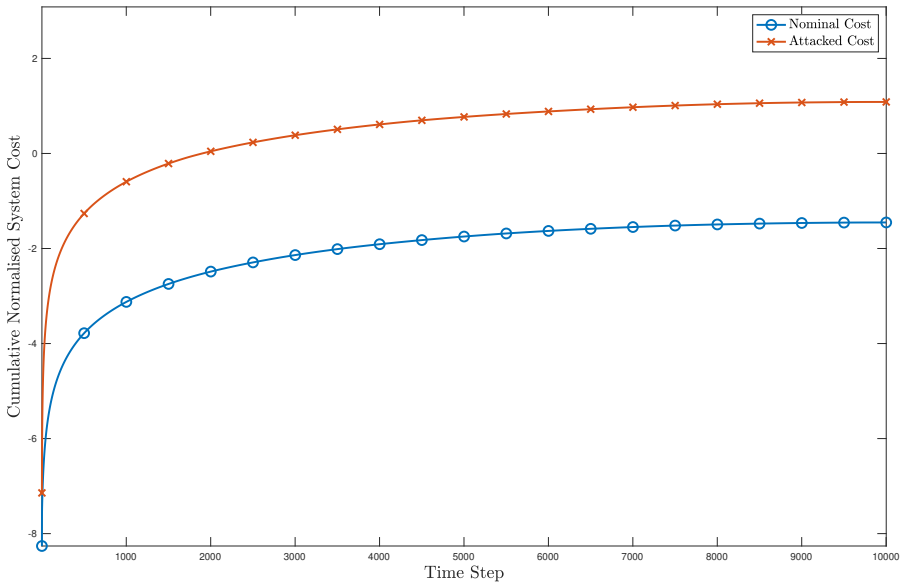


Fig. 8.19 Normalised log cost of the system with a no auxiliary communication channel both under nominal conditions and during the attack.

This is also true when considering the averaged state trajectories. In that the variance of the state trajectories is larger when there is no auxiliary channel, this effect is shown in Fig. 8.20. Note that the variances converge in a similar manner under nominal conditions and when attacked. Yet the value that the variances converged to differ by nearly a factor of 10 for the system with no auxiliary communication channel. Once again, as expected, for the system with the imperfect auxiliary channel the data injection attack increases the averaged cost of the system. This behaviour is seen in Fig. 8.21. However, it may not be obvious from Fig. 8.21 that the cost increase with respect to the nominal system is bounded between the other two cost increases. In order to see this we have also plotted the cost difference of each system in Fig. 8.23. In Fig. 8.23 we have plotted the attacked cost of each respective system minus the cost of each respective system under nominal conditions. In doing so it is seen that the imperfect auxiliary channel systems cost increase lies directly between the other two system cost increases. Interestingly, Fig. 8.23 is reminiscent of Fig. 8.15 in the previous section. This implies that not only does the introduction of an auxiliary channel reduce the average cost of the system, but it also mitigates the effect of

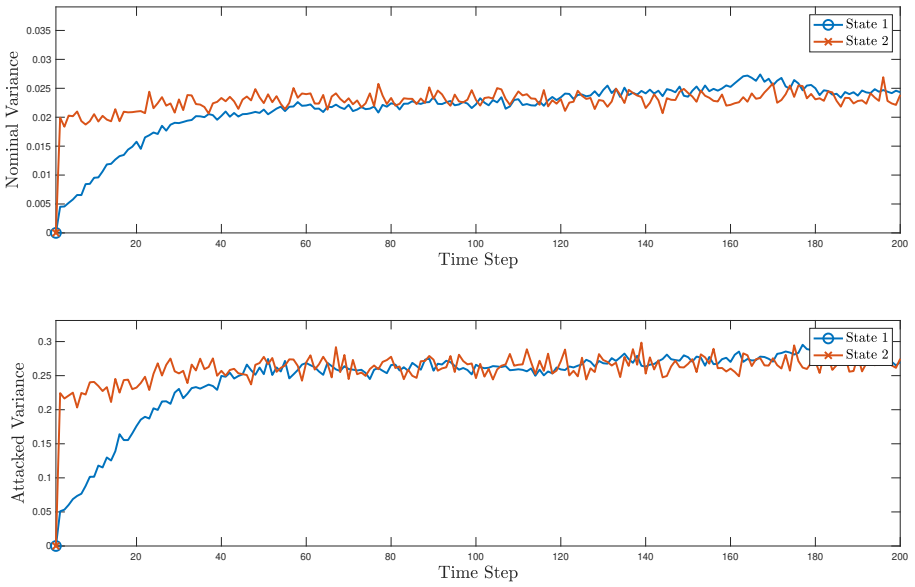


Fig. 8.20 Variance trajectories of the states of the system with a no auxiliary communication channel both under nominal conditions and during the attack.

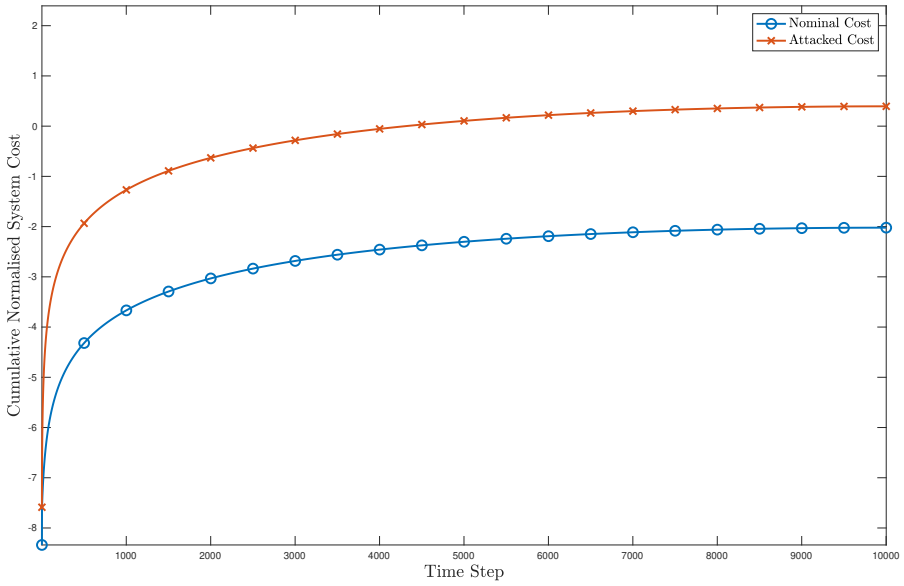


Fig. 8.21 Normalised log cost of the system with an imperfect auxiliary communication channel both under nominal conditions and during the attack.

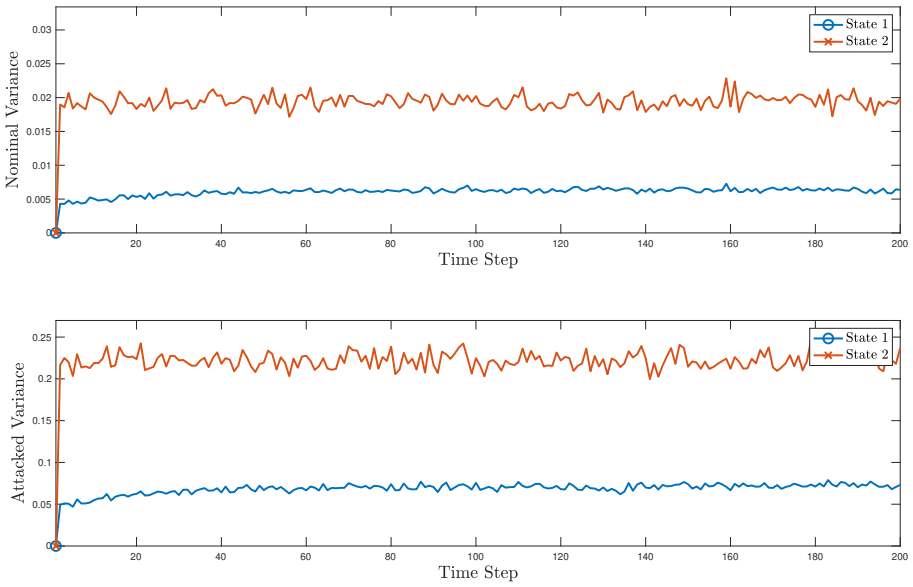


Fig. 8.22 Variance trajectories of the states of the system with an imperfect auxiliary communication channel both under nominal conditions and during the attack.

a data injection attack of the form derived in Chapter 7. As with both previous systems, the variance of the state trajectories shows a similar pattern. Namely, the variances convergence is comparable when under attack yet the values converged to are larger when under attack. This effect for the system with an imperfect communication channel is seen in Fig. 8.22.

Another point of interest is how the choice of $\delta_i$ effects the choice of the optimal data injection attack. This relationship is shown in Fig. 8.24. It is seen in Fig. 8.24 that for small values of $\delta_i$ the relationship is non-linear. Specifically, it is seen to be sub-linear. However, for larger values of $\delta_i$ the optimal data injection attack covariance grows linearly.

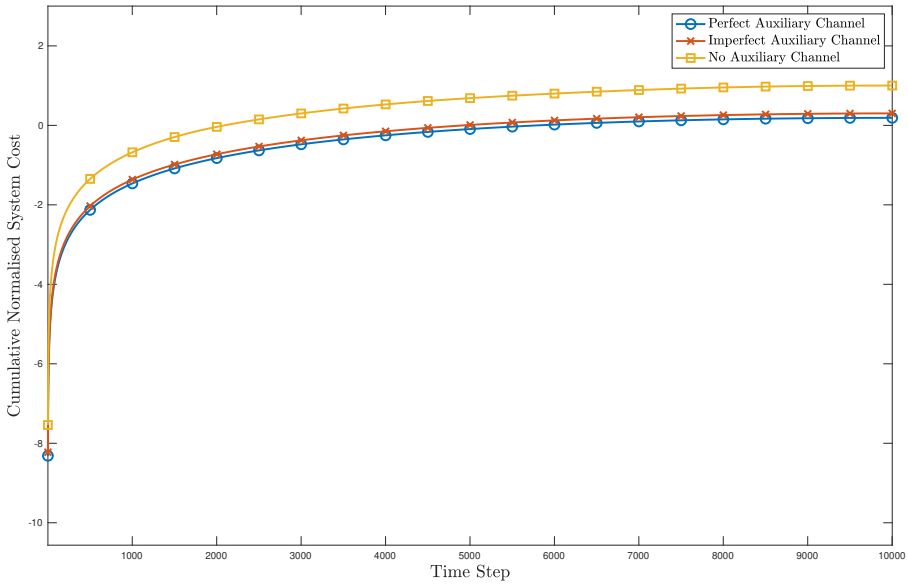


Fig. 8.23 Averaged logarithm of the costs of the systems during the attack.

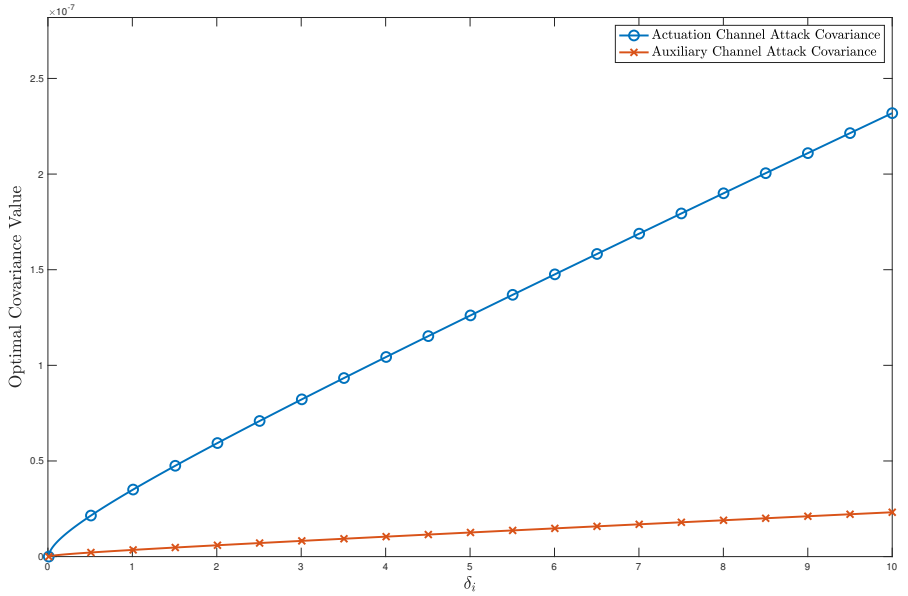


Fig. 8.24 Value of the optimal data injection attack covariance for the actuation communication channel and the auxiliary communication channel as a function of $\delta_i$.

# Chapter 9

# Future Work

## 9.1 Chapter 3

Given the attack derivations within Chapter 3, there is interest in the design of an attack where instead of deciding exactly when a signal is received or not, the attacker only decides when to jam the signal. This means when not jamming the communication channel, the operator receives the nominal IID sequence of packet drops they expect to receive. This attack design helps the attacker minimise attack detection, whilst maximising the cost of the operator. Specifically, it is seen within the case studies in Chapter 8 that the deterministic attack construction results in a repeating pattern of packet drops. Therefore, by *mixing* this deterministic construction with the natural IID sequence of losses, the attacker could hid in the nominal noise in the communication channel.

## 9.2 Chapter 4

Within Chapter 4 we considered the optimal control law for two communication channels. Namely, a communication channel governed by a sequence of IID packet loss and another communication channel governed by a non-stationary sequence of losses. The non-stationary sequence of losses allows the operator to model packet losses where the mean of losses is variable. However, the modelling of the losses does not include the

possibility of a Markovian sequence of packet drops. It is shown within [47] that an optimal LQG controller exists for a sequence of losses governed by a 2-state Markov chain. Given that [47] is the Markovian extension of [59], and that Chapter 4 is the multidimensional extension of [59], it stands to reason that the work in Chapter 4 could be extended to account for Markovian losses within a multidimensional communication channel. This extension however, is by no means trivial. The main issue arises from the need to express the expectation of a Markovian process $N$ time steps into the future. This causes a direct issue with determining $\mathbb{E}[\Upsilon_k]$ which is required in closed form for the calculation of the control law. Additionally, for the UDP-like protocol, there is an additional issue in estimating the state of the Markov chain. Namely, the UDP-like protocol does not monitor the actuation communication channel, and therefore, there would be an additional hurdle for the UDP-like protocol to overcome.

## 9.3 Chapter 5

For this chapter, it was assumed the operator declares an attack and turns off the control system. However, this may not be the optimal choice, as the operator considers random sequences within their nominal communication channel. Therefore, there is a non-zero probability of false alarm. This means that the operator may turn off the control system even when there is no attack present in the communication channel. In order to assess the optimal choice for the operator when an attack is detected, the formulation could be extended to a sequential game theoretic setting. In doing so, the optimal strategy for the operator, and correspondingly for the attacker, can be characterised in terms of a sequential game. We postulate that in this setting the best response dynamics emerging in the sequential game can provide insight into the construction of optimal attacks and defence strategies.

## 9.4 Chapter 6

The optimisation problem within Chapter 6 can be extended for the operator to also include optimisation of the communication channels. This process would take a similar format as that in Chapter 4. Namely, the operator constructs a trade-off between the cost of communication over each individual channel, with the optimal control cost. This would result in optimising over all three covariance matrices $\Sigma_Z$, $\Sigma_{\widetilde{V}}$, and $\Sigma_T$, subject to an additional cost constraint such that the operator minimises a joint control and communication cost. This is slightly different to the derivation in Chapter 6, as the communication channel covariances are seen as fixed constants, and are not treated as variables that which could be tuned and optimised. If however, they were treated as control variables, we postulate that it would result in a water filling argument over the eigenmodes of the covariances matrices.

## 9.5 Chapter 7

Within Chapter 7 the attacker is restricted to IID sequences of data-injected random variables. If this was generalised to non-stationary sequences, or even non-Gaussian sequences, we postulate that the attacker could outperform the results presented. However, the derivations within Chapter 7 are simplified in multiple places through use of the Gaussianity of the injected signals, so the complexity of the derivation would be increased. Additionally, if the attacker considers a non-stationary sequence of variables then the attacker can choose a time varying mean of the vector. This would result in the breaking of the Nash equilibrium, therefore allowing the attacker to potentially obtain the upper hand in this scenario.

# Chapter 10

# Conclusion

The thesis began with the construction of a deterministic attack on the system outlined in [59]. We show that a deterministic attack construction exists that results in a guaranteed cost increase for the operator. This guaranteed cost increase is achieved at the drawback of a large computational cost and attacker information requirements. Specifically, the attacker requires intimate knowledge of the system design, in addition to constant information about the current system states and measurements. These requirements caused us to venture into random attack constructions. Namely, attack constructions that once derived required no knowledge of the system and could be implemented simply.

Within Chapter 4 we obtain the optimal control laws for control systems with multi-dimensional communication channels that are subject to Bernoulli packet loss for both TCP-like and UDP-like packet acknowledgement protocols. This control law is valid for control systems experiencing packet losses that are governed by non-stationary Bernoulli processes on both the actuation and the sensory communication channels. In addition to this, we also show that the expected cost incurred by the UDP-like protocol is strictly larger than that of the TCP-like protocol. Specifically, we show that the expected cost difference between these protocols increases monotonically with the probability of packet loss. These results provide an analytical framework to study the impact of communication channel resources in the performance of the control system. Capitalising on this notion, we have provided a guideline to optimally allocate channel resources for both the UDP-like

and TCP-like protocol and demonstrated the trade-off analysis by applying it in two case studies.

With the system outlined thoroughly, we then proceed to characterise the optimal attack construction for UDP-like and TCP-like systems that utilise this framework. The attacks are proposed as DoS attacks over the actuation communication channel. Additionally, we assume that the attacker has full control over the communication channel. The optimal random attack is constructed under the assumption that the operator monitors the state of the communication channel. The operator performs the optimal detection test on the communication channel. Namely, the operator monitors the average packet loss as the decision statistic. Interestingly, we show that the optimal attack strategy does not always increase the number of packet losses in a communication channel. We have also shown that the IID attack construction is a subset of the possible configurations of a non-stationary attack within a communication channel. We show numerically that the proposed non-stationary attack outperforms the IID attack in most settings. This is achieved at the expense of increasing the number of optimisation variables. We also give bounds on the probability of detection for the attacker. In doing so, we give bounds to inform the attacker and the operator on how to efficiently design their tuning parameters for attack performance/detection.

Within Chapter 6 we implement AWGN communication channels onto both the sensory and the actuation link of a control system. After these communication channels are modelled and discussed, we show that the expected cost of communicating imperfectly can to be quantified exactly. This quantification is applied across three separate system architectures. Namely, we generalise the feedback communication channels in Chapter 4 to AWGN communication channels. This results in two system architectures, one which resembles an AWGN equivalent of the TCP-like protocol and another which is the AWGN equivalent of the UDP-like protocol. In addition to the above two system architectures, we provide a third system model where the feedback communication channel is generalised to an imperfect AWGN communication channel. This is equivalent to the extension of the acknowledgment channel within the TCP-like protocol being extended to the imperfect link,

as seen in [29]. We show, once again, that the inclusion of this feedback communication channel strictly reduces the expected cost of the control system.

Given the explicit characterisation of the communication channels within Chapter 6 we are then able to implement a data-injection attack within each of the three AWGN communication channels. Precisely this, is the purpose of Chapter 7. We characterise the expected cost increase for each of the three system architectures. Following this characterisation we then provide lower bounds on the optimal attack construction for each communication channel in the multidimensional setting. In addition to this, we provide exact solutions for the optimal attack in each of these scenarios for a given detection constraint.

We have also conducted a comparison between control systems with and without an auxiliary feedback communication channels. In Chapters 3, 4, and 5 and this feedback channel took the form of an acknowledgement link. This acknowledgement link was the direct cause of the differing information sets between the TCP-like and the UDP-like protocols. This comparison was then extended to the AWGN communication channels, as seen in Chapters 6 and 7. Namely, system architectures with a perfect auxiliary communication channel and no auxiliary communication channel. The comparison of the feedback channel highlighted the differences between the system responses. It is shown that for both the Bernoulli communication channel and the AWGN communication channel, the nominal expected cost is strictly increased by not having this communication link. It is observed that the feedback communication link also provides the system with additional safeguards against an attack. Specifically, the feedback channel reduces the amount of expected cost increase an attack can cause.

Throughout this thesis we have studied control systems with limited information. These conditions have varied from scenarios that the operator expects to occur, such as Chapter 4 and 6, to scenarios caused by malicious agents, such as Chapters 3, 5, and 7. For these systems operating with limited information we have derived the optimal control laws and their associated costs.

Our aim during this PhD has been to achieve precisely this: to inform the operator of how much efficiency they need to sacrifice for the system to be *safe*.

# Appendix A

# Chapter 3

## A.1 Lemma 1

This Section is dedicated to the proof of Lemma 1. The Lemma is re-stated below.

**Lemma 1.** *The optimal value function (3.22) for the system defined in (3.1) is equivalent to*

$$f_k(X_k) \triangleq \mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{R}_k X_k \middle| \mathcal{A}_k\right] + \ d_k, \quad k = N, \ldots, 0, \tag{A.1}$$

*where the matrix* $\mathbf{R}_k \in \mathbb{R}^{n\times n}$ *and the scalar* $d_k \in \mathbb{R}$ *are recursively calculated according to*

$$\mathbf{R}_k = \mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X + V_k^{A^*}\left(\mathbf{K}^{\mathsf{T}}\left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\right)\mathbf{K} - 2\mathbf{K}^{\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A}\right), \tag{A.2a}$$

$$d_k = \operatorname{tr}\left(\left(\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X - \mathbf{R}_k\right)P_{k|k}\right) + \operatorname{tr}\left(\mathbf{R}_{k+1}\Sigma_W\right) + \mathbb{E}[d_{k+1}|\mathcal{A}_k], \tag{A.2b}$$

*where* $V_k^{A^*}$ *is the optimal choice that maximises the cost function (3.21). Each realisation is determined by the inequality*

$$V_k^{A^*} = \begin{cases} 1 & \text{for} \quad \hat{X}_k^{\mathsf{T}}\left(\mathbf{K}^{\mathsf{T}}\left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\right)\mathbf{K} - 2\mathbf{K}^{\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A}\right)\hat{X}_k > 0, \\ 0 & \text{Otherwise.} \end{cases} \tag{A.3}$$

*Proof.* The following proof takes the form of an induction proof. Namely, after showing the initial conditions hold true it is assumed that (A.1) holds true for time instant $k+1$.

