The University Of Sheffield.

Supervisory Wireless Control for Critical Industrial Applications

Vigneshwaran Venugopalan

Department of Automatic Control and Systems Engineering

The University of Sheffield

A thesis submitted for the degree of

Doctor of Philosophy

September 2014

I would like to dedicate this thesis...

to my parents, Usha Rani and Venugopalan

to my uncle, Gopalswamy

to Priya and Ravinder

to Aarav and Aahana

Who have loved me and supported me always...

பத்தை தரும் படிப்பிலே, முத்தை தரும் சிறப்பிலே
முயன்றிடும் வித்தையில் ஏற்றுவார் யார் என
எவருன்னை கேட்டாலும் கூத்தனூர் வாணியை கூறு.

सरस्वति नमस्तुभ्यं वरदे कामरूपिणि ।
विद्यारम्भं करिष्यामि सिद्धिर्भवतु मे सदा ॥

-Vedas

O Goddess of Knowledge *Saraswathi*, salutations to you,
the Giver of boons, the one who fulfils desires
May all the accomplishments be upon you, I shall begin my studies...

Acknowledgements

All praise and glory is due to Almighty Lord *Sri Hari Narayana*, the lord of the universe, whose mercy and blessings have been bestowed constantly upon me.

I would like to express my deep gratitude to my supervisors, Professor Peter Fleming and Professor Haydn Thompson for giving me the opportunity to pursue my Doctoral research under their guidance. I especially thank Professor Peter Fleming for his excellent guidance, helpful insights and providing great encouragement during my PhD. I feel honoured to have worked under such an experienced supervisor. I sincerely thank Professor Haydn Thompson for passing on his technical knowledge and expertise on wireless control. I appreciate and really value all their feedback and guidance.

I would like to thank the Director of Rolls-Royce UTC, Prof.Visakan Kadirkamanathan for his constant encouragement and advice. I would like to thank my thesis examiners Dr. William Scanlon and Dr. Simon Pope for their positive comments and corrections. I am grateful to Rolls-Royce plc and Engineering and Physical Sciences Research Council (EPSRC) for providing me the necessary financial support through Dorothy Hodgkin Postgraduate Award (DHPA).

My special thanks to Rishi Relan, my colleague and friend, for his invaluable advice, patience and constructive criticism on my research work. I would like to thank Dr. Max Ong for assisting me extensively with his technical expertise in wireless sensing. Ben Taylor deserves special thanks for his assistance in the hardware setup. Also, I would like to express my thanks to Dr. Bryn Jones and Dr. Andy Mills for all the helpful discussions, and many thanks to Renata Ashton for being able to solve just about anything administrative. My profound thanks to my dear friends and members of the UTC for their unconditional support and with whom I had the great luxury of working especially Martha, Hasanin, Rui, Maszatul, Ioannis and others.

Many Thanks goes to my colleagues at GE Aviation, Danny Faulkner, Teri Pragnell, Steve Bonnett, Tim North, Paul Dunning and Ross Young for their understanding and giving me the time during the write-up phase of my thesis.

I would like to express my great appreciation and thanks to my family thousands of miles away in Chennai, India. This work would not have been possible without constant love and prayers from my mother Usha Rani, father Venugopalan, uncle Gopalswamy, my sister Dr.Visalakshi, and brother-in-law Ravinder Ramesh. Special thanks to little Aarav and Aahana for keeping the fun going. I am truly indebted to all their patience, support and understanding. Thank you!

I feel very lucky to have Karthik and Vidhu as my best friends and thanks to them for constantly being there for me in all my journeys, not just this one. Thanks are due to Karthy and Vinothan who made my stay in Sheffield so enjoyable.

I would like to express my immense gratitude to the staff of the Department of Automatic Control and Systems Engineering. Last but not the least; I thank the University of Sheffield for giving me this great opportunity. I feel proud to have been part of this excellent institution.

To all those cited by name here and many others I did not mention by name who supported me during this wonderful journey, I will forever owe you this achievement.

Thank you all very much!

Abstract

There is an increasing interest in the use of wireless communication for critical industrial applications, especially in closed-loop control systems. Wireless networked control systems where the sensors, actuators and controller are connected over a shared communication medium pose problems such as synchronisation issues, packet loss and time delay. The main objective of this thesis is to investigate these issues in detail from an industrial perspective and to propose solutions for a reliable wireless closed-loop control of critical industrial applications such as in aerospace, industrial automation and cyber physical systems.

The thesis highlights a number of standards for industrial wireless communications such as Wi-Fi, Bluetooth, ZigBee, WIA-PA, WirelessHART and ISA 100.11a. The key properties and limitations of these standards are discussed with respect to their application to critical control systems. An overview of specific security threats is given, and potential loopholes and improvements are discussed from a wireless closed-loop control perspective. A supervisory wireless control algorithm based on a hybrid time-triggered and event-triggered control strategy is proposed and demonstrated using a stand-alone wireless hardware demonstrator with no dependency on external processors. The practical issues and design considerations for implementing wireless closed-loop control in embedded systems are discussed.

A sampling interval based clock synchronisation approach based on IEEE 1588 PTP is proposed to overcome the drawbacks of the synchronisation interval based algorithms in wireless closed-loop control. A sensorless supervisory control approach is proposed to address the issue of intermittent data packet loss in a wireless feedback loop. The effectiveness of the proposed approach is evaluated using the embedded wireless hardware demonstrator. Finally, a sliding window based adaptive compensation method is proposed to compensate time-varying delays in industrial wireless control systems and to tackle the drawbacks of conventional Smith predictor based approaches when the delay exceeds the sampling interval.

Contents

List of Figures

List of Tables

Abbreviations

ACK	Acknowledgement
ACL	Access Control List
ADC	Analog to Digital Converter
AES	Advanced Encryption Standard
AES-CBC-MAC	AES with Cipher Block Chaining Message Authentication Code
AES-CCM	AES counter with CBC-MAC
AES-CTR	AES with Counter
AFH	Adaptive Frequency Hopping
AFS	Adaptive Frequency Switch
APP	Application layer
ARF	Automatic Rate Fallback
ARINC	Aeronautical Radio, Incorporated
ARMA	Auto Regressive Moving Average
BLDC	Brushless Direct Control
BP	Bernoulli Packet
CAN	Controller Area Network
CAP	Contention Access Period
CCA	Clear Channel Assessment
CCSDS	Consultative Committee for Space Data Systems
CFP	Contention Free Period
CLKF	Closed Loop Kalman Filter
COTS	Commercially off-the-shelf
CPS	Cyber Physical Systems
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier sense multiple access with collision avoidance
CSMA/CD	Carrier sense multiple access with collision detection
CTP	Control Time Protocol
DARE	Discrete-time Algebraic Ricatti Equation
DFRC	Dryden Flight Research Centre
DMTS	Delay Measurement Time Synchronisation
DoS	Denial of Service
DSN	Delay Sensitive Networks
DSSS	Direct Sequence Spread Spectrum
ECU	Engine Control Unit
EM	Electromagnetic
FAA	Federal Aviation Administration
FADEC	Full Authority Digital Engine Control
FBW	Fly-by-Wire
FDMA	Frequency Division Multiple Access
FMS	Flight Management System
FTC	Fault Tolerant Control
FTSP	Flooding Time Synchronisation Protocol

GE	Gilbert-Elliott
GNS	Global Navigation System
GPIO	General Purpose Input Output
GPS	Global Positioning System
GTS	Guaranteed Time Slot
GUI	Graphical User Interface
HAN	Home area networks
HART	Highway Addressable Remote Transducer Protocol
HMI	Human Machine Interface
HRT	Hard Real-Time
HWD	Hardware Demonstrator
IEC	International Electrotechnical Commission
IFCS	Intelligent Flight Control Systems
IMA	Integrated Modular Avionics
INU	Inertial Navigation Units
ISA	Industrial Society of Automation
ISE	Integrated Squared Error
ISM	Industrial Science and Medicine
ISR	Interrupt Service Routines
ITU	International Telecommunication Union
IWSAN	Industrial Wireless Sensor and Actuator Networks
LCU	Local Control Unit
LLC	Logical Link Control
LoS	Line of Sight
LPC	Linear Prediction Coefficients
LVDT	Linear Variable Differential Transformer
MAC	Medium Access Control layer
MAC	Message Authentication Code
MCU	Micro Controller Unit
MIC	Message Integrity Check
MJLS	Markov Jump Linear Systems
mm-wave	Millimeter Wave
MRAC	Model Reference Adaptive Control
MRAS	Model Reference Adaptive System
MRFI	Minimal Radio Frequency Interface
MSP	Modified Smith Predictor
NEMA	National Electrical Manufacturers Association
NTP	Networked Time Protocol
NWK	Network layer
OLKF	Open Loop Kalman Filter
OSI	Open System Interconnection Model
PAS	Publicly Available Specification
PHY	Physical layer
PID	Proportional Integral Derivative
PTP	Precision Time Protocol
PWM	Pulse Width Modulation
QoC	Quality of Control
QoS	Quality of Service

RBS	Reference Broadcast Synchronisation
RF	Radio Frequency
RTC	Real Time Clock
RTOS	Real-time Operating System
Rx	Reception
SICS	Sampling Interval based Clock Synchronisation
SIG	Special Interest Group
SSID	Service Set Identifier
SU	Supervisory Unit
SWC	Sliding Window Compensation
SWIFT	Scalable Wirelessly Interconnected Flow-control Technology
TDMA	Time Division Multiple Access
TDP	Time Diffusion Protocol
TH	Time Hopping
TKIP	Temporal Key Integrity Protocol
TPSN	Timing-sync Protocol for Sensor Networks
TSF	Time Synchronisation Function
Tx	Transmission
UART	Universal Asynchronous Receiver/Transmitter
UAV	Unmanned Aerial Vehicles
UDP	User Datagram Protocol
UTC	Universal Co-ordinated Time
UWB	Ultra wide-band technology
VoIP	Voice over Internet Protocol
W-ABS	Wireless Aircraft Braking System
WEP	Wired Extension Protocol
WFC	Wireless Feedback Control
WFCS	Wireless Flight Control Systems
WIA-PA	Wireless Industrial Automation – Process Automation
WICAS	Wireless Interconnectivity and Control of Active Systems
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WNCS	Wireless Networked Control Systems
WN-CCS	Wireless Networked – Classical Control Systems
WN-DCS	Wireless Networked – Distributed Control Systems
WN-DeCS	Wireless Networked – Decentralised Control Systems
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Network
WSAN	Wireless Sensor and Actuator Networks
WSN	Wireless Sensor Networks
ZoH	Zero order Hold

Chapter 1

Introduction

1.1 Motivation

Traditionally, industrial control systems have relied on hard-wired information flows for monitoring and processing data. Various communication protocols such as Ethernet, Fieldbus and controller area network (CAN) bus have evolved during the last decade. However, as systems become more complex, more data needs to be processed, and this result in a significant overhead in implementing wired communication networks. Therefore, a more sophisticated approach will be to use wireless sensor networks. Low cost of implementation and hardware wiring reduction are important benefits.

Wireless sensor networks play a vital role in monitoring various control parameters in industrial applications [Willig, 2008],[Thompson, 2004]. These sensors are smart and intelligent devices capable of processing a variety of control data. They can efficiently transmit data from a remote area to a central system for processing the data. Smart sensors can offer self-configuration and self-healing capabilities. They are used in various applications such as machine health monitoring, process supervision and wireless local area networks (LAN). In addition, they can provide safety measures such as alarm generation during life-threatening situations.

Current industrial infrastructures demand more advanced sensor networks that are capable of handling a large number of sensors in a real-time closed-loop network. Hence, there is an increasing interest to implement wireless communications over closed-loop control, especially in critical industrial applications. There are potential benefits arising from the use of wireless feedback control loops in industrial areas such as aerospace, marine and industrial applications. The advantages and flexible nature of industrial wireless sensor and actuator networks (IWSAN) will bring several advantages compared to traditional wired industrial control systems. The benefits of a wireless control loop are:-

- **Reliability and redundancy:** Wireless control loops can act as backup units for many critical control applications. Wireless networks offer a good solution over wired networks, especially when the wired networks are exposed to physical damage.

- **Scalability of the Architecture:** A wireless control network is flexible. Sensor nodes can be added to the network in real-time without making any significant changes in the existing hardware. In addition, the decision-making process can have additional information to decide the control demand.
- **Cost Savings:** Installation and maintenance of wireless networks are much cheaper compared to wired networks.

Utilisation of wireless technologies in industrial control systems is an urgent need [Gungor, 2013]. Implementing wireless technology in closed-loop real-time systems poses significant research challenges. Some of the key issues are:-

- the wireless medium is highly unreliable,
- transmissions are subject to interference and loss of data,
- increased energy consumption by wireless sensors,
- wireless transmissions are prone to hacking and other critical security issues.

This research is intended to address the implementation of wireless sensor networks in closed-loop real-time systems for industrial applications. The key aims of this research are:-

- to assess the application impacts of wireless standards for industrial control and to analyse the effectiveness of security protocols of these standards,
- to investigate the feasibility of wireless transmission in a real-time closed-loop system using a wireless hardware demonstrator, and
- to develop techniques for dealing with time-varying delay, variable sample rates, synchronisation issues and lost communication packets in industrial wireless closed-loop control systems.

1.2 Problem Definition

The Industrial Society of Automation (ISA) has listed application classes (see Fig.1.1) and their criticality level for introducing wireless networks in industrial applications for monitoring and control.

Monitoring: Wireless sensor networking is an active research area which explores issues specific to wireless sensing and monitoring in industrial applications. Many Industries have already deployed wireless sensors for monitoring and sensing activities and have reported maximised efficiency and cost savings [Wireless Control, 2010]. For instance, Rolls-Royce has an active interest to utilise wireless technologies for remote health monitoring, to reduce wiring harness in gas-turbine engines, and to exploit wireless sensing mechanisms in Rolls-Royce aircraft, marine and industrial systems [Thompson, 2009].

Safety	0	Emergency action	Always critical
Control	1	Closed loop Regulatory control	Often critical
	2	Closed loop Supervisory control	Usually non-critical
	3	Open loop control	Human in the loop
Monitoring	4	Alerting	Short-term consequences
	5	Logging Downloading/uploading	No immediate consequences

Figure 1.1: Application classes from ISA100 [Werb, 2012]

Control: ISA100 classifies the control operations in industrial applications using wireless networks as open-loop control (human-in-the-loop), closed-loop control (usually non-critical) and closed-loop regulatory control (often critical). However, closing control loops over a wireless network in critical industrial applications leads to requirements that needs additional functionality to meet performance demands. Therefore, wireless control for critical industrial applications can be classified as shown in Fig.1.2.

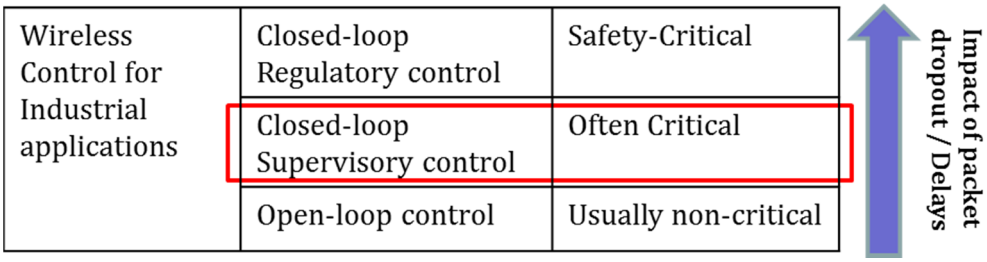

Figure 1.2: Classification of wireless critical control applications

Wireless control is an emerging technology and often relegated to monitoring activities [McKernan, 2010]. Investigating the implementation of wireless networks in critical closed-loop control systems is very much in its infancy and an emerging research area. Therefore, the scope of this research is to investigate various issues associated in closing a feedback control loop over a wireless network with special consideration to synchronisation issues, impact of packet dropout and time delay issues. A wireless control loop for critical industrial applications should be able to address the following requirements:-

- What are the potential control functions where a wireless medium could be of benefit?
- How much latency can be tolerated?
- How frequently does the data need to be transmitted? Does the application need a time-driven or event-driven approach?
- What is the time critical requirements such as deadline, level of synchronisation needed?

- What is the level of interference expected in the environment and the possible radio frequency (RF) sources of interference?
- How far the current industrial wireless standards (such as WirelessHART, ISA100.11a) cater to the needs of the above requirements?

1.3 Outline of Thesis

The thesis is organised as follows:-

Chapter 2 presents the necessary background highlighting key areas that will benefit from wireless controlled applications in future. The evolution and advantage of fly-by-wireless technology in the aerospace industry is highlighted. Three categories of implementing wireless networked control in industrial applications are presented along with their merits and demerits. It points out the challenges in implementing wireless control in real-time and safety-critical systems. The collaborative nature of computing, control and communication is presented, and it is highlighted that research activities in wireless control systems should consider the issues in these three areas collectively. A literature review is given with respect to *Control over Network* issues and solutions. It finally highlights the active research area alongside the present scenario of wireless sensing and control from an industrial perspective.

Chapter 3 presents a review of industrial wireless standards to implement wireless control systems in industrial applications. A comprehensive analysis is undertaken with respect to different aspects of industrial wireless control such as wireless standards, security issues and solutions and issues presented by the radio spectrum. A summary of open research problems is presented highlighting the need for addressing *Control over Network* issues for utilising wireless medium in industrial control.

Chapter 4 presents the design considerations of implementing a wireless closed-loop control using an embedded microcontroller platform. The practical issues in implementing wireless embedded control are discussed in detail and a supervisory closed-loop control approach using a hybrid time-triggered and event-triggered control strategy over a wireless channel is presented. The design and implementation of an embedded wireless hardware demonstrator are explained.

Chapter 5 presents the challenges associated with clock synchronisation in wireless closed-loop control for industrial applications. It is of utmost importance that the sensor nodes in a network have a common understanding of time. For safety-critical systems, it is vital to know when the data was sampled or when a given event happened with respect to real-time. A brief overview of clock synchronisation in wireless networked control systems is presented. An approach to the design of a clock synchronisation algorithm for wireless closed-loop control system based on IEEE 1588 Precision Time Protocol (PTP) is considered.

Chapter 6 describes the issues associated with packet loss in wireless feedback control. Packet loss is an unavoidable phenomenon in wireless sensor networks, especially those operating in harsh industrial environments. The rate of packet loss depends on many different factors such as co-channel interference, deliberate jamming, network traffic load, power consumption of the sensor nodes and transmitting distance. In addition, sensor faults and failures could also contribute to complete packet loss in distributed control systems. A comprehensive study of issues due to packet loss in a wireless control loop is presented in this chapter. A sensorless supervisory wireless control approach is proposed for addressing lost data packets in a feedback loop, and the effectiveness of the proposed approach was demonstrated using the wireless hardware demonstrator. It presents a case study of a wireless aircraft braking system.

Chapter 7 presents the challenges associated with time delay and sampling rate analysis in industrial wireless closed-loop control systems. Time delay in a wireless network poses several challenges for industrial wireless control applications. In addition, as wireless control systems are discrete-time sampled systems, any time delay compensation method should be evaluated against the sampling rate of the system. Therefore, a comprehensive study of time delay and sampling rate analysis for industrial wireless control systems is performed in this chapter. It presents a sliding window based adaptive compensation method to compensate time-varying delays in a wireless closed-loop control system.

Chapter 8 presents the conclusions and future directions for the research.

1.4 Thesis Contribution

Analysis of industrial wireless standards and their suitability for critical control

A state-of-the-art analysis of industrial wireless standards and their suitability for critical control applications is presented. The case for a wireless standard for critical industrial applications and the application impacts of their security protocols is discussed. It is highlighted that wireless standards for safety-critical control have constrained demands as compared to consumer applications. A technical report summarising the key findings under the title “Wireless Real-Time Control,” was, submitted to Rolls-Royce plc, Derby.

[1] Venugopalan, V., (2012). Analysis of Wireless Real-time Control for Safety-Critical Applications. Technical Report. Rolls-Royce Control and Systems UTC, University of Sheffield, UK.

Sensorless supervisory control approach for industrial wireless closed-loop control applications under intermittent data packet loss

A novel sensorless supervisory wireless real-time control approach that addresses the issue of intermittent data packet loss in wireless feedback control loops in critical industrial systems is proposed in Section 6.5. The proposed solution can keep the wireless control loop stable and at the same time provide a methodology with ease of implementation in real-time embedded systems. The effectiveness of the proposed sensorless supervisory control algorithm is further evaluated using a Wireless Aircraft Braking System (W-ABS) model.

A wireless hardware demonstrator is implemented in this research to test the feasibility of the proposed algorithm. In the hardware demonstrator, the burst packet loss is deliberately introduced in the feedback loop by characterising the packet loss using the Gilbert-Elliott (GE) model. Therefore, the results based on the hardware demonstrator are a typical representation of wireless closed-loop control performance under deliberate jamming.

The operation of a supervisory wireless control technique has been successfully demonstrated over what might be considered a relatively low-capacity wireless real-time system in this deliberate exercise. This evidence suggests that there is substantial opportunity to maximise the performance of a future system in aircraft applications if placed in a position to leverage a high-bandwidth network, operate over a dedicated aero frequency spectrum or with use of a proprietary aero-specific wireless protocol.

This contribution was presented in the 9th International Conference on Intelligent Unmanned Systems (ICIUS'2013). This work has also been published in the Journal of Unmanned Systems Technology (JUST).

[2] Venugopalan, V., Relan R., Thompson H.A., Ong, M., Fleming, P.J. (2014). Sensorless Supervisory Wireless Control: Aircraft Braking System Case Study. *Journal of Unmanned Systems Technology (JUST)*. Vol. 2, Issue 2.

A Sampling Interval based Clock Synchronisation (SICS) approach for clock synchronisation in industrial wireless closed-loop control applications

A sampling interval based clock synchronisation (SICS) approach for wireless closed-loop control system using the IEEE 1588 PTP is proposed in Section 5.4.2. The SICS approach is suitable for wireless control loops as synchronisation is achieved using the sampling interval in the slave nodes rather than the synchronisation interval determined by the master. It eliminates the need for multiple synchronisation intervals and the problem of instant clock synchronisation in using PI clock servos. The SICS approach assists the local controller in correcting its clock offset and drift thereby keeping the control process stable. The contribution was presented at the IEEE Indian Control Conference (ICC'2015).

[3] Venugopalan, V., Relan R., Thompson H.A., Ong, M., Fleming, P.J. (2015). A Sampling Interval based Clock Synchronisation approach for Wireless Closed-loop Control. In proceedings of *IEEE Indian Control Conference*, Chennai, India, pp.316 - 321.

A Sliding Window based Adaptive Compensation (SWC) to compensate time delay exceeding the sampling interval in industrial wireless closed-loop control applications

An adaptive compensation method for time-varying delays in an industrial wireless closed-loop control system is proposed in Section 7.3. A Kalman filter based modified Smith predictor for wireless closed-loop control is presented and is also extended with an adaptive sliding window compensation (SWC) technique to tackle the drawbacks of conventional Smith predictor when the delay exceeds the sampling interval. The contribution will be submitted to the Journal of Control, Automation and Systems (IJCAS).

[4] Venugopalan, V., Relan R., Fleming, P.J. (2015). Sliding Window based Adaptive Compensation for Time-Varying Delay in Industrial Wireless Closed-loop Control Systems. *International Journal of Control, Automation and Systems (IJCAS)*. Springer. (to be submitted)

Chapter 2

Background

This chapter presents the necessary background to provide a broad view of introducing wireless communication in industrial applications. The potential area where wireless technologies are of growing interest is highlighted first. It is then followed by some background theories in implementing control loops over a wireless communication network. A literature review is then presented to address the key works undertaken in this area.

2.1 Industrial Examples

2.1.1 Wireless flight control system

Right from the inception of the first aircraft Wright Flyer I by the Wright brothers, the advancement in the communication systems utilised in an aircraft has seen a significant growth. The evolution of the aircraft communication systems is given in Fig.2.1. In the early days, mechanical linkages were used for sending the pilot commands to various control systems in an aircraft.

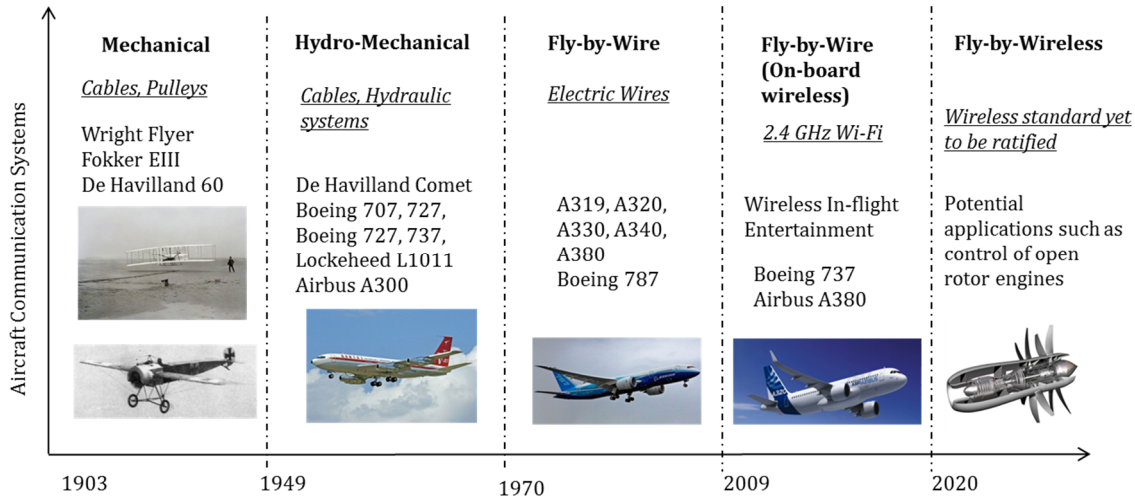

Figure 2.1: Evolution of aircraft communication systems

However, this added significant weight to the overall weight of an aircraft and the increased complexity to the communication systems in the aircraft led to the introduction of hydro-mechanical systems. Fly-by-Wire (FBW) control systems came into use in early 1970's where flight control computers are used to convert the pilot signals to electronic signals and transmit them to the actuators using electrical wires (hence the name fly-by-wire). The set of electronic equipment that is used to control the fly-by-wire mechanism is classified as an Avionic System. The FBW mechanism significantly reduced the constraints involved in using mechanical systems and also offered efficient aero dynamic performance. FBW control systems are predominantly used today by all major aircraft companies due to their reliability and efficiency.

The reliability of fly-by-wire mechanism is ensured by having backup redundant sensors and wires for critical control commands. The FBW mechanism is subject to wiring and cabling faults. The maintenance and troubleshooting of these issues are time-consuming and are not cost-effective for aircraft manufacturers. The concept of Wireless Flight Control System (WFCS) is receiving more attention in the aviation industry in recent years [Yedavalli, 2011]. In wireless flight control systems, the demand and feedback information from flight control computers to the actuators will be sent over a wireless channel. From an industrial perspective, substantial work has not been done yet on solutions for wireless real-time control with packet losses in safety-critical flight control applications. However, a few early initiatives taken in this context are presented here.

Gulfstream demonstrated a wireless control system in 2008 on the Gulfstream GV test aircraft. A direct sequence spread spectrum (DSSS) and coding-based fly-by-wireless system is used to control the mid-spoilers in the aircraft. The mid-spoiler actuation system is an electro-mechanical linear actuator developed by Smiths Aerospace (now GE Aviation). Gulfstream described this as "the first known application of wireless signalling for a primary flight control surface in a civilian or military aircraft" [Gulfstream, 2008]. Though the wireless controlled system was used as a backup system, Gulfstream compared the performance of the wireless system to that offered by a fly-by-wire and fly-by-light control system and noted that, regardless of the actuation technology, consistent characteristics were shown by all the systems.

NASA's Dryden flight research centre (DFRC) developed a wireless flight control system as a proof-of-concept [Chilakala, 2008]. It used the DSSS-based system developed by Invocon to introduce a wireless link between the flight control computers and the actuators in an F-18 Iron Bird aircraft. NASA has initiated key research work in wireless control to explore the possibilities of interlinking different modules in spacecraft through wireless links, interoperability of wireless standards, and reusability of sensors. A test bed has been developed in NASA-JSC [Wagner, 2010] that utilises a TI MSP430 microcontroller and radio modules fixed to specific applications correlated to various aerospace needs. NASA has further initiated research in Intelligent Flight Control Systems (IFCS) to introduce wireless control systems as backup systems in aircraft control systems and to increase reliability and enhanced safety.