After which it is shown that it also holds true for time instant $k$, in doing so the recursive form of $\mathbf{R}_k$ is revealed. The optimal value function, $f_k(X_k)$ is defined in (3.22) to be

$$f_N(X_N) \triangleq \mathbb{E}\left[X_N^{\mathsf{T}}\mathbf{Q}_X X_N \middle| \mathscr{A}_N\right], \tag{A.4a}$$

$$f_k(X_k) \triangleq \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{Q}_X X_k + V_k^{A^*}\hat{X}_k^{\mathsf{T}}\mathbf{K}^{\mathsf{T}}\mathbf{Q}_U\mathbf{K}\hat{X}_k + f_{k+1}(X_{k+1}) \middle| \mathscr{A}_k\right]\right\}. \tag{A.4b}$$

Noting that $\mathbf{R}_N = \mathbf{Q}_X$ and $d_N = 0$ then the initial condition is

$$f_N(X_N) \;=\; \mathbb{E}\left[X_N^{\mathsf{T}}\mathbf{R}_N X_N \,\mathscr{A}_N\right] + \; d_N = \mathbb{E}\left[X_N^{\mathsf{T}}\mathbf{Q}_X X_N \middle| \mathscr{A}_N\right] = J_0(\overline{X}_0, P_0). \tag{A.5}$$

Due to the equivalence in (A.5) the initial conditions holds. Therefore, assuming (A.1) holds at the $k+1$ time step then the $k^{\text{th}}$ time step is

$$f_k(X_k) = \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{Q}_X X_k + V_k^A\hat{X}_k^{\mathsf{T}}\mathbf{K}^{\mathsf{T}}\mathbf{Q}_U\mathbf{K}\hat{X}_k + f_{k+1}(X_{k+1}) \middle| \mathscr{A}_k\right]\right\}, \tag{A.6}$$

$$= \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{Q}_X X_k + V_k^A\hat{X}_k^{\mathsf{T}}\mathbf{K}^{\mathsf{T}}\mathbf{Q}_U\mathbf{K}\hat{X}_k \right.\right.$$
$$\left.\left. + \mathbb{E}\left[X_{k+1}^{\mathsf{T}}\mathbf{R}_{k+1}X_{k+1} \middle| \mathscr{A}_{k+1}\right] + d_{k+1} \middle| \mathscr{A}_k\right]\right\}, \tag{A.7}$$

$$= \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{Q}_X X_k + V_k^A\hat{X}_k^{\mathsf{T}}\mathbf{K}^{\mathsf{T}}\mathbf{Q}_U\mathbf{K}\hat{X}_k \right.\right.$$
$$\left.\left. + X_{k+1}^{\mathsf{T}}\mathbf{R}_{k+1}X_{k+1} + d_{k+1} \middle| \mathscr{A}_k\right]\right\}, \tag{A.8}$$

$$= \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{Q}_X X_k + V_k^A\hat{X}_k^{\mathsf{T}}\mathbf{K}^{\mathsf{T}}\mathbf{Q}_U\mathbf{K}\hat{X}_k + d_{k+1} \right.\right.$$
$$\left.\left. + \left(\mathbf{A}X_k - V_k^A\mathbf{B}\mathbf{K}\hat{X}_k + W_k\right)^{\mathsf{T}}\mathbf{R}_{k+1}\left(\mathbf{A}X_k - V_k^A\mathbf{B}\mathbf{K}\hat{X}_k + W_k\right) \middle| \mathscr{A}_k\right]\right\}, \tag{A.9}$$

where (A.7) follows from substituting $f_k(X_k)$ with (A.1). As reported in [65], it is shown for a monotonically increasing set, $\mathscr{A}_k$, (A.7) is in fact equal to (A.8). Thus, noting that $V_K^A$

is a binary variable in the quadratic expansion yields

$$\begin{aligned} f_k\left(X_k\right) = \max_{V_k^A = f_k(\mathscr{A}_k)} \Big\{ & \mathbb{E}\Big[ X_k^{\mathsf{T}} \left( \mathbf{A}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} + \mathbf{Q}_X \right) X_k + V_k^A \hat{X}_k^{\mathsf{T}} \mathbf{K}^{\mathsf{T}} \mathbf{Q}_U \mathbf{K} \hat{X}_k + d_{k+1} \\ & -2\, V_k^A \hat{X}_k^{\mathsf{T}} \mathbf{K}^{\mathsf{T}} \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} \hat{X}_k + V_k^A \hat{X}_k^{\mathsf{T}} \mathbf{K}^{\mathsf{T}} \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{B} \mathbf{K} \hat{X}_k \\ & + W_k^{\mathsf{T}} \mathbf{R}_{k+1} W_k \Big| \mathscr{A}_k \Big] \Big\}, \end{aligned} \tag{A.10}$$

$$\begin{aligned} = \max_{V_k^A = f_k(\mathscr{A}_k)} \Big\{ & \mathbb{E}\left[ X_k^{\mathsf{T}} \left( \mathbf{A}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} + \mathbf{Q}_X \right) X_k \Big| \mathscr{A}_k \right] + \operatorname{tr}\left( \Sigma_W \mathbf{R}_{k+1} \right) + \mathbb{E}[d_{k+1} | \mathscr{A}_k] \\ & + V_k^A \hat{X}_k^{\mathsf{T}} \left( \mathbf{K}^{\mathsf{T}} \left( \mathbf{Q}_U + \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{B} \right) \mathbf{K} - 2\, \mathbf{K}^{\mathsf{T}} \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} \right) \hat{X}_k \Big\}, \end{aligned} \tag{A.11}$$

where (A.11) follows from the fact that $W_k$ is an IID set of zero mean random variables with covariance matrix $\Sigma_W$. In view of this, to maximise (A.11) with respect to the input variable $V_k^A$ the only way to to affect the cost at each time instant is to actuate only when

$$\hat{X}_k^{\mathsf{T}} \left( \mathbf{K}^{\mathsf{T}} \left( \mathbf{Q}_U + \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{B} \right) \mathbf{K} - 2\, \mathbf{K}^{\mathsf{T}} \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} \right) \hat{X}_k > 0 \tag{A.12}$$

If (A.12) is true at time instance $k$ then $V_k^{A^*}$ equals one, thus increasing the overall cost at this time instant. Otherwise, $V_k^{A^*}$ is zero. This inequality corresponds to (A.2). Combining (A.11) and (A.3) yields

$$\begin{aligned} f_k\left(X_k\right) = & \mathbb{E}\left[ X_k^{\mathsf{T}} \left( \mathbf{A}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} + \mathbf{Q}_X \right) X_k \Big| \mathscr{A}_k \right] + \operatorname{tr}\left( \Sigma_W \mathbf{R}_{k+1} \right) + \mathbb{E}[d_{k+1} | \mathscr{A}_k] \\ & + V_k^{A^*} \hat{X}_k^{\mathsf{T}} \left( \mathbf{K}^{\mathsf{T}} \left( \mathbf{Q}_U + \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{B} \right) \mathbf{K} - 2\, \mathbf{K}^{\mathsf{T}} \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} \right) \hat{X}_k, \end{aligned} \tag{A.13}$$

$$\begin{aligned} = \mathbb{E}\Big[ & X_k^{\mathsf{T}} \Big( \mathbf{A}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} + \mathbf{Q}_X \\ & + V_k^{A^*} \left( \mathbf{K}^{\mathsf{T}} \left( \mathbf{Q}_U + \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{B} \right) \mathbf{K} - 2\, \mathbf{K}^{\mathsf{T}} \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} \right) \Big) X_k \Big| \mathscr{A}_k \Big] \\ & + \operatorname{tr}\left( \Sigma_W \mathbf{R}_{k+1} \right) + \mathbb{E}[d_{k+1} | \mathscr{A}_k] \\ & - \operatorname{tr}\left( V_k^{A^*} \left( \mathbf{K}^{\mathsf{T}} \left( \mathbf{Q}_U + \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{B} \right) \mathbf{K} - 2\, \mathbf{K}^{\mathsf{T}} \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} \right) P_{k|k} \right). \end{aligned} \tag{A.14}$$

Therefore, it follows that $\mathbf{R}_k$ and $d_k$ take the expressions shown in (A.2), substituting them gives

$$f_k(X_k) \;=\; \mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{R}_k X_k \middle| \mathscr{A}_k\right] + \; d_k. \tag{A.15}$$

This concludes the proof. □

## A.2 Lemma 5.1 [59]

This Section is dedicated to the proof of Lemma 5.1 within [59]. The Lemma is restated below.

**Lemma 5.1.** *Assume a linear time varying gain such that the optimal input, $u_k^*$ at time instance, $k$, is represented as $u_k^* = -\mathbf{K}_k^*\hat{x}_{k|k}$. The value function of the system under TCP-like conditions is written as*

$$g_k(X_k) \triangleq \mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{S}_k X_k \middle| \mathscr{O}_k\right] + \; c_k, \quad k = N, \ldots, 0, \tag{A.16}$$

*where $\mathbf{S}_k$ and $c_k$ are*

$$\mathbf{S}_k \triangleq \mathbf{A}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A} + \mathbf{Q}_X - \overline{V}\mathbf{A}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\mathbf{K}_k^*, \tag{A.17a}$$

$$c_k \triangleq \overline{V}\mathrm{tr}(\mathbf{A}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\mathbf{K}_k^* P_{k|k}) + \mathrm{tr}\left(\mathbf{Q}\mathbf{S}_{k+1}\right) + \mathbb{E}\left[c_{k+1}\middle|\mathscr{O}_k\right] \tag{A.17b}$$

*and $\mathbf{K}_k^*$ takes the form*

$$\mathbf{K}_k^* \triangleq \left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\right)^{-1}\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}. \tag{A.18}$$

*Proof.* The following proof takes the form of an induction proof. Namely, after showing the initial conditions hold true it is assumed that (A.1) holds true for time instant $k+1$. After which it is shown that it also holds true for time instant $k$, in doing so the recursive form of $\mathbf{S}_k$ is revealed, and in doing so, the recursive form of the optimal gain, $\mathbf{K}_k^*$. The

optimal value function, $g_k\left(X_k\right)$ is defined as

$$g_N\left(X_N\right) \triangleq \mathbb{E}\left[X_N^{\mathsf{T}}\mathbf{Q}_X X_N \middle| \mathcal{O}_N\right], \tag{A.19a}$$

$$g_k\left(X_k\right) \triangleq \min_{\mathbf{K}_k = g_k(\mathcal{O}_k)} \left\{\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{Q}_X X_k + V_k \hat{X}_k^{\mathsf{T}}\mathbf{K}^{\mathsf{T}}\mathbf{Q}_U\mathbf{K}\hat{X}_k + g_{k+1}(X_{k+1}) \middle| \mathcal{O}_k\right]\right\}. \tag{A.19b}$$

In order to proceed with the proof the initial conditions must be verified. With initial conditions such that, $\mathbf{S}_N = \mathbf{Q}_X$ and $c_N = 0$, it is seen that

$$g_N(X_N) \;=\; \mathbb{E}\left[X_N^{\mathsf{T}}\mathbf{S}_N X_N \middle| \mathcal{O}_N\right] + \; c_N = \mathbb{E}\left[X_N^{\mathsf{T}}\mathbf{Q}_X X_N \middle| \mathcal{O}_N\right] = J_0(\overline{X}_0, P_0). \tag{A.20}$$

Assuming that (A.16) holds for the $k+1$ time instance it shall be proved to also hold for the $k^{th}$ time instance. Beginning at (A.19b) it is seen that

$$g_k\left(X_k\right) = \min_{\mathbf{K}_k = g_k(\mathcal{O}_k)} \left\{\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{W}X_k + V_k\hat{X}_k^{\mathsf{T}}\mathbf{K}_k^{\mathsf{T}}\mathbf{U}\mathbf{K}_k\hat{X}_k + g_{k+1}\left(X_{k+1}\right) \middle| \mathcal{O}_k\right]\right\}, \tag{A.21}$$

$$= \min_{\mathbf{K}_k = g_k(\mathcal{O}_k)} \left\{\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{W}X_k + V_k\hat{X}_k^{\mathsf{T}}\mathbf{K}_k^{\mathsf{T}}\mathbf{U}\mathbf{K}_k\hat{X}_k \right.\right.$$
$$\left.\left. + \mathbb{E}\left[X_{k+1}^{\mathsf{T}}\mathbf{S}_{k+1}X_{k+1} \middle| \mathcal{O}_{k+1}\right] + c_{k+1} \middle| \mathcal{O}_k\right]\right\}, \tag{A.22}$$

$$= \min_{\mathbf{K}_k = g_k(\mathcal{O}_k)} \left\{\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{W}X_k + V_k\hat{X}_k^{\mathsf{T}}\mathbf{K}_k^{\mathsf{T}}\mathbf{U}\mathbf{K}_k\hat{X}_k + c_{k+1} \right.\right.$$
$$\left.\left. + \left(\mathbf{A}X_k - V_k\mathbf{B}\mathbf{K}_k\hat{X}_k + W_k\right)^{\mathsf{T}}\mathbf{S}_{k+1}\left(\mathbf{F}X_k - V_k\mathbf{G}\mathbf{K}_k\hat{X}_k + W_k\right) \middle| \mathcal{O}_k\right]\right\}, \tag{A.23}$$

$$= \min_{\mathbf{K}_k = g_k(\mathcal{O}_k)} \left\{\mathbb{E}\left[X_k^{\mathsf{T}}\left(\mathbf{A}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A} + \mathbf{W}\right)X_k \middle| \mathcal{O}_k\right] + \mathrm{tr}\left(\mathbf{Q}\mathbf{S}_{k+1}\right) + \mathbb{E}\left[c_{k+1} \middle| \mathcal{O}_k\right]\right.$$
$$\left. + \bar{V}\hat{X}_k^{\mathsf{T}}\left(\mathbf{K}_k^{\mathsf{T}}\left(\mathbf{U} + \mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\right)\mathbf{K}_k - 2\,\mathbf{K}_k^{\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}\right)\hat{X}_k\right\}, \tag{A.24}$$

where in (A.22) the lemma from [65][Lemma 1(c)] is utilised. To minimise (A.24) with respect to $\mathbf{K}_k$ the derivative $\partial V_k/\partial\mathbf{K}_k$ is

$$\frac{\partial V_k}{\partial \mathbf{K}_k} = 2\bar{V}\hat{X}_k^{\mathsf{T}}\left(\mathbf{U} + \mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\right)\mathbf{K}_k^*\hat{X}_k - 2\,\bar{V}\hat{X}_k^{\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}\hat{X}_k. \tag{A.25}$$

Setting this derivative equal to 0 and solving yields

$$\left(\mathbf{U}+\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\right)\mathbf{K}_k^*=\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}, \tag{A.26}$$

$$\mathbf{K}_k^*=\left(\mathbf{U}+\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\right)^{-1}\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}. \tag{A.27}$$

This corresponds to (A.18). Substitution of this optimal gain causes (A.24) to become

$$\begin{aligned}g_k\left(X_k\right)=&\mathbb{E}\left[X_k^{\mathsf{T}}\left(\mathbf{A}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}+\mathbf{W}\right)X_k\middle|\mathcal{O}_k\right]+\operatorname{tr}\left(\mathbf{Q}\mathbf{S}_{k+1}\right)+\mathbb{E}\left[c_{k+1}\middle|\mathcal{O}_k\right]\\&+\bar{V}\hat{X}_k^{\mathsf{T}}\mathbf{A}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\left(\mathbf{U}+\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\right)^{-1}\left(\mathbf{U}+\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\right)\left(\mathbf{U}+\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\right)^{-1}\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}\\&-2\bar{V}\hat{X}_k^{\mathsf{T}}\mathbf{A}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\left(\mathbf{U}+\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\right)^{-1}\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}\hat{X}_k.\end{aligned} \tag{A.28}$$

Cancelling out $\left(\mathbf{U}+\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\right)$ with its inverse results in the second term becoming equivalent to the third, causing them to amalgamate.

$$\begin{aligned}g_k\left(X_k\right)=&\mathbb{E}\left[X_k^{\mathsf{T}}\left(\mathbf{A}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}+\mathbf{W}\right)X_k\middle|\mathcal{O}_k\right]+\operatorname{tr}\left(\mathbf{Q}\mathbf{S}_{k+1}\right)+\mathbb{E}[c_{k+1}|\,\mathcal{O}_k]\\&-\bar{V}\hat{X}_k^{\mathsf{T}}\mathbf{A}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\left(\mathbf{U}+\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\right)^{-1}\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}\hat{X}_k.\end{aligned} \tag{A.29}$$

Substituting (A.18) for $\mathbf{K}_k^*$ yields

$$g_k\left(X_k\right)=\mathbb{E}\left[X_k^{\mathsf{T}}\left(\mathbf{A}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}+\mathbf{W}\right)X_k\middle|\mathcal{O}_k\right]+\operatorname{tr}\left(\mathbf{Q}\mathbf{S}_{k+1}\right)+c_{k+1}-\bar{V}\hat{X}_k^{\mathsf{T}}\mathbf{A}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\mathbf{K}_k^*\hat{X}_k, \tag{A.30}$$

$$\begin{aligned}g_k\left(X_k\right)=&\mathbb{E}\left[X_k^{\mathsf{T}}\left(\mathbf{A}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}+\mathbf{W}-\bar{V}\mathbf{A}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\mathbf{K}_k^*\right)X_k\middle|\mathcal{O}_k\right]+\operatorname{tr}\left(\mathbf{Q}\mathbf{S}_{k+1}\right)\\&+\mathbb{E}[c_{k+1}|\,\mathcal{O}_k]+\bar{V}\operatorname{tr}(\mathbf{A}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\mathbf{K}_k^*P_{k|k}),\end{aligned} \tag{A.31}$$

where (A.31) is achieved through use of [65, lemma 1(b)]. The proof of this lemma is supplied in Appendix A.4. This is of the same form as (A.17). Therefore, substitution gives

$$g_k\left(X_k\right)=\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{S}_kX_k\middle|\,\mathbf{A}_k\right]+c_k,\quad k=N,\ldots,0, \tag{A.32}$$

which corresponds to (A.16), as required. This Concludes the proof. □

## A.3 Theorem 1

This Appendix is dedicated to the proof of Theorem 1. The theorem is re-stated below.

**Theorem 1.** *The optimal value function of the attacker, for the system (3.1) where the operator assumes IID packet drops represented by $V_k^A$, is defined as*

$$f_N(X_N) \triangleq \mathbb{E}\left[X_N^{\mathsf{T}}\mathbf{Q}_X X_N \middle| \mathscr{A}_N\right], \tag{A.33a}$$

$$f_k(X_k) \triangleq \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{ \min_{\mathbf{K}_k = g_k(\mathscr{A}_k)} \left\{ \mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{Q}_X X_k + V_k^{A^*}\hat{X}_k^{\mathsf{T}}\mathbf{K}_k^{\mathsf{T}}\mathbf{Q}_U\mathbf{K}_k\hat{X}_k + f_{k+1}(X_{k+1}) | \mathscr{A}_k\right]\right\}\right], \tag{A.33b}$$

*where it is known that the minimising $\mathbf{K}_k$ is (3.30). It is shown that (A.33) is equivalent to*

$$f_k(X_k) \triangleq \mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{R}_k X_k \middle| \mathscr{A}_k\right] + d_k, \quad k = N, \ldots, 0, \tag{A.34}$$

*where the matrix $\mathbf{R}_k \in \mathbb{R}^{n\times n}$ and the scalar $d_k \in \mathbb{R}$ are recursively calculated according to*

$$\mathbf{R}_k = \mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X + V_k^{A^*}\Big(\mathbf{K}_k^{*\mathsf{T}}\Big(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\Big)\mathbf{K}_k^* - 2\mathbf{K}_k^{*\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A}\Big), \tag{A.35}$$

$$d_k = V_k^{A^*}\mathrm{tr}\left(\Big(\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X - \mathbf{R}_k\Big)P_{k|k}\right) + \mathrm{tr}\left(\Sigma_W\mathbf{R}_{k+1}\right) + \mathbb{E}[d_{k+1}|\mathscr{A}_k], \tag{A.36}$$

*where $V_k^{A^*}$ represents the optimal realisation at time $k$ that maximises the cost function of the operator and $\mathbf{K}_k^*$ is the optimal time varying gain that the operator implements at time $k$. The realisation of $V_k^{A^*}$ is determined by the inequality*

$$V_k^{A^*} \triangleq \begin{cases} 1 & \text{for} \quad \hat{X}_k^{\mathsf{T}}\left(\mathbf{K}_k^{*\mathsf{T}}\left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\Big)\mathbf{K}_k^* - 2\mathbf{K}_k^{*\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A}\Big)\hat{X}_k > 0, \\ 0 & \text{Otherwise,} \end{cases} \tag{A.37}$$

$$\mathbf{K}_k^* \triangleq \left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{B}\right)^{-1}\mathbf{B}^{\mathsf{T}}\mathbf{S}_{k+1}\mathbf{A}. \tag{A.38}$$

*Proof.* The following proof takes the form of an induction proof. Namely, after showing the initial conditions hold true it is assumed that (A.34) holds true for time instant $k+1$.

After which it is shown that it holds true for the time instant $k$, in doing so the recursive form of $\mathbf{R}_k$ and $d_k$ are revealed. Proceeding with the dynamic programming algorithm, with initial conditions $\mathbf{R}_N = \mathbf{W}$ and $d_N = 0$ the optimal value function at time $N$ is

$$f_N(X_N) \;=\; \mathbb{E}\left[X_N^{\mathsf{T}}\mathbf{R}_N X_N \middle| \mathscr{A}_N\right] + \; d_N = \mathbb{E}\left[X_N^{\mathsf{T}}\mathbf{Q}_X X_N \middle| \mathscr{A}_N\right] = J_0(\overline{X}_0, P_0). \tag{A.39}$$

Therefore, due to the equivalence, the initial conditions hold. By assuming the definition of the value function holds for the $k+1^{\text{th}}$ time instance it shall be proved to hold for the $k^{\text{th}}$.

$$\begin{aligned}
f_k\left(X_k\right) = & \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{ \min_{\mathbf{K}_k = g_k(\mathscr{A}_k)} \left\{ \mathbb{E}\left[ X_k^{\mathsf{T}}\mathbf{W}X_k + V_k^A \hat{X}_k^{\mathsf{T}}\mathbf{K}_k^{\mathsf{T}}\mathbf{U}\mathbf{K}_k\hat{X}_k \right.\right.\right. \\
& \left.\left.\left. + f_{k+1}\left(X_{k+1}\right) \middle| \mathscr{A}_k \right] \right\} \right\}, \qquad \text{(A.40)} \\
= & \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{ \min_{\mathbf{K}_k = g_k(\mathscr{A}_k)} \left\{ \mathbb{E}\left[ X_k^{\mathsf{T}}\mathbf{W}X_k + V_k^A \hat{X}_k^{\mathsf{T}}\mathbf{K}_k^{\mathsf{T}}\mathbf{U}\mathbf{K}_k\hat{X}_k \right.\right.\right. \\
& \left.\left.\left. + X_{k+1}^{\mathsf{T}}\mathbf{R}_{k+1}X_{k+1} \middle| \mathscr{A}_k \right] \right\} \right\}, \qquad \text{(A.41)} \\
= & \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{ \min_{\mathbf{K}_k = g_k(\mathscr{A}_k)} \left\{ \mathbb{E}\left[ X_k^{\mathsf{T}}\mathbf{W}X_k + V_k^A \hat{X}_k^{\mathsf{T}}\mathbf{K}_k^{\mathsf{T}}\mathbf{U}\mathbf{K}_k\hat{X}_k + d_{k+1} \right.\right.\right. \\
& \left.\left.\left. + \left(\mathbf{A}X_k - V_k^A\mathbf{B}\mathbf{K}_k\hat{X}_k + W_k\right)^{\mathsf{T}}\mathbf{R}_{k+1}\left(\mathbf{A}X_k - V_k^A\mathbf{B}\mathbf{K}_k\hat{X}_k + W_k\right) \middle| \mathscr{A}_k \right] \right\} \right\}, \qquad \text{(A.42)} \\
= & \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{ \min_{\mathbf{K}_k = g_k(\mathscr{A}_k)} \left\{ \mathbb{E}\left[ X_k^{\mathsf{T}}\left(\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{W}\right) X_k \middle| \mathscr{A}_k \right] + \operatorname{tr}\left(\Sigma_W \mathbf{R}_{k+1}\right) \right.\right. \\
& \left.\left. + \mathbb{E}\left[d_{k+1} | \mathscr{A}_k\right] + V_k^A \hat{X}_k^{\mathsf{T}}\left(\mathbf{K}_k^{\mathsf{T}}\left(\mathbf{U} + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\right)\mathbf{K}_k - 2\,\mathbf{K}_k^{\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A}\right)\hat{X}_k \right\} \right\} \qquad \text{(A.43)}
\end{aligned}$$

where the minimising $\mathbf{K}_k$ is calculated from (3.30) or is known by assumption. Therefore, with substitution of the optimal control gain, $\mathbf{K}_k^*$, (A.43) becomes

$$\begin{aligned}
f_k\left(X_k\right) = & \max_{V_k^A = f(\mathscr{A}_k)} \left\{ \mathbb{E}\left[ X_k^{\mathsf{T}}\left(\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{W}\right) X_k \middle| \mathscr{A}_k \right] + \operatorname{tr}\left(\Sigma_W \mathbf{R}_{k+1}\right) + \mathbb{E}\left[d_{k+1} | \mathscr{A}_k\right] \right. \\
& \left. + V_k^A \hat{X}_k^{\mathsf{T}}\left(\mathbf{K}_k^{*\mathsf{T}}\left(\mathbf{U} + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\right)\mathbf{K}_k^* - 2\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\mathbf{K}_k^*\right)\hat{X}_k \right\}. \qquad \text{(A.44)}
\end{aligned}$$

To maximise the value function with respect to $V_k^A$ the fourth term should only be allowed to contribute to the overall value of the function when the term is positive. This decision

corresponds to (A.37). Therefore, (A.44) becomes

$$f_k(X_k) = \mathbb{E}\Big[X_k^{\mathsf{T}}\Big(\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{W} + V_k^{A^*}\Big(\mathbf{K}_k^{\mathsf{T}*}\Big(\mathbf{U} + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\Big)\mathbf{K}_k^* - 2\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\mathbf{K}_k^*\Big)\Big)X_k \Big| \mathscr{A}_k\Big]$$
$$+\mathrm{tr}\left(\Sigma_W\mathbf{R}_{k+1}\right) + \mathbb{E}\left[d_{k+1}|\mathscr{A}_k\right]$$
$$-V_k^{A^*}\mathrm{tr}\left(\Big(\mathbf{K}_k^{\mathsf{T}*}\Big(\mathbf{U} + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\Big)\mathbf{K}_k^* - 2\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\mathbf{K}_k^*\Big)P_{k|k}\right), \quad \text{(A.45)}$$

where (A.45) is achieved through use of [65, lemma 1(b)]. The proof of this step is reported in Appendix A.4. Therefore, if $\mathbf{R}_k$ and $d_k$ are defined recursively as

$$\mathbf{R}_k = \mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X + V_k^{A^*}\Big(\mathbf{K}_k^{*\mathsf{T}}\Big(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\Big)\mathbf{K}_k^* - 2\mathbf{K}_k^{*\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A}\Big), \quad \text{(A.46)}$$
$$d_k = V_k^{A^*}\mathrm{tr}\left(\Big(\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X - \mathbf{R}_k\Big)P_{k|k}\right) + \mathrm{tr}\left(\Sigma_W\mathbf{R}_{k+1}\right) + \mathbb{E}[d_{k+1}|\mathscr{A}_k], \quad \text{(A.47)}$$

then (A.45) becomes

$$f_k(X_k) = \mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{R}_k X_k \Big| \mathscr{A}_k\right] + \; d_k, \quad k = N, \ldots, 0, \quad \text{(A.48)}$$

as required. This concludes the proof. □

## A.4 Lemma 1(b) [65]

This Appendix is dedicated to the proof of Lemma 1(b) reported within [65].