While introducing such wirelessly controlled flight systems offer huge benefits in terms of maintenance, there are several safety-concerns and issues as wireless is an unreliable medium of communication. Therefore, there is a need to evaluate and analyse these issues with respect to aircraft applications before a wireless flight control system can be commissioned. There is a need to develop Federal Aviation Administration (FAA) rules for wireless control as there is none available now. The design and implementation of a potential wireless flight control system is explained in Section 6.6.

In Europe, the WICAS and SWIFT programmes [WICAS, 2011] investigated the wireless monitoring of open-loop control of skin friction reduction systems. Other industrial works in this area are restricted to wireless sensing and monitoring [Song, 2008],[Irwin, 2006]. The opportunities and challenges for using wireless in safety-critical avionics and a wireless avionics network using ultra wide band (UWB) technology are discussed in [Mifdaoui, 2012].

2.1.2 Fly-by-wireless

At present, aircraft manufacturers use a Fly-By-Wire (FBW) mechanism for communicating between the flight control system and various actuators. It replaces the traditional mechanical linkages that were previously used for sending control signals in aircraft. In a FBW system, control signals, sensor information, demand signals are all transmitted as electrical signals to various modules distributed around an aircraft. However, due to the improvement in health monitoring strategies, the number of sensors used in aircraft engine health monitoring and structural health monitoring has increased over recent years [Venugopalan, 2014],[Zaidan, 2013]. Therefore, the use of communication wires for transmitting the sensing information has proportionately increased. This, in turn, has resulted in a significant raise in the overall weight and complexity of the aircraft (see Fig.2.2). For example, the Airbus A380-800 contains 470 km of wire with an overall weight of 5700 kilograms. In the cabin, there are over 100,000 wires and more than 40,000 connectors creating many potential points of failure and areas to inspect and maintain. About 30% of electrical wires are potential candidates for a wireless substitute [Wireless Avionics Intra-Communications, 2012].

Wiring faults in aircraft have been a major concern in aging aircraft and in maintenance. A report by the Flight Safety Foundation [Aircraft wiring, 2004] stated that aircraft electrical wiring damage had led to many incidents, thus showing how prone electrical wiring is to damage occurring over time or being introduced during maintenance or modification action. Therefore, interest in fly-by-wireless technology is increasing where the control systems, actuators, sensors in an aircraft can communicate over a wireless channel. A wireless approach will result in a significant reduction in cables and wiring on board an aircraft with all of the benefits that this provides. However, there is a need to identify the

potential control applications inside an aircraft where wireless communication would offer a significant benefit.

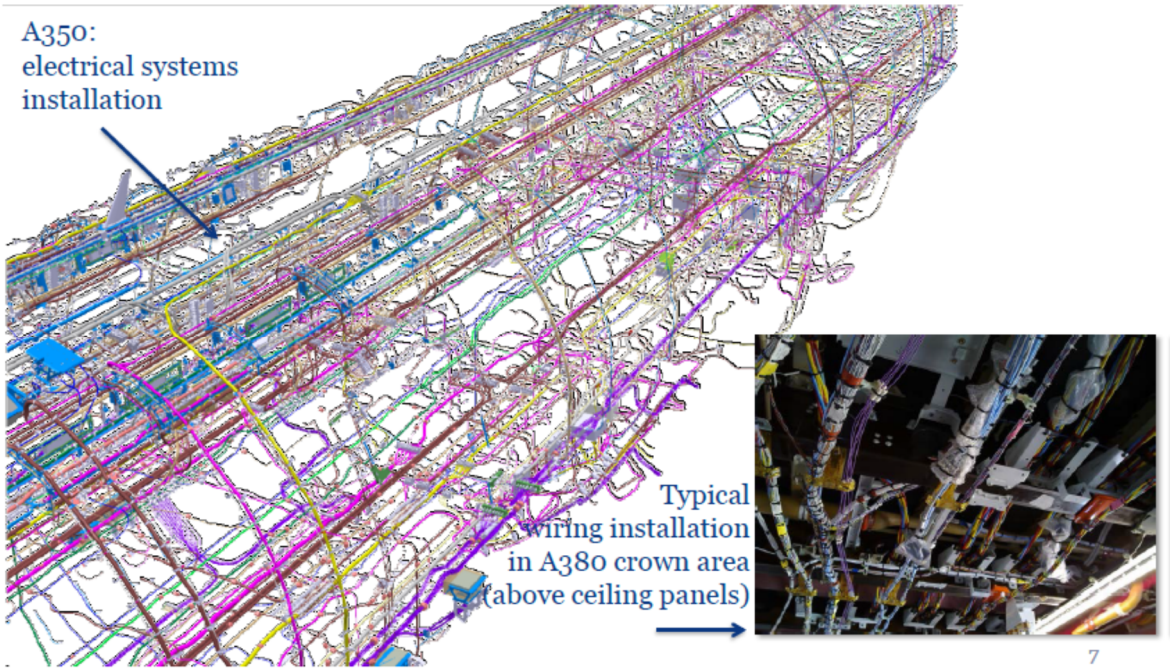

Figure 2.2: Complexity of electrical wiring in modern aircraft [Wireless Avionics Intra-Communications, 2012]

For uninhabited aerial vehicles (UAVs) and military aircraft, wireless sensors can significantly improve their performance by integrating several control modules on board an aircraft and also to communicate with a ground unit in real-time. In addition, a combination of wireless technology and satellite communication enables the ground-based air-traffic control to take over a UAV or military aircraft if the flight deck controls become inoperable or incapacitated [Yedavalli, 2011]. Wireless sensor networks also have a great potential in the development of intelligent flight control systems (IFCS).

Currently, the aerospace industry uses a variety of data bus protocols to transmit information across various flight control systems. One such protocol is ARINC 825 that is the standardisation of CAN for airborne use that was initiated by the Airlines Electronic Engineering Committee. The two major aircraft manufacturers - Airbus and Boeing - have already accommodated a fully functional CAN network in their A380 and Boeing 787 aircraft, respectively, for all sorts of communication between flight control computers, engine control and other electrical systems [Ralph, 2012]. Recently, there have been initiatives to develop a hybrid network between CAN and wireless protocols for industrial usage. A hybrid wireless RF controller area network (CAN) for wireless monitoring and control with energy-efficient self-powered sensor systems has been developed and commissioned by THHINK Wireless Technologies Limited [Ong, 2013].

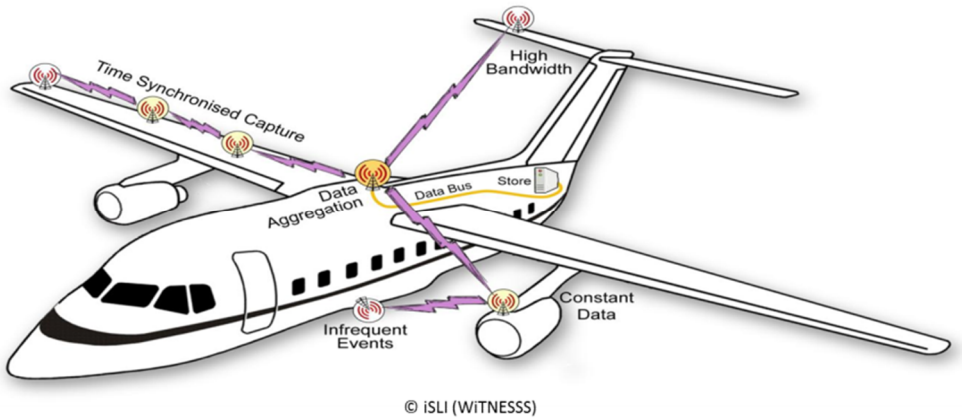

Figure 2.3: Fly-by-wireless systems [WiTNESSS, 2009]

A hybrid approach for utilising wireless sensors for aircraft health monitoring is shown in Fig.2.3. Wireless sensors can be deployed across the aircraft to capture various sensing information and aggregated using a master node, which, in turn, can be connected to a data store inside the aircraft through a wired protocol. The data store can further be connected to a satellite for real-time data monitoring activities. Wireless sensors could offer a great benefit in terms of flexibility and robustness in detecting any faults and failures.

2.1.3 Open rotor control

An open rotor engine is a gas turbine engine that has a unique architecture with the propeller blades towards the end of a jet engine. Open rotor engine lacks a traditional fan case, and the fan blades are placed at the end of the engine rather than in the front nacelle. Due to the design principles, open rotor engines provide various technology challenges. Open rotor engines have been used back in 1970's, however, due to economic and technical hurdles, aircraft manufacturers started using conventional gas-turbine engines. However, due to its ability to increase propulsive efficiency, aero engine manufacturers are keen to implement this engine in next-generation aircraft.

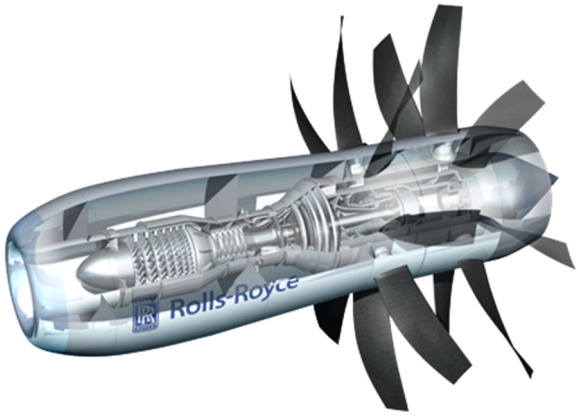

Figure 2.4: Open rotor aircraft engines [Rolls-Royce, 2014]

One of the technology challenges that open rotor engines face is the placement of Engine Control Unit (ECU). In conventional gas-turbine engines, the ECU is placed in the fan case. However, an open rotor lacks a fan case, and due to varying temperature near the nacelle this may not be possible in open rotor engines. This is an active research problem for next-generation Integrated Modular Avionics (IMA's). As explained in Section 2.1.1, current aircraft flight control systems use the fly-by-wire systems for communication. However, due to the architecture of the open rotor engines (see Fig.2.4) complexity of communication increases. For instance, routing wires for blade pitch control and to monitor counter rotating power transmission system becomes difficult [Rolls-Royce, 2014].

Various approaches [Abdul-Aziz, 2013 and references therein] have been proposed to address the communication challenges in open rotor engines such as utilising microwave transmission using waveguides as microwave signals is unlikely to escape from the engine enclosure. Wireless sensors can be used to measure the speed, position and pitch of the rotors. There is a possibility to attach the wireless sensors to the outer annulus (rear of the engine) and measure the speed and position of the rotor per revolution. In addition, wireless control loops will offer a communication link between the stationary and rotational part of an open rotor engine without complex wiring requirements.

During the initial stages, aircraft manufacturers may consider the implementation of a wireless backup control lane to analyse the performance of wireless control loops in open rotor engines in a test bed environment. This will lead the industry to implement a full-fledged fly-by-wireless mechanism in aircraft applications in future.

2.1.4 Cyber physical control

Cyber physical systems (CPS) represent several physical entities connected to the control systems over a collaborative communication network. The new trends such as smart infrastructures and smart cities have triggered active interest in multiple systems communicating over a common communication medium. Cyber physical systems span across various industrial domains such as intelligent transportation, automation, aerospace and marine, process industry, healthcare, smart infrastructures, etc. As more and more systems get connected in a cyber-physical environment, wireless becomes the obvious choice of a communication medium due to flexibility and ease of implementation and maintenance. Wireless sensor and actuator network's (WSANs) is an active and emerging research area in the domain of cyber physical systems (see Fig.2.5).

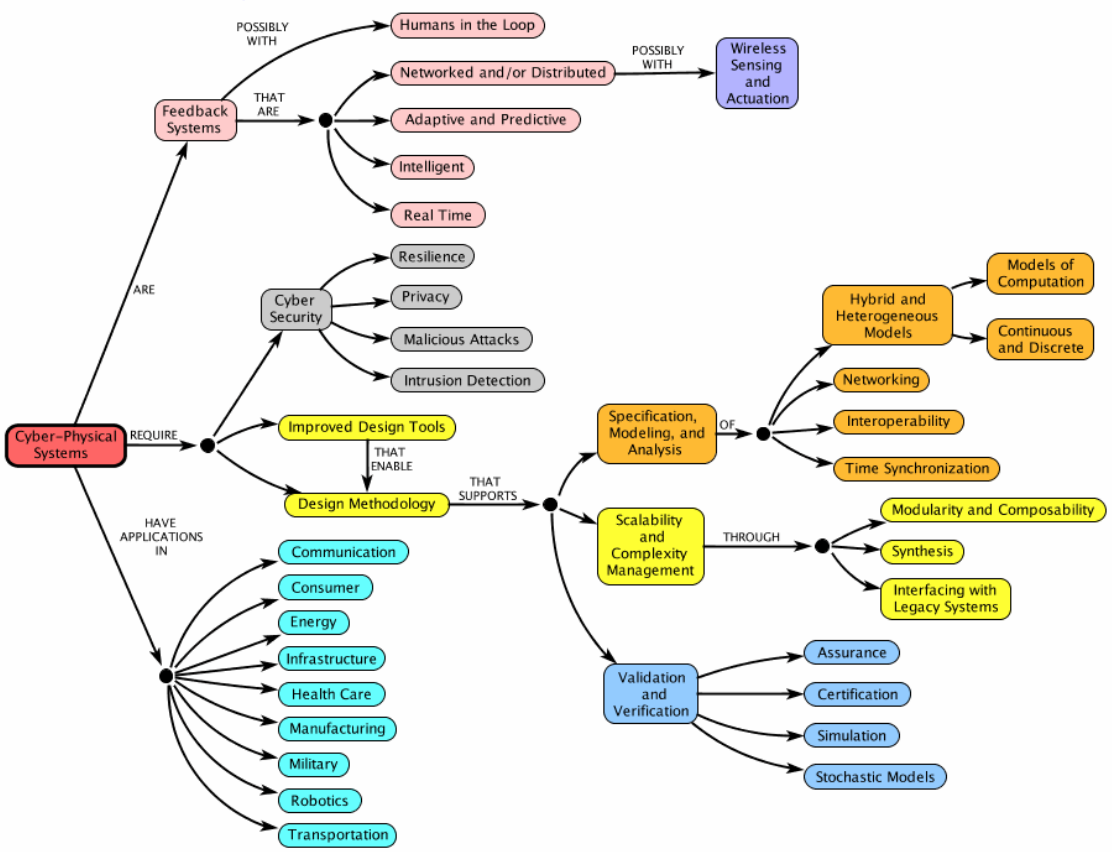

Figure 2.5: Cyber physical systems [Lee, 2014]

As closing a control loop involves both the wireless network and physical entities in a CPS system, WSANs are expected to revolutionise such systems in future [Wu, 2011],[Xia, 2011]. However, several issues such as resource constraints, network traffic, bandwidth utilisation, unreliable communication links, security, etc. may lead to a total network shutdown in a cyber-physical system. As conventional control systems make many idealised assumptions such as non-delayed sensing and actuation, synchronised control, there is a need to study the practical aspects of integrating a wireless communication network in a control framework [Auburn, 2010]. One of the aims of this thesis is to discuss issues that arise due to such assumptions in wireless control and present potential solutions for critical industrial applications.

2.1.5 Industrial benefits

Introducing wireless communication in feedback control loops offers significant benefits in aerospace, marine and industrial applications. In aerospace applications, wireless sensors can significantly improve their performance by integrating several control modules on board an aircraft and also to communicate with a ground unit in real-time. It results in reduced weight and low implementation costs. Also wireless sensors can offer through-life

adaptation from a maintenance perspective. Wireless control channels can act as backup units for hardwired control loops. The key benefits of using wireless sensing, monitoring and control in critical industrial applications with special consideration to aerospace applications as listed by Consultative Committee for Space Data Systems [CCSDS, 2010] are given in Appendix A. It has been demonstrated that wireless-enabled devices have the potential to reduce the cost of installation of transmitters by a significant magnitude in a process plant compared to wired transmitters [Bond, 2006]. Honeywell has reported a financial saving of between 60-90% by using wireless transmitters instead of wired transmitters. The key benefits of wireless control lanes in industrial applications are listed in Fig.2.6.

Benefit	Description
1. Improved reliability	Troublesome wired sensors replaced by wireless counterparts. Wireless may serve as a backup for wired technology.
2. Improved control	Add wireless devices to existing processes for more optimal control.
3. Cost savings	Up to 90% of installed cost of conventional measurement technology can be for cable conduit and related construction. New and existing applications are now economically feasible.

Figure 2.6: Industrial benefits of wireless control lanes [Werb, 2012]

2.2 Wireless Networked Control for Industrial Systems

In a classical control system, sensors are used in the plant to measure various parameters, and this data is passed to a controller that computes the control law and sends a demand to an actuator. Due to recent advancements in the communication and control industry, there is a need to process the data from different sensors placed in a distributed fashion. A networked control system is defined as a control system where sensors, controllers and actuators are placed in a distributed environment and connected through a real-time communication network. Hence, sensor information, control signals and feedback signals are passed as information packets through the network.

Industrial systems make use of various wired communication standards such as HART, DeviceNET, Profibus, 4mA current loop, etc. Communication networks in safety-critical systems such as in aircraft flight control systems use separate standards such as ARINC 664-P7. Wireless communications can be introduced at three levels in an industrial control setup as shown in Fig.2.7.

- **Level 3** represents intranet networks at the corporate level. This involves bulk data-transfer applications, email and Voice over Internet Protocol (VoIP) communications. While the Ethernet standard (IEEE 801) is predominantly used to support communication at this level, recently there has been a growing implementation of IEEE 802.11 WLAN (Wi-Fi) protocol to support communication activities at this level. Today, in many industrial networks, Wi-Fi is used as a redundant back-up network for voice and data communication.
- **Level 2** represents the communication that takes place between remote stations and controllers that in turn control the field devices. For instance, the control demand input and user interactions take place at this level. Wireless communication is not being actively pursued at this level as these communications are critical and any potential implementations need a high level of security.
- **Level 1** represents communications that take place between controllers and field devices such as sensors, actuator nodes, etc. Industries are keen to utilise wireless communications at this level, as wired networks lead to high maintenance and troubleshooting costs. While standards such as HART, FieldBus, DeviceNet is widely used at the moment, many industries have started using wireless sensors for monitoring activities. Due to various advantages, there is a growing interest to utilise wireless communication for closed-loop feedback control applications.

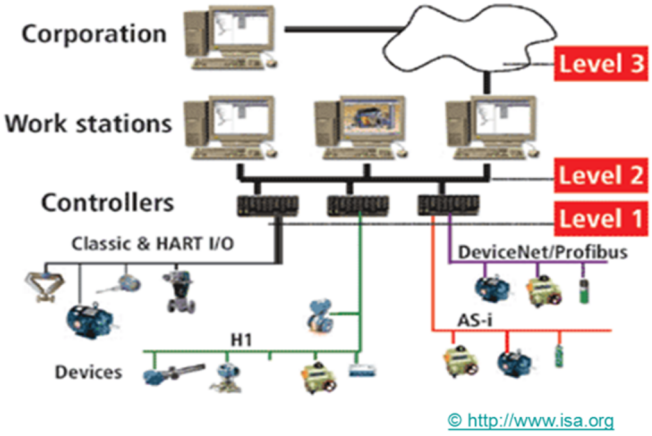

Figure 2.7: Industrial communication levels [Chen, 2004]

Over the past two decades, the communication industry has seen a transition towards Ethernet and currently there is a major drive to take the next step in this evolution by moving to wireless communication. When sensors, actuators and controllers are connected by a wireless communication network, it is termed a wireless networked control system (WNCS). Advantages of WNCS are as follows:-

- Cost of implementation of wireless sensors is very low.
- Flexibility: sensors can be plugged into the network without significant hardware changes.

Wireless networked control systems can further be classified into three types from an industrial perspective.

2.2.1 Wireless networked – Classical control systems (WN-CCS)

The simplest form of WNCS (Fig.2.8.a) is a closed-loop control system wherein the controller, sensors and actuators are connected over a wireless network. Current industrial systems are connected over a wired network in a similar fashion using wired protocols such as CAN, ARINC 429, Fieldbus, HART, etc.

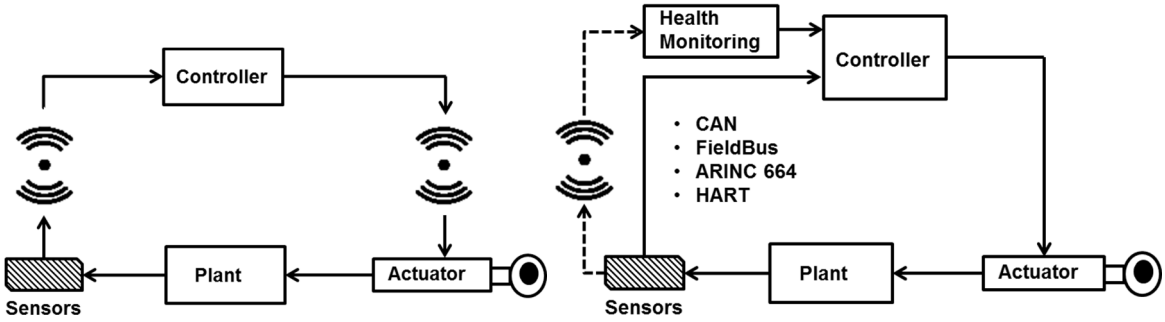

Figure 2.8. a): WN-CCS b): Health monitoring

Many industrial applications in the non-critical domain have started to introduce wireless sensors inside a control system for sensing parameters in case of any faults in wired sensors and for improved maintenance (Fig.2.8.b). Wired protocols such as HART offers a wireless extension known as WirelessHART (discussed in Section 3.1.4.3). Therefore, HART systems can have a wireless capability readily available, however, such wireless protocols have not been used yet for closed-loop control.

2.2.2 Wireless networked – Distributed control systems (WN-DCS)

Distributed control systems are an extension of the classical control systems, wherein there can be multiple controllers that handle a set of sensors and actuators over a wireless network. These individual controllers are known as the local control units. In turn, all these local control units are handled by a master controller known as the supervisory control unit. The supervisory control unit can control a set of sensors and actuators (those with high criticality) on its own as well. DCS is implemented in the safety critical domain such as aerospace, automotive and critical industrial applications. Today's aircraft flight control system is an excellent example of this type of networked control (wired). The flight management system (FMS) acts as the supervisory controller that takes the pilot inputs as well as data from many other sensors, computes the control demand and sends it to local control units distributed across the aircraft such as an engine control unit, braking unit, fuel control unit, wing actuators, etc.

The advantage of DCS is that in the event of a failure of a local control unit, the supervisory control can take direct control of the sensors and actuators controlled by the

failed local controller. However, it has a single point of failure. If a supervisory unit fails, then the whole network will crash. For instance, in Wi-Fi hotspots, if the gateway crashes, then the entire network has to be reset. Due to its simple design and the ability to handle multiple controllers, sensors and actuators this architecture is followed by many industrial standards in the form of star and mesh topology (see Section 3.4.2). Analysing the issues present in such an implementation is the motivation and focus of this thesis.

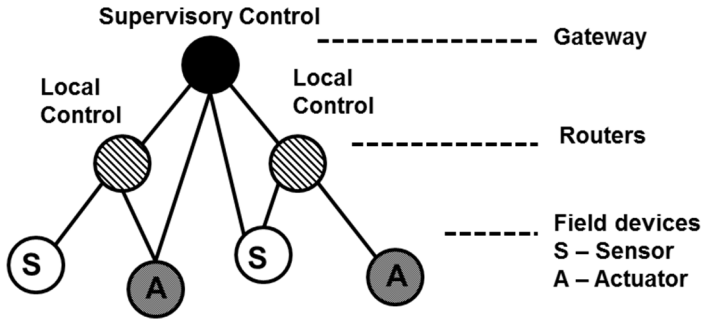

Figure 2.9: Wireless networked – Distributed control systems (WN-DCS)

In a distributed control system (see Fig.2.9), the sensors and actuators are connected to a local control unit, which, in turn, is connected to a supervisory control unit. There can be multiple local control units controlling various sensors and actuators, while the entire network is controlled by a supervisory control unit. This is similar to Wi-Fi hotspots, wherein the portable devices act as the sensors, the wireless router acts as the local control units, while the wireless gateway acts as the supervisory unit. However, it is based upon a star architecture and therefore, there is an issue of single master failure.

2.2.3 Wireless networked – Decentralised control systems (WN-DeCS)

A decentralised control system (DeCS) is a special case of the distributed control systems. In conventional DCS, there is a single point of failure that is if the supervisory control develops a fault, then the entire system is at risk. This is one of the reasons aircraft digital engine control units (FADEC) are provided with dual controllers, so that even if one of the units fails another one can be used by the pilot to land the aircraft safely. However, as this is not possible for all the control units, another potential approach would be to use multiple supervisory units (Master) which in turn control the local controllers (see Fig.2.10).

- A group of controllers and actuators are known as a cluster and if a Master in the cluster fails, then a Master from a neighbouring cluster can take control of the network thus increasing flexibility.
- The master units are inter-connected over a wireless channel and therefore, can share data with each other. Therefore, in the case of a failure of a master unit, another unit can take control of the network, thus decentralising the architecture.

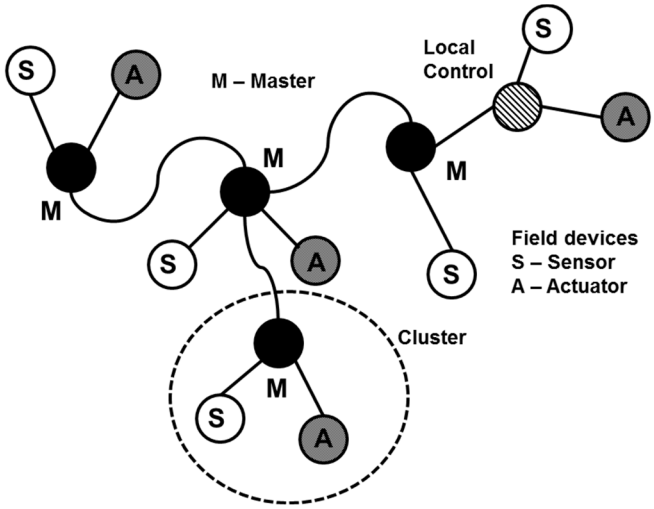

Figure 2.10: Wireless networked – Decentralised control systems (WN-DeCS)

While such architectures provide excellent fault tolerant control, especially in the case of wireless networked control systems, these can increase the complexity of the network. Therefore, DeCS may not be a feasible solution for industrial control applications as it increases cost and maintenance. However, it can offer significant fault tolerance if used in industrial applications where mesh networking (Section 3.4.2) can be supported.

2.2.4 Wireless real-time control systems

Wireless real-time control systems are defined as systems where the control process requires control actions to be executed at an exact physical instant in time as intended by the control algorithm over a wireless network. The system must have strict adherence to deadlines, and its applications can be considered to be mission critical.

Real-time control systems are defined as control systems that have strict deadlines and highly deterministic. Therefore, any time delay or latency in the network may degrade the system performance and eventually render the control system unstable. In general, industrial systems with networked control (be it wired or wireless) are real-time systems. However, the level of determinism and deadline requirements varies according to a given application and the network medium. Therefore, real-time systems are further classified as hard-real time systems and soft-real time systems.

A good example of a hard real-time system is an aircraft engine health monitoring unit. The inputs from various sensors in the aircraft engine are monitored and processed by a flight control system. Any change in the sensor values must be processed, and appropriate control actions need to be taken in real-time. Any delays caused by the communication process will result in a serious problem. Implementing wireless sensors in aircraft is a challenging task as information processing needs to be more robust and reliable.

Hard real-time systems: [Douglass, 2009] defines real-time systems based on a utility function's response (feedback response) of a control system under communication constraints. If the utility function drops step wise from 1 to 0 as shown in Fig.2.11, the system is called hard real-time (HRT). Therefore, any feedback received by the controller after a certain delay is useless. Such systems are regarded as safety-critical and therefore, delayed or missed feedback data might render the system unstable and eventually lead to a system shut down.

Soft real-time systems: If the response received by the feedback controller degrades gradually over time due to various issues in the network, such systems are known as soft real-time systems. Though it affects the overall system performance, the received packets can still be used by the controller. Many industrial systems in the non-critical domain such as process automation are considered to be soft-real time systems.