**Lemma 1(b)** ([65]). *The following facts are true:*

$$\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{R}X_k \Big| \mathscr{A}_k\right] = \hat{X}_k^{\mathsf{T}}\mathbf{R}\hat{X}_k + \mathrm{tr}\left(\mathbf{R}\; P_{k|k}\right) \quad \text{(A.49)}$$

*Proof.* Using standard algebraic operations

$$\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{R}X_k\middle|\mathscr{A}_k\right] = \mathbb{E}\left[\left(X_k+\hat{X}_k-\hat{X}_k\right)^{\mathsf{T}}\mathbf{R}\left(X_k+\hat{X}_k-\hat{X}_k\right)\middle|\mathscr{A}_k\right], \tag{A.50}$$

$$= \hat{X}_k^{\mathsf{T}}\mathbf{R}\hat{X}_k + \mathbb{E}\left[\left(X_k-\hat{X}_k\right)^{\mathsf{T}}\mathbf{R}\left(X_k-\hat{X}_k\right)\middle|\mathscr{A}_k\right]$$

$$+2\mathbb{E}\left[\hat{X}_k^{\mathsf{T}}\mathbf{R}\left(X_k-\hat{X}_k\right)\middle|\mathscr{A}_k\right], \tag{A.51}$$

$$= \hat{X}_k^{\mathsf{T}}\mathbf{R}\hat{X}_k + \mathrm{tr}\left(\mathbf{R}\mathbb{E}\left[\left(X_k-\hat{X}_k\right)\left(X_k-\hat{X}_k\right)^{\mathsf{T}}\middle|\mathscr{A}_k\right]\right)$$

$$+2\mathrm{tr}\left(\mathbf{R}\mathbb{E}\left[\left(X_k-\hat{X}_k\right)\hat{X}_k^{\mathsf{T}}\middle|\mathscr{A}_k\right]\right), \tag{A.52}$$

$$= \hat{X}_k^{\mathsf{T}}\mathbf{R}\hat{X}_k + \mathrm{tr}\left(\mathbf{R}\mathbb{E}\left[e_{k|k}e_{k|k}^{\mathsf{T}}\middle|\mathscr{A}_k\right]\right)$$

$$+2\ \mathrm{tr}\left(\mathbf{R}\mathbb{E}\left[X_k\hat{X}_k^{\mathsf{T}}-\hat{X}_k\hat{X}_k^{\mathsf{T}}\middle|\mathscr{A}_k\right]\right), \tag{A.53}$$

$$= \hat{X}_k^{\mathsf{T}}\mathbf{R}\hat{X}_k + \mathrm{tr}\left(\mathbf{R}\ P_{k|k}\right) + 2\ \mathrm{tr}\left(\mathbf{R}\left(\hat{X}_k\hat{X}_k^{\mathsf{T}}-\hat{X}_k\hat{X}_k^{\mathsf{T}}\right)\right), \tag{A.54}$$

$$\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{R}X_k\middle|\mathscr{A}_k\right] = \hat{X}_k^{\mathsf{T}}\mathbf{R}\hat{X}_k + \mathrm{tr}\left(\mathbf{R}\ P_{k|k}\right). \tag{A.55}$$

This concludes the proof. □

**Remark .** *The derivations in Chapter 3 use this relation with a re-arrangement such that*

$$\hat{X}_k^{\mathsf{T}}\mathbf{R}\hat{X}_k\ = \mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{R}X_k\middle|\mathscr{A}_k\right] - \mathrm{tr}\left(\mathbf{R}\ P_{k|k}\right). \tag{A.56}$$

## A.5 Lemma 6

This Appendix is dedicated to the proof of Lemma 6. The lemma is re-stated below.

**Lemma 6.** *The optimal value function for the attack on the system system (3.20), where the operator assumes IID packet drops, with a time varying detection constraint is defined as*

$$f_N\left(X_N\right) \triangleq \mathbb{E}\left[X_N^{\mathsf{T}}\mathbf{Q}_X X_N\middle|\mathscr{A}_N\right], \tag{A.57a}$$

$$f_k\left(X_k\right) \triangleq \max_{V_k^A = f_k(\mathscr{A}_k)} \Big\{\mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{Q}_X X_k + V_k^A\widehat{X}_k^{\mathsf{T}}\mathbf{K}_k'^{*}\mathbf{Q}_U\mathbf{K}_k^{*}\widehat{X}_k + \widehat{X}_k^{\mathsf{T}}t\left(\Lambda_k\right)\widehat{X}_k\right.$$

$$\left. + f_{k+1}\left(X_{k+1}\right)\middle|\mathscr{A}_k\right]\Big\}, \tag{A.57b}$$

*where* $\Lambda_k$ *is defined as*

$$\Lambda_k = \Lambda \mathbf{R}_{k+1} \sqrt{k}. \tag{A.58}$$

*It holds that (A.5) is equivalent to*

$$f_k(X_k) \triangleq \mathbb{E}\left[ X_k^{\mathsf{T}} \mathbf{R}_k X_k \middle| \mathscr{A}_k \right] + \ d_k, \quad k = N, \ldots, 0, \tag{A.59}$$

*where the matrix* $\mathbf{R}_k \in \mathbb{M}^n$ *and* $d_k \in \mathbb{R}$ *are recursively calculated according to*

$$\begin{aligned} \mathbf{R}_k = \mathbf{A}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} + \mathbf{Q}_X & \\ + V_k^{A^*} \left( \mathbf{K}_k^{*\mathsf{T}} \left( \mathbf{Q}_U + \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{B} \right) \mathbf{K}_k^* - 2 \mathbf{K}_k^{*\mathsf{T}} \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} \right), & \quad \text{(A.60)} \\ d_k = V_k^{A^*} \operatorname{tr}\left( \left( \mathbf{A}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} + \mathbf{Q}_X - \mathbf{R}_k \right) \mathbf{P}_{k|k} \right) + \operatorname{tr}\left( \Sigma_W \mathbf{R}_{k+1} \right) + \mathbb{E}[d_{k+1} | \mathscr{A}_k] & \\ - \widehat{X}_k t\left( \Lambda_k \right) \widehat{X}_k, & \quad \text{(A.61)} \end{aligned}$$

*where* $V_k^{A^*}$ *represents the optimal decision of* $V_i^A$ *that maximises the cost function of the operator. The decision is determined by the inequality*

$$V_k^{A^*} \triangleq \begin{cases} 1 & \text{for} \quad \left( \mathbf{K}_k^{*\prime} \left( \mathbf{Q}_U + \mathbf{B}' \mathbf{R}_{k+1} \mathbf{B} \right) \mathbf{K}_k^* - 2 \mathbf{K}_k^{*\prime} \mathbf{B}' \mathbf{R}_{k+1} \mathbf{A} \right) > t\left( \Lambda_k \right) \\ 0 & \text{otherwise,} \end{cases}, \tag{A.62}$$

*Proof.* The following takes the form of an induction proof. Namely, after showing the initial conditions hold true it is assumed that (A.57) holds true for time instant $k+1$. After which it is shown that it holds true for the time instant $k$, in doing so the recursive form of $\mathbf{R}_k$ and $d_k$ are revealed. Proceeding with the dynamic programming algorithm, with initial conditions $\mathbf{R}_N = \mathbf{Q}_X$ and $d_N = 0$ the optimal value function at time $N$ is

$$f_N(X_N) \ = \ \mathbb{E}\left[ X_N^{\mathsf{T}} \mathbf{R}_N X_N \middle| \mathscr{A}_N \right] + d_N = \mathbb{E}\left[ X_N^{\mathsf{T}} \mathbf{Q}_X X_N \middle| \mathscr{A}_N \right] = J_0(\overline{X}_0, P_0). \tag{A.63}$$

Therefore, due to the equivalence, the initial conditions hold. By assuming the definition of the value function holds for the $k+1^{\text{th}}$ time instance it shall be proved to hold for

the $k^{\text{th}}$.

$$f_k\left(X_k\right) = \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{ \min_{\mathbf{K}_k = g_k(\mathscr{A}_k)} \left\{ \mathbb{E}\left[ X_k^{\mathsf{T}} \mathbf{Q}_X X_k + V_k^A \widehat{X}_k^{\mathsf{T}} \mathbf{K}_k' \mathbf{Q}_U \mathbf{K}_k^* \widehat{X}_k - \widehat{X}_k^{\mathsf{T}} t\left(\Lambda_k\right) \widehat{X}_k \right.\right.\right.$$
$$\left.\left.\left. + d_{k+1} + f_{k+1}\left(X_{k+1}\right) \right| \mathscr{A}_k \right] \right\} \right\}, \tag{A.64}$$

$$= \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{ \min_{\mathbf{K}_k = g_k(\mathscr{A}_k)} \left\{ \mathbb{E}\left[ X_k^{\mathsf{T}} \mathbf{Q}_X X_k + V_k^A \widehat{X}_k^{\mathsf{T}} \mathbf{K}_k' \mathbf{Q}_U \mathbf{K}_k \widehat{X}_k - \widehat{X}_k^{\mathsf{T}} t\left(\Lambda_k\right) \widehat{X}_k \right.\right.\right.$$
$$\left.\left.\left. + X_{k+1}^{\mathsf{T}} \mathbf{R}_{k+1} X_{k+1} \right| \mathscr{A}_k \right] \right\} \right\}, \tag{A.65}$$

$$= \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{ \min_{\mathbf{K}_k = g_k(\mathscr{A}_k)} \left\{ \mathbb{E}\left[ X_k^{\mathsf{T}} \mathbf{Q}_X X_k + V_k^A \widehat{X}_k^{\mathsf{T}} \mathbf{K}_k' \mathbf{Q}_U \mathbf{K}_k \widehat{X}_k - \widehat{X}_k^{\mathsf{T}} t\left(\Lambda_k\right) \widehat{X}_k + d_{k+1} \right.\right.\right.$$
$$\left.\left.\left. + \left(\mathbf{A} X_k - V_k^A \mathbf{B} \mathbf{K}_k \hat{X}_k + W_k\right)^{\mathsf{T}} \mathbf{R}_{k+1} \left(\mathbf{A} X_k - V_k^A \mathbf{B} \mathbf{K}_k \hat{X}_k + W_k\right) \right| \mathscr{A}_k \right] \right\} \right\}, \tag{A.66}$$

$$= \max_{V_k^A = f_k(\mathscr{A}_k)} \left\{ \min_{\mathbf{K}_k = g_k(\mathscr{A}_k)} \left\{ \mathbb{E}\left[ X_k^{\mathsf{T}} \left(\mathbf{A}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} + \mathbf{W}\right) X_k \right| \mathscr{A}_k \right] + \operatorname{tr}\left(\Sigma_W \mathbf{R}_{k+1}\right) \right.$$
$$- \widehat{X}_k^{\mathsf{T}} t\left(\Lambda_k\right) \widehat{X}_k + \mathbb{E}\left[d_{k+1} | \mathscr{A}_k\right]$$
$$\left. + V_k^A \hat{X}_k^{\mathsf{T}} \left(\mathbf{K}_k^{\mathsf{T}} \left(\mathbf{U} + \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{B}\right) \mathbf{K}_k - 2 \mathbf{K}_k^{\mathsf{T}} \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A}\right) \hat{X}_k \right\} \right\}, \tag{A.67}$$

the minimising $\mathbf{K}_k$ is calculated from (3.30) or is known by assumption. Therefore, with substitution of the optimal control gain, $\mathbf{K}_k^*$, (A.67) becomes

$$f_k\left(X_k\right) = \max_{V_k^A = f(\mathscr{A}_k)} \left\{ \mathbb{E}\left[ X_k^{\mathsf{T}} \left(\mathbf{A}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{A} + \mathbf{W}\right) X_k \right| \mathscr{A}_k \right] + \operatorname{tr}\left(\Sigma_W \mathbf{R}_{k+1}\right) + \mathbb{E}\left[d_{k+1} | \mathscr{A}_k\right] \right.$$
$$\left. - \widehat{X}_k^{\mathsf{T}} t\left(\Lambda_k\right) \widehat{X}_k + V_k^A \hat{X}_k^{\mathsf{T}} \left( \mathbf{K}_k^{\mathsf{T}*} \left(\mathbf{U} + \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{B}\right) \mathbf{K}_k^* - 2 \mathbf{A}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{B} \mathbf{K}_k^* \right) \hat{X}_k \right\}. \tag{A.68}$$

To maximise the value function with respect to $V_k^A$ only two terms depend on $V_k^A$. The decision therefore, depends on

$$\hat{X}_k^{\mathsf{T}} \left( \mathbf{K}_k^{\mathsf{T}*} \left(\mathbf{U} + \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{B}\right) \mathbf{K}_k^* - 2 \mathbf{A}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{B} \mathbf{K}_k^* \right) \hat{X}_k - \widehat{X}_k^{\mathsf{T}} t\left(\Lambda_k\right) \widehat{X}_k > 0, \tag{A.69}$$

$$\tag{A.70}$$

or equivalently

$$\hat{X}_k^{\mathsf{T}} \left( \mathbf{K}_k^{\mathsf{T}*} \left(\mathbf{U} + \mathbf{B}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{B}\right) \mathbf{K}_k^* - 2 \mathbf{A}^{\mathsf{T}} \mathbf{R}_{k+1} \mathbf{B} \mathbf{K}_k^* \right) \hat{X}_k > \widehat{X}_k^{\mathsf{T}} t\left(\Lambda_k\right) \widehat{X}_k. \tag{A.71}$$

Note that due to the fact that both terms are scaled by a quadratic in $\hat{X}_k$ the above definition is equivalent (A.62). Therefore, with the maximisation solved, (A.68) becomes

$$\begin{aligned} f_k\left(X_k\right) = \mathbb{E}\Big[X_k^{\mathsf{T}}\Big(\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{W} + V_k^{A^*}\Big(\mathbf{K}_k^{\mathsf{T}*}\Big(\mathbf{U} + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\Big)\mathbf{K}_k^* - 2\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\mathbf{K}_k^*\Big)\Big)X_k\Big|\,\mathscr{A}_k\Big] \\ -\widehat{X}_k^{\mathsf{T}}t\left(\Lambda_k\right)\widehat{X}_k + \operatorname{tr}\left(\Sigma_W\mathbf{R}_{k+1}\right) + \mathbb{E}\left[d_{k+1}|\mathscr{A}_k\right] \\ -V_k^{A^*}\operatorname{tr}\left(\Big(\mathbf{K}_k^{\mathsf{T}*}\Big(\mathbf{U} + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\Big)\mathbf{K}_k^* - 2\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\mathbf{K}_k^*\Big)P_{k|k}\right), \end{aligned} \tag{A.72}$$

where (A.72) is achieved through use of [65, lemma 1(b)]. The proof of this step is reported in Appendix A.4. Therefore, if $\mathbf{R}_k$ and $d_k$ are defined recursively as

$$\begin{aligned} \mathbf{R}_k = \mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X \\ +V_k^{A^*}\left(\mathbf{K}_k^{*\mathsf{T}}\left(\mathbf{Q}_U + \mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{B}\right)\mathbf{K}_k^* - 2\mathbf{K}_k^{*\mathsf{T}}\mathbf{B}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A}\right), \end{aligned} \tag{A.73}$$

$$\begin{aligned} d_k = V_k^{A^*}\operatorname{tr}\left(\left(\mathbf{A}^{\mathsf{T}}\mathbf{R}_{k+1}\mathbf{A} + \mathbf{Q}_X - \mathbf{R}_k\right)\mathbf{P}_{k|k}\right) + \operatorname{tr}\left(\Sigma_W\mathbf{R}_{k+1}\right) + \mathbb{E}[d_{k+1}|\mathscr{A}_k] \\ -\widehat{X}_k t\left(\Lambda_k\right)\widehat{X}_k, \end{aligned} \tag{A.74}$$

Substitution of these definitions results in

$$f_k\left(X_k\right) = \mathbb{E}\left[X_k^{\mathsf{T}}\mathbf{R}_k X_k\middle|\mathscr{A}_k\right] + \; d_k, \tag{A.75}$$

where

$$V_k^{A^*} \triangleq \begin{cases} 1 & \text{for} \quad \left(\mathbf{K}_k^{*\prime}\left(\mathbf{Q}_U + \mathbf{B}'\mathbf{R}_{k+1}\mathbf{B}\right)\mathbf{K}_k^* - 2\mathbf{K}_k^{*\prime}\mathbf{B}'\mathbf{R}_{k+1}\mathbf{A}\right) > t\left(\Lambda_k\right) \\ 0 & \text{otherwise,} \end{cases}, \tag{A.76}$$

as required. This concludes the proof. □

# Appendix B

# Chapter 4

## B.1 Lemma 7

**Lemma 7.** *Consider the system modelled by (4.1) with access to the information sets given by (4.2). Then the following holds*

$$\mathbb{E}\left[\mathbf{E}_k^{\mathsf{T}}\Omega\mathbf{E}_k\middle|\mathcal{F}_k\right] = \operatorname{tr}\left(\Omega_l\Sigma_{\mathcal{W}}\right), \tag{B.1a}$$

$$\mathbb{E}\left[\mathbf{E}_k^{\mathsf{T}}\Omega\mathbf{E}_k\middle|\mathcal{G}_k\right] = \mathcal{U}_k\left(\mathcal{G}_k\right)^{\mathsf{T}}\overline{\Upsilon}\left(\mathbf{I}\odot\Omega_g\right)\left(\mathbf{I}-\overline{\Upsilon}\right)\mathcal{U}_k\left(\mathcal{G}_k\right) + \operatorname{tr}\left(\Omega_l\Sigma_{\mathcal{W}}\right), \tag{B.1b}$$

*where* $\Omega_l = \Lambda\Omega\Lambda$.

*The proof is split into two parts, one for the TCP-like protocol and one for the UDP-like protocol, respectively.*

*Proof.* **TCP-like protocol**

The expected error in TCP-like follows from (4.8a). Substituting this into the left-hand side of (4.15a) yields

$$\begin{aligned}\mathbb{E}\left[\mathbf{E}_k^{\mathsf{T}}\Omega\mathbf{E}_k\middle|\mathcal{F}_k\right] &= \mathbb{E}\left[\mathcal{W}_k^{\mathsf{T}}\Omega_l\mathcal{W}_k\middle|\mathcal{F}_k\right] &\text{(B.2)}\\ &= \operatorname{tr}\left(\Omega_l\Sigma_{\mathcal{W}}\right). &\text{(B.3)}\end{aligned}$$

This completes the TCP-like part of the proof.

**UDP-like protocol**

The error in UDP-like estimation follows from (4.8b). Substituting this into the left-hand side of (4.15b) gives

$$\mathbb{E}\left[\mathbf{E}_k^{\mathsf{T}}\Omega\mathbf{E}_k\middle|\mathcal{G}_k\right] = \mathbb{E}\left[\mathcal{U}_k{}^{\mathsf{T}}\left(\Upsilon_k - \overline{\Upsilon}\right)\Omega_g\left(\Upsilon_k - \overline{\Upsilon}\right)\mathcal{U}_k\middle|\mathcal{G}_k\right] + \mathbb{E}\left[\mathcal{W}_k^{\mathsf{T}}\Lambda\Omega\Lambda\mathcal{W}_k\middle|\mathcal{G}_k\right], \quad \text{(B.4)}$$

where we use the fact that $\mathcal{W}_k$ is zero mean to eliminate the cross terms. Note that the second term is identical to the TCP-like case, in (B.2). Therefore, we have that

$$\mathbb{E}\left[\mathbf{E}_k^{\mathsf{T}}\Omega\mathbf{E}_k\middle|\mathcal{G}_k\right] = \mathbb{E}\left[\mathcal{U}_k{}^{\mathsf{T}}\Upsilon_k\Omega_g\Upsilon_k\mathcal{U}_k\middle|\mathcal{G}_k\right] - \mathcal{U}_k\left(\mathcal{G}_k\right)^{\mathsf{T}}\overline{\Upsilon}\Omega_g\overline{\Upsilon}\mathcal{U}_k\left(\mathcal{G}_k\right) + \operatorname{tr}\left(\Omega_l\Sigma_{\mathcal{W}}\right). \quad \text{(B.5)}$$

It follows from Lemma 21 that

$$\mathbb{E}\left[\mathbf{E}_k^{\mathsf{T}}\Omega\mathbf{E}_k\middle|\mathcal{G}_k\right] = \mathcal{U}_k\left(\mathcal{G}_k\right)^{\mathsf{T}}\overline{\Upsilon}\left(\mathbf{I}\odot\Omega_g\right)\left(\mathbf{I} - \overline{\Upsilon}\right)\mathcal{U}_k\left(\mathcal{G}_k\right) + \operatorname{tr}\left(\Omega_l\Sigma_{\mathcal{W}}\right). \quad \text{(B.6)}$$

This concludes the proof. □

## B.2 Lemma 21

**Lemma 21.** *It holds that*

$$\begin{aligned}\mathbb{E}\left[\mathcal{U}_k{}^{\mathsf{T}}\Upsilon_k{}^{\mathsf{T}}\Omega_g\Upsilon_k\mathcal{U}_k\middle|\mathcal{G}_k\right] = &\mathcal{U}_k\left(\mathcal{G}_k\right)^{\mathsf{T}}\overline{\Upsilon}\Omega_g\overline{\Upsilon}\mathcal{U}_k\left(\mathcal{G}_k\right)\\ &+\mathcal{U}_k\left(\mathcal{G}_k\right)^{\mathsf{T}}\overline{\Upsilon}\left(\mathbf{I}\odot\Omega_g\right)\left(\mathbf{I} - \overline{\Upsilon}\right)\mathcal{U}_k\left(\mathcal{G}_k\right), \quad \text{(B.7)}\end{aligned}$$

*where* $\mathbf{I}$ *is the identity matrix and* $\odot$ *is the element wise Hadamard product.*

*Proof.* The left hand side of (B.7) is scalar, and therefore

$$\begin{aligned}
\mathbb{E}\left[\mathcal{U}_k\left(\mathcal{G}_k\right)^{\mathsf{T}} \ \Upsilon_k{}^{\mathsf{T}}\Omega_g\Upsilon_k\mathcal{U}_k\left(\mathcal{G}_k\right)\middle|\mathcal{G}_k\right] &= \mathbb{E}\left[U_0\left(\mathcal{G}_k\right)\mathbf{V}_0\left(\Omega_g\right)_{1,1}\mathbf{V}_0U_0\left(\mathcal{G}_k\right)\middle|\mathcal{G}_k\right] \\
&\quad+\mathbb{E}\left[U_0\left(\mathcal{G}_k\right)\mathbf{V}_0\left(\Omega_g\right)_{1,2}\mathbf{V}_1U_1\left(\mathcal{G}_k\right)\middle|\mathcal{G}_k\right] \\
&\cdots+\mathbb{E}\left[U_{Nm-1}\left(\mathcal{G}_k\right)\mathbf{V}_{Nm-1}\left(\Omega_g\right)_{Nm,Nm}\mathbf{V}_{Nm-1}U_{Nm-1}\left(\mathcal{G}_k\right)\middle|\mathcal{G}_k\right] \qquad \text{(B.8)} \\
&=\sum_{i=1}^{Nm}\Bigg(U_{i-1}\left(\mathcal{G}_k\right)\mathbf{M}_{i-1}\left(\Omega_g\right)_{i,i}U_{i-1}\left(\mathcal{G}_k\right) \\
&\quad+\sum_{j=1,j\neq i}^{Nm}U_{i-1}\left(\mathcal{G}_k\right)\mathbf{M}_{i-1}\left(\Omega_g\right)_{i,j}\mathbf{M}_{j-1}U_{j-1}\left(\mathcal{G}_k\right)\Bigg) \qquad \text{(B.9)} \\
&=\sum_{i=1}^{Nm}\sum_{j=1}^{Nm}U_{i-1}\left(\mathcal{G}_k\right)\mathbf{M}_{i-1}\left(\Omega_g\right)_{i,i}\left(1-\mathbf{M}_{i-1}\right)U_{i-1}\left(\mathcal{G}_k\right) \\
&\quad+U_{i-1}\left(\mathcal{G}_k\right)\mathbf{M}_{i-1}\left(\Omega_g\right)_{i,j}\mathbf{M}_{j-1}U_{j-1}\left(\mathcal{G}_k\right) \qquad \text{(B.10)} \\
&=\mathcal{U}_k\left(\mathcal{G}_k\right)^{\mathsf{T}}\overline{\Upsilon}\left(\mathbf{I}\odot\Omega_g\right)\left(\mathbf{I}-\overline{\Upsilon}\right)\mathcal{U}_k\left(\mathcal{G}_k\right)+\mathcal{U}_k\left(\mathcal{G}_k\right)^{\mathsf{T}}\overline{\Upsilon}\Omega_g\overline{\Upsilon}\mathcal{U}_k\left(\mathcal{G}_k\right), \qquad \text{(B.11)}
\end{aligned}$$

where $\left(\Omega_g\right)_{i,i}$ represents the $(i,j)$-th element of $\Omega_g$. This concludes the proof. □