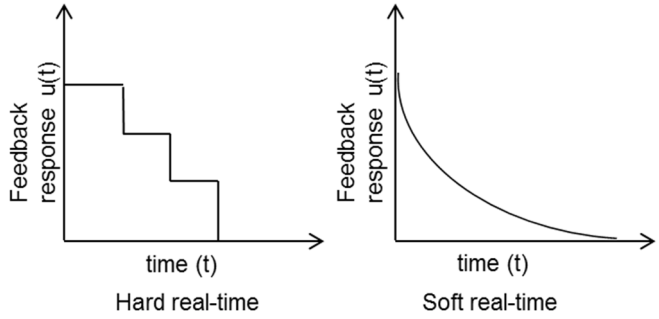

Figure 2.11: Hard real-time vs Soft real-time systems

If the utility function does not show significant drop in regards to the time constant of the control systems, such systems are known as non-real-time systems. However, control systems that are not sensitive to delay or packet loss are quite rare in both critical and non-critical industrial domain. For instance, most of the control systems in an aircraft are hard real-time systems as time delay or lost data packets are not acceptable during any flight stage.

2.2.5 Safety-critical control systems

Safety-critical systems are defined as systems where a failure or malfunction can cause death or injury to human beings, could result in environmental harm, or can cause damage to equipment [Knight, 2002]. Wireless networked control for safety-critical systems requires solutions for a number of crucial underlying technical issues. Wireless closed-loop control is currently an emerging technology for industrial applications, and it is used only for sensing and monitoring applications. There are various key issues that are yet to be addressed in implementing wireless NCS for safety-critical control applications:-

- **Reliability of the wireless link:** Loss of data, loss of acknowledgment signals, stale data being processed, dynamic network architectures, freedom to use desired data rates, energy consumption.
- **Network delays:** Time delays in the wireless path, transmission delays, queuing delays, inconsistency in data rates (jitter).
- **Security:** Hacking, electromagnetic interference, Byzantine disagreement problems, design of security protocols that can offer tight security over the network. This may result in additional bandwidth requirements.
- **Synchronisation issues:** Over time, wireless sensors are subject to clock drifts. Hence, they need to be synchronised with a global time reference such as GPS. As the network enlarges and accommodates more and more sensors, efficient clock synchronisation algorithms are required.
- **Network Protocols:** Currently protocols such as IEEE 802.11(a/b/g/n), IEEE 802.15.4, Zigbee, Zigbee Pro, Bluetooth, WirelessHART and ISA 100.11a exist but how far their performance envelope can be pushed for safety-critical systems remains an open question.

Research in implementing wireless control in critical industrial systems is still in its infancy, and the early solutions available in this domain are simply computer-based simulations or theoretical models.

2.3 Co-design of Wireless Networked Control Systems

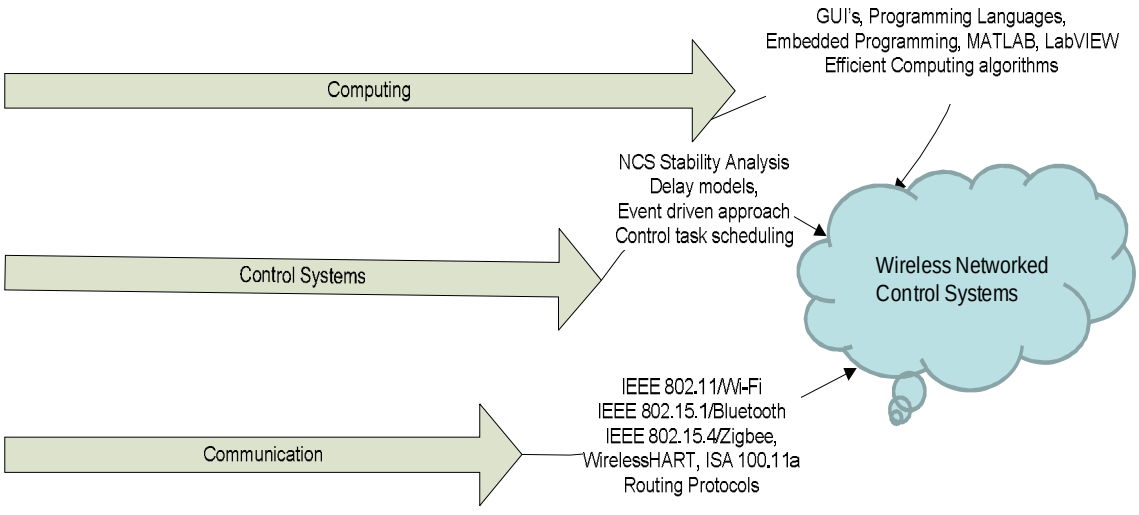

Figure 2.12: Interdependence of Computing, Control and Communication

Over the last few decades, computing, control systems and communication have been three major separate areas of research. Computing has seen a significant growth with various hardware and software solutions. Various simulation tools such as MATLAB and

LabVIEW are available to develop control laws. There are efficient computing algorithms that can perform calculations more quickly and with great accuracy.

Developments in control systems have a dependence on the computing as the control solutions need an efficient software program for better analysis and testing environment. Control systems have proposed various research solutions, in particular, for networked control systems, such as control methodologies for stabilising networked control systems, controllers to handle network delays, solutions to mitigate time delays, control methods for bandwidth contention, etc. Though these methods prove to be efficient from a control perspective, they are based on the assumption that the communication standard is perfect, and this is not practically possible.

The communication industry has a variety of communication standards, especially in wireless communication. Today many non-critical applications are controlled via wireless signals. Nevertheless, extending wireless communication to safety-critical and real-time control applications remains unreliable. Even though many computing algorithms and stability solutions exist, utilising a communication standard effectively is a key issue. Hence, there is a need to acknowledge the interdependence between these three industries. Therefore, the key requirement of a wireless networked control for industrial systems can be defined as,

A valid computing algorithm that can effectively process the control laws in a reliable communication medium is the key requirement for wireless networked control systems.

2.4 Literature Review – Wireless Closed-loop Control

In order to understand the development of wireless closed-loop control in industrial systems, a literature survey is presented here. The problems faced in implementing a wireless control network can be classified as control of network and control over network issues [Gupta, 2010].

Control of network solutions deals with issues that occur due to deterioration of Quality of Service (QoS) parameters of a wireless network such as the overall throughput, bandwidth, data rate, channel error rate, availability, etc. The performance of a wireless network based on these parameters are usually addressed by various layers of a wireless protocol stack, and these are further discussed in Chapter 3. However, issues that affect the network quality such as co-channel interference, poor link quality, bandwidth contention methods, etc. contribute to significant problems in wireless closed-loop control systems such as time delay, packet dropouts, network reliability and stability. As these issues arise when a control loop is closed over a communication network the solutions to these issues are termed as *Control over Network* solutions. *Control over Network* studies the closed loop system performance subject to wireless network constraints when the feedback control

loop is closed via the wireless network. The aim and focus of this thesis is to concentrate on *Control over Network* issues and its solutions.

2.4.1 Stability of wireless networked control systems

Some of the earlier research in networked control systems such as analysing the network topologies and control stability can be found in [Yang, 2006]. [Wang and Liu, 2008] have proposed the linear quadratic regulator approach for networked control stability. The issue of data packet loss and unreliable communication links in both wired and wireless networked control systems has been widely addressed in the literature [Tabbara, 2007]. The communication issues such as packet loss, time delay, network congestion, etc. are addressed using control approaches in WNCS. The design consideration for such approaches in networked control is presented in [Hespanha, 2007],[Lian, 2006],[Liu & Goldsmith, 2004]. These design choices influence the existing control methods by redesigning them according to the network conditions. The design approaches concerning both control and communication issues are discussed in [Naghshtabrizi, 2011], [Willig, 2008],[Graham, 2003].

From a control perspective, the communication issues will affect the stability and reliability of the control performance and eventually would render the system unstable. Therefore, a number of studies [Li, 2012],[Wu, 2007],[Zhang, 2007],[Oh, 2006] have been done on the stability of the networked control systems by modelling the communication issues as network disturbance or noise in control models. The convergence of the system stability is then derived [Zhang, 2012],[Schenato, 2007],[Flardh, 2005] based on the probability and distribution of the noise in the network. However, in order to derive these stability conditions a number of assumptions are made such as both the controller and actuator being time driven, the time delay is within a certain known bound, tight synchronisation of nodes in the network, etc. All or a combination of these may not be practically possible in industrial systems.

2.4.2 Co-design approaches in wireless networked control

Co-design approaches [Björkbom, 2011],[Park, 2011],[Colandairaj, 2007] that acknowledge the interdependence between control and communication parameters have become popular recently. In one aspect of the co-design approach, communication networks with known QoS parameters are chosen for a given application and then new control and observer schemes are designed to improve the control performance. For instance, observer based solutions for varying delay associated with WNCS in regard to network stability and reliability is proposed in [McKernan & Irwin, 2010]. Event-triggered and self-triggered control over wireless sensor and actuator networks are discussed in [Heemels & Johannson, 2012]. More details on these approaches are given in Section 4.2.

On the other hand, a controller with known Quality of Control (QoC) parameters such as stability, overall control performance is chosen for a given application, and a suitable network or communication protocol is designed or additional improvement to existing protocol is done to improve the control performance under delays or packet dropouts. A cross-layer framework is presented in [Liu & Goldsmith, 2004] in which it is highlighted that the choice of data rates, error correction coding and the maximum number of retransmission can significantly affect the performance of a wireless networked control system. However, in both the approaches, the designer is restricted to use one set of degree of freedom either changing QoS parameters or QoC parameters to keep the system stable.

Few works [Colandairaj, 2007] (and references therein) suggest that by utilising variable sampling rates, or adaptive sampling rates based on error rate information, network induced delays can be handled. The effects of range on packet loss and of packet loss on control performance have been studied by adjusting the sampling interval of the controller in [Ploplys, 2003],[Micheli, 2002]. Event-based sampling approaches that utilise threshold detection to control network congestion are discussed in [Wang, 2011]. However, these approaches need a number of samples to be logged in a local controller in order that the threshold values can be determined. Therefore, it may be unsuitable for highly dynamical systems.

The next step in this trend is to combine the solutions from both control and communication approaches and apply them to a real-time industrial problem. For instance, a combination of bandwidth contention methods is used to optimise the QoS parameters which in-turn is used to select the QoC parameters in [Chamaken, 2010]. A brief survey and discussion of design issues in wireless real-time networks are presented in [Hou, 2012]. However, achieving an optimised solution remains an active area of research. While there are theoretical data rates or packet drop out rate bounds for stability, there is a need to measure the control performance related to practical network QoS [Lian, 2002].

2.4.3 Network reliability issues

The key issue in extending the solutions proposed for wired networked control systems to wireless networked control systems is the increase in uncertainty of the network reliability when a wired network is replaced by wireless. The nature of a wireless channel is such that the time delay and packet loss probabilities are much higher [Zhang & Yu, 2007] and new issues such as deliberate jamming, frequency interference, channel blacklisting, and malicious interference of data packets arise in wireless networks.

Issues such as external interference and deliberate jamming can affect QoS and cause data packet loss or lost wireless links. It may be possible to provide these missing samples using model-based control such as model-based predictive networked control [Ulusoy, 2011] model reference adaptive controller (MRAC) [Tahoun, 2011], etc. However, a good model of the control system and modelling the wireless network parameters efficiently is

needed, and this may not be practically possible for many real-time industrial systems operating in harsh and dynamic environments.

While there are simulation models available for analysing wired networked systems, those for wireless networked systems are very scarce [Björkbom, 2011],[Henriksson, 2006] that can be used to test the mathematical solutions. In addition, the existing results in this domain lack an experimental evaluation in a real-time wireless embedded hardware platforms. Though such work is scarce in the safety-critical domain, early research in the non-critical domain is highlighted here.

The effect of sensing and actuation in real-time systems are studied by controlling an inverted pendulum over a wireless network [Hernandez, 2011]. It highlights the need for new control-based approaches for real-time control in wireless systems. A model reference adaptive system (MRAS) [Naman, 2000] is used to guarantee the network reliability of a wireless feedback loop for water level control in the 433MHz wireless range. An ARMA model based technique to ensure stability in wireless control is discussed in [Short, 2011]. However, it utilises a combination of MATLAB model and embedded systems to implement the offline system identification process. Other studies include demonstrating wireless networking in structural control [Seth, 2005] and in real-time data acquisition. While such systems are considered to have tight deadlines, the sensing or sampling is done at long time intervals that are not feasible in closed-loop control applications.

Therefore, it is vital to analyse the issues in wireless networked control from an implementation perspective with the commercially off-the-shelf (COTS) hardware available for implementing wireless control systems. Solutions that are trivial to be implemented in real-time embedded systems are principally aimed at compensating packet loss that occurs based on repeating patterns and may not keep the control process stable if the network conditions change. Some solutions explained earlier would seem to be better suited for wireless networks; however, their implementation could be non-trivial due to the computational complexity [Schenato, 2007]. Another issue that concerns critical industrial applications is certification and safety regulations. For instance, to implement wireless closed-loop control systems in aircraft systems the limitations in implementing the existing solutions in airborne software systems pose a major challenge due to their computational complexity.

Therefore, there is a need for an integrated design for wireless systems that can supervise the real-time control process for deterioration in QoS parameters as well as address the issues such as lost wireless links. Some early research that suggests such integrated design approaches for wireless networked control system is discussed in [Ding, 2013],[Horvath, 2012]. However, there is a need to evaluate such designs for a practical control system, especially in critical domains such as aerospace (see Section 6.6 for more details).

In this research, the focus is on relevant problems and solutions in implementing a real-time wireless closed-loop control system from an industrial perspective. The key issues that impact the industrial control system when the control loop is closed over a wireless

network is mainly considered. A more comprehensive literature review on the predominant *Control over Network* issues such as clock synchronisation, intermittent packet loss and time delays exceeding sampling rate in wireless closed-loop control systems is further presented in Chapters 5, 6 and 7 respectively.

2.4.4 Wireless control – State-of-the-art

From the literature review, it is evident that there is a necessity to appreciate the inter-dependence between control and communication. While issues in wireless networked control systems occur due to unreliable network medium, as evident from the literature, control theory can offer solutions to these communication problems. However, this blend cautions a trade-off between the control and communication parameters depending on the industrial application. For instance, most of the control solutions proposed in the literature assume the nodes in a wireless network to be synchronised at all times and such assumptions may not be feasible in practical applications.

In addition, automotive and aerospace industrial control applications are predominantly classified as real-time critical systems. Therefore, the processors on-board these systems are built to run simplified algorithms with a possibility of redundancy checks in case of any failures. While solutions proposed in predictive control and fault tolerant control (FTC) approaches [Ding, 2013],[Horvath, 2012],[Pajic, 2011] can provide an efficient wireless networked control, there are various limitations in implementing these algorithms in on-board processors due to their computational complexity. Therefore, from the safety-critical industrial perspective, there is a need to understand the performance of the FTC algorithms in an embedded hardware environment.

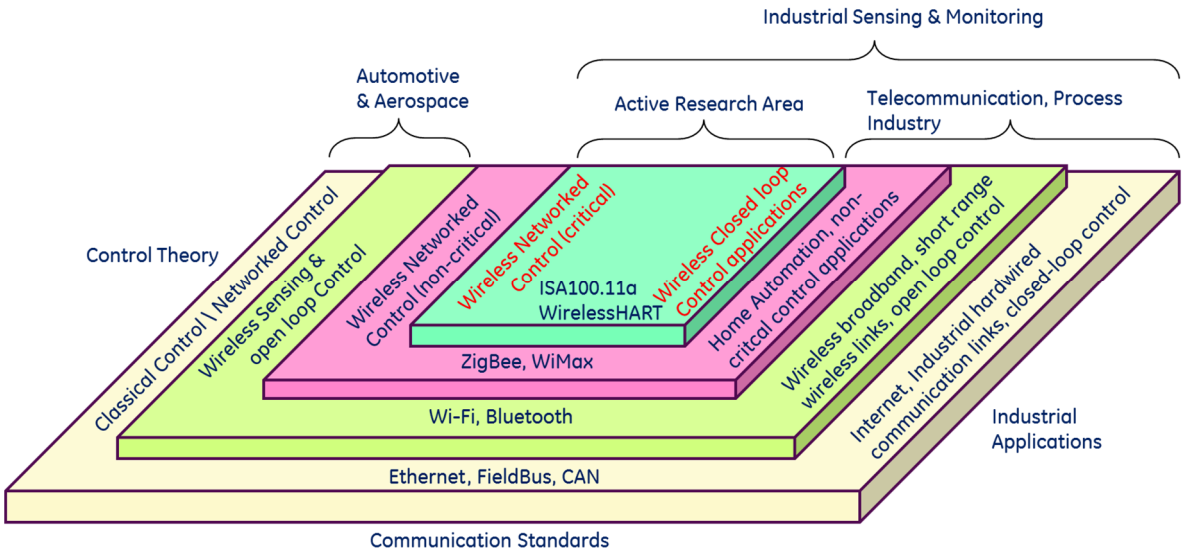

Figure 2.13: Wireless closed-loop control – State-of-the-art

Fig.2.13 shows the evolution of communication standards, control theory and how the combination has been utilised by industrial applications. It can be seen that the automotive and aerospace industry is restricted to the first two levels as the criticality increases at every level. Telecommunication and Process industry have utilised the first three levels of communication standards and wireless networked control applications at a non-critical level. While industrial standards such as WirelessHART and ISA100.11a have started to appear in industrial sensing and monitoring, extending them to wireless closed-loop control applications remains an active area of research. Therefore, the motivation of this research work is to understand the needs of the industrial applications at this level and analysing the predominant issues in implementing a wireless closed-loop control system.

2.5 Summary

It is important to identify a control solution that could solve a communication-related problem with minimum trade-off on other communication parameters. While the process industry has adopted wireless sensor networks for sensing in a large scale, automation and aerospace industry are keen to understand the effectiveness of wireless network in both sensing as well as control applications for maximised benefits. Therefore, in this research work, a joint design of control and communication is proposed to address the problem of introducing wireless communication in feedback control loops. In addition, the following issues based on the key issues identified in the literature review are discussed further in subsequent chapters:-

- In order to validate the assumptions such as tight synchronisation and time delay bounded by the sampling interval that are usually made in the literature, these issues are further explored and optimal solutions are discussed.
- An open-source wireless protocol that can be implemented on IEEE 802.15.4 RF units is considered, and the protocol is further improved to enhance the stability of the control system under connectivity issues.
- A sensorless supervisory control approach is proposed to address the issue of packet loss in feedback loops using an estimator to provide resilience to intermittent bursty packet loss.
- The study is further extended by introducing interference deliberately in the feedback loops using a stand-alone embedded hardware demonstrator thereby analysing the effectiveness of the control solution from a communication perspective.

The next chapter presents a comprehensive review of the industrial wireless standards and other communication issues related to closing a control loop over a communication network.

Chapter 3

Industrial Wireless Control – A Review

The aim of this chapter is to analyse the suitability of the existing wireless standards to deliver communication stability and network reliability in wireless closed-loop control for industrial applications. It provides a comprehensive review of various wireless standards highlighting their merits and demerits with respect to wireless closed-loop control. It assesses the effectiveness and application impacts of security protocols of these standards and their effect on control loop stability. A brief analysis of issues with respect to radio frequency and solutions to mitigate it is presented. It concludes with a summary of open research problems and a summary of key findings that identifies the gap in the existing standards. The key identified issues are then classified as control over network problems and addressed in further chapters.

3.1 Analysis of Wireless Standards

Industrial control systems are subjected to harsh environments such as vibration and various RF sources that may affect the wireless data transmission. Many reliable and efficient protocols have been proposed for wireless sensor networks; however, they are not well suited for industrial control applications [Willig, 2005]. There is a need to analyse the leading wireless standards and understand their suitability for safety-critical systems.

The following is the limitations involved in implementing a wireless control loop in industrial systems:-

- The practical data rate of existing wireless standards is typically only 10-20% of the overall addressed data rate.
- All the existing standards operate in 2.4 GHz. As this is a license-free band, many wireless devices operate at this frequency, and in an industrial environment, this will pose serious electromagnetic interference issues. Therefore, there will be a practical limitation on utilising the 2.4 GHz frequency due to the other RF sources present in the environment.
- The practical limitation in achieving maximum network throughput and in mitigating issues such as transmission delays, packet loss, etc.

Several industrial standards such as HART, Zigbee, Bluetooth and ISA SP100 have developed wireless protocols for industrial automation. Standards for critical control are still under development or are being ratified. Some of the existing wireless standards that are used for wireless sensing and monitoring are discussed in this section. The IEEE LAN/MAN standards committee is responsible for ratifying wireless standards and hence all the wireless standards and their amendments are prefixed with IEEE 802.

3.1.1 Open System Interconnection (OSI) model

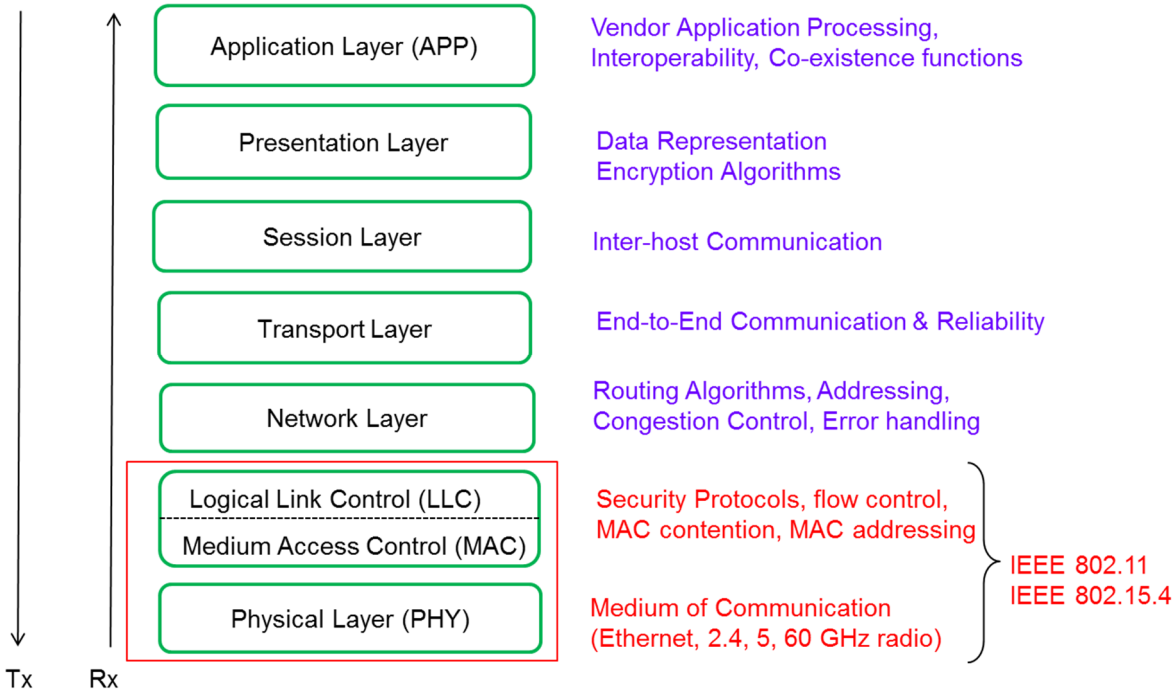

Figure 3.1: Open System Interconnection (OSI) model

Industrial communication standards are supposed to satisfy the OSI model [Abed, 2012]. That is, it should define how the requirements of the 7 layers in the OSI model (see Fig.3.1) are justified. In general, wireless standard/protocol manufacturers and vendors follow the IEEE standard (802.11/802.15.4) at the Physical (PHY) layer and Data link (MAC and LLC) layer. This is to ensure that the standards can be operated universally and have a common agreement on utilising the frequency spectrum. However, the standards can have proprietary definitions for the rest of the layers for maximised efficiency, added security, etc. This type of hybrid standard provides more versatility compared to the traditional wired standards.

The responsibility of different OSI layers is listed below:-

- The PHY layer in wireless standards defines the medium of radio transmission in various frequency spectrums such as 2.4, 5, 60 GHz.
- The Data link layer has two functions logical link control (LLC) to maintain flow control and the Medium Access Control (MAC) which is the most important layer

for communication standards as it handles security, MAC addressing, contention methods, etc. This layer also dictates the network stability.

- The Network layer defines the routing algorithms, addressing and network protocols. The transport and network layer functions together impact the network reliability.
- The Transport layer manages end-to-end communications between two end nodes in the network. It is responsible for the acknowledgement process in wireless standards.
- The Presentation layer deals with data representation, encryption algorithms while session layer deals with inter-host communications. Industrial wireless standards do not explicitly define these two layers and combine their functions at the APP layer.
- The Application (APP) layer contains vendor processing, interoperability and co-existence functions. It is at this layer the standards differentiate themselves. For instance, WirelessHART explicitly defines the HART interface at this level while ISA100.11a does not define adherence to any particular protocol.

3.1.2 IEEE 802.11/Wi-Fi [1]

The IEEE 802.11 was first ratified by the IEEE 802 committee in 1997 for implementing wireless communications in Local Area Networks (LAN). Since its first version, it has been amended over years, and it has multiple versions available for various LAN usages in different frequency bands with varying data rates. However, the most frequently utilised versions are listed below:-

- IEEE 802.11a which can transmit at 5MHz and support data rates up to 54Mbps.
- IEEE 802.11b utilises the 2.4GHz band and handles up to 11Mbps.
- IEEE 802.11g is faster as it offers 54Mbps at 2.4GHz.
- IEEE 802.11n, can offer data rates as high as 140Mbps.
- IEEE 802.11ad, a new standard ratified by IEEE to operate in 60GHz with 7 Gbit/s

The utilisation of IEEE 802.11 in commercial applications is owned by the Wi-Fi alliance [Wi-Fi Alliance, 2014], and it defines Wi-Fi as "*wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards*" [Road, 2014]. IEEE 802.11 is the most common standard for wireless networks today utilised by various devices that supports radio transmission. IEEE 802.11b/g/n standards are widely used by Wi-Fi alliance for home and office broadband and wireless local area networks. However, the data rates addressed by these standards are 'best case' speeds and are not achievable in practice. Though IEEE 802.11 is coming up with new amendments to the existing version, industry remains hesitant to utilise the protocol for wireless networked control applications due to interference and security issues.

[1] All logos presented in this section are trademark of the respective wireless standard

Many experimental results in literature studying WNCS have been undertaken with the IEEE 802.11 standard [Ploplys, 2004]. The suitability of IEEE 802.11b for wireless feedback control quantifying various factors such as channel contention, channel errors and channel bandwidth over an inverted pendulum mounted on a cart was presented in [Colandairaj, 2007]. It is highlighted that channel errors in IEEE802.11b networks could be detrimental and channel bandwidth is extremely important for wireless closed-loop control. The comparison of 802.11 standards with cost, performance and data rates for aircraft applications is given in [Chilakala, 2008].

Summary:

IEEE 802.11 uses the carrier sense multiple access with collision avoidance (CSMA/CA) for MAC contention (see Appendix B for the mechanism of MAC contention methods) as compared to Ethernet, which uses carrier sense multiple access with collision detection (CSMA/CD). As 802.11 is developed for giving a radio interface to existing Ethernet LAN's (so-called Wireless Ethernet) there is a growing interest to utilise it for data collection, web based monitoring and Human Machine Interface (HMI) in industrial applications. Nevertheless, due to its heavy usage, security issues, weak bandwidth contention methods, it is not suitable for critical wireless control applications.

3.1.3 IEEE 802.15.1/Bluetooth

Bluetooth is a wireless personal area network (WPAN) protocol designed based on the IEEE 802.15.1 wireless standard, however, it is now managed and organised by the Bluetooth special interest group (SIG) [Bluetooth, 2014]. It is a packet-based protocol based on a master-slave structure. At any given time, a master can connect with up to 7 slaves in a piconet. The key properties of Bluetooth are:

- It offers low-cost and low-power requirements for effective transmissions.
- It operates in the 2.4GHz license-free ISM band.
- It follows the spread spectrum frequency hopping (1600 times per second) to utilise the data transmissions without interference.

While Wi-Fi is intended for LAN communications, Bluetooth is targeted at short-range transmissions with low power consumption needs thus making it a suitable candidate for both industrial and home applications. The use of Bluetooth for feedback control is studied in [Suri, 2005],[Horjel, 2001]. It has been highlighted that while Bluetooth supports interoperability of other wireless devices, it presents a problem for feedback control under non synchronised scatter-nets. Bluetooth has been experimented along with WLAN in industrial applications for monitoring purposes [Ramamurthy, 2007]. Bluetooth Smart, the commercial name for the Bluetooth version 4 (v4) offers considerable reduction in power consumption and cost while it retains many other functions of the classical Bluetooth (version 1 to version 3) such as communication range, data rates, etc.

Summary:

While Bluetooth and its different versions are used in monitoring in low level process automation, it's unlikely that Bluetooth will be considered for implementation in safety-critical control due to its frequency limitations and self-configuring issues. In addition, it has security issues such as "Bluebugging" (manipulating Bluetooth devices by compromising its security [Becker, 2007]) that are of concern for critical control applications.

3.1.4 IEEE 802.15.4 WPAN

As Wi-Fi and Bluetooth have high power consumption as the data rate increases, the IEEE 802.15 standard was ratified by the IEEE 802 group to satisfy the requirements for a standard that can offer low power consumption and low data rate applications. It has two versions. One version is for a high data rate wireless personal area network (WPAN) targeted at personal applications that need high data rate and QoS (Quality of Service) such as multimedia applications. The second version is for low data rate (up to 256 kbps) WPAN and aims at applications that demand ultra-low power consumption especially in ad-hoc networks. Various industrial wireless standards have been proposed based on the IEEE 802.15.4 standard as it is specifically intended for industrial applications with low power consumption. A performance analysis of these leading wireless standards and their suitability for critical industrial systems is presented in this section.

3.1.4.1 ZigBee

ZigBee network has three components, a Zigbee Coordinator, router and end nodes [ZigBee Alliance, 2014]. The ZigBee coordinator is the most capable device in the network that is responsible for managing all the nodes in a ZigBee network and ensures appropriate monitoring and performance of the end nodes. The router is similar to the gateway in a Wi-Fi protocol and requires a separate power line for its operation. ZigBee offers many services such as:-

- An asymmetric link to ensure reliability of communications. It helps to identify and configure the best possible routes between two nodes and it offers self-healing techniques.
- It supports various data rates such as 20, 40 and 250 kbps and it operates in the 2.4GHz band.

The ZigBee PRO network supports efficient mesh networking; however, an end node that is too far from the router cannot communicate as it does not support peer-to-peer networking. Therefore, it limits the network coverage. Boughanmi et al has analysed the Beacon-enabled mode of IEEE 802.15.4/Zigbee for WNCS [Boughanmi, 2008]. The limits

of Zigbee for real-time control loops have been shown where the lower bound of the sampling period of the control loop is 5.3 ms and the number of control loops are limited to two.

Summary:

ZigBee is targeted at home area networks (HAN) and is the most obvious candidate for monitoring and control of smart appliances, home automation devices, etc. It does not meet the needs of safety-critical systems. ZigBee also has problems with interoperability; that is, different products from different suppliers do not necessarily talk to each other.

3.1.4.2 WIA-PA

Wireless Industrial Automation – Process Automation (WIA-PA) is a new Chinese standard based on the IEEE 802.15.4 standard designed for utilising wireless networks in measuring, monitoring and open loop control in industrial automation [Zhong, 2010]. WIA-PA exhibits similar characteristics to WirelessHART and ISA100.11a standards, but offers additional flexibility. However, it is only aimed at Chinese market at the moment, and hence it cannot be utilised for wireless critical applications on a global scale. More details on WIA-PA can be found in Appendix C.4.

3.1.4.3 WirelessHART

WirelessHART was ratified by the HART Communication Foundation in September 2007, and it is the first open wireless standard specifically designed for process measurement and control applications [WirelessHART, 2014]. At the physical layer, it adopts the same IEEE 802.15.4 wireless standard as ZigBee. It differs from ZigBee in the fact that WirelessHART defines its own MAC protocol. Some of the key features are that:

- It follows the Time Division Multiple Access (TDMA) approach for contention thus providing a strict time slot of 10 milliseconds (ms).
- It provides frequency hopping and channel blacklisting to prevent noisy channels.
- It has a central network manager that manages the routing protocol and communication schedules.
- It offers tight security protocols.
- Its advantages include low power consumption per node, immunity to interference issues, reliable communication links, and it can handle up to 1000 nodes.

WirelessHART has been widely analysed in the literature for its performance, effectiveness and application impacts in monitoring and control [Han, 2010], [Saifullah, 2010].

Summary:

WirelessHART has been officially approved by the International Electrotechnical Commission (IEC 62591). It is being marketed by many companies such as Emerson, ABB and Siemens and actively being used for industrial sensing mechanisms. Some of the initial products include a wireless adaptor for control valves, process transmitters and gateways to connect to industrial field buses and to Ethernet. WirelessHART is a good standard for real-time industrial applications; however, more research needs to be done to utilise the protocol in critical applications. It offers a strict 10ms time slot for nodes to transmit/receive data to ensure deterministic communications; however, the feature may not be desirable for all critical control applications.

3.1.4.4 ISA 100.11a

ISA 100.11a is the open wireless networking technology standard developed by the International Society of Automation (ISA) [ISA-100, 2014].

- It is intended to provide reliable and secure wireless operations for non-critical monitoring, supervisory control, open-loop control and closed-loop control applications.
- It offers a routing protocol, network scheduling and security specifications for applications supporting very low power consumption requirements.
- ISA 100.11a runs at 2.4GHz with direct sequence spread spectrum (DSSS) and offers channel hopping as well as channel blacklisting techniques to avoid noisy channels.
- Parts of ISA 100.11a derive from the WirelessHART in terms of network and application layer of the OSI stack. It follows the TDMA approach as well as support for mesh networks, but the difference is that the TDMA in ISA 100.11a is flexible rather than utilising fixed time slots of 10ms as in WirelessHART.
- In addition to the IEEE 802.15.4 frame format, it supports frame formats for transmission of Internet Protocol version 6 (IPv6) packets as well. This provides interoperability with IP based wireless networks (6LoWPAN).
- It defines network and transport layers for interoperable channel hopping.

ISA 100.11a targets low data rate applications. It follows the IEEE 802.15.4 standard at the physical layer of the OSI model which has a data rate of ~250kbps. In addition, ISA 100.11a implements backbone routing to avoid network congestion. Wireless nodes are connected to specific routers in a network. The routers are in-turn connected to a high-quality backbone network for transmission. For flexibility, ISA100.11a does not specify what the backbone network is, as it could be any high data rate network, including wireless or wired Ethernet [Bourke, 2010]. Hence, this reduces the number of channels required for transmission.

Summary:

In order to meet industrial wireless requirements, ISA 100.11a provides robustness in the presence of interference found in harsh industrial environments. It can provide co-existence with other wireless standards that can be used in industrial environments. ISA100.11a can be incorporated easily into any industrial system that supports HART, Profibus, Fieldbus, DeviceNet or any other industrial communication protocols. ISA100.11a has been approved by IEC as an international wireless standard in October 2014 titled "Industrial networks - Wireless communication network and communication profiles - ISA 100.11a" (IEC 62734) [Ristaino, 2014].

3.1.5 The case for wireless standards for critical control

It is evident from the above discussion that Bluetooth, Zigbee, ISA100.11a and WirelessHART have all been used for sensing and monitoring in industrial real-time applications and to a certain extent for open-loop control in research experiments. This sub-section presents a comparative analysis between these standards for their suitability in critical control applications.

Bluetooth, ZigBee, WirelessHART and ISA100.11a operate in the same license-free 2.4GHz ISM radio band. They all support channel hopping and frequency agility to avoid noisy channels. Except Bluetooth, they all share the same IEEE 802.15.4 standard at the Physical layer. Nevertheless, safety-critical applications may sometimes require data transmissions every second. Bluetooth and ZigBee do not provide guaranteed node-to-node communication without data loss whereas WirelessHART defines its own medium access control (MAC) protocol with a time division multiple access (TDMA) approach that offers a strict time slot of 10ms for each node.

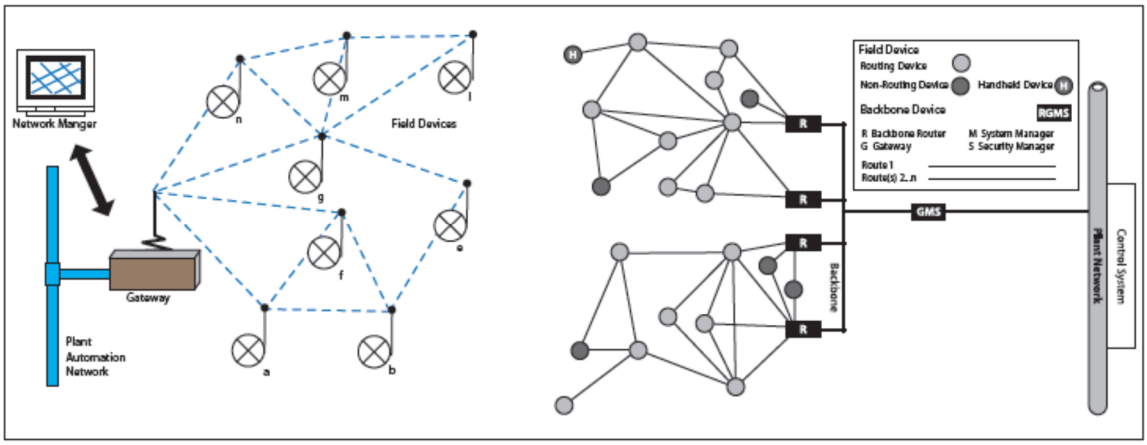

Figure 3.2.a): WirelessHART (no-backbone) b) ISA100.11a (with backbone network) [Bourke, 2010]

Bluetooth and ZigBee do offer channel hopping techniques, but industrial control systems are subjected to harsh interference issues. Bluetooth has limitations on transmission range corresponding to the class of the Bluetooth device. The most commonly used devices are from class 2, which are restricted to a transmission range of 10 meters. Also in a local network, a Bluetooth master can only control 7 active slave nodes in a star topology. ZigBee follows the standard frequency hopping methodology offered by the IEEE 802.15.4 standard. WirelessHART however, provides frequency hopping along with channel blacklisting that blacklists the noisy channel completely [Song, 2008].

Therefore, WirelessHART seems to be a good candidate for industrial automation over Bluetooth and Zigbee. However, ISA 100.11a exhibits features that are desirable for industrial environments in addition to the features offered by WirelessHART. For instance, the ISA100.11a follows a flexible TDMA approach rather than WirelessHART's fixed time slot of 10ms. This results in saving power consumption in wireless networks. WirelessHART has a maximum data rate of ~250kbps at 2.4GHz and therefore, forcing strict 10ms time slots may result in network congestion in case of high-traffic conditions. ISA 100.11a follows a backbone routing approach (see Fig.3.2.b) to avoid network congestion and to increase transmission bandwidth.

ISA 100 ranks industrial automation usages into 5 classes starting from 0 (safety-critical systems) to 5 (no immediate operational consequence). ISA100.11a is targeted at classes from 1 to 5 (non-critical applications) [ISA-100, 2014]. Other standards from ISA in this context are listed in Table 3.1.

ISA 100.12	Aimed at converging ISA 100.11a and WirelessHART.
ISA 100.14	For trustworthy wireless links
ISA 100.15	Wireless backhaul network (connecting ISA100.11a networks to control systems)
ISA 100.21	People asset tracking and identification.

Table 3.1: Other works by ISA SP100

Specifications	Wi-Fi	Bluetooth	ZigBee	WirelessHART	ISA 100.11a
Target Market	Consumer	Consumer & Commercial	Consumer & Commercial	Industrial	Industrial
Target Applications	Home & office Broadband	Remote applications	Home Area networks	Industrial Control	Process Control, Factory Automation
Topology	Infrastructure, Ad hoc, star	Piconet	Mesh, Tree	Mesh	Mesh, Tree
IEEE standard	802.11(a/b/g/n)	802.15.1	802.15.4	802.15.4	802.15.4
Data Rate	~11Mbps	~1,3 Mbps	~ 250kbps	~250Kbps	~250Kbps
Latency	100ms	50ms	~16ms	10ms	10ms
Encryption	WPA2	SAFER	AES 128	AES 128	AES 128
Blacklisting	No	No	No	Yes	Yes

Table 3.2: Comparison of wireless standards

Therefore, both WirelessHART and ISA100.11a provide more reliable and secured channels suitable for real-time industrial applications compared to other standards.

ISA100.11a purposefully states that it is targeted at non-critical applications. More research needs to be done to justify either of these standards as a de facto standard for critical industrial applications. A brief comparison of the wireless standards across various specifications is provided in Table 3.2.

The case for wireless standards for industrial monitoring and control is presented in Fig.3.3 by analysing the wireless standards data rate vs power consumption. It should be noted that though the wireless standards commence from a point where the average throughput occurs, they all can exist right from the beginning of 2.4 GHz band and 20 kbps data rate. This shows how crowded the industrial control zone can get in terms of co-existing devices across different wireless standards.

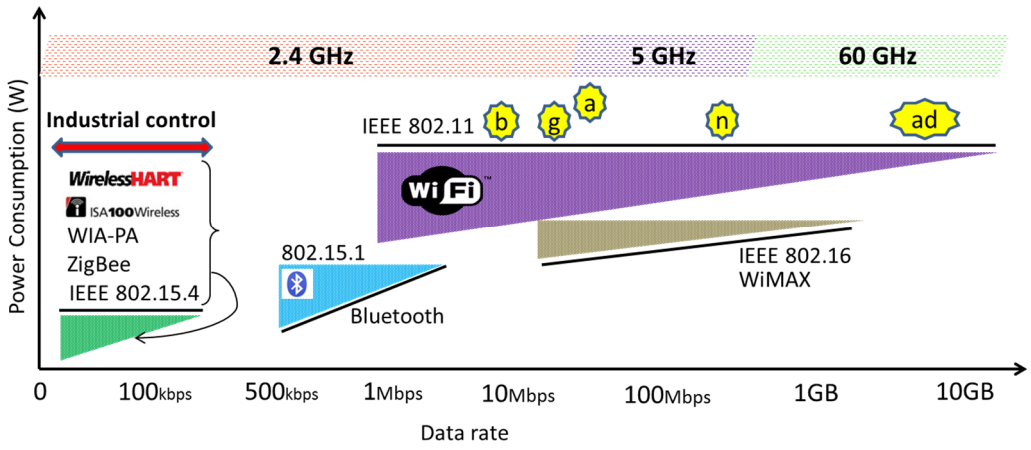

Figure 3.3: Comparison of wireless standards

The following key points can be made with respect to industrial wireless control:-

- The power consumption of wireless standards increases as the need for data rates increases. This is one reason Wi-Fi is not being considered for industrial automation and control as its power consumption is much higher (in Watts) than standards based on Bluetooth (milliW) or IEEE 802.15.4 (inμW). While Wi-Fi standards can offer data rates on an average of 1 Mbps to 7 Gbps, such high data rates are only needed for multimedia applications (WiMAX) or high data transfer such as video streaming, etc.
- Industrial sensor data and control demands do not need such high data rates as these can be sufficiently transmitted within 250 kbps. However, as all the standards can support data rates from ~10kbps and operate in 2.4 GHz, this could significantly impact the performance of industrial standards operating in the 2.4 GHz and 250 kbps zone. Therefore, the standards operating in the industrial control zone (red double headed arrow in Fig.3.3) need advanced mechanisms to avoid interference, unreliable links, etc.

Towards 60 GHz frequency band, there are few devices operating. IEEE 802.11ad is the only standard that supports this frequency band, and the wireless devices are just starting to appear. Due to this, there will be less interference, and it may be a suitable zone for safety-critical control. However, as it can offer data rates up to 7 Gbits/s, the power

consumption is very high. Nevertheless, there is an increasing interest to use 60 GHz for aircraft in-flight entertainment (see Section 3.3.1) and maintenance activities.

Therefore, both academic and industrial research in wireless networked control is predominantly concentrated in improving the robustness of IEEE 802.15.4 based standards as this is specifically ratified for low power and low data rate applications. The supervisory wireless control based hardware demonstrator developed in this research is based on a proprietary wireless protocol from Texas Instruments (TI) that can be used on IEEE 802.15.4 supported devices.

3.2 Security Issues in Wireless Protocols

One of the key issues in implementing wireless technology for industrial systems is security of the wireless network. Security in wireless networks involves several things such as preventing any unauthorised access to the network, damage to the network resulting in network crash, deliberate jamming, data corruption, etc. The worst case of a security violation in an industrial wireless network could lead to the hacker taking control over the network with malicious intent.

3.2.1 Security issues in industrial wireless control

Confidentiality: Confidentiality refers to keeping transmitted data safe from hackers or nodes unauthorised by the network. Eavesdropping is one of the many issues in wireless data transmission as hackers can easily access an open port in a wireless network using proxy servers and be there even without the knowledge of the network manager or gateway. This is especially the case in ad-hoc networks where an external node picks up the broadcasted message from the access point in the neighbouring network, however, the ACK (acknowledgement) can be turned off, and the node will remain as a passive listener in the network without the knowledge of the access point. Confidentiality is usually enforced in wireless networks using data encryption methods such as encrypting the data payload using a unique key which is shared only with the legitimate nodes in the network. However, an encryption scheme should not only try to stop illegal access to the transmitted message but also ensure the messages are not received even partially by the unauthorised nodes. These can be done using a cryptographic nonce with the encrypted data (see Appendix C for more information).

Integrity: Another significant security issue is tampering of the transmitted data by unauthorised users thus compromising the integrity of the wireless network. In unsecured wireless networks, a hacker node can easily register as a participating node, and it can modify a message from the authorised sender by adding some fragments while the

message is in transit or even a send a bogus message in place of the transmitted data. This is a crucial issue in safety-critical systems as modifying emergency data can lead to adverse conditions.

Integrity is ensured by utilising Message Authentication Code (**MAC**[2]) which is computed using a shared cryptographic key among authorised users. As illegal nodes do not have the **MAC** information even if it alters the transmitted message the receivers can identify this by lack of a **MAC** and reject these forged messages.

Authentication: Every node in a wireless network needs to authenticate itself whenever it joins the network, transmits and receives data. In addition, each node in the network should ensure that it is receiving the data from an authorised sender. This is usually achieved using encrypted passwords, Service Set Identifiers (SSIDs) and the MAC data used to ensure integrity. In addition, wireless networks also transmit the MAC address when it joins the network so that the receiver can identify the received messages using its MAC address.

Availability: Network availability can be reduced by adversary nodes by consuming bandwidth, computational resources, disrupting the routing data, etc. This can increase the time delay in transmitting control or feedback data across the network and result in system instability. At times, the adversary nodes can crash the network by introducing too much interference thus significantly reducing the network efficiency.

Denial of Service (Dos): Denial of Service is a result of network availability issues and deliberate jamming. In this case, the hackers or adversary nodes can prevent the authorised nodes from using the network efficiently by consuming the network resources. The adversary nodes can capture a legitimate node's network resources and thus deny any network allocation to the node and completely prevent it from data transmission.

Jamming: Jamming is an important security concern in wireless networks where the wireless nodes are prevented from transmitting and receiving by reducing its signal strength using a Jammer. Jamming is an active research problem, and many intrusion-detection schemes have been proposed in the literature to address this issue [Mitchell, 2014]. Nevertheless, it is difficult to eliminate the source of jamming as it affects the received signal strength. Hence, it is against the law to attempt jamming radio signals in the UK, USA and many other countries. However, in certain countries, including the UK, it's only allowed for military agencies and by prison inspectors and exemptions are granted only under certain circumstances [Ofcom, 2014].

Replay attacks: Replay attacks refer to sending old data by an adversary node or hacker in a wireless network. An adversary node that listens to the communication between two authorised nodes can replay a message sent already. Since the message originated from an authorised sender which will have a legitimate MAC, the receiver will accept this data

[2] Message Authentication Code (**MAC**) is represented in Bold to differentiate it from Medium Access Control (MAC).

resulting in a replay attack. Replay protection can be offered by allocating monotonically increasing sequence numbers to each data packet and enabling the receiver to reject any data packets that has a sequence number less than the latest sequence number.

Security Manager: A security manager is responsible for encryption and decryption of data packets and managing various keying algorithms effectively. Almost all industrial wireless standards define a security manager that monitors the joining and leaving requests of various sensor nodes in a wireless network. A security manager has an access control list (ACL) that has the information of all authorised nodes and their related permissions. Lack of a security manager can result in poor co-ordination of security process and expose the network to hacking attacks.

3.2.2 Security in Wi-Fi

Wireless security protocols have always been an area of intense research. WEP (Wired extension protocol) and WPA (Wi-Fi Protected Access) are the two major security protocols followed for Wi-Fi applications. Wi-Fi alliance introduced the WPA that uses a message integrity check (MIC) to ensure the integrity of the messages and a temporal key integrity protocol (TKIP) to enhance data encryption.

IEEE 802.11i (Robust Security Networks): IEEE 802.11i is the newest standard for wireless security that uses the advanced encryption standard (AES) cipher, instead of the RC4 cipher used by WPA and WEP. Nevertheless, none of these protocols have been proved to be completely free from hacking and other security concerns. Hence, identifying a security protocol for safety-critical systems remains an open problem and an active area of research worldwide.

3.2.3 Security in IEEE 802.15.4

Security algorithms for any communication protocol (wired or wireless) are generally implemented along the various layers of the OSI model. IEEE 802.15.4 standard defines security specifications at the data link layer of the OSI model. Any security protocol at the data link layer should provide four basic security services: access control, message integrity, message confidentiality, and replay protection [Sastry, 2004].

The IEEE 802.15.4 standard defines various security suites as given in Table 3.3 to implement the security for the transmitted data. All the security keys used in the various suites are computed using the Advanced Encryption Standard (AES) cipher and hence prefixed to all security suites. The security mechanism of the suites in Table 3.3 is further explained in Appendix C. The AES-CCM (counter with CBC-MAC) security suite offers both encryption and authentication and is widely used by wireless standards.

Name	Description
Null	No Security
AES-CTR	Encryption only, CTR Mode
AES-CBC-MAC-128 AES-CBC-MAC-64 AES-CBC-MAC-32	128 bit MAC 64 bit MAC 32 bit MAC
AES-CCM-128 AES-CCM-64 AES-CCM-32	Encryption & 128 bit MAC Encryption & 64 bit MAC Encryption & 32 bit MAC

Table 3.3: Security suites supported by IEEE802.15.4 [Sastry, 2004]

In general, all the standards define a security manager to create, administer and manage the security keys used at various layers in the standard. WirelessHART does not define the security manager structure explicitly whereas ISA100.11a and WIA-PA define them in the standard. Zigbee defines a concept known as Trust centre, which has the capability to change the network keys periodically and update the whole network accordingly. This is usually integrated with the network coordinator.

The security protocol implemented in industrial wireless standards with respect to the OSI layer is shown in Fig.3.4. WirelessHART, ISA100.11a and WIA-PA follow the same structure of security implemented across the OSI layers in network layer and data link layer. It can be seen that the data payload is encapsulated at each layer, and the security key is added to the payload at network and data link layer.

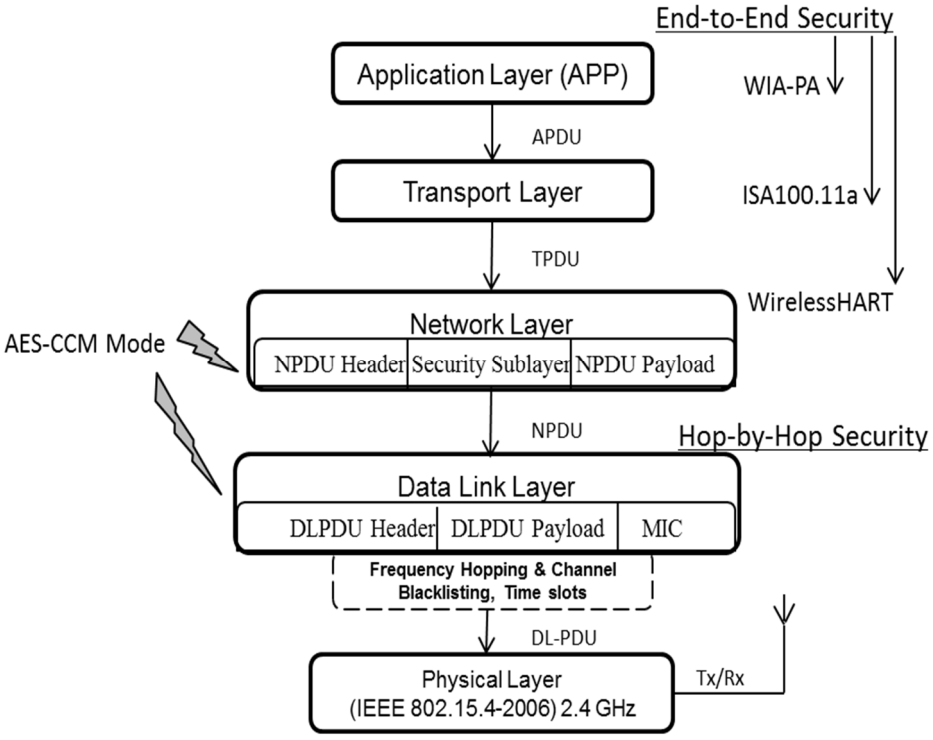

Figure 3.4: Security in industrial wireless standards

The network layer offers end-to-end security between two points in a network whereas data link layer offers hop-by-hop security between neighbouring devices. The hop-by-hop security in data link layer utilise a network key provided by the network manager which is initially used by the nodes that attempt to join the network. IEEE 802.15.4 standards define security only at this level. The industrial standards utilise the AES-CCM mode (mechanism is explained in Appendix C). However, this security alone would make the network easily vulnerable as all nodes advertise this key to join the network which could be easily picked up by an adversary node. Therefore, ISA100.11a, WirelessHART and WIA-PA offer additional security at the network layer which uses the AES-CCM (Join key) to provide integrity and authentication to the data once the connection is established. The Join key is distributed by the Security Manager manually to all the nodes in the network which in turn is used by the device to authenticate to the Network manager.

The ZigBee node also provides additional security at the application (APP) layer using AES keys; however, this is rarely used. It uses a different set of security keys as compared to the other standards such as a master key which is similar to the join key in Wi-HART, a network key which is shared by all devices in the network to authenticate at the network level, and a link key used for end-to-end encryption. In addition to this, the wireless standards (ISA100.11a, Wi-HART and WIA-PA) offer additional security features such as frequency hopping, channel blacklisting and configurable time slots at the data link layer to increase the network robustness towards security issues. However, ZigBee does not offer any of the above features; a major drawback in ZigBee networks compared to the other industrial standards. Table 3.4 provides a comparison of wireless standards based on their functionalities across the OSI layers.

OSI Layers	ZigBee	WirelessHART	ISA100.11a	WIA-PA
Layer 7 Application	Zigbee Device Object, Application support sublayer (APS) , Application layer security	HART 7 Protocol	Object-oriented communication, Support for other communication standards	Application dependent, end-to-end security
Layer 6 Presentation	(Not defined explicitly. Few functions are covered in Application or lower layers)			
Layer 5 Session				
Layer 4 Transport	Not defined	end-to-end acknowledgements	end-to-end security	Not defined
Layer 3 Network	ZigBee co-ordinators, Routing algorithms, end-to-end security	Graph routing, mesh network, end-to-end security	6LoWPAN, Fragmentation and backbone routing	Star-mesh routing, Data aggregation
Layer 2 Data Link	Slotted CSMA-CA Time frame (15 ms to 245 s)	Time slotted (fixed 10 ms) Frequency Hopping hop-by-hop security	Time slotted (flexible) Frequency Hopping hop-by-hop security	Time slotted (flexible), IEEE 802.15.4 beacons, Frequency Hopping hop-by-hop security
Layer 1 Physical	IEEE 802.15.4 (2.4 GHz)	IEEE 802.15.4-2006	IEEE 802.15.4-2006	IEEE 802.15.4-2006

Table 3.4: Comparison of Wireless Standards based on OSI Layers

3.2.4 Drawbacks of security algorithms in wireless standards

From the above discussions, it is evident that industrial wireless standards are robust to many security issues that compromise the integrity, confidentiality and availability of the network. However, there are various other security concerns that are not explicitly addressed or included in these standards [Raza, 2009]. The most prominent issues are listed below:-

Jamming: As explained earlier, jamming is a critical issue that reduces the network resources and affects the signal strength. As jamming is not something that can be dealt with using cryptographic keys, wireless control networks should be robust enough to identify jamming and report it to the network manager immediately. The 60 GHz frequency band offers an excellent solution as millimetre wave (mm-wave) transmissions can easily detect any adversary nodes present in the wireless path [60 GHz, 2014].

De-synchronisation: False timing information can be introduced by hackers in the network, and hence additional network resources have to be dedicated in re-synchronising the network. This is especially a crucial issue in wireless closed-loop control where the sensing and control data transmission have tight time constraints. Therefore, there is a need for a good clock synchronisation algorithm.