## B.3 Theorem 2

**Theorem 2.** *Consider the closed-loop system with plant dynamics given in (4.1), protocol dependent information sets given in (4.2) and controller cost function given in (4.10). Then the optimal cost for the TCP-like protocol is*

$$J^*\left(\mathcal{F}_k\right)=X_k^{\mathsf{T}}\left(\mathbf{Q}+\Omega_p\right)X_k+\operatorname{tr}\left(\Sigma_{\mathcal{W}}\Omega_l\right)-X_k^{\mathsf{T}}\mathbf{F}^{\mathsf{T}}\mathbf{G}^{-1}\left(\mathcal{F}_k\right)\overline{\Upsilon}\mathbf{F}X_k, \qquad \text{(B.12)}$$

*and the optimal cost for the UDP-like protocol is*

$$J^*\left(\mathcal{G}_k\right)=X_k^{\mathsf{T}}\left(\mathbf{Q}+\Omega_p\right)X_k+\operatorname{tr}\left(\Sigma_{\mathcal{W}}\Omega_l\right)-X_k^{\mathsf{T}}\mathbf{F}^{\mathsf{T}}\mathbf{G}^{-1}\left(\mathcal{G}_k\right)\overline{\Upsilon}\mathbf{F}X_k. \qquad \text{(B.13)}$$

*As with Lemma 7 the proof is split into two parts to account for both protocols.*

*Proof.* **Optimal Cost for the TCP-like Protocol**

Substituting (4.15a) into (4.14), noting that under the TCP-like protocol the error term does not depend on $\mathcal{U}_k$, gives

$$J^*\left(\mathscr{F}_k\right) = X_k^{\mathsf{T}}\left(\mathbf{Q}+\Omega_p\right)X_k + \operatorname{tr}\left(\Omega_l\Sigma_{\mathcal{W}}\right) + \min_{\mathcal{U}_k(\mathscr{G}_k)}\left\{\mathcal{U}_k\left(\mathscr{G}_k\right)^{\mathsf{T}}\overline{\Upsilon}\left(2\mathbf{F}X_k + \left(\Omega_g\overline{\Upsilon}+\Psi\right)\mathcal{U}_k\left(\mathscr{G}_k\right)\right)\right\}. \tag{B.14}$$

Note that $\left(\Omega_g\overline{\Upsilon}+\Psi\right)$ is positive definite, and therefore, (B.14) is convex. Taking the derivative of the cost with respect to $\mathcal{U}_k$ yields

$$\frac{\partial J^*\left(\mathscr{F}_k\right)}{\partial \mathcal{U}_k} = 2\overline{\Upsilon}\left(\mathbf{F}X_k + \left(\Omega_g\overline{\Upsilon}+\Psi\right)\mathcal{U}_k\left(\mathscr{F}_k\right)\right). \tag{B.15}$$

Solving for all $\overline{\Upsilon} \neq \mathbf{0}$, the minimising value of $\mathcal{U}_k\left(\mathscr{F}_k\right)$ is

$$\mathcal{U}_k^*\left(\mathscr{F}_k\right) \triangleq -\left(\Omega_g\overline{\Upsilon}+\Psi\right)^{-1}\mathbf{F}X_k. \tag{B.16}$$

Denoting $\left(\Omega_g\overline{\Upsilon}+\Psi\right)$ by $\mathbf{G}^{-1}\left(\mathscr{F}_k\right)$ and substituting $\Upsilon^*_{k|\mathcal{F}_k}$ into (B.14) results in the optimal expected cost for the operator:

$$J^*\left(\mathscr{F}_k\right) = X_k^{\mathsf{T}}\left(\mathbf{Q}+\Omega_p\right)X_k + \operatorname{tr}\left(\Sigma_{\mathcal{W}}\Omega_l\right) - X_k^{\mathsf{T}}\mathbf{F}^{\mathsf{T}}\mathbf{G}^{-1}\left(\mathscr{F}_k\right)\overline{\Upsilon}\mathbf{F}X_k.$$

This concludes the TCP-like part of the proof.

**Optimal Cost for the UDP-like Protocol**

Combining (4.15b) and (4.14) the optimal cost function for the UDP-like protocol is given by

$$J^*\left(\mathscr{G}_k\right) = X_k^{\mathsf{T}}\left(\mathbf{Q}+\Omega_p\right)X_k + \operatorname{tr}\left(\Omega_l\Sigma_{\mathcal{W}}\right) + \min_{\mathcal{U}_k(\mathscr{G}_k)}\left\{\mathcal{U}_k\left(\mathscr{G}_k\right)^{\mathsf{T}}\overline{\Upsilon}\left(2\mathbf{F}X_k + \left(\Omega_g\overline{\Upsilon}+\Psi+\left(\mathbf{I}\odot\Omega_g\right)\left(\mathbf{I}-\overline{\Upsilon}\right)\right)\mathcal{U}_k\left(\mathscr{G}_k\right)\right)\right\}. \tag{B.17}$$

Following the same process as with the TCP-like case, noting that $\left(\Omega_g\overline{\Upsilon}+\Psi+\left(\mathbf{I}\odot\Omega_g\right)\left(\mathbf{I}-\overline{\Upsilon}\right)\right)$ is positive definite, and that therefore the minimisation is convex, yields

$$\frac{\partial J^*\left(\mathcal{G}_k\right)}{\partial\mathcal{U}_k}=2\overline{\Upsilon}\left(\mathbf{F}X_k+\left(\Omega_g\overline{\Upsilon}+\Psi+\left(\mathbf{I}\odot\Omega_g\right)\left(\mathbf{I}-\overline{\Upsilon}\right)\right)\mathcal{U}_k\left(\mathcal{G}_k\right)\right),$$

with the optimal value of $\mathcal{U}_k^*\left(\mathcal{G}_k\right)$ given by

$$\mathcal{U}_k^*\left(\mathcal{G}_k\right)\triangleq-\left(\Psi+\left(\mathbf{I}\odot\Omega_g\right)\left(\mathbf{I}-\overline{\Upsilon}\right)+\Omega_g\overline{\Upsilon}\right)^{-1}\mathbf{F}X_k. \tag{B.18}$$

Re-labelling $\left(\Psi+\left(\mathbf{I}\odot\Omega_g\right)\left(\mathbf{I}-\overline{\Upsilon}\right)+\Omega_g\overline{\Upsilon}\right)$ as $\mathbf{G}\left(\mathcal{G}_k\right)$ and substituting $\mathcal{U}_k^*\left(\mathcal{G}_k\right)$ into (B.14) yields the optimal expected cost for the operator:

$$J^*\left(\mathcal{G}_k\right)=X_k^{\mathsf{T}}\left(\mathbf{Q}+\Omega_p\right)X_k+\mathrm{tr}\left(\Sigma_{\mathcal{W}}\Omega_l\right)-X_k^{\mathsf{T}}\mathbf{F}^{\mathsf{T}}\mathbf{G}^{-1}\left(\mathcal{G}_k\right)\overline{\Upsilon}\mathbf{F}X_k. \tag{B.19}$$

This concludes the proof. □

## B.4 Lemma 8

**Lemma 8.** *Let us define the cost difference between the UDP-like and the TCP-like protocols as*

$$J_\Delta^*\left(\overline{\Upsilon}\right)\triangleq J^*\left(\mathcal{G}_k\right)-J^*\left(\mathcal{F}_k\right)\ >\ 0. \tag{B.20}$$

*The derivative of this cost difference is*

$$\begin{aligned}\frac{\partial J_\Delta^*\left(\overline{\Upsilon}\right)}{\partial\overline{\Upsilon}}=X_k^{\mathsf{T}}\mathbf{F}^{\mathsf{T}}\Big(&\mathbf{G}^{-1}\left(\mathcal{G}_k\right)\Big(\left(1-2\overline{\Upsilon}\right)\Omega_d\\&-\overline{\Upsilon}\left(1\text{-}\overline{\Upsilon}\right)\left[\Omega_h\mathbf{G}^{-1}\left(\mathcal{G}_k\right)\Omega_d+\Omega_d\mathbf{G}^{-1}\left(\mathcal{F}_k\right)\Omega_g\right]\Big)\mathbf{G}^{-1}\left(\mathcal{F}_k\right)\Big)\mathbf{F}X_k,\end{aligned} \tag{B.21}$$

*where* $\Omega_d=\left(\mathbf{I}\odot\Omega_g\right)$ *and* $\overline{\Upsilon}\in[0,1]$.

*Proof.* In order to proceed with the proof we analyse the matrices $\mathbf{G}^{-1}(\mathscr{F}_k)$ and $\mathbf{G}^{-1}(\mathscr{G}_k)$.

We define the mapping $\mathbf{G_I}(\alpha, \mathbf{A}, \mathbf{B}) : \mathbb{R} \times \mathbb{R}^{nN\times nN} \times \mathbb{R}^{nN\times nN} \to \mathbb{R}^{nN\times nN}$

$$\mathbf{G_I}(\alpha, \mathbf{A}, \mathbf{B}) = (\alpha\mathbf{A} + \mathbf{B})^{-1}, \tag{B.22}$$

where $\alpha \in [0, 1]$, $\mathbf{A} \in \mathbb{R}^{nN\times nN}$, and $\mathbf{B} \in \mathbb{R}^{nN\times nN}$. Note that $\mathbf{G_I}(\alpha, \Omega_g, \Psi) = \mathbf{G}^{-1}(\mathscr{F}_k)$ and $\mathbf{G_I}(\alpha, \Omega_h, [\Omega_d + \Psi]) = \mathbf{G}^{-1}(\mathscr{G}_k)$. Additionally, all arguments of $\mathbf{G_I}(\alpha, \mathbf{A}, \mathbf{B})$ are symmetric and $\mathbf{B}$ is a diagonal positive definite matrix for both protocols. From this point, due to the fact that the matrices $\mathbf{A}$ and $\mathbf{B}$ are constants, we simplify the notation to $\mathbf{G_I}(\alpha)$ and note that the results below apply to both the UDP-like and the TCP-like protocols. The first derivative of the function $\mathbf{G_I}(\alpha)$ is

$$\begin{aligned}\frac{\partial}{\partial\beta}\mathbf{G_I}(\beta) &= \frac{\partial}{\partial\beta}(\beta\mathbf{A} + \mathbf{B})^{-1} \\ &= -(\beta\mathbf{A} + \mathbf{B})^{-1}\left[\frac{\partial}{\partial\beta}(\beta\mathbf{A} + \mathbf{B})\right](\beta\mathbf{A} + \mathbf{B})^{-1},\end{aligned} \tag{B.23}$$

where in (B.23) the derivative is recast according to [30, 17.3(a)]. The derivative results in

$$\frac{\partial}{\partial\beta}\mathbf{G_I}(\beta) = -\mathbf{G_I}(\beta)\,\mathbf{A}\mathbf{G_I}(\beta). \tag{B.24}$$

In view of this the derivative of the cost difference is

$$\frac{\partial J^*_\Delta\left(\overline{\Upsilon}\right)}{\partial\overline{\Upsilon}} = \left[\frac{\partial}{\partial\overline{\Upsilon}}\overline{\Upsilon}\left(1-\overline{\Upsilon}\right)\mathrm{tr}\left(\mathbf{G_G}\left(\overline{\Upsilon}\right)\Omega_d\mathbf{G_F}\left(\overline{\Upsilon}\right)\mathbf{L}\right)\right] \tag{B.25}$$

$$\begin{aligned}&= \left[\frac{\partial}{\partial\overline{\Upsilon}}\overline{\Upsilon}\left(1-\overline{\Upsilon}\right)\right]\mathrm{tr}\left(\mathbf{G_G}\left(\overline{\Upsilon}\right)\Omega_d\mathbf{G_F}\left(\overline{\Upsilon}\right)\mathbf{L}\right) \\ &\quad + \overline{\Upsilon}\left(1-\overline{\Upsilon}\right)\mathrm{tr}\left(\left[\frac{\partial\mathbf{G_G}\left(\overline{\Upsilon}\right)}{\partial\overline{\Upsilon}}\right]\Omega_d\mathbf{G_F}\left(\overline{\Upsilon}\right)\mathbf{L}\right) \\ &\quad + \overline{\Upsilon}\left(1-\overline{\Upsilon}\right)\mathrm{tr}\left(\mathbf{G_G}\left(\overline{\Upsilon}\right)\Omega_d\left[\frac{\partial\mathbf{G_F}\left(\overline{\Upsilon}\right)}{\partial\overline{\Upsilon}}\right]\mathbf{L}\right),\end{aligned} \tag{B.26}$$

where (B.26) follows from applying property [30, 17.5] in conjunction with the product rule. At this stage, implementing the result seen in (B.24) yields

$$\frac{\partial J_{\Delta}^{*}\left(\overline{\Upsilon}\right)}{\partial\overline{\Upsilon}} = X_k^{\mathsf{T}}\mathbf{F}^{\mathsf{T}}\left[\mathbf{G}_{\mathbf{G}}\left(\overline{\Upsilon}\right)\left[\left(1-2\overline{\Upsilon}\right)\Omega_d - \overline{\Upsilon}\left(1\text{-}\overline{\Upsilon}\right)\left[\Omega_h\mathbf{G}_{\mathbf{G}}\left(\overline{\Upsilon}\right)\Omega_d + \Omega_d\mathbf{G}_{\mathbf{F}}\left(\overline{\Upsilon}\right)\Omega_g\right]\right]\mathbf{G}_{\mathbf{F}}\left(\overline{\Upsilon}\right)\right]\mathbf{F}X_k, \tag{B.27}$$

which corresponds to (4.36). This concludes the proof. □

## B.5 Lemma 9

**Lemma 9.** *The relation*

$$det\Big(\mathbf{G}_{\mathbf{G}}\left(\overline{\Upsilon}\right)\left[\left(1-2\overline{\Upsilon}\right)\Omega_d - \overline{\Upsilon}\left(1\text{-}\overline{\Upsilon}\right)\left[\Omega_h\mathbf{G}_{\mathbf{G}}\left(\overline{\Upsilon}\right)\Omega_d + \Omega_d\mathbf{G}_{\mathbf{F}}\left(\overline{\Upsilon}\right)\Omega_g\right]\right]\mathbf{G}_{\mathbf{F}}\left(\overline{\Upsilon}\right)\Big) = 0 \tag{B.28}$$

*has $2Nm$ many solutions. Specifically:*

$$\overline{\Upsilon}_{2i-1}^{D} = \frac{1}{1+\sqrt{1+\lambda_i}}, \tag{B.29a}$$

$$\overline{\Upsilon}_{2i}^{D} = \frac{1}{1-\sqrt{1+\lambda_i}}, \tag{B.29b}$$

*where $\overline{\Upsilon}_i^D$ correspondences to the i-th solution for (4.38) and $\lambda_i$ is the i-th eigenvalue of the matrix,*

$$\left(\Omega_g\Omega_d^{-1}\left(\Omega_g+\Psi\right)+\Psi\Omega_d^{-1}\Omega_h\right)\left(\Omega_g+\Psi\right)^{-1}\Omega_d\Psi^{-1}. \tag{B.30}$$

*Proof.* Multiplying (4.38) from the left and right by $\det\left(\Omega_d^{-1}\right)\det\left(\mathbf{G}_{\mathbf{G}}^{-1}\left(\overline{\Upsilon}\right)\right)$ and $\det\left(\mathbf{G}_{\mathbf{F}}^{-1}\left(\overline{\Upsilon}\right)\right)\det\left(\Omega_d^{-1}\right)$ respectively gives

$$\det\left(\left[\left(1\text{-}2\overline{\Upsilon}\right)\Omega_d^{-1}\text{-}\overline{\Upsilon}\left(1\text{-}\overline{\Upsilon}\right)\left[\Omega_d^{-1}\Omega_h\mathbf{G}_{\mathbf{G}}\left(\overline{\Upsilon}\right)+\mathbf{G}_{\mathbf{F}}\left(\overline{\Upsilon}\right)\Omega_g\Omega_d^{-1}\right]\right]\right)=0.$$

Multiplying the left by $\det\left(\mathbf{G}_{\mathbf{F}}^{-1}\left(\overline{\Upsilon}\right)\right)$ and the right by $\det\left(\mathbf{G}_{\mathbf{G}}^{-1}\left(\overline{\Upsilon}\right)\right)$ and then re arranging yields

$$\det\Big(\overline{\Upsilon}^2\left[\Omega_g\Omega_d^{-1}\left[\Omega_g+\Psi\right]+\Psi\Omega_d^{-1}\Omega_h\right] \\ +2\overline{\Upsilon}\Psi\Omega_d^{-1}\left(\Omega_d+\Psi\right)-\Psi\Omega_d^{-1}\left(\Omega_d+\Psi\right)\Big)=0. \tag{B.31}$$

The above is a quadratic in the, $\overline{\Upsilon}$. However, note that due to the determinant (B.31) is of order $Nm$ in $\overline{\Upsilon}$. To see this, operate the determinant as follows

$$\overline{\Upsilon}^{Nm}\det\Big(-\frac{1}{\overline{\Upsilon}^2}\Psi\Omega_d^{-1}\left(\Omega_d+\Psi\right)+2\frac{1}{\overline{\Upsilon}}\Psi\Omega_d^{-1}\left(\Omega_d+\Psi\right) \\ +\left[\Omega_g\Omega_d^{-1}\left[\Omega_g+\Psi\right]+\Psi\Omega_d^{-1}\Omega_h\right]\Big)=0. \tag{B.32}$$

Additionally, by assumption $\overline{\Upsilon}\neq 0$ , and therefore, dividing by $-\overline{\Upsilon}^{Nm}$ gives

$$\det\Big(\Big(\frac{1}{\overline{\Upsilon}^2}-2\frac{1}{\overline{\Upsilon}}\Big)\underbrace{\left[\Psi\Omega_d^{-1}\left(\Omega_d+\Psi\right)\right]}_{\mathbf{H}}-\underbrace{\left[\Omega_g\Omega_d^{-1}\left[\Omega_g+\Psi\right]+\Psi\Omega_d^{-1}\Omega_h\right]}_{\mathbf{T}}\Big)=0. \tag{B.33}$$

From the above it follows that the matrix $\mathbf{H}$ is positive definite and diagonal. Additionally, some manipulation reveals that $\mathbf{T}$ is symmetric. Therefore, multiplying the left and right by $\det\left(\mathbf{S}^{\mathbf{T}}\right)$ and $\det\left(\mathbf{S}\right)$ respectively gives [30, 16.51(c)]

$$\det\Big(\frac{1}{\overline{\Upsilon}^2}\mathbf{I}-2\frac{1}{\overline{\Upsilon}}\mathbf{I}-\Lambda\Big)=0, \tag{B.34}$$

where $\Lambda$ is the diagonal matrix where the diagonal entries $\lambda_i$ are the eigenvalues of the matrix $\mathbf{T}\mathbf{H}^{-1}$. The above is equivalent to

$$\prod_{i=1}^{Nm}\Big(\frac{1}{\overline{\Upsilon}^2}-2\frac{1}{\overline{\Upsilon}}-\lambda_i\Big)=0. \tag{B.35}$$

Note that (B.35) a polynomials on $\overline{\Upsilon}$ of order $Nm$ with solutions

$$\begin{aligned} \overline{\Upsilon}^D_{2i-1} &= \frac{1}{1+\sqrt{1+\lambda_i}}, \\ \overline{\Upsilon}^D_{2i} &= \frac{1}{1-\sqrt{1+\lambda_i}}, \end{aligned} \tag{B.36}$$

where $\overline{\Upsilon}^D_i$ is the $i$-th solution of (4.38). This concludes the proof. □

# Appendix C

# Chapter 5

## C.1 Lemma 12

This Appendix is dedicated to the proof of Lemma 12. The lemma is re-stated below.

**Lemma 12.** *Let (5.23) be concave in $\alpha$ over $\mathscr{C}(\mu,\epsilon)$. Then the maximum of the function is given by*

$$\max\{f(\alpha)\} = \max\left\{f(\min\{\mathscr{C}(\mu,\epsilon)\}), f(\max\{\mathscr{C}(\mu,\epsilon)\}), f(\mathbb{1}_{\mathscr{C}(\mu,\epsilon)}\alpha_{\max})\right\} \tag{C.1}$$

*where $\mathbb{1}_{\mathscr{B}}$ denotes the indicator function over the set $\mathscr{B}$.*

*Proof.* In the concave case a global maximum exists, but is not necessarily within the interval $\mathscr{C}(\mu,\epsilon)$, and therefore, we restrict the domain to the safe operation region with the indicator function

$$\mathbb{1}_{\mathscr{C}(\mu,\epsilon)} = \begin{cases} 1 & \alpha \in \mathscr{C}(\mu,\epsilon) \\ 0 & \alpha \notin \mathscr{C}(\mu,\epsilon) \end{cases}. \tag{C.2}$$

The concavity of the function implies

$$f'(\alpha) = \Upsilon_k^{*\mathsf{T}}(\mathscr{G}_k)\left(2\alpha\Omega_g + (1-2\alpha)(\mathbf{I}\odot\Omega_g) + \Psi - 2\mathbf{G}(\mathscr{G}_k)\right)\Upsilon_k^*(\mathscr{G}_k), \tag{C.3}$$

$$f''(\alpha) = 2\Upsilon_k^{*\mathsf{T}}(\mathscr{G}_k)\left(\Omega_g - (\mathbf{I}\odot\Omega_g)\right)\Upsilon_k^*(\mathscr{G}_k) < 0, \tag{C.4}$$

where (C.4) follows from the strict concavity of (5.23). Setting (C.3) equal to zero gives

$$\Upsilon_k^{*\mathsf{T}}\left(\mathcal{G}_k\right)\left(2\alpha\Omega_g+\left(1-2\alpha\right)\left(\mathbf{I}\odot\Omega_g\right)+\Psi-2\mathbf{G}\left(\mathcal{G}_k\right)\right)\Upsilon_k^{*}\left(\mathcal{G}_k\right)=0,$$

which results in

$$\begin{aligned}2\alpha X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}\left(\mathcal{G}_k\right)\left(\Omega_g-\left(\mathbf{I}\odot\Omega_g\right)\right)\mathbf{G}^{-1}\left(\mathcal{G}_k\right)\Omega_{gp}X_k=\\ X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}\left(\mathcal{G}_k\right)\left(2\mathbf{G}\left(\mathcal{G}_k\right)-\Psi-\left(\mathbf{I}\odot\Omega_g\right)\right)\mathbf{G}^{-1}\left(\mathcal{G}_k\right)\Omega_{gp}X_k.\end{aligned}\tag{C.5}$$

It follows from the strict concavity of (5.23), as in (C.4), that

$$X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}\left(\mathcal{G}_k\right)\left(\Omega_g-\left(\mathbf{I}\odot\Omega_g\right)\right)\mathbf{G}^{-1}\left(\mathcal{G}_k\right)\Omega_{gp}X_k\neq 0,\tag{C.6}$$

and therefore, (C.5) can be solved for $\alpha$ yielding

$$\alpha_{\max}=\frac{1}{2}h_{\mathrm{UDP}}^{-1}\left(X_k^{\mathsf{T}}\Omega_{gp}^{\mathsf{T}}\mathbf{G}^{-1}\left(\mathcal{G}_k\right)\left(2\mathbf{G}\left(\mathcal{G}_k\right)-\Psi-\left(\mathbf{I}\odot\Omega_g\right)\right)\mathbf{G}^{-1}\left(\mathcal{G}_k\right)\Omega_{gp}X_k\right),\tag{C.7}$$

where $h_{\mathrm{UDP}}\triangleq\Upsilon_k^{*\mathsf{T}}\left(\mathcal{G}_k\right)\left(\Omega_g-\left(\mathbf{I}\odot\Omega_g\right)\right)\Upsilon_k^{*}\left(\mathcal{G}_k\right)$. The global maximum is the solution when $\alpha_{\max}\in\mathscr{C}\left(\mu,\epsilon\right)$, i.e. the term $\alpha_{\max}\mathbb{1}_{\mathscr{C}(\mu,\epsilon)}$ in (C.1). When $\alpha_{\max}\notin\mathscr{C}\left(\mu,\epsilon\right)$ the solution follows as in the convex scenario by noticing that the inequality is strict and in the opposite direction. Therefore, when $\alpha_{\max}\notin\mathscr{C}\left(\mu,\epsilon\right)$ the attack construction reverts to selecting the value of $\alpha$ on the maximising boundary. For a concave function this is equivalent to finding the boundary that is closest to $\alpha_{\max}$. Let $a,b\in\mathscr{C}\left(\mu,\epsilon\right)$ and assume $f(a)>f(b)$ and $|a-\alpha_{\max}|<|b-\alpha_{\max}|$, then

$$f(b)\;<\;tf(a)+\;(1-t)f(\alpha_{\max}).\tag{C.8}$$

However, this line segment lies above the function which contradicts the fact that this function is concave, and therefore, the maximising $\alpha$ is on the boundary that is closest to $\alpha_{\max}$. This concludes the proof. □

## C.2 Lemma 15

This Appendix is dedicated to the proof of Lemma 15. The lemma is re-stated below.