Wormhole: Hackers can intrude with the network routing algorithms and compromise the links between different nodes in the network known as Wormhole attack. WirelessHART and ISA100.11a relies on network graphs and backbone networking respectively. Therefore, they are easily prone to such attacks and this issue leads to lost wireless links that cannot be controlled by the security algorithms.

Spoofing: In WirelessHART networks, the well-known key is used by the devices to initially join the networks. Therefore, these can be picked up by fake devices and exist in the network and cause a network blockage. The network manager should be much more agile in adapting to different network keys in such scenarios.

Since data is transmitted over air, it is very easy to intercept the signal, eavesdrop, and even alter the intended behaviour of the signals. Though industrial wireless standards can, to a certain extent, offer security, there is no guarantee they guard against all threats. In addition, different security protocols present different overheads in terms of power consumption and memory usage. The implementation of a specific security protocol requires analysis of the level of protection it provides, e.g. potential loop holes and security threats versus the implementation costs and practical usability. Some fine-tuning of the algorithms to provide more immunity towards specific security threats may be required. The current security protocols of the industrial wireless standards are given in Table 3.5.

Wireless Standards	Security Protocols
IEEE 802.11 (a/b/g/n)	Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2, IEEE 802.11i)
IEEE 802.15.1 (Bluetooth)	Secure and Fast Encryption Routine (SAFER) and Pairing Mechanisms
IEEE 802.15.4 (Zigbee, WirelessHART, ISA 100.11a, WIA-PA)	Advanced Encryption Standard (AES 128)

Table 3.5: Security protocols

3.2.5 Potential solutions for security issues

While there is seemingly growing interest to implement wireless technologies in control systems, on the other hand, there are issues such as interference (or noise) from co-existing wireless systems and deliberate security attacks on the wireless link. Table 3.6 shows the robustness of the industrial standards to key security issues that can affect the wireless control network. High indicates that the wireless standard has a pre-defined solution. Medium indicates that the solution may not be pre-defined in the wireless standard but can be included and low indicates it cannot be supported by the wireless stack and has to be addressed using additional methods. In addition, it presents the effects of the security issues on the wireless closed-loop control performance.

Security Issue	Wireless Standards	Potential Solution	Wireless Control Effect
Confidentiality	High (defined)	Encryption Keys	Reliability
Integrity	High (defined)	Message authentication code	Reliability
Authentication	High (defined)	MAC addressing, passwords	Reliability
Denial of Service	Low (undefined)	Redundant backup networks	Leads to Instability
Replay attacks	Medium (supported)	Increasing monotonic sequence	Stale data, Overshoots
Jamming	Low (undefined)	Channel blacklisting	Packet loss, Instability
De-synchronisation	Medium (supported)	Robust clock sync algorithms	Offset, Drift, Instability
Wormhole	Low (undefined)	Packet leashing	Lost wireless links
Spoofing	Low (undefined)	Changing network keys	False sensor data
Collision	High (defined)	CSMA/CA, TDMA, FH	Packet loss, Instability

Table 3.6: Solutions for security issues in wireless control

A detailed security analysis of wireless sensor networks in highly critical systems due to interference, hacking and deliberate jamming is performed in [Lopez, 2009], [Alcaraz, 2010]. Three wireless standards, Zigbee PRO, Wireless HART and ISA 100.11a have been reviewed, and their security protocols are analysed.

3.3 Radio Frequency Issues

Wireless standards are operated in the unlicensed frequency bands in order to provide interoperability and to cover a wide range of customers. These are known as open spectrum frequencies that allow applications that can be used by all (see Table 3.7). Some of these ranges may differ slightly among different countries based on the purpose of usage. The most commonly used frequency spectrum by wireless standards includes:-

- 2.4 GHz ISM (Industrial, Science and Medicine) band
- 5 GHz band (In UK, band A and B is license-free and band C is licensed)
- Ultra wide band (UWB) that operates over a large bandwidth (>500MHz)

Frequency bands	Applications	Wireless Standards	Merits & de-merits
2.4 GHz	TV, cordless phones, cellular applications, Wi-Fi systems, microwave ovens, car alarm, video devices, etc.	Bluetooth IEEE 802.15.4 IEEE 802.11(a/b/g) Wi-Fi ZigBee Wireless HART ISA 100.11a	Intended for industrial, science and medicine usage. Nevertheless, used for wireless communication by various vendors. Due to this devices are potentially susceptible to electromagnetic interference.
5 GHz	Aimed at wireless internet service providers, devices by Wi-Fi alliance compatible with 5 GHz, wireless mesh networking	IEEE 802.11 (a/n)	Better transmission and scattering properties. Less radio congestion. Orthogonal frequency-division multiplexing. Requires high power level to transmit.
3.1 - 10.6 GHz	Wireless printers, Real-time location systems, RF sensitive environments like health care units	Ultra wide band (UWB)	Immunity to multipath shading, very low energy levels, high-bandwidth communications, high noise level.

Table 3.7: License-free spectrum for wireless communications

WirelessHART and ISA 100.11a may extend the physical layer of the OSI model to operate at 5 GHz in future though there is not enough information available right now. Exploring 5 GHz and ultra-wide band technologies for safety-critical applications remains an open problem. Moreover, current research focuses more on addressing network stability issues for the available wireless standards rather than ratifying interference-free frequency

bands. As explained in Section 2.3, communication standards are not efficient enough to implement all the control suggestions available. Therefore, there will be a constraint imposed by these frequency bands as to how far wireless standards can be utilised for mission-critical applications.

3.3.1 Utilising 60 GHz technology for aircraft applications

Recently, there has been increasing interest in investigating the feasibility of using the 60 GHz frequency band for aircraft applications. The advantage of the 60 GHz frequency band is that it exhibits a unique property called oxygen absorption. That is, at 60 GHz, oxygen attenuates transmission signals. So the transmitted beam coupled with oxygen absorption can offer immunity to interference from other signals. Transmission range is restricted to around 10m but as a consequence intercepting a 60 GHz signal is difficult and hence this offers security advantages [60 GHz, 2014]. Airbus supports various projects in the European Union regarding the deployment of 60 GHz technology for wireless in-flight entertainment, wireless intra-communications between sensors and crew communication applications [Luo, 2008].

3.3.2 Summary

Interference cannot be tolerated in safety-critical systems. For instance, FAA has regulated the use of cell phones on board aircraft stating that the devices must be used in airplane mode or with the cellular connection disabled [Greco, 2013].

Another problem is the requirement of sufficient bandwidth for communication. Not all frequencies are desirable for all wireless applications. For low data rates, a narrow frequency band in the lower frequency range is required. For broadband applications, wide bandwidth and higher frequency range are needed but as frequency increases, problems such as attenuation and shadowing increase. A trade-off exists between the bandwidth that can be utilised and the transmission efficiency that can be achieved.

Most of the wireless standards, in particular, the industrial standards such as WirelessHART and ISA 100.11a, currently operate only in the 2.4 GHz frequency band. This is a license-free frequency band, and therefore, it is utilised by many other devices that use radio communication. How far the performance envelope (data throughput rate, transmission efficiency, etc.) of these wireless standards can be pushed for safety-critical systems under radio interference remains an open problem.

3.4 Summary of Open Research Problems

From the literature survey, it is clear that there has been substantial work performed in proving the performance of control solutions in wireless networked control systems. However, the question that remains is "**how well these control suggestions can work when implemented with the available wireless protocols?"** This section provides a summary of key findings from the literature review and lists the areas of open problems. An overview is given in Fig.3.5.

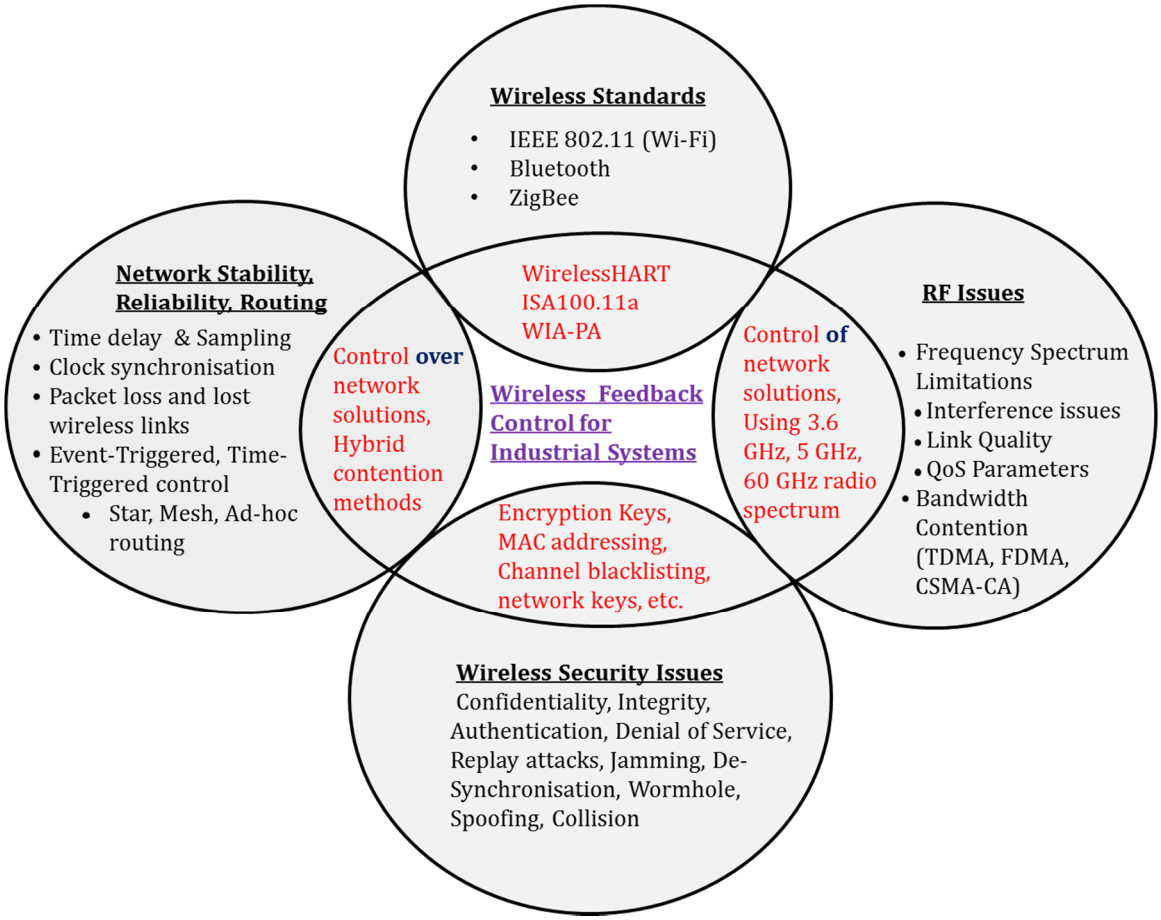

Figure 3.5: Summary of key findings and open problems

3.4.1 Lack of complete protocol for OSI layer

Many vendors follow the IEEE standard only at the PHY layer and define their own MAC and APP layer. This type of hybrid standard provides more versatility compared to the traditional wired standards. For instance, Wi-Fi follows IEEE 802.11b in all the eight layers, whereas WirelessHART and ISA100.11a follow IEEE 802.15.4 only at the PHY

layer and define different MAC and APP layers. This is one of the reasons they are ratified for industrial purposes. These standards define a TDMA approach at the MAC layer in addition to the traditional CSMA-CA of the IEEE 802.15.4. Defining their own APP layer enables the vendor to implement co-existence with their previous versions.

All the problems that are faced by IEEE 802.15.4 at the PHY layer are equally applicable for these standards. Again, having different protocols at each layer raises interoperability issues. Industrial usage is sometimes subjected to harsh RF environments, but this is not the case always. So there is a difference of opinion on using TDMA or CSMA-CA for bandwidth contention at the MAC layer. One point worth mentioning is that ISA100.11a utilises both these methods, but there are not enough results available of its performance on industrial control systems. So identifying a unique OSI protocol for mission-critical systems remains an open problem.

3.4.2 Network Architecture

Network architecture is an important issue when considering the stability of WNCS. Wireless networks are generally configured in three main topologies; star, mesh and tree as shown in Fig.3.6.

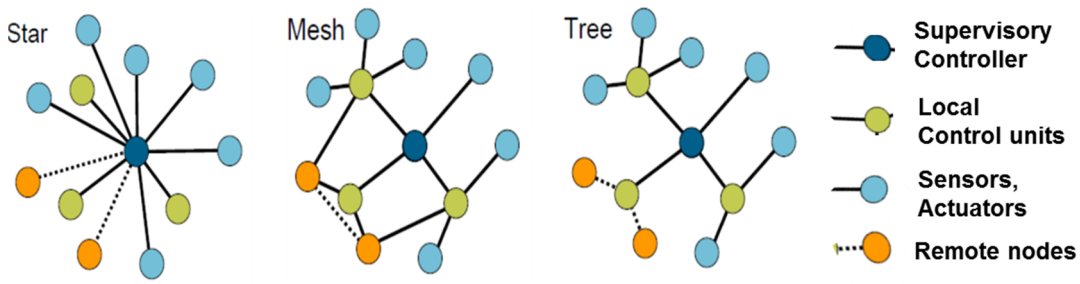

Figure 3.6: Wireless network architecture [Lau & Fuhr, 2014]

Star: It is a very simple architecture and managing the entire network is simple. Almost all the existing products in the wireless industry follow the star topology. While a star topology offers a simple and reliable wireless link, it has only a single route for communication.

Mesh: Mesh networking offers multiple paths for transmission between the sensor nodes and the gateway. Every node participating in a mesh network remains active, and they can transmit data to adjacent nodes as well as to the gateway. These networks are called multi-hop networks as such networks can provide a different route for transmission in the case of a link failure. However, the system becomes more complicated as the number of hops is unknown for a particular transmission.

Tree (Ad-hoc networks): This is an interesting architecture specifically addressed for wireless communication that follows a peer-to-peer network fashion. It is a decentralised architecture where nodes are connected in a distributed fashion. Ad-hoc networks offer mobility as nodes can enter or leave the network in a random fashion. If the network is battery-powered, there may be power constraints imposed on the network as new nodes join the network. However, it has an advantage over mesh networking in that all the nodes need not be active, thus saving power while the nodes are idle.

Summary: Wireless control applications may predominantly be based on a star topology as actuator and sensor node are connected to a single master (controller). However, they also have the potential to be implemented in a mesh/ad-hoc fashion depending on the application needs. Analysing these networks for a safety-critical environment is an active area of research and identifying a suitable topology still remains an open problem [Lau & Fuhr, 2014].

3.4.3 Power consumption issues and energy harvesting

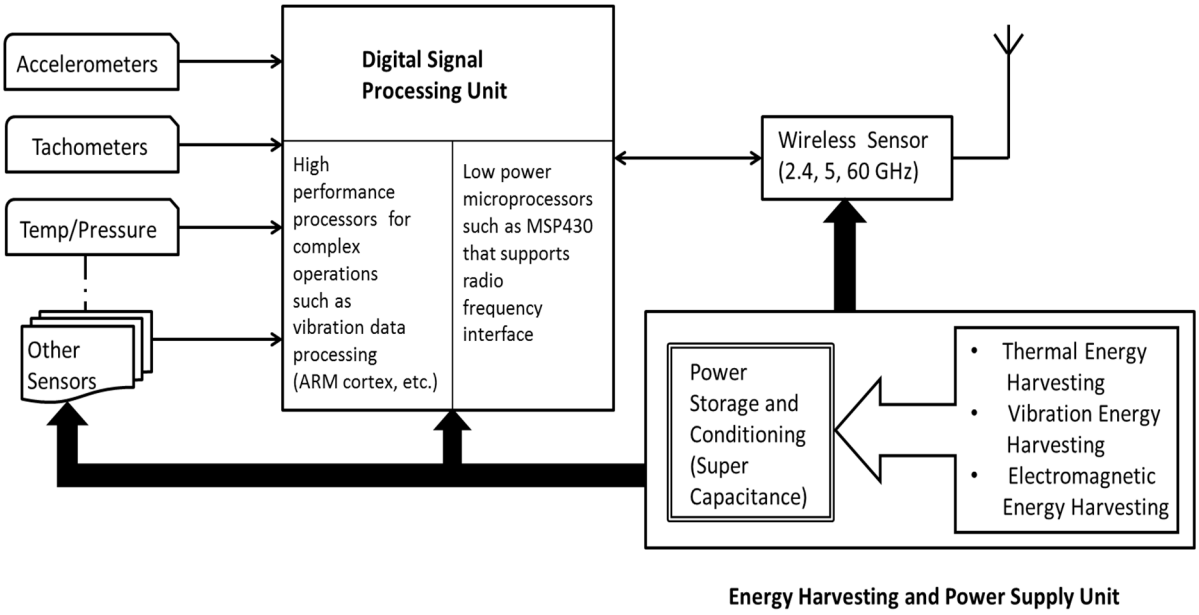

Figure 3.7: Energy harvesting in wireless closed-loop control

One of the key challenges in implementing wireless sensor networks on a full-fledged scale, especially in closed-loop control systems, is power consumption. Whilst wireless sensor networks are very flexible in terms of increasing the number of sensors in the network, there would be a substantial increase in the power consumption. For instance, the available power on board an aircraft is very limited and therefore, this puts a major limitation on utilising wireless communication for health monitoring activities in a wide scale. Wireless sensors have the ability to be used in remote areas; however, availability of

power source in remote locations becomes an issue. Therefore, there is a need to exploit alternate energy sources using energy harvesting techniques. Energy harvesting is an active area of research [Thompson, 2009] and there are various technologies to harvest energy from different sources. A methodology for energy harvesting and sourcing wireless sensors in a wireless closed-loop control setup handling various sensors such as accelerometers, tachometers, etc. is shown in Fig.3.7.

The potential energy harvesting techniques for wireless sensors include vibration energy harvesting, thermal energy harvesting and electromagnetic energy harvesting. Thermoelectric generators (TEG) can be used to harvest energy from hot areas such as engines and vibration energy harvesters could be used mainly in rotorcrafts (pitch link, mast). The electromagnetic energy harvesting may include both unintended and intended radiated electromagnetic sources. The harvested energy would be regulated and stored using super capacitors in a power conditioning circuit to power the wireless sensor. Depending on the data transmitted and the frequency, wireless sensors operation can be optimised to utilise minimum power.

Recently, the growth in the semiconductor industry has introduced low-power microprocessors that can have an RF interface. Power consumption is saved in these processors by utilising various functionalities such as sleep mode, wake up mode, etc. This property is further utilised in the design of the wireless hardware demonstrator in this research, and the corresponding RF power profile is explained in Section 4.5.4 in the next chapter.

3.4.4 RF issues and frequency hopping techniques

Wireless Standards	Frequency Hopping Techniques
IEEE 802.11(b/g)	Direct Sequence Spread Spectrum (DSSS)
IEEE 802.11 (a/g/n)	Orthogonal Frequency Division Multiplexing (OFDM)
Bluetooth	Frequency Hopping Spread Spectrum (FHSS) - 1600 times/sec
ZigBee	Direct Sequence Spread Spectrum (DSSS)
WirelessHART	DSSS (for each message transmission), FHSS (based on sequence of time slots - 1500 times/sec)
ISA 100.11a	DSSS, FHSS (Adaptive hopping), Channel Blacklisting
WIA-PA	Adaptive Frequency Switch (AFS), Adaptive Frequency Hopping (AFH), Timeslot Hopping (TH)

Table 3.8: Frequency hopping techniques

Frequency hopping is used by radio modules to hop between different frequencies to avoid interference. This provides reliable wireless links and enables fast data transmission. Wireless standards offer a range of frequency hopping and channel blacklisting techniques. In addition to this, wireless standards allow users to specify frequency agility protocols.

The analysis and performance of these techniques need to be explored further. A frequency diversity strategy is explained and implemented in the hardware demonstrator to enhance the ability of the system to switch channels quickly in Section 4.5.4. The wireless standards and their corresponding frequency hopping techniques are given in Table 3.8.

ISA100.11a supports slotted hopping between different time slots in the same superframe as well as between consecutive superframes whereas WirelessHART supports only the latter. ISA100.11a also supports slow hopping patterns for event-based data transmission and a hybrid between slotted and slow hopping algorithms (see Appendix C.2).

3.4.5 Network stability and reliability

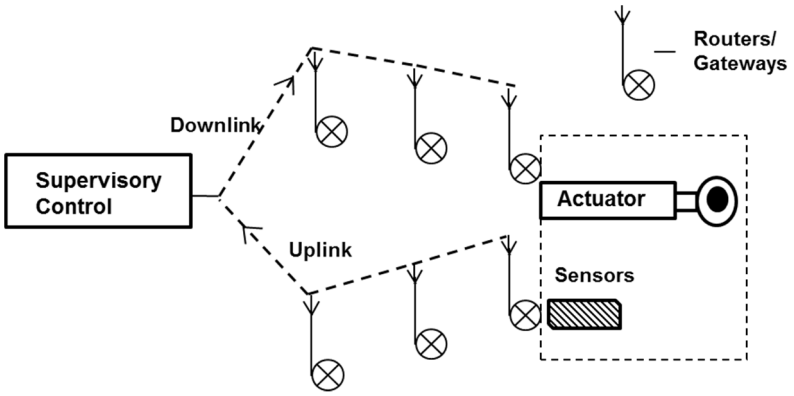

Figure 3.8: Link quality in wireless closed-loop control

One of the major concerns for a wireless networked control system is the reliability of the wireless links due to the uncertain nature of the wireless medium. While from a communication perspective, it affects the reliability of the network, from a controls perspective, deteriorating conditions of a network may render the wireless controlled system unstable. The reliability of a wireless networked control system is collectively addressed by the transport, network and data link layers of the OSI model. The link quality of a wireless transmission is categorised using uplink (data transmitted from sensors to the supervisory controller) and downlink (data transmitted from supervisory to actuators) streams in wireless closed-loop control as shown in Fig.3.8.

In IEEE 802.11 and Wi-Fi standards, the reliability is ensured at the medium access control part of the data link layer using two co-ordination functions known as point coordinated functions and distributed coordinated functions. WirelessHART enforces reliability of wireless links at the network layer and the data link layer. WirelessHART utilises the TDMA approach at the medium access control part of the data link layer to enforce a strict 10ms time slot for each wireless device in the network. The total payload in WirelessHART network is 159 bytes. (MAC payload is 133 bytes and ACK packet is 26 bytes). Given that the data rate of IEEE 802.5.4 networks is 256 kbps, the total

transmission time (t_{T_x}) for a single data packet in a WirelessHART network can be calculated as [Petersen, 2009],

$$t_{T_x} = \frac{159\ bytes}{256\ kbps} = \frac{1272\ bits}{256 \times 10^3 bits/s} = 5.088\ ms$$

Therefore, the time taken to transmit a data packet is well within the 10 ms time slot offered by WirelessHART for each node. It only takes 50% of the total time slot to transmit the data; nevertheless, the next wireless node should wait until the entire time slot is used up, which avoids issues due to data packets catching up the preceding packets, especially during time delay [Uchimura, 2009].

ISA100.11a offers the network reliability at both data link and network layers similar to WirelessHART protocol. In WirelessHART networks, the data link layer offered the communication reliability between neighbouring nodes whereas the end-to-end link reliability between two nodes across the network was determined by the network layer. However, in ISA100.11a, the data link layer ensures end-to-end delivery across neighbouring nodes in a given subnet up to the backbone network. Communication reliability beyond backbone networks (gateway, network manager, etc.) is taken care by the network layer. Lost wireless links and missed data packets are usually detected using acknowledgement (ACK) signals at the transport layer.

However, one major issue with WirelessHART and ISA100.11a is that out of IEEE 802.15.4's 15 channels (11 – 25) of the 2.4 GHz spectrum, around 12 channels overlap with the channels utilised by the IEEE 802.11 Wi-Fi devices. As WirelessHART and ISA100.11a devices have to co-exist with WLANs in an industrial setup, the reliability of the wireless links can be heavily impacted by the presence of 802.11 networks (Wi-Fi) and other sources of interference such as portable communication devices. ISA100.11a offers an additional channel 26 (optional) for operation clear of Wi-Fi interference. A more detailed analysis of the network layer, hopping patterns and transport layer function in handling network reliability is presented in Appendix C.

3.4.6 Control over Network issues

The issues mentioned in the preceding sections in turn contribute to various other significant problems in a wireless closed-loop control scenario such as,

- Co-design issues,
- Clock Synchronisation,
- Packet dropouts and Control stability,
- Time delay and Sampling rate issues

As the solutions are aimed at issues that arise when a control loop is closed over a communication network these solutions are termed as *Control over Network* solutions. The *Control over Network* solutions for addressing the communication induced issues such as synchronisation, congestion and interference that lead to packet loss, time-varying delay are subsequently investigated in Chapters 5, 6 and 7 respectively.

3.5 Summary

This chapter presented a comprehensive review of industrial wireless standards that are suitable for wireless closed-loop control applications. It presents a state-of-the-art analysis and a unique evaluation by comparing the functionality of the standards against each OSI layer. Therefore, it identifies the area of improvement with respect to each layer, which is essential to develop an application-specific protocol for critical control in future. Some of the key points arising from the overview presented in this chapter are:-

- Most of the research solutions on wireless networked control systems are concerned only with non-critical applications.
- Wireless standards addressed for industrial applications, such as WirelessHART and ISA100.11a, need more research analysis in order to extend them to safety-critical applications.
- Currently, the automation industry uses wireless technology, mostly for monitoring without involving any feedback loops.
- Most solutions are based on the assumption that the sensor nodes are tightly synchronised but this is not practically possible without an appropriate synchronisation mechanism.

Potential problem areas such as interference, network reliability and wireless security are highlighted, and some possible solutions are described. A summary of open research problems and key findings is presented finally. The key issues identified are taken for further investigation in the subsequent chapters.

Chapter 4

Design and Implementation of a Supervisory Wireless Real-Time Closed-loop Control System

This chapter presents the design considerations of implementing a wireless real-time closed-loop control on an embedded firmware. It is essential for the embedded processors to implement an efficient control strategy to monitor the timing of the sensing and control computations. Therefore, potential control strategies that can be applied for wireless closed-loop critical control are presented first followed by the design of a wireless embedded hardware demonstrator for wireless closed-loop control. A supervisory closed-loop control approach using a hybrid time-triggered and an event-triggered control strategy over a wireless channel is presented.

4.1 Embedded Control Systems

Performance of real-time control applications is impacted by features of the embedded control hardware and firmware being used such as memory, multithreading capabilities, timer accuracy, etc. Currently, a wide range of microcontrollers and microprocessors is available to implement real-time control algorithms. However, designing a cross framework between traditional processors and wireless medium in feedback control loops poses serious challenges in practical implementations. The Wi-Fi LAN cards installed in many applications are based on the assumption that the data packet loss is susceptible and acceptable [Ali, 2012]. Though problems introduced by processors are very minimal, at times issues such as memory leak, incorrect timer interrupts can cause significant issues in critical control applications. For instance, in a WLAN video or audio transmission, loss of data packets will not affect the quality of the received information significantly as long as the loss is kept under a certain limit. However, in a real-time application such as a feedback control loop, control action needs to be taken frequently based on the dynamics of the system being controlled. Therefore, even a small error will render the system unstable. In this sense, feedback control applications over a wireless channel are considered to be critical. Such applications cannot be handled by scheduling policy utilised by general-purpose operating systems due to the requirements such as time delay and jitter

limitation. Therefore, the control strategies must be executed as real-time tasks under a real-time scheduling policy [Liu, 2006],[Albertos, 2005].

In real-time control applications on embedded systems, the entire control operation is based on a microcontroller and other components handled by the embedded system. For instance, an aircraft fly-by-wire system consists of sensors such as LVDT's, inertial navigation units (INU), acceleration sensors, GPS units, etc. A processor is used to process the data from these sensors and control laws and send them to actuators in engine control units, ailerons, tail plane, etc. The timing of the sensors and actuators are crucial in deciding the control inputs. The INU for instance, outputs its measurements 1000 times per second whereas a pilot stick outputs its measurements only 500 times per second [Henzinger, 2003].

4.2 Control Strategies

While today's embedded processors are highly efficient to process many complex algorithms one important concern is power consumption. Depending on the control algorithm the microprocessor may have to perform unceasingly or go into sleep mode after completion of a task and until the next event. Several control strategies have been proposed in the literature [Pajic, 2012],[Arzen, 2006] to utilise the wireless network resources in an embedded platform in an efficient way.