**Lemma 15.** *The maximisation defined in (5.58) is convex in* $\overline{\Upsilon}^{\alpha}$.

*Proof.* We begin by defining a function that is equivalent to the cost function that which we are attempting to maximise:

$$\mathcal{J}\left(\overline{\Upsilon}^{\alpha}\right) = \operatorname{tr}\left(\left[\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha} - \overline{\Upsilon}^{\alpha}\left(2\overline{\Upsilon}\Omega_g + \Psi\right)\right]\mathcal{U}_k^{*}\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\right). \tag{C.9}$$

We proceed by showing the above function is convex, after which we obtain the global minimum of (C.9). To that end the first derivative of $\mathcal{J}\left(\overline{\Upsilon}^{\alpha}\right)$ with respect to $\overline{\Upsilon}^{\alpha}$ is defined as

$$\begin{aligned}\frac{\partial\mathcal{J}\left(\overline{\Upsilon}^{\alpha}\right)}{\partial\overline{\Upsilon}^{\alpha}} = &\frac{\partial\operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathcal{U}_k^{*}\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\right)}{\partial\overline{\Upsilon}^{\alpha}} \\ &-\frac{\partial\operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\left(2\overline{\Upsilon}\Omega_g + \Psi\right)\mathcal{U}_k^{*}\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\right)}{\partial\overline{\Upsilon}^{\alpha}}.\end{aligned} \tag{C.10}$$

The second term is linear in $\overline{\Upsilon}^{\alpha}$ and is easier to evaluate. Notice that

$$\frac{\partial\operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\left(2\overline{\Upsilon}\Omega_g + \Psi\right)\mathcal{U}_k^{*}\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\right)}{\partial\overline{\Upsilon}^{\alpha}} = \frac{\partial\operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\mathbf{K}\mathbf{H}\right)}{\partial\overline{\Upsilon}^{\alpha}}, \tag{C.11}$$

where $\mathcal{U}_k^{*}\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right) = \mathbf{H}$ and $\left(2\overline{\Upsilon}\Omega_g + \Psi\right) = \mathbf{K}$. Using the cyclic properties of the trace operator and the fact that $\overline{\Upsilon}^{\alpha}$ is diagonal, it follows from [30, pg 366. 17.39] that

$$\begin{aligned}\frac{\partial\operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\mathbf{K}\mathbf{H}\right)}{\partial\overline{\Upsilon}^{\alpha}} &= \frac{\partial\operatorname{tr}\left(\mathbf{K}\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\overline{\Upsilon}^{\alpha}}, && \text{(C.12)}\\ &= \mathbf{I}\odot\left[\mathbf{H}\mathbf{K} + \mathbf{K}^{\mathsf{T}}\mathbf{H}^{\mathsf{T}} - \mathbf{I}\odot\left[\mathbf{H}\mathbf{K}\right]\right], && \text{(C.13)}\\ &= \mathbf{I}\odot\left[\mathbf{H}\mathbf{K}\right] + \mathbf{I}\odot\left[\mathbf{K}^{\mathsf{T}}\mathbf{H}^{\mathsf{T}}\right] - \mathbf{I}\odot\mathbf{I}\odot\left[\mathbf{H}\mathbf{K}\right], && \text{(C.14)}\\ &= \mathbf{I}\odot\left[\mathbf{K}^{\mathsf{T}}\mathbf{H}\right], && \text{(C.15)}\\ &= \mathbf{I}\odot\left[2\left(\Omega_g\overline{\Upsilon} + \Psi\right)\mathcal{U}_k^{*}\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\right], && \text{(C.16)}\end{aligned}$$

where (C.13) follows from the diagonal constraint of $\overline{\Upsilon}^{\alpha}$ and (C.15) is a result of the symmetry of $\mathbf{K}$. Therefore, (C.10) becomes

$$\frac{\partial \mathcal{T}\left(\overline{\Upsilon}^{\alpha}\right)}{\partial \overline{\Upsilon}^{\alpha}} = \frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g \overline{\Upsilon}^{\alpha}\mathcal{U}_k^*\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\right)}{\partial \overline{\Upsilon}^{\alpha}} - \mathbf{I} \odot \left[\left(2\Omega_g \overline{\Upsilon} + \Psi\right)\mathcal{U}_k^*\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\right]. \tag{C.17}$$

Similar to the previous term, through use of [30, pg. 367, 17.41],

$$\begin{aligned}
\frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g \overline{\Upsilon}^{\alpha}\mathcal{U}_k^*\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\right)}{\partial \overline{\Upsilon}^{\alpha}} &= \frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g \overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial \overline{\Upsilon}^{\alpha}} && \text{(C.18)}\\
&= \mathbf{I} \odot \Big[\mathbf{H}\overline{\Upsilon}^{\alpha}\Omega_g + \Omega_g \overline{\Upsilon}^{\alpha}\mathbf{H} + \left(\mathbf{H}\overline{\Upsilon}^{\alpha}\Omega_g + \Omega_g \overline{\Upsilon}^{\alpha}\mathbf{H}\right)^{\mathsf{T}} \\
&\qquad - \mathbf{I} \odot \left[\mathbf{H}\overline{\Upsilon}^{\alpha}\Omega_g + \Omega_g \overline{\Upsilon}^{\alpha}\mathbf{H}\right]\Big] && \text{(C.19)}\\
&= \mathbf{I} \odot \left[\mathbf{H}\overline{\Upsilon}^{\alpha}\Omega_g + \Omega_g \overline{\Upsilon}^{\alpha}\mathbf{H}\right] + \mathbf{I} \odot \left[\left(\mathbf{H}\overline{\Upsilon}^{\alpha}\Omega_g + \Omega_g \overline{\Upsilon}^{\alpha}\mathbf{H}\right)^{\mathsf{T}}\right] \\
&\qquad - \mathbf{I} \odot \mathbf{I} \odot \left[\mathbf{H}\overline{\Upsilon}^{\alpha}\Omega_g + \Omega_g \overline{\Upsilon}^{\alpha}\mathbf{H}\right] && \text{(C.20)}\\
&= \mathbf{I} \odot \left[\left(\mathbf{H}\overline{\Upsilon}^{\alpha}\Omega_g + \Omega_g \overline{\Upsilon}^{\alpha}\mathbf{H}\right)^{\mathsf{T}}\right] && \text{(C.21)}\\
&= \mathbf{I} \odot \left[\mathbf{H}\overline{\Upsilon}^{\alpha}\Omega_g^{\mathsf{T}} + \Omega_g^{\mathsf{T}} \overline{\Upsilon}^{\alpha}\mathbf{H}\right] && \text{(C.22)}\\
&= \mathbf{I} \odot \left[\mathcal{U}_k^*\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\overline{\Upsilon}^{\alpha}\Omega_g\right] \\
&\qquad + \mathbf{I} \odot \left[\Omega_g \overline{\Upsilon}^{\alpha}\mathcal{U}_k^*\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\right] && \text{(C.23)}
\end{aligned}$$

where (C.22) follows from the symmetry of $\mathbf{H}$ and $\Omega_g$. Therefore, the first derivative of (C.10) is

$$\begin{aligned}
\frac{\partial \mathcal{T}\left(\overline{\Upsilon}^{\alpha}\right)}{\partial \overline{\Upsilon}^{\alpha}} &= \mathbf{I} \odot \left[\mathcal{U}_k^*\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\overline{\Upsilon}^{\alpha}\Omega_g + \Omega_g \overline{\Upsilon}^{\alpha}\mathcal{U}_k^*\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\right] \\
&\qquad - \mathbf{I} \odot \left[\left(2\overline{\Upsilon}\Omega_g + \Psi\right)\mathcal{U}_k^*\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\right] \\
&= \mathbf{I} \odot \left[2\Omega_g \overline{\Upsilon}^{\alpha}\mathcal{U}_k^*\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\right] - \mathbf{I} \odot \left[\left(2\overline{\Upsilon}\Omega_g + \Psi\right)\mathcal{U}_k^*\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\right]. && \text{(C.24)}
\end{aligned}$$

Only the first term of (C.24) depends on $\overline{\Upsilon}^{\alpha}$, and therefore, the second derivative is equivalent to

$$\frac{\partial^2 \mathcal{T}\left(\overline{\Upsilon}^{\alpha}\right)}{\partial \overline{\Upsilon}^{\alpha}\partial \overline{\Upsilon}^{\alpha}} = \frac{\partial\left(\mathbf{I} \odot \left[2\Omega_g \overline{\Upsilon}^{\alpha}\mathcal{U}_k^*\left(\mathcal{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{F}_k\right)\right]\right)}{\partial \overline{\Upsilon}^{\alpha}}. \tag{C.25}$$

It should be noted that performing a derivative twice with respect to a matrix is equivalent to

$$\frac{\partial^2 \mathscr{T}\left(\overline{\Upsilon}^{\alpha}\right)}{\partial \overline{\Upsilon}^{\alpha} \partial \overline{\Upsilon}^{\alpha}} = \frac{\partial^2 \mathscr{T}\left(\overline{\Upsilon}^{\alpha}\right)}{\partial \mathrm{vec}\left(\overline{\Upsilon}^{\alpha}\right) \partial \mathrm{vec}\left(\overline{\Upsilon}^{\alpha}\right)^{\mathsf{T}}} = \frac{\partial \mathscr{T}\left(\overline{\Upsilon}^{\alpha}\right)}{\partial\left(\overline{\Upsilon}^{\alpha} \otimes \overline{\Upsilon}^{\alpha}\right)}, \tag{C.26}$$

where the $\mathrm{vec}(\cdot)$ operator yields a vector that is formed with the stacked columns of the matrix input [30]. From this interpretation it becomes clear that to find the second derivative one must simply perform the derivative with respect the diagonal and symmetric matrix $\overline{\Upsilon}^{\alpha} \otimes \overline{\Upsilon}^{\alpha}$ of size $N^2 m^2$. Therefore,

$$\frac{\partial^2 \mathrm{tr}\left(\overline{\Upsilon}^{\alpha} \Omega_g \overline{\Upsilon}^{\alpha} \mathcal{U}_k^*\left(\mathscr{F}_k\right) \mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right)}{\partial \overline{\Upsilon}^{\alpha} \partial \overline{\Upsilon}^{\alpha}} = \frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha} \Omega_g \overline{\Upsilon}^{\alpha} \mathcal{U}_k^*\left(\mathscr{F}_k\right) \mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right)}{\partial\left(\overline{\Upsilon}^{\alpha} \otimes \overline{\Upsilon}^{\alpha}\right)}. \tag{C.27}$$

This is now equivalent to finding a single derivative of a scalar function, and therefore, results in a matrix of size $N^2 m^2$. As before note that

$$\frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha} \Omega_g \overline{\Upsilon}^{\alpha} \mathcal{U}_k^*\left(\mathscr{F}_k\right) \mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right)}{\partial\left(\overline{\Upsilon}^{\alpha} \otimes \overline{\Upsilon}^{\alpha}\right)} = \frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha} \Omega_g \overline{\Upsilon}^{\alpha} \mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha} \otimes \overline{\Upsilon}^{\alpha}\right)}. \tag{C.28}$$

Then the derivative is

$$
\begin{aligned}
\frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)} &= \begin{pmatrix} \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{1,1}} & \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{1,2}} & \cdots & \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{1,N^2m^2}} \\ \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{2,1}} & \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{2,2}} & \cdots & \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{2,N^2m^2}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{N^2m^2,1}} & \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{N^2m^2,2}} & \cdots & \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{N^2m^2,N^2m^2}} \end{pmatrix} \\
&= \begin{pmatrix} \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{1,1}} & 0 & \cdots & 0 \\ 0 & \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{2,2}} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{N^2m^2,N^2m^2}} \end{pmatrix} \\
&= \begin{pmatrix} \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}_1^{\alpha}\overline{\Upsilon}_1^{\alpha}\right)} & 0 & \cdots & 0 \\ 0 & \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}_1^{\alpha}\overline{\Upsilon}_2^{\alpha}\right)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \frac{\partial \operatorname{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_g\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}_{Nm}^{\alpha}\overline{\Upsilon}_{Nm}^{\alpha}\right)} \end{pmatrix} \\
&= \begin{pmatrix} \Omega_{g_{1,1}}\mathbf{H}_{1,1} & 0 & \cdots & 0 \\ 0 & \Omega_{g_{1,1}}\mathbf{H}_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \Omega_{g_{Nm,Nm}}\mathbf{H}_{Nm,Nm} \end{pmatrix} \qquad \text{(C.29)} \\
&= \mathbf{I} \odot (\Omega_g \otimes \mathbf{H}) \qquad \text{(C.30)} \\
&= \mathbf{I} \odot \left[\Omega_g \otimes \left(\mathcal{U}_k^* \left(\mathscr{F}_k\right) \mathcal{U}_k^{*\mathsf{T}} \left(\mathscr{F}_k\right)\right)\right], \qquad \text{(C.31)}
\end{aligned}
$$

from this it can be seen that

$$
\frac{\partial^2 \mathscr{T}\left(\overline{\Upsilon}^{\alpha}\right)}{\partial\overline{\Upsilon}^{\alpha}\partial\overline{\Upsilon}^{\alpha}} = \mathbf{I} \odot \left[\Omega_g \otimes \left(\mathcal{U}_k^* \left(\mathscr{F}_k\right) \mathcal{U}_k^{*\mathsf{T}} \left(\mathscr{F}_k\right)\right)\right] \succ 0, \qquad \text{(C.32)}
$$

where second derivative is strictly positive definite assuming the i-th element of $\mathcal{U}_k\left(\mathscr{F}_k\right)$ is non-zero for all $i \in \{1, \ldots, Nm\}$. This assumption is true with probability 1 as the initial condition is a zero mean Gaussian, i.e. $\mathbb{P}\left[X_k = 0\right] = 0$. Therefore, from the strict positive definiteness of the second derivative the function (5.57) is convex in $\overline{\Upsilon}^{\alpha}$ almost surely. This concludes the proof. □

## C.3 Corollary 6

This Appendix is dedicated to the proof of Corollary 6. The corollary is re-stated below.

**Corollary 6.** *There exists a global minimum of the function (5.58) that is defined as*

$$\overline{\Upsilon}^{\alpha}_{\min} = \frac{1}{2}\left(\mathbf{I} \odot \Omega_g^{-1}\left[\left(2\overline{\Upsilon}\Omega_g + \Psi\right)\mathcal{U}_k^*\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\left(\mathbf{I} \odot \left[\mathcal{U}_k^*\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)^{-1}. \tag{C.33}$$

*This is not equal to operator's postulate IID variable,* $\overline{\Upsilon}$.

*Proof.* From Lemma 15 it follows that there exists a single global minimum of (5.58). This is found from the solution of the first derivative of (5.58). The minimising solution of (C.24) is found as follows

$$\frac{\partial\mathscr{T}\left(\overline{\Upsilon}^{\alpha}\right)}{\partial\overline{\Upsilon}^{\alpha}} = \mathbf{I} \odot \left[2\Omega_g\overline{\Upsilon}^{\alpha}_{\min}\mathcal{U}_k^*\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right] - \mathbf{I} \odot \left[\left(2\overline{\Upsilon}\Omega_g + \Psi\right)\mathcal{U}_k^*\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]. \tag{C.34}$$

Setting this equal to $\mathbb{0}$ and solving yields

$$\mathbf{I} \odot \left[2\Omega_g\overline{\Upsilon}^{\alpha}_{\min}\mathcal{U}_k^*\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right] = \mathbf{I} \odot \left[\left(2\overline{\Upsilon}\Omega_g + \Psi\right)\mathcal{U}_k^*\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]. \tag{C.35}$$

Converting the Hadamard products to Kronecker products yields [30, pg. 251, 11.38ai]

$$\begin{aligned}\varphi\left(\mathbf{I} \otimes \left[2\Omega_g\overline{\Upsilon}^{\alpha}_{\min}\mathcal{U}_k^*\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\varphi^{\mathsf{T}} \\ = \varphi\left(\mathbf{I} \otimes \left[\left(2\overline{\Upsilon}\Omega_g + \Psi\right)\mathcal{U}_k^*\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\varphi^{\mathsf{T}},\end{aligned} \tag{C.36}$$

where $\varphi = \sum_{i=1}^{N^2m^2} e_i \left(e_i \otimes e_i\right)^{\mathsf{T}}$. From the positive definiteness of $\Omega_g$ its inverse exists and therefore

$$\begin{aligned}
&\varphi\left(\mathbf{I}\otimes\Omega_g^{-1}\right)\varphi^{\mathsf{T}}\varphi\left(\mathbf{I}\otimes\left[2\Omega_g\overline{\Upsilon}^{\alpha}_{\min}\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\varphi^{\mathsf{T}}\\
&\qquad=\varphi\left(\mathbf{I}\otimes\Omega_g^{-1}\right)\varphi^{\mathsf{T}}\varphi\left(\mathbf{I}\otimes\left[\left(2\overline{\Upsilon}\Omega_g+\Psi\right)\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\varphi^{\mathsf{T}}, \quad \text{(C.37)}\\
&\varphi\left(\mathbf{I}\otimes\Omega_g^{-1}\right)\left(\mathbf{I}\otimes\left[2\Omega_g\overline{\Upsilon}^{\alpha}_{\min}\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\varphi^{\mathsf{T}}\\
&\qquad=\varphi\left(\mathbf{I}\otimes\Omega_g^{-1}\right)\left(\mathbf{I}\otimes\left[\left(2\overline{\Upsilon}\Omega_g+\Psi\right)\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\varphi^{\mathsf{T}}. \quad \text{(C.38)}
\end{aligned}$$

Through use of [30, pg. 238, 11.11] in (C.38) it is seen that

$$\begin{aligned}
&\varphi\left(\mathbf{I}\otimes\Omega_g^{-1}\left[2\Omega_g\overline{\Upsilon}^{\alpha}_{\min}\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\varphi^{\mathsf{T}}\\
&\qquad=\varphi\left(\mathbf{I}\otimes\Omega_g^{-1}\left[\left(2\overline{\Upsilon}\Omega_g+\Psi\right)\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\varphi^{\mathsf{T}}, \quad \text{(C.39)}\\
&\varphi\left(\mathbf{I}\otimes 2\left[\overline{\Upsilon}^{\alpha}_{\min}\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\varphi^{\mathsf{T}}\\
&\qquad=\varphi\left(\mathbf{I}\otimes\Omega_g^{-1}\left[\left(2\overline{\Upsilon}\Omega_g+\Psi\right)\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\varphi^{\mathsf{T}}, \quad \text{(C.40)}\\
&2\overline{\Upsilon}^{\alpha}_{\min}\left(\mathbf{I}\odot\left[\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\\
&\qquad=\varphi\left(\mathbf{I}\otimes\Omega_g^{-1}\left[\left(2\overline{\Upsilon}\Omega_g+\Psi\right)\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\varphi^{\mathsf{T}}. \quad \text{(C.41)}
\end{aligned}$$

As stated before $\left(\mathbf{I}\odot\left[\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)$ is positive definite and therefore its inverse exists, which results in

$$\begin{aligned}
\overline{\Upsilon}^{\alpha}_{\min} &= \frac{1}{2}\varphi\left(\mathbf{I}\otimes\Omega_g^{-1}\left[\left(2\overline{\Upsilon}\Omega_g+\Psi\right)\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\varphi^{\mathsf{T}}\left(\mathbf{I}\odot\left[\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)^{-1} \quad \text{(C.42)}\\
&= \frac{1}{2}\left(\mathbf{I}\odot\Omega_g^{-1}\left[\left(2\overline{\Upsilon}\Omega_g+\Psi\right)\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)\left(\mathbf{I}\odot\left[\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right]\right)^{-1}. \quad \text{(C.43)}
\end{aligned}$$

Therefore, the global minimum of (5.58) is (5.59). This concludes the proof. □

## C.4 Lemma 16

This Appendix is dedicated to the proof of Lemma 16. The lemma is re-stated below.

**Lemma 16.** *The objective function of the optimisation problem*

$$\begin{aligned} \max_{\overline{\Upsilon}^{\alpha}} \quad & \operatorname{tr}\left(\left[\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha} - \overline{\Upsilon}^{\alpha}\left((\mathbf{I}\odot\Omega_g) + \Psi + 2\overline{\Upsilon}\Omega_H\right)\right]\mathcal{U}_k^{*}\left(\mathcal{G}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{G}_k\right)\right), \\ s.t. \quad & \mathbf{M}_k^{\alpha} \in \mathcal{C}^{\epsilon}\left(\mathbf{M},\mathbf{L}\right) \qquad \text{for } k \in \mathbb{N}, \end{aligned} \tag{C.44}$$

*is neither convex nor concave in* $\overline{\Upsilon}^{\alpha}$ *and the second derivative is equal to* $\mathbb{0}$.

*Proof.* We define the function

$$\mathcal{W}\left(\overline{\Upsilon}^{\alpha}\right) \triangleq \operatorname{tr}\left(\left[\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha} - \overline{\Upsilon}^{\alpha}\left((\mathbf{I}\odot\Omega_g) + \Psi + 2\overline{\Upsilon}\Omega_H\right)\right]\mathcal{U}_k^{*}\left(\mathcal{G}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathcal{G}_k\right)\right). \tag{C.45}$$

The second derivative of (C.45) with respect to $\overline{\Upsilon}^{\alpha}$ is

$$
\begin{aligned}
\frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)} &= \begin{pmatrix}
\frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{1,1}} & \frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{1,2}} & \cdots & \frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{1,N^2m^2}} \\
\frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{2,1}} & \frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{2,2}} & \cdots & \frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{2,N^2m^2}} \\
\vdots & \vdots & \ddots & \vdots \\
\frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{N^2m^2,1}} & \frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{N^2m^2,2}} & \cdots & \frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{N^2m^2,N^2m^2}}
\end{pmatrix} \\
&= \begin{pmatrix}
\frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{1,1}} & 0 & \cdots & 0 \\
0 & \frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{2,2}} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & \frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}\otimes\overline{\Upsilon}^{\alpha}\right)_{N^2m^2,N^2m^2}}
\end{pmatrix} \\
&= \begin{pmatrix}
\frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}_{1}\overline{\Upsilon}^{\alpha}_{1}\right)} & 0 & \cdots & 0 \\
0 & \frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}_{1}\overline{\Upsilon}^{\alpha}_{2}\right)} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & \frac{\partial \mathrm{tr}\left(\overline{\Upsilon}^{\alpha}\Omega_H\overline{\Upsilon}^{\alpha}\mathbf{H}\right)}{\partial\left(\overline{\Upsilon}^{\alpha}_{Nm}\overline{\Upsilon}^{\alpha}_{Nm}\right)}
\end{pmatrix} \\
&= \begin{pmatrix}
\Omega_{H\,1,1}\mathbf{H}_{1,1} & 0 & \cdots & 0 \\
0 & \Omega_{H\,1,1}\mathbf{H}_{2,2} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & \Omega_{H\,Nm,Nm}\mathbf{H}_{Nm,Nm}
\end{pmatrix} \\
&= \mathbf{I}\odot\left(\Omega_H\otimes\mathbf{H}\right) \\
&= \mathbf{I}\odot\left[\Omega_H\otimes\left(\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right)\right],
\end{aligned}
\tag{C.46}
$$

from this it follows that

$$
\frac{\partial^2\mathscr{T}\left(\overline{\Upsilon}^{\alpha}\right)}{\partial\overline{\Upsilon}^{\alpha}\partial\overline{\Upsilon}^{\alpha}} = \mathbf{I}\odot\left[\Omega_H\otimes\left(\mathcal{U}_k^{*}\left(\mathscr{F}_k\right)\mathcal{U}_k^{*\mathsf{T}}\left(\mathscr{F}_k\right)\right)\right]. \tag{C.47}
$$

Unfortunately, the Kronecker product of the hollow matrix $\Omega_H$, with any other matrix produces another hollow matrix. Therefore, the term on the right hand side in (C.47) is hollow. When the Hadamard product is then applied all non-diagonal elements become zero. This means the above derivative is the zero matrix, that is

$$\frac{\partial^2 \mathcal{J}\left(\overline{\Upsilon}^{\alpha}\right)}{\partial \overline{\Upsilon}^{\alpha} \partial \overline{\Upsilon}^{\alpha}} = \mathbb{0} \tag{C.48}$$

The objective function is neither convex nor concave. This concludes the proof. □

## C.5 Theorem 12

This Appendix is dedicated to the proof of Theorem 12. The theorem is re-stated below.

**Theorem 12.** *The minimising value of $\lambda$ for the function*

$$\Psi_{T_k}(\lambda) = \log\left(\mathbb{E}\left[e^{\lambda Z_k}\right]\right). \tag{C.49}$$

*For a centered sequence of Bernoulli random variables is*

$$\lambda_{\mathbf{T}} = \log\left(\left(\frac{\mathbf{T}}{k} + \mathbf{M}^{\alpha}\right)\left(\mathbf{I} - \mathbf{M}^{\alpha}\right)\left(\mathbf{I} - \frac{\mathbf{T}}{k} - \mathbf{M}^{\alpha}\right)^{-1}\left(\mathbf{M}^{\alpha}\right)^{-1}\right). \tag{C.50}$$

*Proof.* For the centered Bernoulli sequence

$$\begin{aligned}
\Psi_{T_k}(\lambda) &= \log\left(\prod_{i=1}^{k} \mathbb{E}\left[e^{\lambda\left(V_i^A - \mathbf{M}^{\alpha}\right)}\right]\right) && \text{(C.51)}\\
&= \sum_{i=1}^{k} \log\left(\mathbb{E}\left[e^{\lambda\left(V_i^A - \mathbf{M}^{\alpha}\right)}\right]\right) && \text{(C.52)}\\
&= -k\lambda\mathbf{M}^{\alpha} + \sum_{i=1}^{k} \log\left(\mathbb{P}\left[V_i^A = \mathbf{I}\right]e^{\lambda\cdot\mathbf{I}} + \mathbb{P}\left[V_i^A = \mathbb{0}\right]e^{\lambda\mathbb{0}}\right) && \text{(C.53)}\\
&= -k\lambda\mathbf{M}^{\alpha} + \sum_{i=1}^{k} \log\left(\mathbf{M}^{\alpha}e^{\lambda} + \left(\mathbf{I} - \mathbf{M}^{\alpha}\right)\right) && \text{(C.54)}\\
&= k\left(\log\left(\mathbf{M}^{\alpha}e^{\lambda} + \left(\mathbf{I} - \mathbf{M}^{\alpha}\right)\right) - \lambda\mathbf{M}^{\alpha}\right). && \text{(C.55)}
\end{aligned}$$

The next object to be computed is $\lambda_{\mathbf{T}}$. It should be noted however that for our case we have parallelised the probability of detection for each channel. Therefore, the following derivative follows a slight abuse of notation. This is due to the fact that we are actually performing $m$ separate scalar differentiations and not a single matrix differentiation. Performing this derivative yields

$$\mathbf{T} = \frac{\partial \Psi_{T_k}(\lambda)}{\partial \lambda} \tag{C.56}$$

$$= \frac{\partial \sum_{i=1}^{k} \log\left(\mathbf{M}^{\alpha} e^{\lambda} + (\mathbf{I} - \mathbf{M}^{\alpha})\right)}{\partial \lambda} - k\mathbf{M}^{\alpha} \tag{C.57}$$

$$= \sum_{i=1}^{k} \frac{\partial \log\left(\mathbf{M}^{\alpha} e^{\lambda} + (\mathbf{I} - \mathbf{M}^{\alpha})\right)}{\partial \lambda} - k\mathbf{M}^{\alpha} \tag{C.58}$$

$$\mathbf{T} + k\mathbf{M}^{\alpha} = \sum_{i=1}^{k} \left(\mathbf{M}^{\alpha} e^{\lambda} + (\mathbf{I} - \mathbf{M}^{\alpha})\right)^{-1} \frac{\partial \left(\mathbf{M}^{\alpha} e^{\lambda} + (\mathbf{I} - \mathbf{M}^{\alpha})\right)}{\partial \lambda} \tag{C.59}$$

$$\mathbf{T} + k\mathbf{M}^{\alpha} = k\left(\mathbf{M}^{\alpha} e^{\lambda} + (\mathbf{I} - \mathbf{M}^{\alpha})\right)^{-1} \mathbf{M}^{\alpha} e^{\lambda} \tag{C.60}$$

After performing the derivative, rearranging to give the $\lambda_{\mathbf{T}}$ yields

$$\frac{\mathbf{T}}{k} + \mathbf{M}^{\alpha} = \left(\mathbf{M}^{\alpha} e^{\lambda} + (\mathbf{I} - \mathbf{M}^{\alpha})\right)^{-1} \mathbf{M}^{\alpha} e^{\lambda} \tag{C.61}$$

$$\mathbf{M}^{\alpha} e^{\lambda} = \left(\frac{\mathbf{T}}{k} + \mathbf{M}^{\alpha}\right)\left(\mathbf{M}^{\alpha} e^{\lambda} + (\mathbf{I} - \mathbf{M}^{\alpha})\right) - \mathbf{M}^{\alpha} e^{\lambda} \tag{C.62}$$

$$e^{\lambda}\mathbf{M}^{\alpha}\left(\mathbf{I} - \frac{\mathbf{T}}{k} - \mathbf{M}^{\alpha}\right) = \left(\frac{\mathbf{T}}{k} + \mathbf{M}^{\alpha}\right)(\mathbf{I} - \mathbf{M}^{\alpha}) \tag{C.63}$$

$$\lambda_{\mathbf{T}} = \log\left(\left(\frac{\mathbf{T}}{k} + \mathbf{M}^{\alpha}\right)(\mathbf{I} - \mathbf{M}^{\alpha})\left(\mathbf{I} - \frac{\mathbf{T}}{k} - \mathbf{M}^{\alpha}\right)^{-1}(\mathbf{M}^{\alpha})^{-1}\right). \tag{C.64}$$

□

## C.6 Theorem 13

This Appendix is dedicated to the proof of Theorem 13. The theorem is re-stated below.

**Theorem 13.** *The minimising value of $\lambda_{\mathbf{T}}$ results in the following probability of detection bound*

$$\mathbb{P}_D \quad \leq e^{-k\mathcal{D}\left(\frac{\lfloor k(\mathbf{M}+\mathbf{L})\rfloor}{k}\|\mathbf{M}^\alpha\right)} + e^{-k\mathcal{D}\left(\frac{\lceil k(\mathbf{M}-\mathbf{L})\rceil}{k}\|\mathbf{M}^\alpha\right)}. \tag{C.65}$$

*Proof.* We begin with the substitution of the optimal $\lambda_{\mathbf{T}}$ into the definition of the optimal function

$$\begin{aligned}
\Psi^*_{T_k}(\mathbf{T}) &= \lambda_{\mathbf{T}}\mathbf{T} - \Psi_{T_k}(\lambda_{\mathbf{T}}) && \text{(C.66)}\\
&= \mathbf{T}\log\left(\left(\frac{\mathbf{T}}{k}+\mathbf{M}^\alpha\right)(\mathbf{I}-\mathbf{M}^\alpha)\left(\mathbf{I}-\frac{\mathbf{T}}{k}-\mathbf{M}^\alpha\right)^{-1}(\mathbf{M}^\alpha)^{-1}\right)\\
&\qquad +k\left(\log\left(\mathbf{M}^\alpha e^{\lambda_{\mathbf{T}}}+(\mathbf{I}-\mathbf{M}^\alpha)\right)-\lambda_{\mathbf{T}}\mathbf{M}^\alpha\right) && \text{(C.67)}\\
&= \mathbf{T}\log\left(\left(\frac{\mathbf{T}}{k}+\mathbf{M}^\alpha\right)(\mathbf{I}-\mathbf{M}^\alpha)\left(\mathbf{I}-\frac{\mathbf{T}}{k}-\mathbf{M}^\alpha\right)^{-1}(\mathbf{M}^\alpha)^{-1}\right)\\
&\qquad +k\log\left(\left(\frac{\mathbf{T}}{k}+\mathbf{M}^\alpha\right)(\mathbf{I}-\mathbf{M}^\alpha)\left(\mathbf{I}-\frac{\mathbf{T}}{k}-\mathbf{M}^\alpha\right)^{-1}+(\mathbf{I}-\mathbf{M}^\alpha)\right)\\
&\qquad -k\mathbf{M}^\alpha\log\left(\left(\frac{\mathbf{T}}{k}+\mathbf{M}^\alpha\right)(\mathbf{I}-\mathbf{M}^\alpha)\left(\mathbf{I}-\frac{\mathbf{T}}{k}-\mathbf{M}^\alpha\right)^{-1}(\mathbf{M}^\alpha)^{-1}\right). && \text{(C.68)}
\end{aligned}$$

Dividing through by $k$ and noting that the first and last logarithm contain the same terms within yields

$$\begin{aligned}\frac{1}{k}\Psi^*_{T_k}(t) &= \left(\frac{\mathbf{T}}{k}+\mathbf{M}^\alpha\right)\log\left(\left(\frac{\mathbf{T}}{k}+\mathbf{M}^\alpha\right)(\mathbf{I}-\mathbf{M}^\alpha)\left(\mathbf{I}-\frac{\mathbf{T}}{k}-\mathbf{M}^\alpha\right)^{-1}(\mathbf{M}^\alpha)^{-1}\right)\\ &\quad+\log\left(\left(\left(\frac{\mathbf{T}}{k}+\mathbf{M}^\alpha\right)\left(\mathbf{I}-\frac{\mathbf{T}}{k}-\mathbf{M}^\alpha\right)^{-1}+\mathbf{I}\right)(\mathbf{I}-\mathbf{M}^\alpha)\right) \qquad \text{(C.69)}\\ &= \left(\frac{\mathbf{T}}{k}+\mathbf{M}^\alpha\right)\log\left(\left(\frac{\mathbf{T}}{k}+\mathbf{M}^\alpha\right)(\mathbf{I}-\mathbf{M}^\alpha)\left(\mathbf{I}-\frac{\mathbf{T}}{k}-\mathbf{M}^\alpha\right)^{-1}(\mathbf{M}^\alpha)^{-1}\right)\\ &\quad+\log\left((\mathbf{I}-\mathbf{M}^\alpha)\left(\mathbf{I}-\frac{\mathbf{T}}{k}-\mathbf{M}^\alpha\right)^{-1}\right) \qquad \text{(C.70)}\\ &= \left(\frac{\mathbf{T}}{k}+\mathbf{M}^\alpha\right)\log\left(\left(\frac{\mathbf{T}}{k}+\mathbf{M}^\alpha\right)(\mathbf{M}^\alpha)^{-1}\right)\\ &\quad+\left(\mathbf{I}+\frac{\mathbf{T}}{k}+\mathbf{M}^\alpha\right)\log\left((\mathbf{I}-\mathbf{M}^\alpha)\left(\mathbf{I}-\frac{\mathbf{T}}{k}-\mathbf{M}^\alpha\right)^{-1}\right). \qquad \text{(C.71)}\end{aligned}$$

At this stage we substitute the variable $\mathbf{T}$ for the region we want the probability of detection to be calculated for. We first calculate the probability for the region governed by the event $\theta_1$. The derivation of the secondary event follows trivially. With that in mind, we set $\mathbf{T} = \lfloor k(\mathbf{M}+\mathbf{L})\rfloor - k\mathbf{M}^\alpha$. Substitution of this yields

$$\begin{aligned}\frac{1}{k}\Psi^*_{T_k}(\lfloor k(\mathbf{M}+\mathbf{L})\rfloor - k\mathbf{M}^\alpha) &= \left(\frac{\lfloor k(\mathbf{M}+\mathbf{L})\rfloor}{k}\right)\log\left(\left(\frac{\lfloor k(\mathbf{M}+\mathbf{L})\rfloor}{k}\right)(\mathbf{M}^\alpha)^{-1}\right)\\ &\quad+\left(\mathbf{I}+\frac{\lfloor k(\mathbf{M}+\mathbf{L})\rfloor}{k}\right)\log\left((\mathbf{I}-\mathbf{M}^\alpha)\left(\mathbf{I}-\frac{\lfloor k(\mathbf{M}+\mathbf{L})\rfloor}{k}\right)^{-1}\right). \qquad \text{(C.72)}\end{aligned}$$

Making substitution of $\mathbf{Q} = \frac{\lfloor k(\mathbf{M}+\mathbf{L})\rfloor}{k}$.

$$\begin{aligned}\frac{1}{k}\Psi^*_{T_k}(\lfloor k(\mathbf{M}+\mathbf{L})\rfloor - k\mathbf{M}^\alpha) &= \mathbf{Q}\log\left(\mathbf{Q}(\mathbf{M}^\alpha)^{-1}\right)\\ &\quad+(\mathbf{I}+\mathbf{Q})\log\left((\mathbf{I}-\mathbf{M}^\alpha)(\mathbf{I}-\mathbf{Q})^{-1}\right). \qquad \text{(C.73)}\end{aligned}$$

The above relation is actually the KL divergence between two distributions. Therefore, we have shown that

$$\Psi^*_{T_k}\left(\lfloor k\left(\mathbf{M}+\mathbf{L}\right)\rfloor - k\mathbf{M}^\alpha\right) = k\mathcal{D}\left(\mathbf{Q}\|\,\mathbf{M}^\alpha\right) \tag{C.74}$$

$$= k\mathcal{D}\left(\frac{\lfloor k\left(\mathbf{M}+\mathbf{L}\right)\rfloor}{k}\middle\|\,\mathbf{M}^\alpha\right), \tag{C.75}$$

where through a slight abuse of notation we have expressed the KL divergence of $m$ scalar distributions as a single KL-divergence between matrix inputs. This abuse of notation has originated from the choice to solve the probabilities of detection in a parallelised fashion. By substitution, the probability of detection is upper bounded by

$$\mathbb{P}^1_D = \mathbb{P}\left[T_k \geq \lfloor k\left(\mathbf{M}+\mathbf{L}\right)\rfloor - k\mathbf{M}^\alpha\right] \leq e^{-k\mathcal{D}\left(\frac{\lfloor k(\mathbf{M}+\mathbf{L})\rfloor}{k}\|\mathbf{M}^\alpha\right)}. \tag{C.76}$$

Note that due to (5.67) we have a closed form expression for the optimal value of $\mathbf{M}^\alpha$. Substitution of this into the bound above yields

$$\mathbb{P}^1_D \leq e^{-k\mathcal{D}\left(\frac{\lfloor k(\mathbf{M}+\mathbf{L})\rfloor}{k}\|\mathbf{M}+\beta\epsilon\mathbf{L}\right)}. \tag{C.77}$$

In order to obtain the bound for the lower half of the hypercube, we utilise the fact that the distribution of $T_k$ is symmetric. Note however, that the region is not symmetric. Therefore,

$$\mathbb{P}^2_D = \mathbb{P}\left[T_k \leq \lceil k\left(\mathbf{M}-\mathbf{L}\right)\rceil - k\mathbf{M}^\alpha\right] = \mathbb{P}\left[T_k \geq \lceil k\left(\mathbf{M}-\mathbf{L}\right)\rceil - k\mathbf{M}^\alpha\right]. \tag{C.78}$$

From this it follows that

$$\mathbb{P}^2_D = \mathbb{P}\left[T_k \leq \lceil k\left(\mathbf{M}-\mathbf{L}\right)\rceil - k\mathbf{M}^\alpha\right] \leq e^{-k\mathcal{D}\left(\frac{\lceil k(\mathbf{M}-\mathbf{L})\rceil}{k}\|\mathbf{M}+\beta\epsilon\mathbf{L}\right)}. \tag{C.79}$$

Combining (C.77) and (C.79) yields

$$\mathbb{P}_D \quad \leq e^{-k\mathcal{D}\left(\frac{\lfloor k(\mathbf{M}+\mathbf{L})\rfloor}{k}\|\mathbf{M}+\beta\epsilon\mathbf{L}\right)} + e^{-k\mathcal{D}\left(\frac{\lceil k(\mathbf{M}-\mathbf{L})\rceil}{k}\|\mathbf{M}+\beta\epsilon\mathbf{L}\right)}. \tag{C.80}$$

This concludes the proof. □

# Appendix D

# Chapter 6

## D.1 Theorem 15

This Section is dedicated to the proof of Theorem 15. The Theorem is re-stated below.

**Theorem 15.** *The updated state estimate*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_{k}\left(Y_{k}-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)\right), \tag{D.1}$$

*is equivalent to the fully observed state space system,*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{D.2a}$$

$$\widehat{Y}_{k}=\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{D.2b}$$

*where* $\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right)$ *is defined as*

$$\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right)=\mathbf{G}E_{k}^{U}+\mathbf{L}_{k}\left(\mathbf{H}\left(\mathbf{F}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right)+W_{k}\right)+V_{k+1}\right), \tag{D.3}$$

*and* $\mathbf{L}_{k}$ *is the optimal Kalman filter gain at time step* $k$*.*

*Proof.* In the standard Kalman filter the state estimate is updated according to

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_{k}\left(Y_{k+1}-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)\right), \tag{D.4}$$

where $\mathbf{L}_k$ is defined as,

$$\mathbf{L}_k = \mathbf{R}_k \mathbf{H}^\mathsf{T} \left( \mathbf{H} \mathbf{R}_k \mathbf{H}^\mathsf{T} + \Sigma_{V'} \right)^{-1}, \tag{D.5}$$

and $\mathbf{R}_k$ is the Algebraic Ricatti Equation

$$\mathbf{R}_{k+1} = \mathbf{F} \mathbf{R}_k \mathbf{F}^\mathsf{T} + \Sigma_W - \mathbf{F} \mathbf{R}_k \mathbf{H}^\mathsf{T} \left( \mathbf{H} \mathbf{R}_k \mathbf{H}^\mathsf{T} + \Sigma_{V'} \right)^{-1} \mathbf{H} \mathbf{R}_k \mathbf{F}^\mathsf{T}. \tag{D.6}$$

Note the dependence on the statistics of the random variables $W_k$ and $V'_k$. This is due to the fact that the Kalman filter is designed to mitigate the effect of these variables and not the effect of the channels. As a result of this the optimal Kalman filter is designed independently of the system architecture. Substitution of $Y_k$ into the state estimate update yields

$$\begin{aligned} \widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) &= \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) + \mathbf{L}_k \left( \mathbf{H} X_{k+1} + V_{k+1} - \mathbf{H} \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) \right) && \text{(D.7)} \\ &= \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) + \mathbf{L}_k \mathbf{H} \left( \mathbf{F} X_k + \mathbf{G} U_k + \widetilde{W}_k - \mathbf{F} \widehat{X}_k\left(\mathscr{P}_k^D\right) - \mathbf{G} U_k - \overline{W}_k\left(\mathscr{P}_k^D\right) \right) \\ &\quad + \mathbf{L}_k V_{k+1}. && \text{(D.8)} \end{aligned}$$

Substituting the values for $\overline{W}_k\left(\mathscr{P}_k^D\right)$ and $\widetilde{W}_k$ yields

$$\begin{aligned} \widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) = \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) &+ \mathbf{L}_k \mathbf{H} \left( \mathbf{F} \left( E_k^X\left(\mathscr{P}_k^D\right) - \mathbb{E}\left[ E_k^X\left(\mathscr{P}_k^D\right) \middle| \mathscr{P}_{k+1}^D \right] \right) \right. \\ &\left. + \mathbf{G} \left( E_k^U - \mathbb{E}\left[ E_k^U \middle| \mathscr{P}_{k+1}^D \right] \right) + \left( W_k - \mathbb{E}\left[ W_k \middle| \mathscr{P}_{k+1}^D \right] \right) \right) + \mathbf{L}_k V_{k+1}. \end{aligned} \tag{D.9}$$

Note that in (D.9) the set $\mathscr{P}_{k+1}^D$ contains the variable $\widetilde{U}_k$ and therefore the expectation does not go to zero and the two actuation error terms cancel one another. Operating the expectation operator for each other random variable yields

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) = \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) + \mathbf{L}_k \mathbf{H} \left( \mathbf{F} E_k^X\left(\mathscr{P}_k^D\right) + W_k \right) + \mathbf{L}_k V_{k+1}. \tag{D.10}$$

At this stage the predicted state trajectory can be expanded according to (6.20) to give

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right) = \mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right) + \mathbf{G}U_k + \overline{W}_{k}\left(\mathscr{P}_{k}^{D}\right) + \mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right) + W_k\right) + \mathbf{L}_k V_{k+1} \tag{D.11}$$

$$= \mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right) + \mathbf{G}U_k + \overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{D.12}$$

where $\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right)$ is defined as

$$\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right) = \mathbf{G}E_{k}^{U} + \mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right) + W_k\right) + \mathbf{L}_k V_{k+1}. \tag{D.13}$$

This is now in the form of a fully observed state space system. Namely, the state space system

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right) = \mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right) + \mathbf{G}U_k + \overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{D.14a}$$

$$\widehat{Y}_k = \widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right). \tag{D.14b}$$

This concludes the proof.

□

## D.2 Lemma 17

This Section is dedicated to the proof of Lemma 17. The Lemma is re-stated below.

**Lemma 17.** *All of the variables within $\overline{\overline{W}}_k$ are uncorrelated.*

*Proof.* The actuation error is defined as

$$E_{k}^{U} = \widetilde{U}_k - U_k = Z_k. \tag{D.15}$$

Therefore, the actuation error $E_{k}^{U}$ is independent of the control law $U_k$. By definition $Z_k$ is independent of all other random variables. Therefore, the actuation error $E_{k}^{U}$ is independent of the predicted state estimation error $E_{k+1}^{X}\left(\mathscr{P}_{k}^{D}\right)$ and the process noise $W_k$ for all $k$. Similarly, $W_k$ and $V_k$ are defined as independent of all other random variables.

The predicted estimation error is

$$E_{k+1}^{X}\left(\mathscr{P}_{k}^{D}\right)=X_{k+1}-\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right) \tag{D.16}$$

$$=\left(\mathbf{F}X_{k}+\mathbf{G}U_{k}+\widetilde{W}_{k}\right)-\left(\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{W}_{k}\left(\mathscr{P}_{k}^{D}\right)\right) \tag{D.17}$$

$$=\mathbf{F}\left(E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right)-\mathbb{E}\left[\mathbf{F}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right)\middle|\mathscr{P}_{k}^{D}\right]\right)+\mathbf{G}\left(E_{k}^{U}-\mathbb{E}\left[E_{k}^{U}\middle|\mathscr{P}_{k}^{D}\right]\right)$$
$$+\left(W_{k}-\mathbb{E}\left[W_{k}\middle|\mathscr{P}_{k}^{D}\right]\right) \tag{D.18}$$

$$=\mathbf{F}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}E_{k}^{U}+W_{k}. \tag{D.19}$$

As shown in [71], the prediction estimate is uncorrelated with the process noise, $W_k$. Additionally, due to knowledge of the realisation of $\widetilde{U}_k$ the error corresponding to this term is removed entirely, which results in

$$E_{k+1}^{X}\left(\mathscr{P}_{k+1}^{D}\right)=X_{k+1}-\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right) \tag{D.20}$$

$$=\mathbf{F}X_{k}+\mathbf{G}U_{k}+\widetilde{W}_{k}-\left(\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right)\right) \tag{D.21}$$

$$=\mathbf{F}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right)+\widetilde{W}_{k}-\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right) \tag{D.22}$$

$$=\left(\mathbf{I}-\mathbf{L}_{k}\mathbf{H}\right)\left(\mathbf{F}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right)+W_{k}\right)-\mathbf{L}_{k}V_{k+1}. \tag{D.23}$$

The state estimation error is uncorrelated with the process noise $W_k$. In our scenario there are additional random variables present within the updated state error. The results presented in [71] still hold and the state estimation error is uncorrelated with all other random variables, provided they are independent, which as shown above, holds. To see this note that (D.23) is rewritten as

$$E_{k+1}^{X}\left(\mathscr{P}_{k+1}^{D}\right)=\widetilde{\mathbf{F}}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right)+\widetilde{\overline{W}}_{k}, \tag{D.24}$$

where $\widetilde{\mathbf{F}}=\left(\mathbf{I}-\mathbf{L}_{k}\mathbf{H}\right)\mathbf{F}$ and

$$\widetilde{\overline{W}}_{k}=\left(\mathbf{I}-\mathbf{L}_{k}\mathbf{H}\right)W_{k}-\mathbf{L}_{k}V_{k+1}. \tag{D.25}$$

The proof of Lemma 3.2 in [71] holds with a change of variables. Therefore, the updated error is uncorrelated with all other random variables. This concludes the proof. □

## D.3 Theorem 16

This Section is dedicated to the proof of Theorem 16. The Theorem is re-stated below.