4.2.1 Time-triggered control

In time-triggered control, a processor allocates individual time slots to the available tasks in a control application (see Fig.4.1). This provides smooth operation of the control process as it is ensured that each task in the control process is completed sequentially. Time-triggered control was predominantly used in the past in classical control systems where the control/actuation takes place based on sampling a continuous time signal with equal time period. The sensor sampling takes place on a fixed sample frequency, and the literature on sampled systems are based on the assumption that real-time firmware are able to guarantee these deterministic sampling time [Kopetz, 1993].

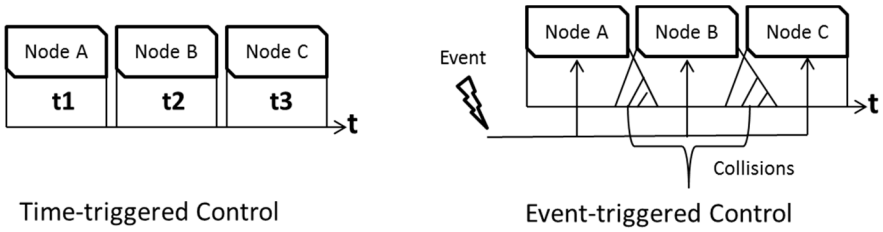

Figure 4.1: Time-triggered control vs Event-triggered control

Utilising time-triggered control in networked control systems will lead to guaranteed actuation/sensing events as no other process is allowed to intervene when a time slot is allocated to a particular node. Most of the industrial wireless standards offer the TDMA based contention method at the MAC layer which is a form of time-triggered control. For instance, WirelessHART offers strict 10 ms time slots for each node to transmit data and ISA100.11a offers a flexible time slot. The IEEE 802.15.4 offers the GTS (guaranteed time slot) mechanism in its contention free-period to offer the network nodes to transmit data exclusively. However, in networked control systems due to various issues such as time delay, jitter, synchronisation, etc. the deterministic assumption made by the time-triggered control systems may not be possible always. In addition, modern firmware and embedded platform are influenced by other tasks such as multi-threading and vast instruction pipelines, which may sometimes affect the regular interval at which the control/actuation is performed. In addition, time-triggered control consumes significant bandwidth as each node must be allocated with a time slot and if a particular node does not have anything to transmit, then the bandwidth is wasted.

4.2.2 Event-triggered control

In event-triggered control, a processor executes a task based on occurrence of a given event (see Fig.4.1). A control process that includes multiple events follows a pre-emptive priority scheduling to execute a task that has the highest priority. Based on the criticality of the algorithm, a task scheduler maintains the priority level for each task. In wireless networked control systems, event-triggered control is implemented such that the process is monitored for a change in the state at which the control input needs to be calculated. The advantages of an event-triggered system over a time-triggered system are as follows:-

- Event-triggered control systems offer better resource utilisation. As wireless real-time control systems are implemented using embedded microprocessors, utilising the central processing unit (CPU) time for various tasks is critical.
- Time-triggered systems utilise the CPU time for performing control calculations even if no significant change in control demand or system state has happened, however, event-triggered systems eliminate this issue by utilising the CPU resources only if an event occurs.
- In wireless closed-loop control systems, utilisation of network bandwidth should be optimal and reduced consumption of network resources results in reduced power consumption. As the number of control input transmission is reduced in event-triggered systems, this would further save the network resources.

However, if events are triggered randomly it may result in collision of data packets resulting in data packet loss as shown in Fig.4.1. In few applications, event-triggered control systems work based on a threshold of a system state to detect an event (such as the system state deviating from a desired behaviour). Therefore, there is more emphasis on tracking the threshold value at all times. This requires the processor that tracks the threshold value to be awake at all times and costs in terms of energy. In addition, the

scheduling of control, sensing and actuation tasks becomes difficult as the event is dynamically changing and is not known in advance.

In wireless control systems, deciding a suitable strategy depends on the need of the particular application and available computing resources. In general, event-triggered systems can be used in control applications with non-deterministic tasks whereas deterministic tasks can be executed using time-triggered strategies.

4.2.3 Self-triggered control

Self-triggered control is a model-based emulation of event-triggered control where the system instead of tacking a particular system state identifies certain time events at which the triggering condition is satisfied. Self-triggered control takes into consideration the plant model, the last received measurement of the system state and the overall performance of the system. The estimation of the timing events between two consecutive updates [Araujo, 2011] is given by,

$$T_i = t_{i+1} - t_i = \mathrm{g}(\mathrm{x}(t_i), S) \tag{4.1}$$

where T_i is the inter-transmission time, t_i is the time instant of the consecutive updates, g is the self-triggering function, $\mathrm{x}(t_i)$ is the last measurement of the state of the system and S is the acceptable control performance specification.

Self-triggered control offers the ability for the network scheduler to allocate the control, actuation tasks based on the time events. It also performs better than event-triggered control as it depends on the last received state measurement instead of tracking the system states at all times. However, self-triggered control concentrates more on transmitting the control demands based on the timing events. As it depends on the last received data for triggering the next control input estimation, it may not perform well if the data is lost or delayed in transit.

4.3 Design Issues in Embedded Wireless Control System

Wireless networked control for real-time control systems requires solutions for a number of crucial underlying technical issues. Wireless networking is currently an emerging technology for industrial applications, and it is used only for sensing and monitoring applications. There are various key issues that are yet to be addressed in implementing wireless networking in practical control applications. The main concerns relating to embedded system design are discussed in this section.

4.3.1 Interrupt handling

In real-time control applications, there may be multiple tasks that need to be serviced based on certain events. Interrupt Service Routines (ISR) are used for this purpose. These are based on an interrupt handling strategy wherein each task generates an interrupt when they need to be executed and the task that has the highest priority is processed. Whenever, an interrupt occurs, the processor finishes the current task and passes the control to the interrupt service routine. Once the ISR is completed, the processor resumes from the point where the execution is transferred. Sometimes, there is a possibility of multiple interrupt service routines that need to be serviced quickly. Therefore, a processor should have enough memory allocation to queue the interrupts and process them in real-time based on their priority and to avoid issues like interrupt latency. Any issues in interrupt handling will result in the control process being disturbed (see Fig.4.12 and discussion).

4.3.2 Clock oscillators

One of the major problems faced by real-time processors is clock inaccuracies. It is essential that clock oscillators in a processor provide accurate timing in order for all the scheduled tasks to be processed on time. Safety-critical control systems will pose stringent real-time deadlines for different tasks. Therefore, all the wireless nodes in the network must have a common understanding of time. Over time, clocks are subjected to drift and clock skew, and therefore, they may introduce jitter and latency in the processing cycles. Maintaining accurate clock timing using synchronisation algorithms is important for control applications. For wireless safety-critical systems, the frequency of synchronisation is important, as synchronisation messages occupy significant bandwidth if transmitted frequently (see Chapter 5 for more details).

4.3.3 Parallel processors

Execution of multiple tasks at the same time depends on the processors speed and memory allocation in real-time. In case of wireless control loops, demand and feedback information may be sampled very frequently. Therefore, a processor may have to respond to these interrupts and also maintain other important tasks such as executing the control algorithm efficiently. This may not always be possible in systems with a fast dynamic response. Therefore, parallel processors can be used to handle the tasks simultaneously and to offer multithreading capabilities. Though it increases cost and complexity of the process, it will improve the performance of critical control systems significantly. In general, real-time processors are known as Kernels in embedded systems that take care of thread synchronisation, computational processing and inter-process communication.

4.3.4 Real-Time Operating System

A real-time operating system (RTOS) is used to service processor requests in real-time eliminating the latency and delay involved in processing control tasks. It will reduce the processing delay in a network to a great extent as compared to traditional embedded programming. RTOS follows a scheduling policy such as rate monotonic, pre-emptive scheduling, earliest deadline first, etc. to allocate memory to various tasks and manage them. However, they increase the cost and maintenance of the control firmware. Real-time operating systems such as VxWorks, LynxOS are widely used for critical real-time embedded applications and in avionics software development [Hedlund, 2002]. However, features that support a wireless control process with tight real-time requirements are very limited.

4.4 Design Considerations for Wireless Real-time Control

Wireless sensor networks have been widely used in industrial applications over the last decade and are now reaching a high degree of maturity due to technological advancements in wireless standards. Many industries in process automation and chemical plants have adopted wireless sensors for monitoring temperature, pressure, flow rate, etc. However, utilising wireless in real-time closed-loop systems is less well developed. Few of the early experiments have been in non-critical and soft real-time systems such as building management and structural monitoring [Lynch, 2008].

Therefore, there is increasing interest to introduce wireless communication in high demanding industrial applications and fast dynamic systems. Many critical industrial domains such as aerospace and marine are seeking a fault-tolerant communication medium between stationary and rotational parts where wired connections are hard to reach. However, as discussed in Section 2.3, there is a need for an integrated design for wireless systems that can address the issues arising due to control, communication and computing. Such integrated design needs to incorporate an efficient controller and a fault-tolerant control methodology to keep the network stable during faulty conditions and to maximise the overall performance throughput of the wireless network. Therefore, the potential configurations for a wireless real-time control system that can address the above design issues in an industrial application are discussed in this section.

4.4.1 Supervisory wireless control

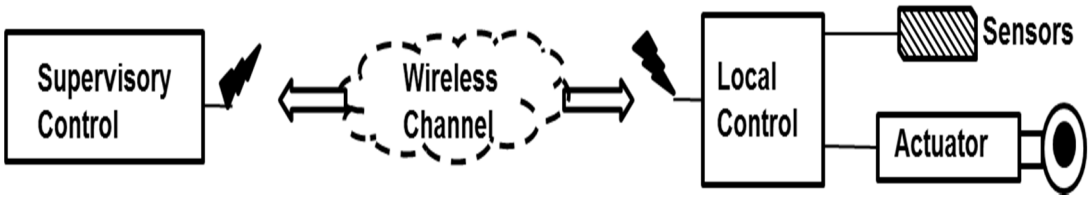

Figure 4.2: Supervisory wireless real-time closed-loop control system

Supervisory control is based on the wireless networked distributed control systems (WN-DCS) explained in Section 2.2.2. From a wireless real-time control design perspective, this approach uses a supervisory control unit that acts as the Master controller. The actuators and sensors associated to a given control system is managed by a local control unit as shown in Fig.4.2. The key aspect of this design approach is that the local control unit can keep the sensors and actuators synchronised using a global reference time. For instance, in an aircraft, a Flight Management System (FMS) acts as a supervisory control unit that receives the input demand such as those from the cockpit, and then estimates the control input considering various other parameters for a given aircraft operating stage such as taxiing, climb, cruise, approach and landing. The local control unit receives the control input and controls the actuator accordingly. The local control unit is also responsible to receive the sensor inputs and sends them as feedback information back to the supervisory control over the wireless channel. The advantage of this approach is that while a supervisory unit provides the adjustments to the control demands a local control unit can take control of the critical loops.

This approach is more suitable for critical control applications as this comes with an in-built fault tolerance. If the supervisory control fails or if the demand is lost over the wireless medium, the local control unit can control the actuator with the last received value and thereby keep the control system stable. The supervisory control is widely used in the industry for wired networks. It has even been tried out with a wireless Ethernet [Lu, 2014]. Therefore, the challenge now is to implement a Supervisory wireless closed-loop control system as discussed in this thesis.

4.4.2 Full feedback wireless control

Full feedback wireless control approach is when the supervisory controller directly controls the sensors and actuators over the wireless channel without any local control units (see Fig.4.3). This is a less common approach; however, the main interest is in aerospace applications due to the significant reduction in overall weight as the local controller is removed. However, it loses the fault tolerance the local control unit offers and therefore, the supervisory control seems to be more robust to handle any faults or failures. The

configuration is quite difficult to implement from a feedback control loop perspective, as packet loss and time delays are possible in both sending demand and receiving feedback information. To complicate things, synchronising the sensors and actuators with a global time reference is difficult to achieve. Therefore, it is possible for data samples to be skewed with respect to the status of the plant. However, due to its flexible architecture, multiple supervisory units can be used that can interact and share data with each other as discussed in the WN-DeCS (Section 2.2.3). This could offer benefits in aircraft test beds and maintenance works.

Figure 4.3: Full feedback wireless real-time control system

4.4.3 Wireless real-time closed-loop control

The next step in this research area is to design a wireless control loop for systems that have tight real-time constraints. There is a need to explore the possibility of transmitting both the control data and feedback over the wireless channel simultaneously. ISA100 has listed three ways of introducing wireless communication in an Industrial wireless real-time control system.

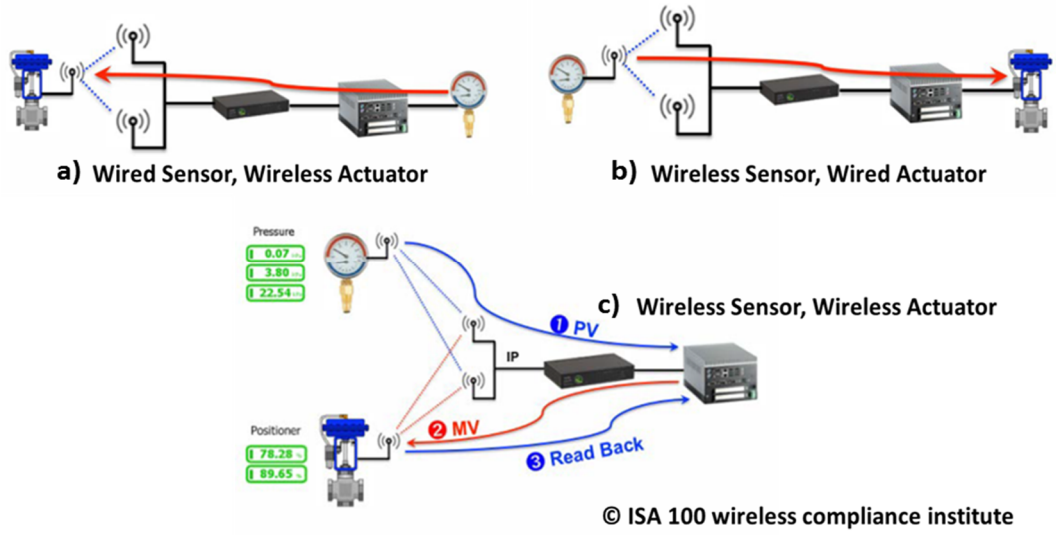

Figure 4.4: Wireless real-time control systems [Werb, 2012]

Wired Sensor, Wireless Actuator: See Fig.4.4(a). In industrial environments the wireless sensor measurements can be interrupted due to high interference. Therefore, the sensor interface could be wired and the actuator is controlled over a wireless network.

Wireless Sensor, Wired Actuator: See Fig.4.4(b). The sensor data is sent over the wireless channel while the actuator is controlled using a wired interface (Wireless monitoring).

Wireless Sensor, Wireless Actuator: See Fig.4.4(c). In this control approach, both the sensor data and the actuator are controlled over a wireless channel.

Traditional solutions for controlling motors and actuators using a wireless channel are done by transmitting a signal at a particular frequency. Based on the received signal the receiver takes a control action. However, transmitting the actual control demand over a wireless channel remains an open research problem due to the unreliable nature of the wireless network. Most of the available solutions have either the sensor or actuator wired due to various resource constraints.

In this work, a supervisory control approach is implemented. A supervisory controller handles the control algorithm while a local control unit is used to manage the sensor and actuators. In addition, a wireless sensor, wireless actuator interface similar to Fig.4.4(c) is implemented such that both the demand and feedback are sent over the wireless channel. The feedback is sent on time slots based on time-triggered control while the demand is sent based on occurrence of feedback data (event-triggered control).

4.5 Design and Implementation

In order to represent a real-time control system, the speed of a brushless DC motor is controlled over a wireless channel representing a wireless closed-loop control system. A brushless DC motor is a typical component in safety-critical and real-time control systems in the automation industry. For instance, in an aircraft environment, DC motors are used in flight controls, utility actuation, to name but a few. The brushless DC motor is modelled as a discrete-time state space model for the wireless real-time control system.

4.5.1 Modelling of Brushless DC (BLDC) motor

Nomenclature:

θ_m	=	Rotor position	(rad/sec)
ω_m	=	Rotor speed	(rad/sec)
i_a	=	Armature current	(A)
V_a	=	Input voltage	(volts)
R_a	=	Armature resistance	(ohms)
L_a	=	Armature inductance	(mH)
J	=	Inertia of the motor	(kg-m^2)

T_L	=	Load torque	(N-m)
T_{em}	=	Electromagnetic torque	(N-m)
K_t	=	Torque constant	(N-m/A)
K_e	=	Back EMF constant	(V.s/rad)
b	=	Damping coefficient	

Motor Parameters:

Motor Type	: Brushless permanent magnet motor
Number of pole pairs	: 4
Back-emf Constant	: 0.21 V.s/rad
Synchronous Inductance	: 5.0 mH
Phase resistance	: 1.8 Ω
Motor Inertia	: $4.9 \times 10^{-5} kgm^2$

The BLDC motor is modelled as a discrete-time state space model. The system states are $x_1 = \theta_m, x_2 = \omega_m, x_3 = i_a$.

Phase Voltage,
$$V_a = R_a i_a + L_a \frac{di_a}{dt} + E \tag{4.2}$$

Electromagnetic Torque,
$$T_{em} = J \frac{d\omega_m}{dx} + b\omega_m + T_L \tag{4.3}$$

Rotor Speed,
$$\dot{x}_1 = \frac{dx_1}{dt} = \frac{d\theta_m}{dt} = \omega_m = x_2 \tag{4.4}$$

$$\dot{x}_2 = \frac{dx_2}{dt} = \frac{d\omega_m}{dt} = \frac{T_{em}}{J} - \frac{T_L}{J} - \frac{b\omega}{J} \tag{4.5}$$

$$\dot{x}_3 = \frac{dx_3}{dt} = \frac{di_a}{dt} = \frac{V_a}{L_a} - \frac{E}{L_a} - \frac{R_a i_a}{L_a} \tag{4.6}$$

Solving (4.4),(4.5),(4.6), the state space representation of the DC motor is given by,

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & -\frac{b}{J} & \frac{K_t}{J} \\ 0 & -\frac{K_e}{L_e} & -\frac{R_a}{L_a} \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & -\frac{1}{J} \\ \frac{1}{L_a} & 0 \end{bmatrix} [V_a \quad T_L] \tag{4.7}$$

The pseudo code of the control algorithm implemented is given in Fig.4.5. A hybrid time-triggered and event-triggered control strategy is implemented for an efficient control process. A time-driven feedback data sampling ensures sensing data is captured at regular intervals. An event-driven strategy is used for controller action (sensor feedback acts as event) as well as for actuation (control input acts as event). Event-driven strategy helps in reduced power consumption at both the supervisory unit and the local control unit.

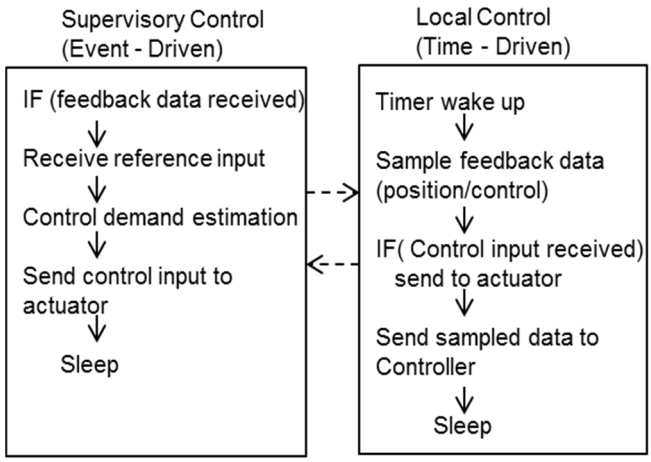

Figure 4.5: Wireless control – Pseudo-code

4.5.2 MATLAB Simulink Model

For the simulation model, the Truetime networked control system simulation tool [Henriksson, 2006] is used to design the wireless network and the controllers. Truetime is a MATLAB/Simulink based simulation tool that can be used to simulate wireless networked control systems. The Truetime kernel is used as the supervisory and local control unit (see Fig.4.6). The IEEE 802.15.4 radio option is used for wireless transmission. It offers a data rate of 256 kbps. The sensor, actuator and control nodes are tightly synchronised using a sampling interval based clock synchronisation algorithm as explained in Chapter 5.

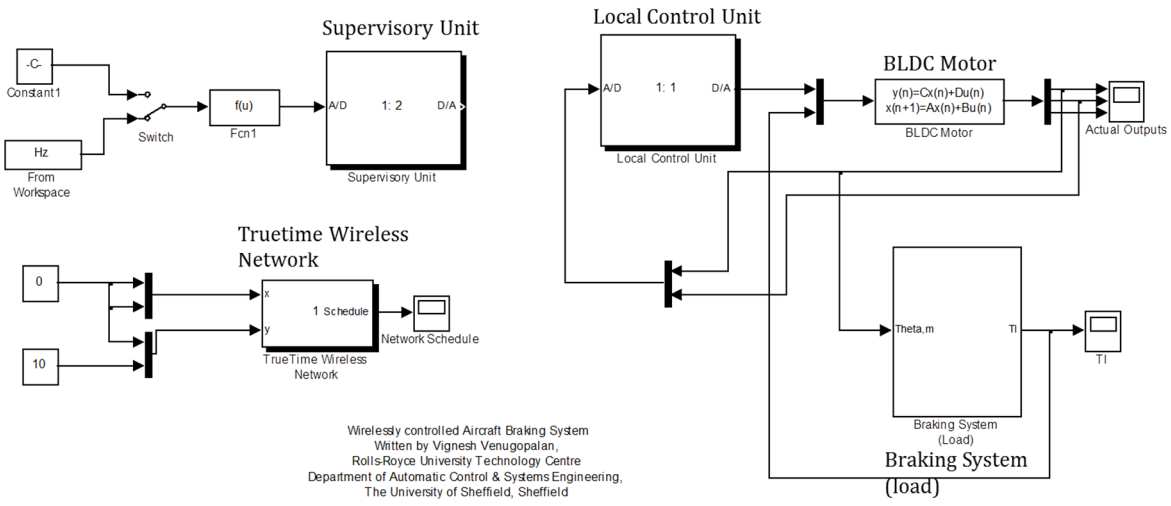

Figure 4.6: Truetime simulation model

In order to have a robust control strategy, a cascaded position and speed PID controller is used to decide the control input to control the Brushless DC (BLDC) motor (see Fig.4.7).

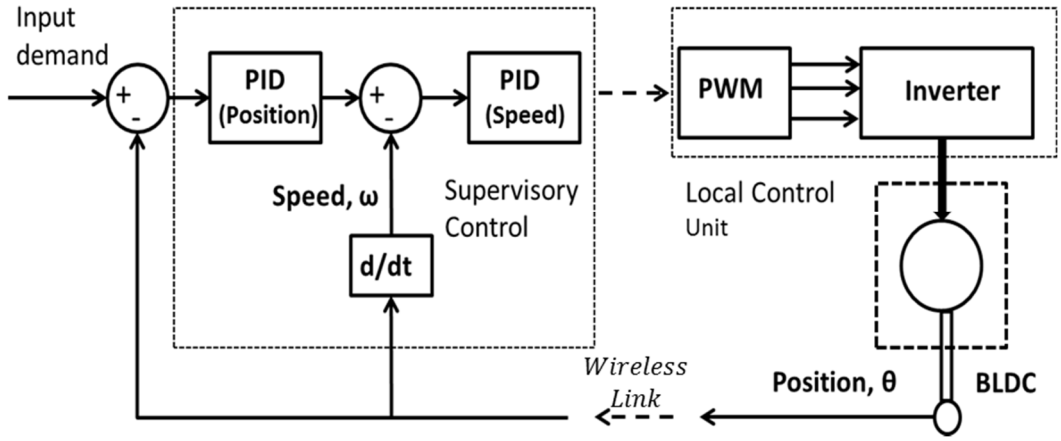

Figure 4.7: PID Controller block diagram

Many existing industrial processes are controlled using PID controllers [Åström and Hägglund, 1995] and optimising the performance of PID controllers on embedded systems is an active research area. PID stands for proportional-integral-derivative control. The PID controller is implemented according to the following equations:-

$$P(k) = K_p.\left(y_{sp}(k) - y(k)\right) \tag{4.8}$$

$$I(k+1) = I(k) + K_i\left(y_{sp}(k) - y(k)\right) \tag{4.9}$$

$$D(k) = D(k-1) + K_d\left(y(k-1) - y(k)\right) \tag{4.10}$$

$$u(k) = P(k) + I(k) + D(k) \tag{4.11}$$

$P(k)$ is proportional control term, $I(k)$ is integral term, $D(k)$ is derivative term, y_{sp} is set point, y is feedback, K_p is proportional constant, K_i is integral constant, K_d is derivative constant, $u(k)$ is the control input and k is the time instant.

The PID controller is tuned using the eqns. (4.8), (4.9) and (4.10). The position controller gains are chosen based on trial and error such that K_p=90, K_i=200, K_d=3.5. The speed controller gains are chosen such that K_p=0.0005, K_i=3, K_d=0.

The position and speed of a three phase BLDC motor are controlled over the wireless channel. The network schedule of the wireless control system is shown in Fig.4.8. Every module (sensor, actuator and controller) is raised to a high whenever it is scheduled to transmit or receive. As soon as the transfer is completed the module is put to low. The time taken between the start of sensor task and the start of controller task is the actuator-controller time delay (t_{ac}) and the time delay between the completion of the controller task and the start of actuator task is the controller-actuator time delay(t_{ca}). Together they contribute to the round trip time delay(t_{rtd}). The sensing is time driven, and therefore, the sensing is done periodically at 5 ms (200 Hz). The sampling interval is chosen based on the simulation model and the best sampling interval possible between the various tasks (sampling, actuation, scheduling, etc.) managed by the network scheduler.

As shown in Fig.4.8, the controller action follows after successful reception of sensor data and then the control input is transmitted over the wireless channel for actuation. The actuation is completed before the next sensing task. Thus a tightly coupled deterministic behaviour is implemented in the wireless closed-loop control system. The position response of the BLDC motor with time delay bounded by the sampling interval is shown in Fig.4.9.

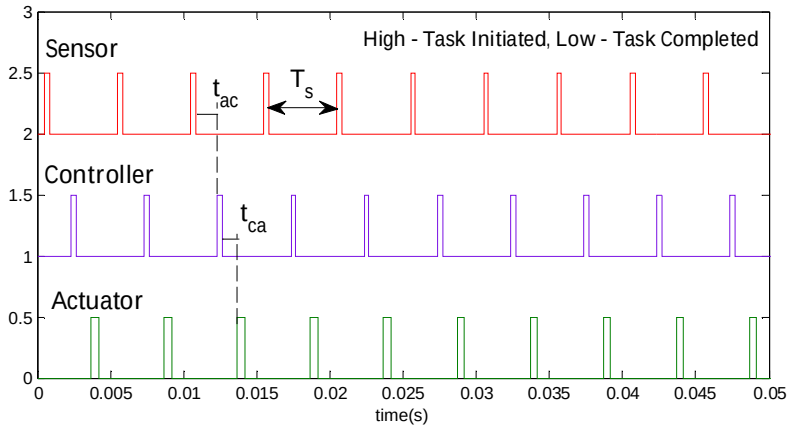

Figure 4.8: Wireless closed-loop control - Network schedule

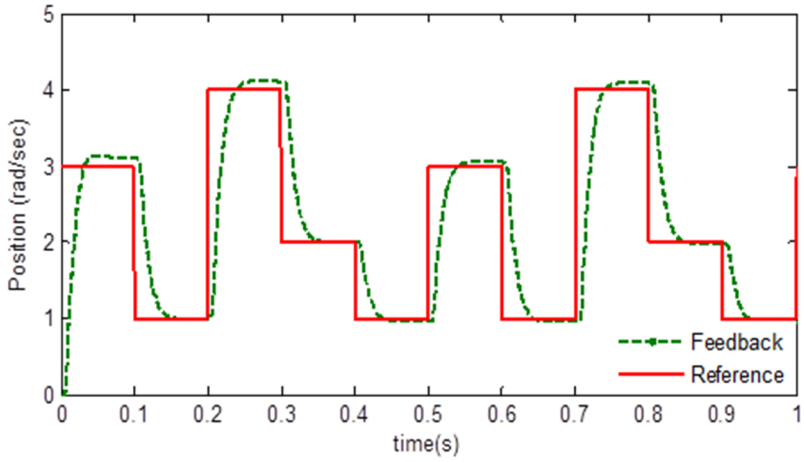

Figure 4.9: Wireless closed-loop control performance – Position profile

4.5.3 Wireless hardware demonstrator

This section explains the design of the hardware demonstrator implemented in this research work. The choice of the design framework is based on the issues explained in the previous sections and the commercially available hardware units. The hardware implementation is based on a distributed networked control strategy. In order to

experiment the performance of a wireless control loop, there is a need for a control system that would exhibit the features of a real-time control system in a lab environment.