**Theorem 16.** *The updated state estimate*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_{k}\left(Y_{k}-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)\right), \tag{D.26}$$

*is equivalent to the state space system*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{D.27a}$$

$$\widehat{Y}_{k}=\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{D.27b}$$

*where* $\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right)$ *is defined as*

$$\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right)=\mathbf{L}_{k}\mathbf{H}\left(\mathbf{F}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}E_{k}^{U}+W_{k}\right)+\mathbf{L}_{k}V_{k+1}, \tag{D.28}$$

*and* $\mathbf{L}_k$ *is the optimal Kalman filter gain at time step* $k$*.*

*Proof.* The standard Kalman filter is adopted as is defined in (D.5). As mentioned before this optimal Kalman filter design is the same irregardless of the system architecture. The updated state estimate is therefore defined as

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_{k}\left(Y_{k+1}-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)\right). \tag{D.29}$$

Substitution of $Y_k$ into the state estimate update yields

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right)=\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)+\mathbf{L}_k\left(\mathbf{H}\left(X_{k+1}+V_{k+1}\right)-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)\right) \tag{D.30}$$

$$=\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)+\mathbf{L}_k\mathbf{H}\left(\mathbf{F}X_k+\mathbf{G}U_k+\widetilde{W}_k-\left(\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right)+\mathbf{G}U_k+\overline{W}_k\left(\mathscr{P}_k^D\right)\right)\right)$$

$$+\mathbf{L}_kV_{k+1}. \tag{D.31}$$

Substituting in the values for $\overline{W}_k\left(\mathscr{P}_k^D\right)$ and $\widetilde{W}_k$ while noting the information set for the expectation yields

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right)=\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)+\mathbf{L}_k\mathbf{H}\left(\mathbf{F}\left(E_k^X\left(\mathscr{P}_k^D\right)-\mathbb{E}\left[E_k^X\left(\mathscr{P}_k^D\right)\middle|\mathscr{P}_k^D\right]\right)\right.$$

$$\left.+\mathbf{G}\left(E_k^U-\mathbb{E}\left[E_k^U\middle|\mathscr{P}_k^D\right]\right)+\left(W_k-\mathbb{E}\left[W_k|\mathscr{P}_k^D\right]\right)\right)+\mathbf{L}_kV_{k+1}. \tag{D.32}$$

Operating the expectation operator for each random variable within (D.32) yields

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right)=\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)+\mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right)+\mathbf{G}E_k^U+W_k\right)+\mathbf{L}_kV_{k+1}. \tag{D.33}$$

At this stage the predicted state trajectory can be expanded according to (6.44) to give

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right)=\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right)+\mathbf{G}U_k+\overline{W}_k\left(\mathscr{P}_k^D\right)+\mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right)+\mathbf{G}E_k^U+W_k\right)$$

$$+\mathbf{L}_kV_{k+1} \tag{D.34}$$

$$=\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right)+\mathbf{G}U_k+\overline{\overline{W}}_k\left(\mathscr{P}_k^D\right), \tag{D.35}$$

where it should be noted that $\overline{W}_k\left(\mathscr{P}_k^D\right)$ is a zero mean random variable and therefore has expectation $\mathbf{0}$, and $\overline{\overline{W}}_k\left(\mathscr{P}_k^D\right)$ is defined as

$$\overline{\overline{W}}_k\left(\mathscr{P}_k^D\right)=\mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right)+\mathbf{G}E_k^U+W_k\right)+\mathbf{L}_kV_{k+1}. \tag{D.36}$$

This is now in the form of a fully observed state space system. Namely, the state space system,

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{D.37a}$$

$$\widehat{Y}_{k}=\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right). \tag{D.37b}$$

This concludes the proof. □

## D.4 Theorem 17

This Section is dedicated to the proof of Theorem 17. The Theorem is re-stated below.

**Theorem 17.** *The updated state estimate*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_{k}\left(Y_{k}-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)\right), \tag{D.38}$$

*is equivalent to the state space system,*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{D.39a}$$

$$\widehat{Y}_{k}=\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{D.39b}$$

*where* $\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right)$ *is defined as*

$$\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right)=\mathbf{L}_{k}\mathbf{H}\left(\mathbf{F}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}T_{k}+W_{k}\right)+\mathbf{L}_{k}V_{k+1}, \tag{D.40}$$

*and* $T_k$ *is the zero mean AWGN introduced by the imperfect auxiliary communication channel with covariance* $\Sigma_T$*.*

*Proof.* In the standard Kalman filter the state estimate is updated according to

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_{k}\left(Y_{k+1}-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)\right) \tag{D.41}$$

where $\mathbf{L}_k$ is defined in (D.5). Substitution of $Y_k$ into the state estimate update yields

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) = \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) + \mathbf{L}_k\left(\mathbf{H}\left(X_{k+1}+V_{k+1}\right) - \mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)\right) \tag{D.42}$$

$$= \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) + \mathbf{L}_k\mathbf{H}\left(\mathbf{F}X_k + \mathbf{G}U_k + \widetilde{W}_k - \left(\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{W}_k\left(\mathscr{P}_k^D\right)\right)\right)$$

$$+\mathbf{L}_k V_{k+1}. \tag{D.43}$$

Substituting in the values for $\overline{W}_k\left(\mathscr{P}_k^D\right)$ and $\widetilde{W}_k$ while noting the information set for the expectation yields

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) = \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) + \mathbf{L}_k\mathbf{H}\left(\mathbf{F}\left(E_k^X\left(\mathscr{P}_k^D\right) - \mathbb{E}\left[E_k^X\left(\mathscr{P}_k^D\right)\middle|\mathscr{P}_k^D\right]\right)\right.$$

$$\left.+\mathbf{G}\left(E_k^U - \mathbb{E}\left[E_k^U\middle|\mathscr{P}_k^D\right]\right) + \left(W_k - \mathbb{E}\left[W_k|\mathscr{P}_k^D\right]\right)\right) + \mathbf{L}_k V_{k+1}. \tag{D.44}$$

This is where the derivation diverges from the previous two. This is due to the fact that at this point the operator has access to the measurement of the signal $\widetilde{U}_k$. However, it is corrupted by the noise within the imperfect auxiliary communication channel. Specifically, the operator has the variable $\widetilde{\widetilde{U}}_k$. This variable is defined as

$$\widetilde{\widetilde{U}}_k = \widetilde{U}_k + T_k, \tag{D.45}$$

where $T_k \in \mathbb{R}^m$ is a vector of Gaussian distributed variables with mean $\mathbf{0}$ and covariance $\Sigma_T$. Therefore, with this information available to the operator they can remove the effect of the noisy actuation signal from the estimate at the cost of introducing the detrimental effect of the random variable $T_k$. Performing this substitution in tandem with computing the expectation for each random variable yields

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) = \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) + \mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right) - \mathbf{G}T_k + W_k\right) + \mathbf{L}_k V_{k+1}. \tag{D.46}$$

Note that the operator introduces the addition of a zero mean random variable. Therefore, the predicted state estimate is expanded according to (6.44) to give

$$\begin{aligned}\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right) &= \mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right) + \mathbf{G}U_k + \overline{W}_{k}\left(\mathscr{P}_{k}^{D}\right) + \mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right) + \mathbf{G}T_k + W_k\right) \\ &\quad + \mathbf{L}_k V_{k+1} \qquad \text{(D.47)} \\ &= \mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right) + \mathbf{G}U_k + \overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right), \qquad \text{(D.48)}\end{aligned}$$

where it should be noted that $\overline{W}_{k}\left(\mathscr{P}_{k}^{D}\right)$ is a zero mean random variable and therefore has expectation $\mathbf{0}$. Additionally, $\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right)$ is defined as

$$\overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right) = \mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_{k}^{X}\left(\mathscr{P}_{k}^{D}\right) + \mathbf{G}T_k + W_k\right) + \mathbf{L}_k V_{k+1}. \qquad \text{(D.49)}$$

It is seen that (D.48) is in the form of a fully observed state space system. Namely, the state space system

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right) = \mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right) + \mathbf{G}U_k + \overline{\overline{W}}_{k}\left(\mathscr{P}_{k}^{D}\right), \qquad \text{(D.50a)}$$

$$\widehat{Y}_k = \widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right). \qquad \text{(D.50b)}$$

This concludes the proof. □

# Appendix E

# Chapter 7

## E.1 Theorem 22

This Section is dedicated to the proof of Theorem 22. The Theorem is re-stated below.

**Theorem E.1.** *The updated state estimate of the system under attack,*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_{k}\left(Y_{k}-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)\right). \tag{E.1}$$

*Is equivalent to the state space system,*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right), \tag{E.2a}$$

$$\widehat{Y}_{k}=\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right). \tag{E.2b}$$

*where* $\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right)$ *is defined as*

$$\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right)=\mathbf{G}E_{k}^{U^{A}}+\mathbf{L}_{k}\mathbf{H}\left(\mathbf{F}E_{k}^{X^{A}}\left(\mathscr{P}_{k}^{D}\right)+W_{k}\right)+\mathbf{L}_{k}\left(V_{k+1}+A_{k+1}^{X}\right), \tag{E.3}$$

*and* $\mathbf{L}_k$ *is the optimal Kalman filter gain at time step* $k$*, as defined in Theorem 15.*

*Proof.* The Kalman filter gain remains unchanged during the attack as the operator is unaware of the attack and its statistics. Therefore, substitution of $Y_k$ into the state

estimate update yields,

$$\begin{aligned}\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right) &= \widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_k\left(\mathbf{H}X_{k+1}+V_{k+1}+A_{k+1}^{X}-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)\right) &\text{(E.4)}\\ &= \widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_k\mathbf{H}\left(\mathbf{F}X_k+\mathbf{G}U_k+\widetilde{W}_k^{A}-\left(\mathbf{F}\widehat{X}_k\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_k+\overline{W}_k^{A}\left(\mathscr{P}_{k}^{D}\right)\right)\right)\\ &\quad+\mathbf{L}_k\left(V_{k+1}+A_{k+1}^{X}\right). &\text{(E.5)}\end{aligned}$$

Substituting in the values for $\overline{W}_k^{A}\left(\mathscr{P}_{k}^{D}\right)$ and $\widetilde{W}_k^{A}$ while noting the information set for the expectation yields

$$\begin{aligned}\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right) &= \widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_k\mathbf{H}\left(\mathbf{F}\left(E_k^{X^A}\left(\mathscr{P}_{k}^{D}\right)-\mathbb{E}\left[E_k^{X^A}\left(\mathscr{P}_{k}^{D}\right)\middle|\mathscr{P}_{k+1}^{D}\right]\right)\right.\\ &\quad\left.+\mathbf{G}\left(E_k^{U}+A_k^{U}-\mathbb{E}\left[E_k^{U}+A_k^{U}\middle|\mathscr{P}_{k+1}^{D}\right]\right)+\left(W_k-\mathbb{E}\left[W_k\middle|\mathscr{P}_{k}^{D}\right]\right)\right)\\ &\quad+\mathbf{L}_k\left(V_{k+1}+A_{k+1}^{X}\right). &\text{(E.6)}\end{aligned}$$

Operating the expectation for each random variable, once again noting the information available at this stage yields

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_{k}^{D}\right)+W_k\right)+\mathbf{L}_k\left(V_{k+1}+A_{k+1}^{X}\right). \tag{E.7}$$

At this stage the predicted state trajectory can be expanded according to (7.27) to give,

$$\begin{aligned}\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right) &= \mathbf{F}\widehat{X}_k\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_k+\overline{W}_k^{A}\left(\mathscr{P}_{k}^{D}\right)\\ &\quad+\mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}E_k^{U^A}+W_k\right)+\mathbf{L}_k\left(V_{k+1}+A_{k+1}^{X}\right). &\text{(E.8)}\\ &= \mathbf{F}\widehat{X}_k\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_k+\overline{\overline{W}}_k^{A}\left(\mathscr{P}_{k}^{D}\right), &\text{(E.9)}\end{aligned}$$

where, it should be noted once again that $\overline{W}_k\left(\mathscr{P}_{k}^{D}\right)$ now has access to the realisation of the actuation that entered the plant, which includes the attack variable. Additionally, $\overline{\overline{W}}_k^{A}\left(\mathscr{P}_{k}^{D}\right)$ is defined as

$$\overline{\overline{W}}_k^{A}\left(\mathscr{P}_{k}^{D}\right)=\mathbf{G}E_k^{U^A}+\mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_{k}^{D}\right)+W_k\right)+\mathbf{L}_k\left(V_{k+1}+A_{k+1}^{X}\right). \tag{E.10}$$

This is now in the form of a fully observed state space system. Namely, the state space system,

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right), \tag{E.11a}$$

$$\widehat{Y}_{k}=\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right). \tag{E.11b}$$

This concludes the proof. □

## E.2 Lemma 18

This Section is dedicated to the proof of Lemma 18. The Lemma is re-stated below.

**Lemma 18.** *All of the variables within* $\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right)$ *are uncorrelated.*

*Proof.* The actuation error is

$$E_{k+1}^{UA}=\widetilde{U}_{k+1}^{A}-U_{k+1} \tag{E.12}$$

$$=U_{k+1}+Z_{k+1}+A_{k+1}^{U}-U_{k+1} \tag{E.13}$$

$$=E_{k}^{U}+A_{k+1}^{U}. \tag{E.14}$$

As seen in the proof of Lemma 17 $E_{k+1}^{U}$ is independent of all other random variables. Additionally, the actuation communication channel attack variable, $A_{k+1}^{U}$, is defined as independent of all other random variables. Therefore, the actuation error when under attack, (E.14), is independent of the predicted state estimation error and the plant noise.

The predicted state estimation error is

$$
\begin{aligned}
E_{k+1}^{X^A}\left(\mathscr{P}_k^D\right) &= X_{k+1} - \widehat{X}_{k+1}\left(\mathscr{P}_k^D\right) && \text{(E.15)}\\
&= \mathbf{F}X_k + \mathbf{G}U_k + \widetilde{W}_k^A - \left(\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{W}_k^A\left(\mathscr{P}_k^D\right)\right) && \text{(E.16)}\\
&= \mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}A_k^U + \widetilde{W}_k - \overline{W}_k^A\left(\mathscr{P}_k^D\right) && \text{(E.17)}\\
&= \mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}A_k^U + \mathbf{G}E_k^U + W_k \\
&\qquad -\mathbb{E}\left[\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}\left(E_k^U + A_k^U\right) + W_k \middle| \mathscr{P}_k^D\right] && \text{(E.18)}\\
&= \mathbf{F}\left(E_k^{X^A}\left(\mathscr{P}_k^D\right) - \mathbb{E}\left[E_k^{X^A}\left(\mathscr{P}_k^D\right)\middle|\mathscr{P}_k^D\right]\right) + \mathbf{G}\left(A_k^U - \mathbb{E}\left[A_k^U\middle|\mathscr{P}_k^D\right]\right) \\
&\qquad +\mathbf{G}\left(E_k^U - \mathbb{E}\left[E_k^U\middle|\mathscr{P}_k^D\right]\right) + W_k && \text{(E.19)}\\
&= \mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}A_k^U + \mathbf{G}E_k^U + W_k. && \text{(E.20)}
\end{aligned}
$$

Note that the actuation communication channel attack effects the predicted state error. This is due to the fact that this data injection attack actually enters the system whereas the sensory communication channel only effects the measurements of the states. The updated state estimate is defined as

$$
\begin{aligned}
E_{k+1}^{X^A}\left(\mathscr{P}_{k+1}^D\right) &= X_{k+1} - \widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right) && \text{(E.21)}\\
&= \mathbf{F}X_k + \mathbf{G}U_k + \widetilde{W}_k^A - \left(\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right) + \mathbf{G}U_k + \overline{\overline{W}}_k^A\left(\mathscr{P}_k^D\right)\right) && \text{(E.22)}\\
&= \mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \widetilde{W}_k^A - \overline{\overline{W}}_k^A\left(\mathscr{P}_k^D\right) && \text{(E.23)}\\
&= \mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + \mathbf{G}A_k^U + \mathbf{G}E_k^U + W_k - \mathbf{G}E_k^{U^A} - \mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + W_k\right) \\
&\qquad -\mathbf{L}_k\left(V_{k+1} + A_{k+1}^X\right) && \text{(E.24)}\\
&= \widetilde{\mathbf{L}}_k\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right) + W_k\right) - \mathbf{L}_k\left(A_{k+1}^X + V_{k+1}\right), && \text{(E.25)}
\end{aligned}
$$

In (E.25) the error is in the same form as (D.23). Therefore, the results from Lemma 3.2 in [71] holds with a change of variables. Thus, all random variables are uncorrelated. This concludes the proof. □

## E.3 Lemma 19

This Section is dedicated to the proof of Lemma 19. The Lemma is re-stated below.

**Lemma 19.** *The derivative of*

$$f(\mathbf{A}) = \operatorname{tr}(\mathbf{B}\mathbf{A}) + \alpha\left(\operatorname{tr}\left(\mathbf{C}^{-1}\mathbf{A}\right) - \log\left|\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right| - \beta\right), \tag{E.26}$$

*with respect to the matrix* $\mathbf{A} \in S_+^n$ *is*

$$\begin{aligned}\frac{\partial f(\mathbf{A})}{\partial \mathbf{A}} = &\mathbf{B} + \mathbf{B}^\mathsf{T} + 2\alpha\mathbf{C}^{-1} - \alpha\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1}\mathbf{C}^{-1} - \alpha\mathbf{C}^{-1}\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1} \\ &-\mathbf{I} \odot \left[\mathbf{B} + \alpha\mathbf{C}^{-1} - \alpha\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1}\mathbf{C}^{-1}\right],\end{aligned} \tag{E.27}$$

*where* $\odot$ *is the Hadamard product, and therefore,* $\mathbf{I} \odot (\cdot) = diag(\cdot)$.

*Proof.* The first two terms within (7.58) and the last are trivial to compute and the derivative is expressed as

$$\frac{\partial f(\mathbf{A})}{\partial \mathbf{A}} = \mathbf{B} + \mathbf{B}^\mathsf{T} + 2\alpha\mathbf{C}^{-1} - \mathbf{I} \odot \left[\mathbf{B} + \alpha\mathbf{C}^{-1}\right] - \frac{\partial \log\left|\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right|}{\partial \mathbf{A}}, \tag{E.28}$$

where the additional terms arise due to the symmetry of $\mathbf{A}$. Within the determinant there is a matrix function of $\mathbf{A}$, let this be defined as $\mathbf{M}(\mathbf{A})$. Therefore, the remaining term to be evaluated is,

$$\frac{\partial \log|\mathbf{M}(\mathbf{A})|}{\partial \mathbf{A}} \tag{E.29}$$

As seen in [30, 17.52, pg. 369] the derivative of the nesting of functions $\log \circ \det$ is simplified to

$$\frac{\partial}{\partial \mathbf{A}} \log|\mathbf{M}(\mathbf{A})| = |\mathbf{M}(\mathbf{A})|^{-1} \frac{\partial |\mathbf{M}(\mathbf{A})|}{\partial \mathbf{A}} \tag{E.30}$$

From this stage, the derivative of the determinant needs to be calculated. This is

$$\frac{\partial \left|\mathbf{M}\left(\mathbf{A}\right)\right|}{\partial \mathbf{A}} = \left|\mathbf{M}\left(\mathbf{A}\right)\right| \operatorname{tr}\left(\mathbf{M}\left(\mathbf{A}\right)^{-1} \frac{\partial \mathbf{M}\left(\mathbf{A}\right)}{\partial \mathbf{A}}\right). \tag{E.31}$$

Executing the above identities, while noting that the determinants cancel, gives

$$\frac{\partial}{\partial \mathbf{A}} \log \left|\mathbf{M}\left(\mathbf{A}\right)\right| = \mathbf{M}\left(\mathbf{A}\right)^{-1} \mathbf{C}^{-1} + \mathbf{C}^{-1^{\mathsf{T}}} \mathbf{M}\left(\mathbf{A}\right)^{-1^{\mathsf{T}}} - \mathbf{I} \odot \left[\mathbf{M}\left(\mathbf{A}\right)^{-1} \mathbf{C}^{-1}\right]. \tag{E.32}$$

Note that the terms $\mathbf{M}\left(\mathbf{A}\right)$ and $\mathbf{C}$ are symmetric. Utilising this fact in (E.28) yields

$$\begin{aligned}\frac{\partial f\left(\mathbf{A}\right)}{\partial \mathbf{A}} = \mathbf{B} + \mathbf{B}^{\mathsf{T}} + 2\alpha \mathbf{C}^{-1} \text{-} \mathbf{I} \odot \left[\mathbf{B} + \alpha \mathbf{C}^{-1}\right] \text{-} \alpha \mathbf{M}\left(\mathbf{A}\right)^{-1} \mathbf{C}^{-1} - \alpha \mathbf{C}^{-1^{\mathsf{T}}} \mathbf{M}\left(\mathbf{A}\right)^{-1^{\mathsf{T}}} \\ + \mathbf{I} \odot \left[\alpha \mathbf{M}\left(\mathbf{A}\right)^{-1} \mathbf{C}^{-1}\right].\end{aligned} \tag{E.33}$$

Simplification and substitution of the function $\mathbf{M}\left(\mathbf{A}\right)$ gives

$$\begin{aligned}\frac{\partial f\left(\mathbf{A}\right)}{\partial \mathbf{A}} = \mathbf{B} + \mathbf{B}^{\mathsf{T}} + 2\alpha \mathbf{C}^{-1} - \alpha \left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1} \mathbf{C}^{-1} - \alpha \mathbf{C}^{-1} \left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1} \\ - \mathbf{I} \odot \left[\mathbf{B} + \alpha \mathbf{C}^{-1} - \alpha \left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1} \mathbf{C}^{-1}\right].\end{aligned} \tag{E.34}$$

Which corresponds to (7.59). This concludes the proof. □

## E.4 Lemma 20

This Section is dedicated to the proof of Lemma 20. The Lemma is re-stated below.

**Lemma 20.** *It is to be shown that solving*

$$\begin{aligned}\mathbb{0} = \mathbf{B} + \mathbf{B}^{\mathsf{T}} + 2\alpha \mathbf{C}^{-1} - \alpha \left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1} \mathbf{C}^{-1} - \alpha \mathbf{C}^{-1} \left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1} \\ - \mathbf{I} \odot \left[\mathbf{B} + \alpha \mathbf{C}^{-1} - \alpha \left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1} \mathbf{C}^{-1}\right],\end{aligned} \tag{E.35}$$

*is equivalent to solving*

$$2\mathbf{B} + 2\alpha\mathbf{C}^{-1} - 2\alpha\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1}\mathbf{C}^{-1} = \mathbb{0} \tag{E.36}$$

*Proof.* Initially, it is seen that (7.62) is simplified through the fact that $\mathbf{B}$, in this setting, is symmetric. Therefore, (7.62) becomes

$$\begin{aligned}\mathbb{0} = \; & 2\mathbf{B} + 2\alpha\mathbf{C}^{-1} - \alpha\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1}\mathbf{C}^{-1} - \alpha\mathbf{C}^{-1}\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1} \\ & -\mathbf{I} \odot \left[\mathbf{B} + \alpha\mathbf{C}^{-1} - \alpha\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1}\mathbf{C}^{-1}\right].\end{aligned} \tag{E.37}$$

At this stage the second line poses the largest issue with simplification. We begin by simplifying the first line of (E.37). In the following it is shown that $\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1}$ and $\mathbf{C}^{-1}$ commute. To see this note that it is know that $\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1}$ is non-negative definite and $\mathbf{C}^{-1}$ is positive definite. Therefore, linear combinations of the two matrices exist that which are positive definite. Trivially, an example is

$$\left[\mathbf{I} + \Sigma_Z^{-1}\Sigma_{A^U}\right]^{-1} + \Sigma_Z^{-1} \succ \mathbb{0}. \tag{E.38}$$

If a real linear combination of two matrices exists that is positive definite then these two matrices are simultaneously diagonalisable [30, 16.51(b) pg.345]. This required condition holds, as seen in (E.38). Therefore, an $\mathbf{R} \in \mathbb{R}^{n\times n}$ exists such that $\left[\mathbf{I} + \mathbf{C}^{-1}\mathbf{A}\right]^{-1} = \mathbf{R}^\intercal\mathbf{D}^{\left[\mathbf{I}+\mathbf{C}^{-1}\mathbf{A}\right]^{-1}}\mathbf{R}$ and simultaneously $\mathbf{C}^{-1} = \mathbf{R}^\intercal\mathbf{D}^{\mathbf{C}^{-1}}\mathbf{R}$, where $\mathbf{D}^{\left[\mathbf{I}+\mathbf{C}^{-1}\mathbf{A}\right]^{-1}}$ and $\mathbf{D}^{\mathbf{C}^{-1}}$

are diagonal matrices. From this, it is seen that

$$\left[\mathbf{I}+\mathbf{C}^{-1}\mathbf{A}\right]^{-1}\mathbf{C}^{-1} = \mathbf{R}^{\intercal}\mathbf{D}^{\left[\mathbf{I}+\mathbf{C}^{-1}\mathbf{A}\right]^{-1}}\mathbf{R}\mathbf{R}^{\intercal}\mathbf{D}^{\mathbf{C}^{-1}}\mathbf{R} \tag{E.39}$$

$$= \mathbf{R}^{\intercal}\mathbf{D}^{\left[\mathbf{I}+\mathbf{C}^{-1}\mathbf{A}\right]^{-1}}\mathbf{D}^{\mathbf{C}^{-1}}\mathbf{R} \tag{E.40}$$

$$= \mathbf{R}^{\intercal}\mathbf{D}^{\mathbf{C}^{-1}}\mathbf{D}^{\left[\mathbf{I}+\mathbf{C}^{-1}\mathbf{A}\right]^{-1}}\mathbf{R} \tag{E.41}$$

$$= \mathbf{R}^{\intercal}\mathbf{D}^{\mathbf{C}^{-1}}\mathbf{R}\mathbf{R}^{\intercal}\mathbf{D}^{\left[\mathbf{I}+\mathbf{C}^{-1}\mathbf{A}\right]^{-1}}\mathbf{R} \tag{E.42}$$

$$= \mathbf{C}^{-1}\left[\mathbf{I}+\mathbf{C}^{-1}\mathbf{A}\right]^{-1}. \tag{E.43}$$

Therefore, these matrices commute. This fact allows (E.37) to be simplified once more

$$\begin{aligned}\mathbb{0} = \; & 2\mathbf{B}+2\alpha\mathbf{C}^{-1}-2\alpha\left[\mathbf{I}+\mathbf{C}^{-1}\mathbf{A}\right]^{-1}\mathbf{C}^{-1} \\ & -\mathbf{I}\odot\left[\mathbf{B}+\alpha\mathbf{C}^{-1}-\alpha\left[\mathbf{I}+\mathbf{C}^{-1}\mathbf{A}\right]^{-1}\mathbf{C}^{-1}\right].\end{aligned} \tag{E.44}$$

In (E.44), all terms within the diagonal operator are a scalar multiple of the terms outside of the diagonal operator. This means that if the terms outside of the diagonal operator sum to the $\mathbb{0}$ matrix then necessarily the terms inside of the operator also sum to the $\mathbb{0}$ matrix. In light of this, (7.60) is simplified to

$$2\mathbf{B}+2\alpha\mathbf{C}^{-1}-2\alpha\left[\mathbf{I}+\mathbf{C}^{-1}\mathbf{A}\right]^{-1}\mathbf{C}^{-1}=\mathbb{0}. \tag{E.45}$$

Which corresponds to (7.63). This concludes the proof. □

## E.5 Theorem 23

This Section is dedicated to the proof of Theorem 23. The Theorem is re-stated below.

**Theorem 23.** *The updated state estimate of the system under attack,*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_k\left(Y_k-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)\right). \tag{E.46}$$

*Is equivalent to the state space system,*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right), \tag{E.47a}$$

$$\widehat{Y}_{k}=\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right), \tag{E.47b}$$

*where* $\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right)$ *is defined as*

$$\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right)=\mathbf{L}_{k}\mathbf{H}\left(\mathbf{F}E_{k}^{X^{A}}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}E_{k}^{U^{A}}+W_{k}\right)+\mathbf{L}_{k}\left(V_{k+1}+A_{k+1}^{X}\right), \tag{E.48}$$

*and* $\mathbf{L}_k$ *is the optimal Kalman filter gain at time step* $k$*.*

*Proof.* The Kalman filter gain remains unchanged during the attack as the operator is unaware of the attack and its statistics. Therefore, substitution of $Y_k$ into the state estimate update yields,

$$\begin{aligned}\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)&=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_{k}\left(\mathbf{H}X_{k+1}+V_{k+1}+A_{k+1}^{X}-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)\right) &\text{(E.49)}\\ &=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_{k}\mathbf{H}\left(\mathbf{F}X_{k}+\mathbf{G}U_{k}+\widetilde{W}_{k}^{A}-\left(\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{W}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right)\right)\right)\\ &\quad+\mathbf{L}_{k}\left(V_{k+1}+A_{k+1}^{X}\right), &\text{(E.50)}\end{aligned}$$

substituting in the values for $\overline{W}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right)$ and $\widetilde{W}_{k}^{A}$ while noting the information set for the expectation yields,

$$\begin{aligned}\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)&+\mathbf{L}_{k}\mathbf{H}\left(\mathbf{F}\left(E_{k}^{X^{A}}\left(\mathscr{P}_{k}^{D}\right)-\mathbb{E}\left[E_{k}^{X^{A}}\left(\mathscr{P}_{k}^{D}\right)\middle|\mathscr{P}_{k}^{D}\right]\right)\right.\\ &\left.+\left(W_{k}-\mathbb{E}\left[W_{k}\middle|\mathscr{P}_{k}^{D}\right]\right)+\mathbf{G}\left(E_{k}^{U}+A_{k}^{U}-\mathbb{E}\left[E_{k}^{U}+A_{k}^{U}\middle|\mathscr{P}_{k}^{D}\right]\right)\right)\\ &+\mathbf{L}_{k}\left(V_{k+1}+A_{k+1}^{X}\right). \qquad \text{(E.51)}\end{aligned}$$

Operating the expectation operator for each random variable yields

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_{k}\mathbf{H}\left(\mathbf{F}E_{k}^{X^{A}}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}E_{k}^{U^{A}}+W_{k}\right)+\mathbf{L}_{k}\left(V_{k+1}+A_{k+1}^{X}\right). \tag{E.52}$$

At this stage the predicted state trajectory can be expanded according to (7.120) to give,

$$\begin{aligned}\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)&=\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{W}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_{k}\mathbf{H}\left(\mathbf{F}E_{k}^{X^{A}}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}E_{k}^{U^{A}}+W_{k}\right)\\&\quad+\mathbf{L}_{k}\left(V_{k+1}+A_{k+1}^{X}\right),\qquad\text{(E.53)}\\&=\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right),\qquad\text{(E.54)}\end{aligned}$$

where it should be noted that $\overline{W}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right)$ is a zero mean random variable and $\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right)$ is defined as

$$\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right)=\mathbf{L}_{k}\mathbf{H}\left(\mathbf{F}E_{k}^{X^{A}}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}E_{k}^{U^{A}}+W_{k}\right)+\mathbf{L}_{k}\left(V_{k+1}+A_{k+1}^{X}\right).\qquad\text{(E.55)}$$

This is now in the form of a fully observed state space system. Namely, the state space system,

$$\begin{aligned}\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)&=\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right),\qquad\text{(E.56a)}\\\widehat{Y}_{k}&=\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right).\qquad\text{(E.56b)}\end{aligned}$$

This concludes the proof. □

## E.6 Theorem 24

This Section is dedicated to the proof of Theorem 24. The Theorem is re-stated below.

**Theorem 24.** *The updated state estimate,*

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)=\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{L}_{k}\left(Y_{k}-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_{k}^{D}\right)\right).\qquad\text{(E.57)}$$

*Is equivalent to the state space system,*

$$\begin{aligned}\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^{D}\right)&=\mathbf{F}\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right)+\mathbf{G}U_{k}+\overline{\overline{W}}_{k}^{A}\left(\mathscr{P}_{k}^{D}\right),\qquad\text{(E.58a)}\\\widehat{Y}_{k}&=\widehat{X}_{k}\left(\mathscr{P}_{k}^{D}\right),\qquad\text{(E.58b)}\end{aligned}$$

*where* $\overline{\overline{W}}_k\left(\mathscr{P}_k^D\right)$ *is defined as*

$$\overline{\overline{W}}^A\left(\mathscr{P}_k^D\right)=\mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right)+\mathbf{G}\left(T_k+A_k^A\right)+W_k\right)+\mathbf{L}_k\left(V_{k+1}+A_{k+1}^X\right). \tag{E.59}$$

*Proof.* In the standard Kalman filter the state estimate is updated according to,

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right)=\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)+\mathbf{L}_k\left(Y_{k+1}-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)\right), \tag{E.60}$$

where $\mathbf{L}_k$ is defined in (D.5). Substitution of $Y_k$ into the state estimate update yields

$$\begin{aligned}\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right)&=\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)+\mathbf{L}_k\left(\mathbf{H}X_{k+1}+V_{k+1}+A_k^X-\mathbf{H}\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)\right) &\text{(E.61)}\\ &=\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)+\mathbf{L}_k\mathbf{H}\left(\mathbf{F}X_k+\mathbf{G}U_k+\widetilde{W}_k^A-\left(\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right)+\mathbf{G}U_k+\overline{W}_k^A\left(\mathscr{P}_k^D\right)\right)\right)\\ &\quad+\mathbf{L}_k\left(V_{k+1}+A_{k+1}^X\right). &\text{(E.62)}\end{aligned}$$

Substituting in the values for $\overline{W}_k^A\left(\mathscr{P}_k^D\right)$ and $\widetilde{W}_k^A$ while noting the information set for the expectation yields,

$$\begin{aligned}\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right)=\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)&+\mathbf{L}_k\mathbf{H}\left(\mathbf{F}\left(E_k^{X^A}\left(\mathscr{P}_k^D\right)-\mathbb{E}\left[E_k^{X^A}\left(\mathscr{P}_k^D\right)\middle|\mathscr{P}_k^D\right]\right)\right.\\ &\left.+\mathbf{G}\left(E_k^{U^A}-\mathbb{E}\left[E_k^{U^A}\middle|\mathscr{P}_k^D\right]\right)+\left(W_k-\mathbb{E}\left[W_k\middle|\mathscr{P}_k^D\right]\right)\right)+\mathbf{L}_k\left(V_{k+1}+A_k^X\right).\end{aligned}$$

This is where the derivation diverges from the previous two. This is due to the fact that at this point the operator has access to the measurement of the signal $\widetilde{U}_k^A$. However, it is corrupted by the noise within the imperfect auxiliary communication channel. Additionally, it is also corrupted by the additional attack vector, $A_k^A$. Specifically, the operator has the variable $\widetilde{\widetilde{U}}_k^A$. This variable is defined as

$$\widetilde{\widetilde{U}}_k^A=\widetilde{U}_k^A+T_k+A_k^A, \tag{E.63}$$

Therefore, with this information available to the operator they can remove the effect of the attacked noisy actuation signal from the estimate at the cost of introducing the detrimental

effect of the random variables $T_k$ and $A_k^A$. Performing this substitution in tandem with operating the expectation operator for each other random variable yields

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right)=\widehat{X}_{k+1}\left(\mathscr{P}_k^D\right)+\mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right)\right.$$
$$\left.+\mathbf{G}\left(E_k^U+A_k^U-E_k^U-A_K^U-T_k-A_k^A\right)+W_k\right)+\mathbf{L}_k\left(V_{k+1}+A_k^X\right). \quad \text{(E.64)}$$

The negation of a zero mean Gaussian random variable is equivalent to the addition of a zero mean Gaussian random variable. Therefore, the predicted state estimate is expanded according to (7.120) to give

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right)=\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right)+\mathbf{G}U_k+\overline{W}_k^A\left(\mathscr{P}_k^D\right)+\mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^X\left(\mathscr{P}_k^D\right)+\mathbf{G}\left(T_k+A_k^A\right)+W_k\right)$$
$$+\mathbf{L}_k\left(V_{k+1}+A_k^X\right) \quad \text{(E.65)}$$
$$=\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right)+\mathbf{G}U_k+\overline{\overline{W}}_k^A\left(\mathscr{P}_k^D\right), \quad \text{(E.66)}$$

where $\overline{W}_k^A\left(\mathscr{P}_k^D\right)$ is a zero mean random variable and $\overline{\overline{W}}_k^A\left(\mathscr{P}_k^D\right)$ is defined as

$$\overline{\overline{W}}^A\left(\mathscr{P}_k^D\right)=\mathbf{L}_k\mathbf{H}\left(\mathbf{F}E_k^{X^A}\left(\mathscr{P}_k^D\right)+\mathbf{G}\left(T_k+A_k^A\right)+W_k\right)+\mathbf{L}_k\left(V_{k+1}+A_{k+1}^X\right). \quad \text{(E.67)}$$

It is seen that (E.66) is in the form of a fully observed state space system. Namely, the state space system,

$$\widehat{X}_{k+1}\left(\mathscr{P}_{k+1}^D\right)=\mathbf{F}\widehat{X}_k\left(\mathscr{P}_k^D\right)+\mathbf{G}U_k+\overline{\overline{W}}_k^A\left(\mathscr{P}_k^D\right), \quad \text{(E.68a)}$$
$$\widehat{Y}_k=\widehat{X}_k\left(\mathscr{P}_k^D\right). \quad \text{(E.68b)}$$

This concludes the proof. □

# References


[1] Adams, M. R. and Guillemin, V. (1996). *Measure theory and probability*. Springer.

[2] Aksel N. Heirung, T., Joel A. Paulson, Jared O'Leary, and Ali Mesbah (2018). Stochastic model predictive control - how does it work? *Computers & Chemical Engineering*, 114:158 – 170. FOCAPO/CPC 2017.

[3] Applebaum, D. (1996). *Probability and information: An integrated approach*. Cambridge University Press.

[4] Arrieta, M., Esnaola, I., and Effros, M. (2019). Universal Privacy Guarantees for Smart Meters. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 2154–2158.

[5] Astrom, K. J. and Murray, R. M. (2008). *Feedback Systems: An Introduction for Scientists and Engineers*. Princeton University Press, Princeton, NJ, USA.

[6] Bencsáth, B., Pék, G., Buttyán, L., and Félegyházi, M. (2012). The Cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet*, 4(4):971–1003.

[7] Bertsekas, D. (1987). *Dynamic Programming: Deterministic and Stochastic Models*. Cambridge Studies in Early Modern His. Prentice-Hall.

[8] Bertsekas, D. P., Gallager, R. G., and Humblet, P. (1992). *Data networks*, volume 2. Prentice-Hall International New Jersey, Second edition.

[9] Beutler, F. J. (1989). Dynamic programming: Deterministic and stochastic models (dimitri p. bertsekas). *SIAM Review*, 31(1):132.

[10] Bloch, M. (2008). *Physical-layer security*. PhD thesis, Georgia Institute of Technology.

[11] Bodenham, D. (2014). *Adaptive estimation with change detection for streaming data*. Imperial College London.

[12] Bodenham, D. A. and Adams, N. M. (2016). A comparison of efficient approximations for a weighted sum of chi-squared random variables. *Statistics and Computing*, 26(4):917–928.

[13] Borella, M. S., Swider, D., Uludag, S., and Brewster, G. B. (1998). Internet packet loss: measurement and implications for end-to-end Qos. In *Proceedings of the 1998 ICPP Workshop on Architectural and OS Support for Multimedia Applications Flexible Communication Systems. Wireless Networks and Mobile Computing (Cat. No.98EX206)*, pages 3–12.

[14] Boucheron, S., Lugosi, G., and Massart, P. (2013). *Concentration Inequalities: A Nonasymptotic Theory of Independence*. OUP Oxford.

[15] Boyd, S., Ghaoui, L., Feron, E., and Balakrishnan, V. (1994). *Linear matrix inequalities in system and control theory*. SIAM studies in applied mathematics. Society for Industrial and Applied Mathematics.

[16] Branquinoho, M. (2018). Ransomware in Industrial Control Systems. What Comes After Wannacry and Petya Global Attacks? *WIT Trans. on The Built Environment*, 174:329–334.

[17] Bryson, A. E. (2018). *Applied optimal control: optimization, estimation and control*. Routledge.

[18] Buckley, M. and Eagleson, G. (1988). An Approximation To The Distribution Of Quadratic Forms In Normal Random Variables. *Australian Journal of Statistics*, 30A(1):150–159.

[19] Casbolt, W., Esnaola, I., and Jone, B. (2020). Denial of Service Attacks on Control Systems with Packet Loss. *IFAC-PapersOnLine*, 53(2):3488–3495. 21st IFAC World Congress.

[20] Casbolt, W., Jones, B., and Esnaola, I. (2019). Optimal Control of Systems with Multichannel Packet Loss. *arXiv preprint arXiv:1911.07548*.

[21] Chen, G., Chen, G., and Hsu, S.-H. (1995). *Linear stochastic control systems*, volume 3. CRC press.

[22] Chen, L., Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., and Smith Tone, D. (2016). *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology.

[23] Claude, S. (1949). Communication Theory of Secrecy Systems*. *Bell System Technical Journal*, 28(4):656–715.

[24] Colbert E.J.M., Kott, A. (2016). *Cyber-security of SCADA and Other Industrial Control Systems*. Springer International Publishing.

[25] Cover, T. and Thomas, J. (2006). *Elements of Information Theory*. A Wiley-Interscience publication. Wiley.

[26] Daniel Genkin, Adi Shamir, and Eran Tromer (2014). RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. In *Advances in Cryptology – CRYPTO 2014*, pages 444–461. Springer Berlin Heidelberg.

[27] Deadman, E. and Relton, S. D. (2016). Taylor's theorem for matrix functions with applications to condition number estimation. *Linear Algebra and its Applications*, 504:354–371.

[28] Doob, J. (1994). *Measure Theory*. Graduate Texts in Mathematics. Springer New York.

[29] Garone, E., Sinopoli, B., and Casavola, A. (2008). LQG control over lossy TCP-like networks with probabilistic packet acknowledgements. In *2008 47th IEEE Conference on Decision and Control*, pages 2686–2691.

[30] George D. F. Seber (2007). *A Matrix Handbook for Statisticians*. Wiley-Interscience, New York, NY, USA, First edition.

[31] Hasslinger, G. and Hohlfeld, O. (2008). The gilbert-elliott model for packet loss in real time services on the internet. In *14th GI/ITG Conference - Measurement, Modelling and Evalutation of Computer and Communication Systems*, pages 1–15.

[32] Horn, R. A. and Johnson, C. R. (1990). *Matrix Analysis*. Cambridge University Press, Cambridge, Second edition.

[33] Jeffryes W. Chapman and Litt, J. (2017). Control Design for an Advanced Geared Turbofan Engine. In *53rd AIAA/SAE/ASEE Joint Propulsion Conference*.

[34] Ke Sun, Iñaki Esnaola, Perlaza, S., and Vincent Poor, H. (2017). Information-theoretic Attacks in the Smart Grid. pages 455–460.

[35] Kolias, C., Kambourakis, G., Stavrou, A., and Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. *Computer*, 50(7):80–84.

[36] Korkua, S. K. and Lee, W. (2009). Wireless sensor network for performance monitoring of electrical machine. In *Proc. North American Power Symposium*, pages 1–5.

[37] Kostina, V. and Hassibi, B. (2016). Rate-cost tradeoffs in control. In *2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1157–1164.

[38] Kushner, D. (2013). The real story of Stuxnet. *IEEE spectrum*.

[39] Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security Privacy*, 9(3):49–51.

[40] Langner, R. (2013). To kill a centrifuge: A technical analysis of what stuxnet's creators tried to achieve. *The Langner Group*.

[41] Leen, G. and Heffernan, D. (2002). Expanding automotive electronic systems. *Computer*, 35(1):88–93.

[42] Lenstra, A. K. and Verheul, E. R. (2000). Selecting Cryptographic Key Sizes. In Imai, H. and Zheng, Y., editors, *Public Key Cryptography*, pages 446–465, Berlin, Heidelberg. Springer Berlin Heidelberg.

[43] Löfberg, J. (2004). Yalmip : A Toolbox for Modeling and Optimization in Matlab. In *In Proceedings of the CACSD Conference*, Taipei, Taiwan.

[44] Marcocchio, A. V. (2018). Wireless Vibration Sensing with Local Signal Processing for Condition Monitoring within a Gas Turbine Engine.

[45] Massey, J. (1990). Causality, feedback and directed information. In *In Proc. Int. Symp. Inf. Theory Applic.(ISITA-90)*, pages 303–305.

[46] Mo, Y., Garone, E., and Sinopoli, B. (2013). LQG control with Markovian packet loss. *In Proc. European Control Conference*, pages 2380–2385.

[47] Mo, Y., Garone, E., and Sinopoli, B. (2013). LQG control with Markovian packet loss. In *2013 European Control Conference (ECC)*, pages 2380–2385.

[48] Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., and Sinopoli, B. (2012). Cyber Physical Security of a Smart Grid Infrastructure. *Proc. IEEE Proc. IRE*, 100(1):195–209.

[49] Mo, Y. and Sinopoli, B. (2009a). Secure control against replay attacks. In *Proc. Allerton Conference on Communication, Control, and Computing*, pages 911–918.

[50] Mo, Y. and Sinopoli, B. (2009b). Secure control against replay attacks. *2009 47th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2009*, pages 911–918.

[51] Mo, Y., Weerakkody, S., and Sinopoli, B. (2015). Physical Authentication of Control Systems: Designing Watermarked Control Inputs to Detect Counterfeit Sensor Outputs. *IEEE Control Systems Magazine*, 35(1):93–109.

[52] Morton, K. and Grace, D. (2012). A case study on Stuxnet and Flame Malware. *General Science and Philosophy*.

[53] Pasqualetti, F., Dörfler, F., and Bullo, F. (2011). Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In *Proc. IEEE Conference on Decision and Control and European Control Conference*, pages 2195–2201.

[54] Pasqualetti, F., Dörfler, F., and Bullo, F. (2013). Attack Detection and Identification in Cyber-physical Systems. *IEEE Trans. Autom. Control*, 58(11):2715–2729.

[55] Poor, H. V. (2013). *An introduction to signal detection and estimation*. Springer Science & Business Media.

[56] Quevedo, D. E., Silva, E. I., and Goodwin, G. C. (2007). Packetized predictive control over erasure channels. In *2007 American Control Conference*, pages 1003–1008.

[57] Salyers, D. C., Striegel, A. D., and Poellabauer, C. (2008). Wireless reliability: Rethinking 802.11 packet loss. In *2008 International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pages 1–4.

[58] Schenato, L. (2009). To Zero or to Hold Control Inputs With Lossy Links? *IEEE Trans. Autom. Control*, 54(5):1093–1099.

[59] Schenato, L., Sinopoli, B., Franceschetti, M., Poolla, K., and Sastry, S. S. (2007). Foundations of Control and Estimation Over Lossy Networks. *In Proc. IEEE*, 95(1):163–187.

[60] Shannon, C. E. (2001). A mathematical theory of communication. *ACM SIGMOBILE mobile computing and communications review*, 5(1):3–55.

[61] Shomorony, I. and Avestimehr, A. S. (2012). Is Gaussian noise the worst-case additive noise in wireless networks? In *2012 IEEE International Symposium on Information Theory Proceedings*, pages 214–218.

[62] Sidney Edwards (2020). Extension of Algebraic Solutions Using The Lambert W Function.

[63] Sinopoli, B., Schenato, L., Franceschetti, M., Poolla, K., Jordan, M. I., and Sastry, S. S. (2004a). Kalman filtering with intermittent observations. *IEEE Trans. Autom. Control*, 49(9):1453–1464.

[64] Sinopoli, B., Schenato, L., Franceschetti, M., Poolla, K., Jordan, M. I., and Sastry, S. S. (2004b). Kalman filtering with intermittent observations. *IEEE Trans. Autom. Control*, 49(9):1453–1464.

[65] Sinopoli, B., Schenato, L., Franceschetti, M., Poolla, K., and Sastry, S. S. (2005). Optimal control with unreliable communication: the TCP case. volume 5, pages 3354–3359, Portland, OR, USA.

[66] Sinopoli, B., Schenato, L., Franceschetti, M., Poolla, K., and Sastry, S. S. (2006). Optimal linear LQG control over lossy networks without packet acknowledgment. *Asian J. Control*, 10(1):3–13.

[67] Sinopoli, B., Schenato, L., Franceschetti, M., Poolla, K., and Sastry, S. S. (2006). Optimal linear LQG control over lossy networks without packet acknowledgment. *Asian Journal of Control*, 10(1):3–13.

[68] Skogestad, S. and Postlethwaite, I. (2005). *Multivariable Feedback Control: Analysis and Design*. Wiley.

[69] Song Fang and Quanyan Zhu (2020). Independent Gaussian Distributions Minimize the Kullback-leibler (KL) Divergence from Independent Gaussian Distributions. *CoRR*, abs/2011.02560.

[70] Streltsov, L. (2017). The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. *European Journal for Security Research*, (41125):147–184.

[71] Tatikonda, S., Sahai, A., and Mitter, S. (2004). Stochastic linear control over a communication channel. *IEEE Transactions on Automatic Control*, 49(9):1549–1561.

[72] Teixeira, A., Pérez, D., Sandberg, H., and Johansson, K. H. (2012). Attack Models and Scenarios for Networked Control Systems. In *Proc. of the 1st International Conference on High Confidence Networked Systems*, HiCoNS '12, pages 55–64, New York, NY, USA. ACM.

[73] Turnbull, H. (1930). A matrix form of Taylor's theorem. *Proceedings of the Edinburgh Mathematical Society*, 2(1):33–54.

[74] Usman, M., Mian Ahmad Jan, and Xiangjian He (2017). Cryptography-based secure data storage and sharing using Hevc and public clouds. *Information Sciences*, 387:90 – 102.

[75] Varma, V. S., Postoyan, R., Quevedo, D. E., and Morărescu, I.-C. (2020). Time-based transmission power policies for energy-efficient wireless control of nonlinear systems. In *2020 59th IEEE Conference on Decision and Control (CDC)*, pages 1854–1859.

[76] Vernam, G. S. (1926). Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications. *Trans. of the American Institute of Electrical Engineers*, XLV:295–301.

[77] Yu, S., Zhou, W., and Doss, R. (2008). Information theory based detection against network behavior mimicking DDoS attacks. *IEEE Communications Letters*, 12(4):318–321.

[78] Zhang, H., Cheng, P., Shi, L., and Chen, J. (2016). Optimal DoS Attack Scheduling in Wireless Networked Control System. *IEEE Trans. Autom. Control*, 24(3):843–852.