The aim of this section is to implement a supervisory wireless control algorithm on a low-cost low-power microcontroller and use minimal hardware so as to control a BLDC motor over a wireless channel. In addition, such a system should have a wireless interface to test the wireless feasibility in the control loop. Servo control systems that are available in the market are standalone Commercially-off-the-shelf (COTS) modules. However, they lack a wireless interface or any feature for transmitting data across a wireless medium. So the research needs a servo system that can efficiently perform the control process as well as offer a wireless interface. Another concern is to decide the suitable parameters that can be transmitted over a wireless channel.

Actuator: A Brushless DC motor is used as actuator. Brushless motors are usually controlled using an electronic controller. Based on the commutation sequence of the motor generated by Hall sensors/encoder unit, the controller decides the voltage to be applied to the 3 phase windings of the motor.

Inverter: Brushless DC motors are commutated using electronic controllers. Various control strategies are used to generate the correct voltage for the phase windings of the motor. In this application, a Pulse Width Modulated (PWM) controller is used to control the speed of the motor. A PWM controller outputs a duty-cycle waveform based on the commutation sequence of the motor. The duty cycle waveform controls a 3-phase H-Bridge inverter using the upper modulation technique. According to the upper modulation technique, the top three transistors of the 3Ø H-Bridge Inverter is controlled using the duty cycle of the PWM waveform while the lower three transistors are controlled using the ON-OFF sequence of the waveform. By controlling the duty cycle of the PWM waveform, the speed of the motor is controlled.

4.5.4 Wireless protocol

TI's CC2500 radio units [CC2500, 2014] are used as wireless transceivers in this application and are representative of typical low-power COTS available RF transceiver modules that will operate in the license-free ISM frequency spectrum. The radio follows the direct sequence spread spectrum (DSSS) for modulation and works in the 2.4 GHz frequency band. The RF module is capable of a theoretical peak data rate of 256 kbps inclusive of overheads. It should be noted that, in this particular configuration, the effective 'payload' data rate is actually closer to a quarter of that claimed figure. It offers clear channel assessment (CCA) at the MAC layer and cyclic redundancy check (CRC) for error correction.

The SimpliciTI wireless protocol [SimpliciTI, 2014] from Texas Instruments is used for managing the radio operations by the CC2500 module. SimpliciTI is aimed at small RF networks based on the MSP430 microcontrollers and the CC2500 transceivers. It is a TI proprietary low-power RF protocol that enables the microcontroller units (MCUs) to enter into sleep mode when a transmission/reception is completed. SimpliciTI offers both star with extender and p2p (peer-to-peer) topology. The star topology is used in the design of the wireless hardware demonstrator. SimpliciTI uses MRFI[3] at the PHY layer and a well-defined network layer to handle the Rx and Tx queues.

As SimpliciTI is an open-source protocol, it offers user-defined optimisation at the Application Programming Interface (API) as well as handling the data packets at the network layer. For this demonstrator, configuration of the low-power wireless network protocol has been examined in detail to optimise its performance and fault-tolerance through systematic link Quality-of-Service (QoS) management. Techniques used in this work include:-

- modulating radio output signal strength to address attenuation
- data redundancy and error correction techniques to address packet error
- message receipt acknowledgement scheme to address lost messages
- frequency diversity to mitigate external interference
- antenna diversity to mitigate multipath (scatter) issues

Frequency Diversity: A frequency hopping strategy is implemented to enhance the ability of the system to switch channels quickly if and when there is a connectivity issue between master and slave nodes. This is triggered by the master when it experiences channel congestion "noisy" based on a specified listening period before it transmits anything (based on SimpliciTI's built-in network stack). By default, every node before transmitting will listen briefly, then if necessary, will back-off for a small random period when the channel is not clear to send. Hence, after a number of repeated back-offs, the master will switch channel to the next channel in a pre-specified list of channels that are optimised to avoid commonly used Wi-Fi channel bands. Master node broadcast a "channel hop" instruction to each slave, so if they are listening, they will switch channel immediately then resume communications. Otherwise, if slaves find they cannot re-establish with their master due to a poor channel, they automatically "roam" a channel list to re-establish with their master. Internally, nodes store their messages in a queue (of limited size) so they are able to transmit again once the connection is re-established. In addition, it will be useful to timestamp each message with the transmission time if longer link downtime is expected. This is implemented using a suitable clock synchronisation algorithm (see Chapter 5).

An example of an efficient power profile for a single wireless transmit cycle that averages around 10mW for 2.4 GHz RF (CC2500 radio chip) with 100m Line of Sight (LoS) range is shown in Fig.4.10. It shows the different stages of the CC2500 radio chip's power

[3] MRFI – Minimal Radio Frequency Interface

consumption while transmitting or receiving data over the wireless channel. It can be noticed (yellow line) the radio chip consumes a maximum of 31 mV during transmission (6) and lesser than that during reception (9). The rest of the time the power consumption is very low (1,12) as the radio chip is put into sleep mode thus saving power.

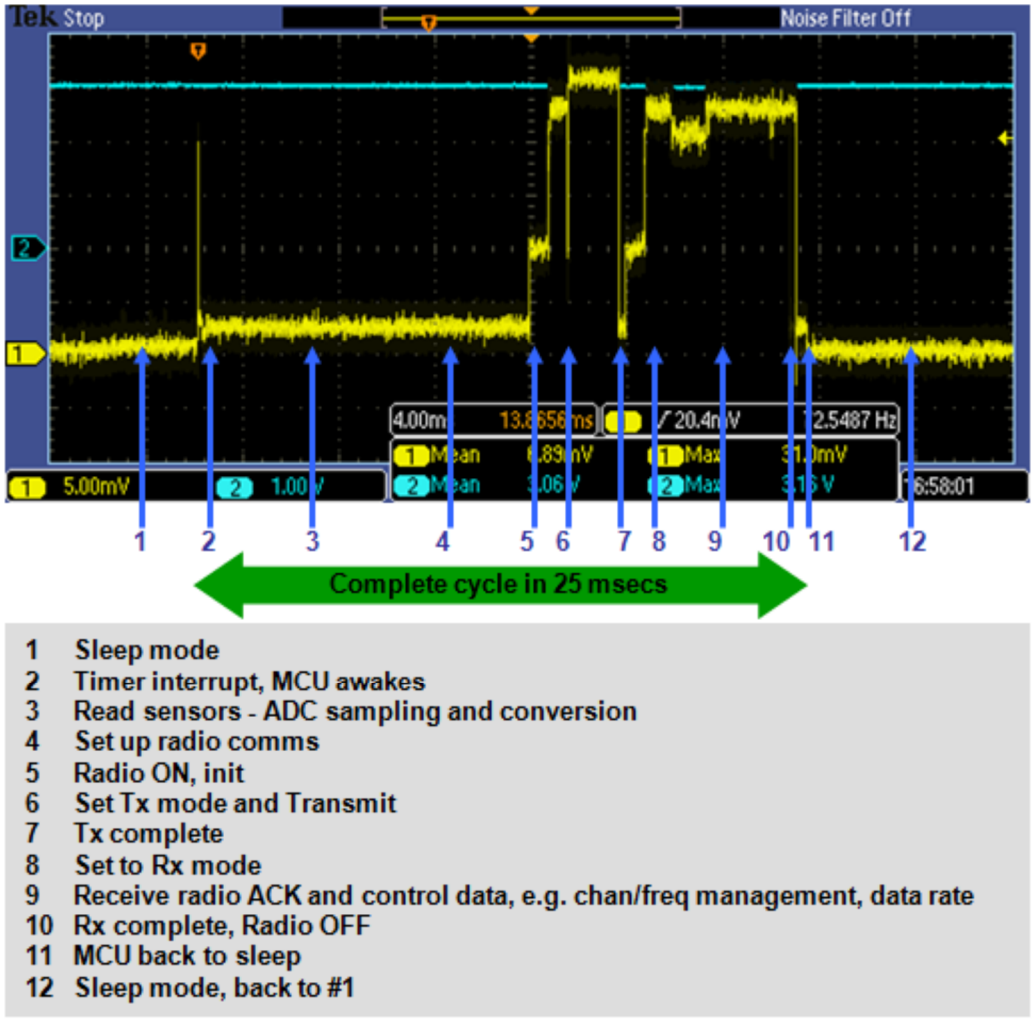

Figure 4.10: RF2500 power profile [Ong, 2011]

4.5.5 Block diagram and Processor design

The block diagram of the proposed wireless real-time control system is shown in Fig.4.11. A supervisory unit is used as a master that sends the control demand over the wireless channel to a local control unit. The local control unit receives the control demand and controls the speed of the BLDC motor accordingly. The local control unit also computes

the feedback information based on the Hall sensor inputs and sends the feedback information back to the supervisory unit over the wireless channel.

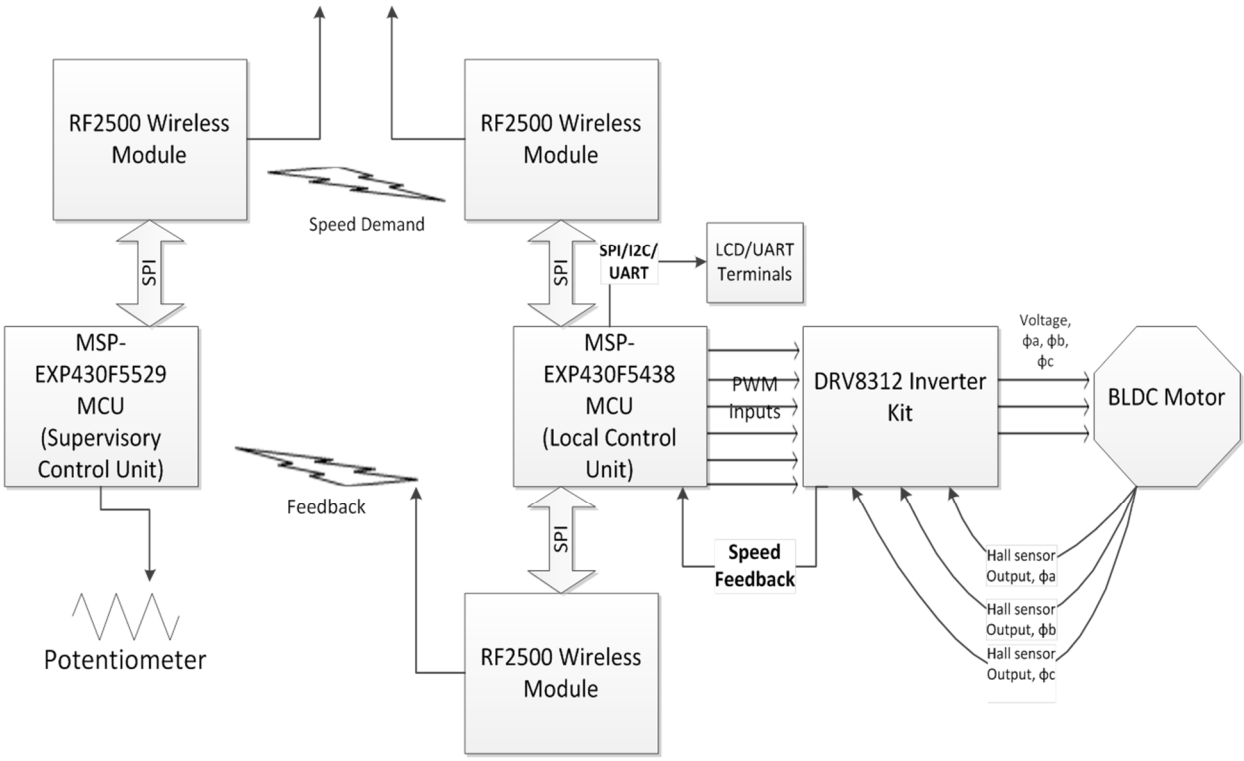

Figure 4.11: Wireless real-time control – Block diagram

The processor used in the experiment was chosen such that it can handle the following functions:-

- The motor control algorithm to generate PWM signals to control the 3φ inverter
- Deal with the radio hardware units for both receiving the speed demand and sending the feedback information.
- Handle multiple interrupts such as those from Hall sensor units, ADC units, etc.

In order to handle such tight real-time demands the MSP430F5xxx series microcontrollers [MSP430x5xx, 2013] from Texas Instruments is used. A DRV8312 inverter and associated power electronics, and a NEMA 17 BLDC motor are used for servo-motor control. Hall sensor outputs available from the BLDC motor are used as feedback signals to form a closed-loop control system. An over-current protection circuit is implemented along with the DRV8312 inverter which is an important feature in control of servo motors using embedded systems.

Supervisory control unit:

A supervisory control unit using the MSP430F5529 series microcontroller is utilised to implement a closed-loop control algorithm using a PID controller. The F5529

microcontroller unit is implemented such that it can take the input demand using two interfaces,

- From a potentiometer using an ADC interrupt service routine (analog).
- From the LabVIEW GUI interface using the UART commands (digital).

In addition, the microcontroller unit (MCU) handles the CC2500 radio modules using timer-based interrupt service routines. The SimpliciTI wireless protocol is implemented in the MCU along with the PID control algorithm. The MCU receives the input speed demand using the ADC/UART interfaces and then transmits over the wireless channel using the CC2500 radio units. The ADC interrupts are handled by the processor using a threshold value based on the input demand. The embedded pseudo code for the supervisory control unit is given below:

```
MCU_Init();                              //Initialise microprocessor
__interrupt Timer :: readInput();        //ISR to read input demand
MRFI_Receive();                          //Radio packet received
__interrupt Event :: receiveFeedback();  //ISR to process the data packet
computeControlinput();                   //Calculate control input
MRFI_Transmit();                         //Radio packet transmitted
MRFI_Sleep();                            //MCU put to sleep (saves power)
```

Local control unit:

A local control unit using the MSP430F5438 MCU is implemented separately to handle the algorithm to control the BLDC motor. The local control unit handles the following functions:-

- It sends the PWM signals waveforms to the DRV8312 inverter using PWM module and GPIO pins.
- F5438 MCU handles the reception of control input demand, and the transmission of feedback data (speed) measured using the Hall sensors back to the supervisory unit over the wireless channel.

The F5438 handles the motor control algorithm along with the SimpliciTI protocol using event-based interrupt service routines. As Hall sensor events are asynchronous events, a separate interrupt service routine is triggered every time a Hall sensor event is received. Therefore, three separate GPIO pins in F5438 MCU are configured as hardware interrupt pins. In the associated software interrupt service routine, based on the rising and falling edges of the Hall events, the speed of the motor is calculated. It will then be transmitted to the supervisory unit using the CC2500 units.

In addition, whenever a speed demand is received the radio interrupt service routine is triggered based on the hardware interrupt pin configured for the CC2500 units. The embedded pseudo code for the local control unit is given below:-

```
MCU_Init();                              //Initialise microprocessor
MRFI_Receive();                          //Radio packet received
__interrupt Event :: receiveDemand();    //ISR to process the data packet
__interrupt Timer :: commutateMotor();   //PWM signal processing
__interrupt Event :: readHallsensor();   //ISR to read Hall events
computeSpeed();                          //Calculate speed feedback
MRFI_Transmit();                         //Radio packet transmitted
MRFI_Sleep();                            //Radio unit put to sleep (saves power)
```

Fig.4.12 shows the issues in utilising a single microcontroller in handling the motor control algorithm and radio units. The purple and green line shows the PWM inputs (only Phase A and B is shown for clarity) to the motor. It can be noticed that after a speed demand is received (blue line) via the CC2500 radio units, the PWM outputs stall for some time before it can activate the motor windings. The ISR of the SimpliciTI protocol freezes the F5438 MCU for other processing when a radio packet is transmitted or received to ensure robustness. Though the wireless reception takes less than 3ms to complete, it takes 125 ms for the motor to resume normal operation from a radio interrupt service routine.

Figure 4.12: Control timing analysis – single processor

Therefore, every time a radio packet is received the motor blips for a certain duration which is highly undesirable. This is due to the fact that the radio interrupt event overlaps with the Hall interrupt event and hence disturbs motor commutation sequence. As this sequence gets disturbed during the wireless transmission, it takes 125 ms (to get the hall events correct again) for the MCU to set the motor running again. The following observation was made from the behaviour of the designed embedded wireless control system:-

- The microcontroller unit (MCU) in the Supervisory controller was able to handle both the control algorithm and the radio transmission. This is due to the timer-based ISR's where the control input estimation and the radio transmission happen in separate fixed time slots.

- However, the MCU in the local control unit that handles the PWM control process ran into interrupt latency. This is due to the event-based ISR's where the MCU has to respond to a radio interrput service routine (which happens when a data packet is received) in-turn disturbs the Hall sensor events.
- It should be noted utilising a timer-based ISR in the local control unit would keep on polling the radio interface for new data packet leading to increased power consumption.
- Therefore, while wireless standards can support sensing and monitoring activities (predominantly a time-triggered activity) using the same MCU, the same will not be possible in a closed-loop control setup.
- Therefore, there is a need for parallel processors in wireless real-time control systems where a separate MCU is used to handle the radio operations while the control algorithms are handled by another parallel MCU in-order to ensure reliability.

Parallel Processor:

In order to overcome the issues faced with single processor, in the designed wireless real-time control system, separate RF2500 wireless module is used in the local control unit to handle radio transmissions which in-turn sends the input demand to the F5438 MCU. Therefore, the SimpliciTI wireless protocol is now handled by the RF2500 module which has an in-built F2274 MCU. The motor control algorithm, hall sensor events, feedback calculations are handled by the F5438 MCU. The control performance using parallel processors is shown in Fig.4.13.

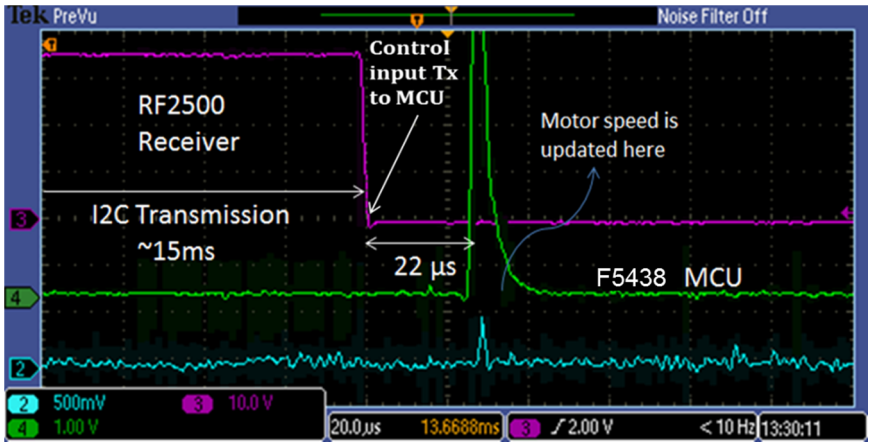

Figure 4.13: Control timing analysis – parallel processor

The purple line shows the timing response of the RF2500 receiver which uses the I2C protocol to transmit the received control demand to the MSP430F5438 which uses it to calculate the PWM signals. The I2C transmission takes around 15ms to transmit the received data to the F5438 MCU. It takes a further 22 µs to update the PWM duty cycle. On a whole, it takes less than 20ms to control the speed of the motor. Also there are no sudden blips between the speed update, and it happens gradually as the radio operation and

PWM regulation is handled separately by the parallel processors. The parallel processing offers another advantage due to the fact that the RF2500 modules can go to sleep mode after the radio packet is received thus saving power.

The highlights of the designed wireless hardware demonstrator are as follows:

1. An MSP430F5529 board was used in the supervisory unit in order to implement the PID controller and other control algorithms to address network stability and reliability issues.
2. A CC2500 radio unit is utilised by the F5529 MCU in supervisory unit to process the radio operations (control demand transmission and feedback reception).
3. A separate MSP430F5438 MCU was used in the local control unit to regulate the PWM process and the motor control.
4. Two separate radio modules using RF2500 is used to process the radio operations (control demand reception and feedback transmission) in parallel to the MSP430F5438 board in the local control unit.

4.5.6 Hardware implementation

The supervisory wireless control process explained in Section 4.4.1 is implemented in the wireless real-time control hardware. In real-time control, the demand and the feedback data must be sent instantaneously. Any delay could make the system unstable. Therefore, separate wireless radio modules are used in the local control unit, one to receive the speed demand and another to feedback the actual speed of the motor. As a fail-safe measure and to overcome lost control demand inputs, the two wireless modules act as masters to the local control unit. In case of a lost wireless link at the local control unit, the wireless module will retain the last demand value received and will run the motor in a default condition until the connection is re-established. In this state, the hardware framework will behave as a decentralised control system.

The MSP-EXP430F5529 board is used in the supervisory unit which would take the user demand input using the potentiometer unit/LabVIEW interface, and a PID control algorithm is implemented in the supervisory unit. The MSP-EXP430F5438 board is used in the local control unit to handle the PWM regulation and the reception of control demand input from the radio modules. Hall sensors are used to sample the speed of the BLDC motor. It is also responsible for calculating the speed information from the Hall sensors. Two RF2500 modules are used at the local control unit for radio transmission, one to receive the demand and the other one to feedback the speed data as shown in Fig.4.14.

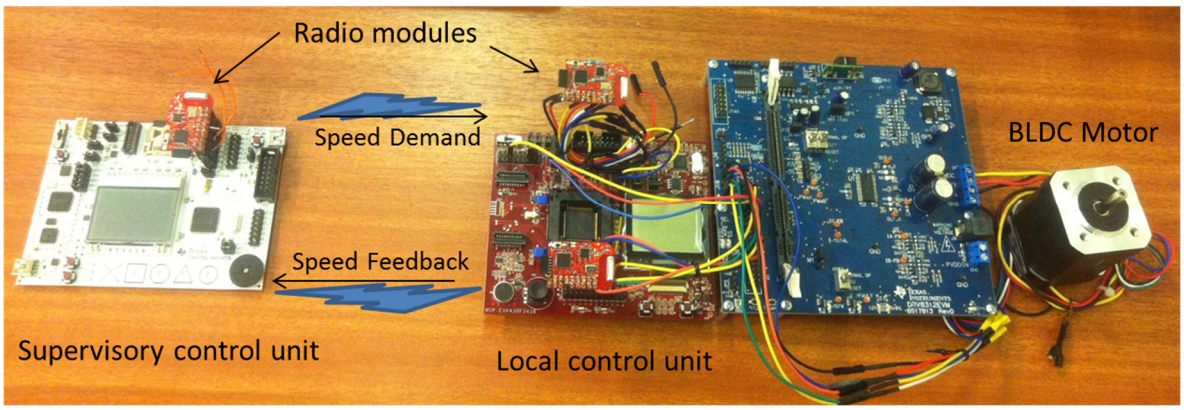

Figure 4.14: Wireless real-time control – Hardware implementation

4.5.7 Wireless control algorithm

Fig.4.15 shows the flowchart of the wireless speed control algorithm that is used to control the BLDC motor. Speed demand was sent across the wireless channel in terms of the PWM duty cycle. The sender and the receiver radio module are configured to send and receive the data packets using separate interrupt service routines. The data is then sent to the local control unit, which in turn updates the PWM duty cycles sent to the inverter. Thus the speed of the BLDC motor is controlled. For results and analysis purpose, in addition to the potentiometer, a LabVIEW communication interface has been implemented to plot the speed data in real-time. The speed demand (in rpm) is given using the LabVIEW interface. A co-design of the control strategies explained in Section 4.2 is used to implement the control algorithm.

- An event-triggered protocol is used at the supervisory control unit which on reception of the feedback data calculates the control demand and transmits using the radio interface.

- A time-triggered protocol based on the MCU timer is used to sample the speed information at the local control unit and transmit it over the wireless channel.

- The local control unit regulates the PWM cycle as soon as the control demand from the supervisory control unit is received.

Thus a hybrid time-triggered and event-triggered protocol is utilised to implement the wireless closed-loop control algorithm for maximised efficiency and robustness.

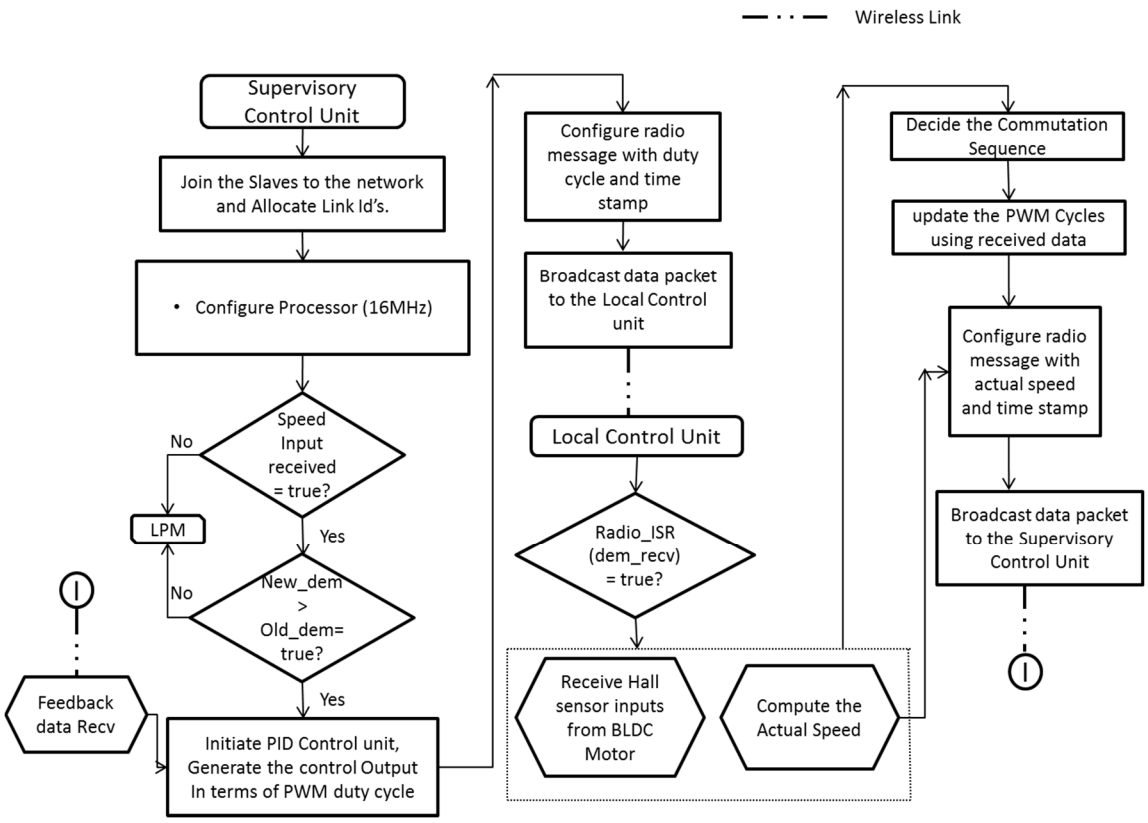

Figure 4.15: Wireless speed control algorithm

4.6 Results

4.6.1 Wireless network time delay

Time delay in a wireless network poses several challenges for real-time control applications. The total delay in a wireless networked control system comprises of the following components.

- ❖ Processing delay
- ❖ Access delay
- ❖ Propagation delay
- ❖ Reception delay

Processing delay is the time taken to frame the message in the application layer and send it to the radio interface. Access delay is the time taken to transmit the data on a particular wireless channel. For instance, this would be the time taken for the right time slot to be reached in time-triggered systems. Propagation delay is the time taken to transmit the message over air. This delay involves uncertainties due to lost data packets. Reception

delay is the time taken by the receiver to send the message to the application layer where the message has to be processed. In general, the access, reception and processing delay are comparatively negligible and added to the propagation delay without loss of generality. Therefore, the propagation delay is important in wireless control applications.

Round trip delay time is defined as the average time taken to transmit a message and receive a acknowledgment between master and slave over a wireless channel. In wireless networks with symmetric network delays, propagation delay is half of round trip delay time. However, in systems with asymmetric network delays, propagation delay has to be estimated separately.

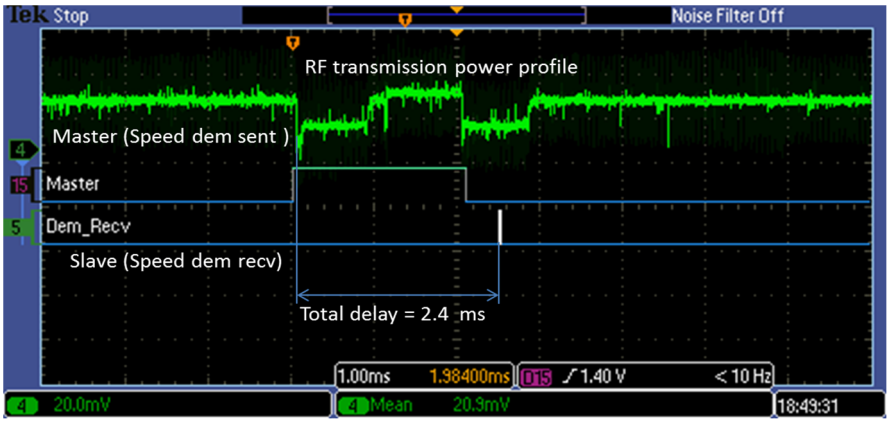

Figure 4.16: Wireless network time delay – Demand

In the designed control process, in order to process the demand and feedback data efficiently two different radio modules are used in the local control unit. Therefore, the propagation delay has to be measured separately for sending the demand and the feedback data. In Fig.4.16, the propagation delay for transmitting a message from a supervisory control unit to the radio module in the local control unit is shown. On an average a delay of 2.4 ms is observed. Fig.4.17 shows the delay in the network while sending the feedback data from the local control unit to the supervisory unit. An average delay of 2.3 ms is observed. It can be noticed that the average delay in the network is approximately symmetric (i.e., the onward and feedback wireless links experience the same amount of delay across the wireless channel).

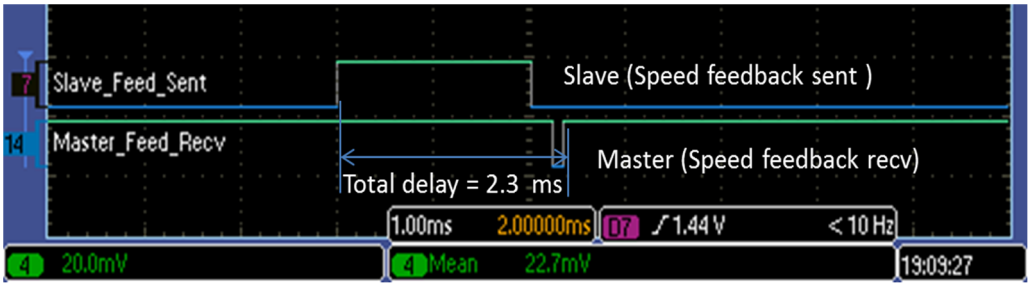

Figure 4.17: Wireless network time delay – Feedback

4.6.2 Wireless open-loop control

Fig.4.18 shows the output of the open-loop wireless control. In this approach, the demand is sent at certain pre-defined sampling intervals over the wireless channel without any feedback data. The motor speed is updated whenever a new demand request is received. It can be seen from Fig.4.18, that the output tracks the input reference speed demand under no data packet loss. However, when interference (software-based interference by deliberately corrupting the received demand data) is introduced in the wireless network at 36s, while the demand is transmitted; the system performance degrades due to the nature of open-loop control. The experiment was repeated for several sampling intervals, and Fig.4.18 represents the control performance when the control demand is sampled at 200 ms. As the total delay involved in transmitting the demand is around 2.4 ms (negligible compared to the chosen sampling rate), the motor speed was updated immediately after the deliberate interference is removed.

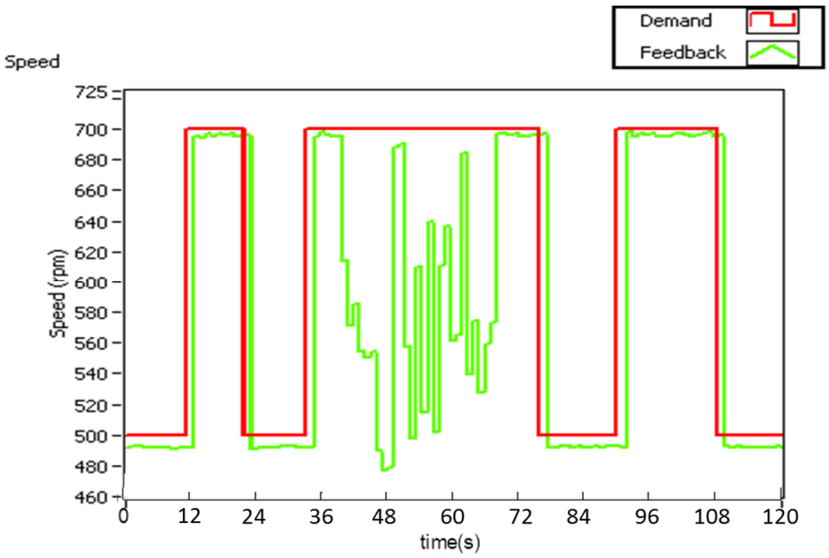

Figure 4.18: Wireless open-loop control

4.6.3 Wireless closed-loop control (Proportional controller)

In the open-loop control, though the output speed was close to the input reference speed, the speed was never able to reach the desired demand, and also the interference made the system performance degrade. Therefore, a Proportional controller based on eqn. (4.8) was introduced at the supervisory unit to control the speed of the DC motor.

In a proportional controller, a proportional gain term is used to amplify the error between the set point and the feedback data. However, proportional gain introduces a constant steady-state error. The proportional gain is chosen in such a way that the control error is reduced and the system becomes less responsive to variation in system parameters. The

proportional controller is tuned by calculating the proportional term using eqn. (4.8) and by choosing the value of K_p = 0.25. In this case, the K_p value is obtained by trial and error, however, it is chosen such that the overshoots and the steady-state error are reduced in a short time interval considering the time delay (2.4 ms) taken to transmit the demand and feedback over the wireless channel.

Fig.4.19 shows the effect of the proportional term in the designed wireless control process. It can be seen that there is an initial overshoot which is reduced by the proportional gain. However, it can be noted that the feedback data hunts around the reference point and there is a constant steady-state error. Deliberate interference (software-based interference by corrupting the demand/feedback data) is introduced at 84s which results in signifcant overshoots. However, the proportional controller is able to reduce the overshoots and keep the system stable as soon as the interference is removed.

Also, the sampling rate of how frequently the data is transmitted over the wireless channel plays a key role in the system response [Taylor, 2010]. Choosing the same sampling rate for both the feedback and control demand introduced the interrupt latency issue discussed in Section 4.5.5. This is due to the reason that there is a chance that the feedback interrupt (event-driven) might overlap with the control demand sampling (time-driven) leading to interrupt deadlock situations. However, the issue was resolved by increasing the sampling rate of the control demand more than the feedback sampling rate. Therefore, the control demand is sampled at a rate of 140 ms and the feedback is sampled at a rate of 250 ms. The sampling rates are chosen such that a satisfactory system response is obtained. The same solution was not possible in the local control unit due to the fact that neither hall events nor the received demand over the wireless channel is time-triggered and hence needs to be addressed using parallel processors.

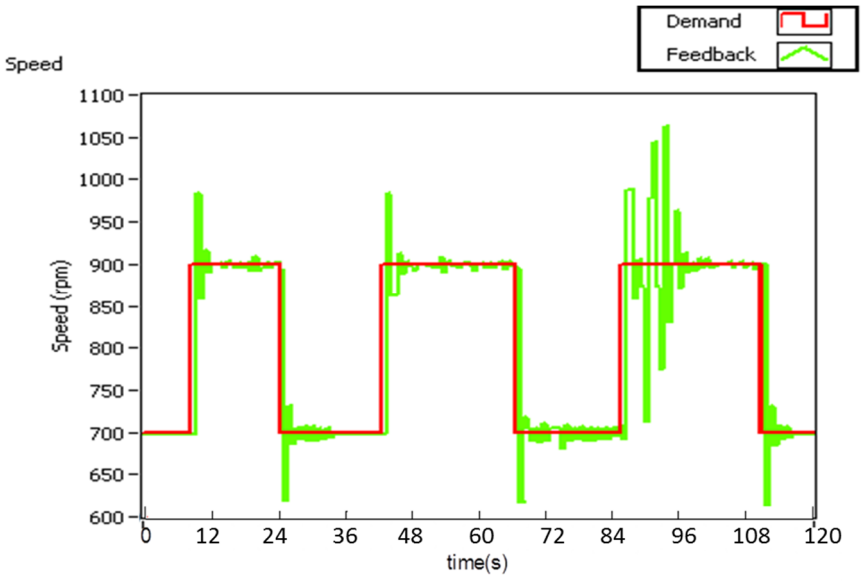

Figure 4.19: Wireless closed-loop control – Proportional controller

4.6.4 Proportional Integral Control (PI Controller)

In order to reduce the hunting introduced by the proportional term, an integral term is introduced. The integral term is calculated using eqn. (4.9) and by choosing the value of K_i = 0.115 (trial and error). The aim of the integral term is to reduce the constant steady-state error and make the system's output response smooth. The output of the PI controller is shown in Fig.4.20. It can be seen the output is much smoother compared to the proportional controller.

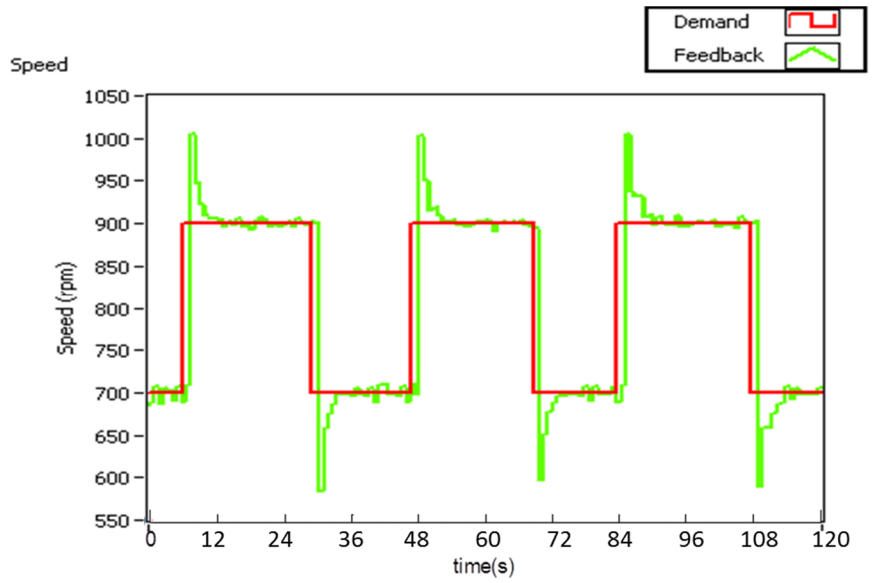

Figure 4.20: Wireless closed-loop control – PI controller

4.6.5 PI control under interference

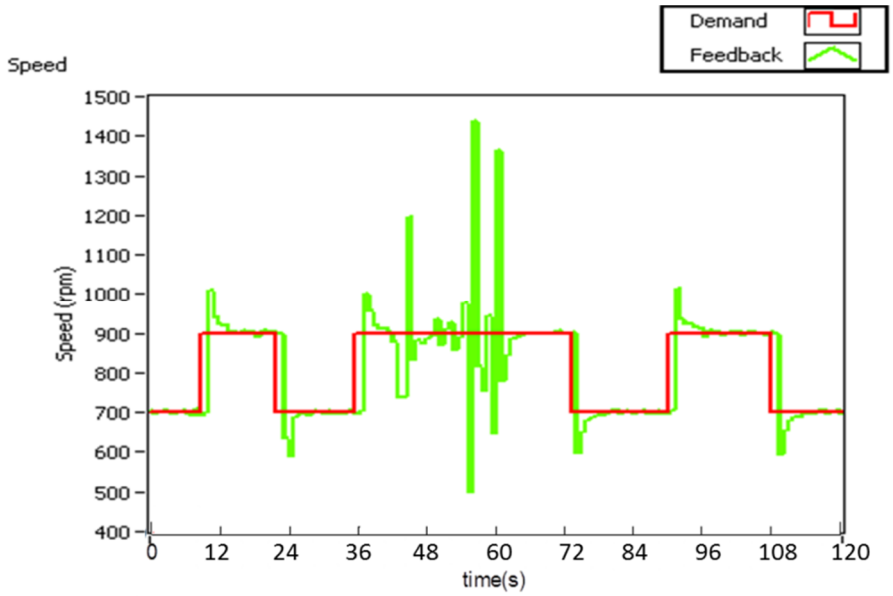

Figure 4.21: Wireless closed-loop control – PI controller with interference

The system response with deliberate interference (software-based interference by corrupting the demand/feedback data) is shown in Fig.4.21. It can be seen the system performance starts degrading around 40 seconds as soon as the interference is introduced, however, the designed PI controller is able to get the system under control and provide a smooth output response even after drastic noise disturbances. The control input is sampled at the same rate of 140 ms as the proportional controller.

4.6.6 Observations

Key observations made in the wireless real-time control process are listed below:-

- The sampling rate at which the speed demand is sent over the wireless channel plays a key role in keeping the closed-loop control system stable. Based on Nyquist sampling theory applied to a control system, to achieve a good performance with digital control, it is necessary to sample the controlled variable at a rate faster than twice the highest frequency significant for control [Verhamme, 2011]. In general, the response of the system is better if the data is sampled frequently. However, in a wireless control process, there is a risk of losing wireless links and data packets. Therefore, the sampling rate has to be dynamic according to the dynamics of the wireless system whilst satisfying Nyquist criterion. Based on the empirical evidence by subjecting the designed embedded wireless control loop to various sampling rates, the sampling policy of the wireless closed-loop control with respect to system stability can be represented as,

$$\begin{cases} stable: & if \;\; h_c > h_f, T_c < T_f \\ unstable: & if \; h_c \leq h_f, T_c \geq T_f \end{cases}$$

  where, h_c and h_f is the sampling rate of the controller and feedback data respectively. T_c and T_f is the sampling time of the controller and feedback data respectively.

- In embedded systems, the processing speed and the interrupt handling capability of the real-time processors used affects the overall performance of the system. The data received by the radio module is sent to the local processor unit using interrupt handlers. It is essential that the interrupt service routine should be prioritised and handled without any disruptions. This depends on the memory resources and the processing speed of the processor used.

- A little offset is seen in the system's output response (see Fig.4.21) with respect to the reference point. This was due to the small variations in the clocking speed used to read the Hall sensor interrupts. A negligible ± 5 rpm error is observed. Therefore, tight clock synchronisation algorithms to control the clock skew rate are needed.

- Based on the results discussed, it was observed that the wireless control process was effective under no packet loss or no lost wireless links while satisfying the following conditions:-
  - If the wireless control loop is free from interference.
  - If the time delay in the wireless network is minimal compared to the dynamics of the plant being controlled.

  However, it is not practically possible to maintain the above conditions in industrial systems. These issues are further discussed in Chapter 6 and 7.

4.7 Summary

This chapter presented the design considerations and issues related to wireless embedded systems. It highlighted the merits and demerits of various control strategies in wireless closed-loop control. A novel wireless hardware demonstrator is implemented highlighting the need for parallel processing in wireless control systems. The feasibility of wireless transmission over a closed-loop control system is then demonstrated. In literature, adaptive sampling rate based solutions for networked control are widely considered to handle time delay issues. While most of the studies suggest approaches to overcome time delay in the feedback loop, the effects this will have in sampling the control demand in embedded systems are not considered. In this chapter, the issues in utilising adaptive sampling rates, in embedded systems are discussed and a sampling policy is proposed such that the control demand sampling must always be higher than the feedback data sampling.

The operation of the wireless control technique has been successfully demonstrated over what might be considered a relatively low-capacity wireless system in this deliberate exercise. This evidence suggests that there is substantial opportunity to maximise the performance of a future system if placed in a position to leverage a high-bandwidth network, operate over a dedicated aero frequency spectrum or with use of a proprietary aero-specific wireless protocol. In order to study the effects of interference in wireless feedback loops, the implemented system is subjected to interference sources and deliberate jamming in Chapter 6. As there is a need to keep the system tightly synchronised for the time-triggered and event-triggered strategies to work well, a novel clock synchronisation approach is proposed in the next chapter.

Chapter 5

Clock Synchronisation Issues in Industrial Wireless Closed-loop Control Systems

This chapter presents the challenges associated with clock synchronisation in a wireless closed-loop control system. A comprehensive analysis of existing clock synchronisation methods in industrial automation is presented. The effect of clock inaccuracies such as clock offset and drift in a wireless closed-loop control system is discussed and in order to tackle these issues a Sampling Interval based Clock Synchronisation (SICS) approach based on IEEE 1588 Precision Time Protocol (PTP) is proposed. Finally, the proposed clock synchronisation approach is tested in the simulation environment and also in real-time using the wireless hardware demonstrator. A synchronisation accuracy of 1.3 milliseconds is achieved using the proposed algorithm in real-time.

5.1 Need for Clock Synchronisation

Wireless control loops are classified as hard real-time and soft real-time control systems. Hard real-time systems need to adhere to tight deadlines, and any time delay or time inaccuracy in critical systems will cause undesirable performance and at times may eventually lead to a system shut down. Soft real-time systems, on the other hand, can still perform the control tasks; however, the overall performance will degrade over time. Therefore, it is important to have each node (actuator/sensor) tightly synchronised in the control loop.

Clock synchronisation is one of the major issues in industrial applications where the controllers and actuators have a deterministic behaviour and need to guarantee tight real-time demands. Over time, internal clocks of wireless sensors can develop issues such as clock offset, clock drift, jitter, latency, etc. which results in each sensor in a network following a different time base. This is critical in industrial applications that involve data fusion, real-time control, etc. where the sampling and actuation instants must be precisely known according to the control process timing and network delay. This is possible only if all the sensors have a common understanding of time also known as ‘common notion of

time' [Eidson, 2003]. However, due to the inaccuracies which can develop over time in clocks, it is practically not possible to have a perfect clock across all the control units, sensors and actuators in a wireless real-time control loop. The issues of clock synchronisation in data acquisition and sensing in real-time industrial wireless systems are discussed in [Flammini, 2010].

5.1.1 Motivation

Data from multiple sensors distributed across a wireless network can be collected and fused over time, and this can enable the control and monitoring system to have a better understanding of the system. However, for successful data fusion, the data must have been collected from each of the sensors at specified intervals. Data fusion is an important aspect of wireless sensor networks, which combines data from multiple sensors into high level data and therefore, needs a high level of time synchronisation between the nodes [Sichitiu, 2003].

Inaccuracies such as clock drift can be significantly higher due to changes in temperature [Raouf, 2014]. This is a crucial problem in aircraft and space applications as the control systems are subjected to different temperatures during flight. The key benefit of introducing wireless sensors in aircraft applications is the ability to spread sensors across an aircraft surface without the need for physical cables and their enclosures. Therefore, wireless sensors will be subjected to continuous change in temperature and hence the real-time clocks in these sensors have a high chance of drifting in a short period of time.

In safety-critical control areas such as nuclear power plants and aerospace applications, the sensor data is crucial in determining the next control action. Any lead or lag in the arrival of these sensor data with respect to the real-time could cause a serious damage to the overall system. Therefore, the control systems need to be repeatedly synchronised in such systems even if the rate of clock drift or offset is slow.

5.1.2 Clock Inaccuracies

Clock offset (clock skew) is defined as the time offset of the local control unit (slave,C_s) from the supervisory unit's (master,C_m) clock in a wireless closed-loop control. It could either be a positive offset or a negative offset depending on whether the slave's clock is leading or lagging the master's clock. Clock offset in the local control unit can cause significant problem to the actuator response leading to degraded system performance. The fast clock region and slow clock region with respect to the ideal clock $C(s)$ is shown in

Fig.5.1. Clock offset is the difference between the mater's clock and slave clock over time and it will be constant at any given time.

$$\text{Offset, } \tilde{O} = |C_m - C_s| \tag{5.1}$$

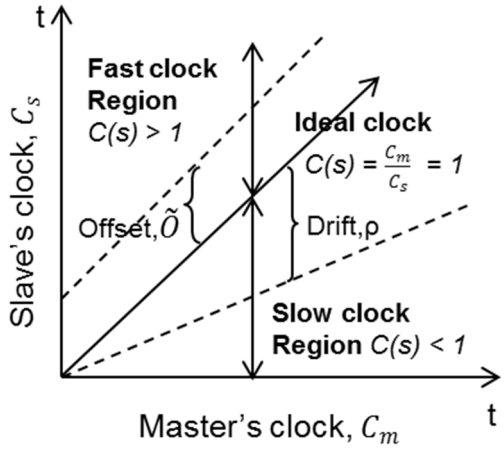

Figure 5.1: Clock Inaccuracies

Clock drift, on the other hand, occurs when the frequency of the clock oscillator changes over time due to age of the clock's crystal or external factors such as temperature, harsh environments, etc. It is the rate of change of clock ticks with respect to the ideal clock. It can be represented as,

$$1 - \rho \leq \frac{dC}{dt} \leq 1 + \rho \tag{5.2}$$

Where, ρ is the maximum drift rate specified for a clock crystal and C is the change of the clock's time. Ordinary quartz crystals used in most of today's clocks drift by ~1 sec in 11-12 days (10^{-6} secs/sec). High precision quartz crystals such as those used in microprocessors drift by $\sim 10^{-7}$or 10^{-8} secs/sec [Nielsen, 2014]. Atomic clocks can be refined such that it drifts no more than 1 nanosecond (ns) in 10 days [DeepSpace, 2014]. Atomic clocks are used as the source for clocks in satellites that provide the GPS signal thus guaranteeing synchronisation accuracy in ns by GPS systems. However, the clocks used in the industrial systems may not have such a high precision crystal or an atomic clock base. Hence, there is a need for clock synchronisation algorithms in wireless networked control systems especially those that have tight deadlines.

Therefore, in this chapter the effects of clock offset and clock drift in wireless closed-loop control systems is considered. A Sampling Interval based Clock Synchronisation (SICS) approach based on the IEEE 1588 Precision Time Protocol (PTP) is proposed for correcting the clock offset/drift in wireless closed-loop control. The next section presents a brief overview of related work.

5.1.3 Related work

Clock synchronisation in wireless distributed and real-time industrial systems has been an active area of research [Junior, 2010],[Minghu, 2008],[Mock, 2000] over the last few decades. Clock synchronisation in wireless sensor networks has been widely discussed in the research community compared to the wired networks. This is due to the implementation of wireless networks in industrial monitoring and control in recent years. Survey of clock synchronisation approaches for wireless sensor networks based on accuracy, precision, cost and complexity are presented in [Sundararaman, 2005]. It is highlighted that traditional synchronisation protocols used in wired networks cannot be applied for wireless sensor networks due to scalability issues and unreliable wireless medium. It should be noted that many of these approaches have a line-of-sight requirement between the sensor nodes for accurate synchronisation and also a perfect master clock in case of distributed networks. A performance analysis of clock synchronisation algorithms proposed specifically for wireless sensor networks and methods for estimating clock offset and skew is presented in [Rhee, 2009].

Fault tolerance in clock synchronisation has been researched widely [Ramanathan, 1990], [Gaderer, 2004] as it guarantees a tight synchronisation using redundant time information using past deviations between master and slave clocks. However, most of these approaches rely on the successful reception of data and a reliable network medium. There are many synchronisation algorithms available in literature that proposes various methodologies to estimate the clock inaccuracies such as delay, jitter, latency, etc. and apply a suitable synchronisation process to reduce the error in these parameters. However, in wireless networked control systems, these inaccuracies may further introduce issues in a control system's stability and reliability. Therefore, there is a need to evaluate the synchronisation mechanisms with respect to the stability of the control process.

Synchronisation in networked control systems [Pacner, 2013],[Marti, 2008] is focussed on solving the system stability issues in addition to correcting the clock inaccuracies. The challenges in communication and control in real-time systems is discussed in [Baillieul, 2007]. Earlier research work [Uchimura, 2009] attempted to control the delay in the communication medium within a known bound to ensure the stability of the system thus eliminating the need for synchronising the clocks. A simple synchronisation approach by exploiting the time-driven and event-driven communication process between the controller and actuator in a closed-loop control of distributed systems using wireless communication was discussed in [Kim, 2006],[Ploplys, 2003]. However, it does not correct for any clock inaccuracies, and delays are bound to change over time. The control time protocol (CTP) [Solis, 2006] estimates the offset using an approach where all the data sent by the controller or a master node is time stamped. In CTP, the delay in the entire network is not considered, and the offset estimated is assumed to be correct at all times. Some research work [Seuret, 2012],[Lorand, 2006] have proposed numerical solutions to address the synchronisation issue errors in discrete-time feedback loops. While these algorithms suggest robust mathematical models extending them to wireless control remains an open problem due to the computational complexity and the assumptions made.

The IEEE 1588 precision time protocol (PTP) [IEEE 1588 PTP, 2008] proposed for clock synchronisation in distributed measurement and control is actively researched [Weibel, 2005] for its suitability in networked control especially in wireless systems. The design consideration for the software based implementation of IEEE 1588 and a clock offset correction method using a PI clock servo for computer networks is discussed in [Correll, 2005]. Other research [Abubakari, 2008] discusses a PI clock servo-based correction for clock drift estimated using the IEEE 1588 protocol. A PI controller-based clock synchronisation over a closed-loop control using multiple synchronisation events for networked control systems is discussed in [Liu, 2014].

Utilisation of the PTP protocol for wireless closed-loop control systems is very much in its infancy and to the best of the author's knowledge, substantial work is not available in the literature so far. The key issues identified from the literature in utilising clock synchronisation algorithms for wireless control are:-

- Most of the existing protocols repeat the synchronisation process many times before a high synchronisation accuracy can be achieved.
- Wireless closed-loop control systems have tight real-time demands, and therefore, synchronisation should be achieved within a certain interval since the start of the control process.
- The clock offset or skew must be corrected gradually as immediate synchronisation will cause abnormal behaviour if the offset is high.
- The delay estimation process should be part of the synchronisation process, and the estimated delay should be within a certain known bound.
- Fault tolerant synchronisation process is needed in hard real-time wireless control loops to address packet loss, interference, etc.

The pragmatic solutions to the above issues from an industrial perspective are discussed in this chapter. The next section describes various clock synchronisation approaches followed in industrial systems.

5.2 Clock Synchronisation in Industrial Systems

Over the last decade, various clock synchronisation algorithms have been proposed for synchronising industrial control systems. However, the following approaches are widely used in industrial monitoring and control applications.

5.2.1 Networked Time Protocol (NTP)

Networked time protocol proposed in 1985 by the University of Delaware is widely used in packet-switched variable delay networked systems [Mills, 1991]. The protocol uses a client-server architecture wherein the client requests a clock sync message to the server. The server stores the received time stamp and sends it in the response back to the client. The client records the received time stamp, and with server's time stamp in the received

packet, it can calculate the propagation delay in the network and then correct its own clock accordingly. NTP follows multiple levels of servers and clients known as a stratum. The topmost level (stratum 0) acts as the master while the subsequent levels acts as the client to the level above it and parent to the level below it. Clients can request for sync message from multiple servers and also in a peer-peer to fashion to other clients in the same level. The protocol is used in industrial control systems using Ethernet and UDP protocol as well as in internet communication networks. It can offer synchronisation accuracy in μs (microseconds). However, a client using NTP needs a number of sync pulses known as 'sanity check' before it can synchronise its clock. Also, due to the network congestion, it can take a long time (in minutes) before synchronisation can be achieved. NTP is also known for its security issues. Therefore, NTP may not satisfy the tight time constraints of a real-time wireless closed-loop control system.

5.2.2 Global Positioning System (GPS)

GPS is based on satellite systems and global navigation systems (GNS) [Kline, 1997]. The GPS used in satellites uses a set of atomic clocks that synchronises itself to a global time such as Universal Co-ordinated Time (UTC) time. GPS receivers can be used wherever a GPS synchronisation is needed, and these receivers will receive a periodic sync pulse from a GPS satellite system. As GPS systems use high atomic precision clocks, they can offer synchronisation accuracy in ns (nanoseconds). Clock synchronisation using GPS does not follow a specific synchronisation approach or delay measurement techniques. A GPS receiver will set its clock immediately as soon as a time pulse is received from a GPS system. As the accuracy is in sub-milliseconds to nanoseconds, this accuracy works well for many industrial systems. However, GPS relies on satellite coverage and antenna tuning, which might be difficult in indoor systems. Also, for hard real-time systems gradual correction of a clock is needed as instant correction might render the system unstable, especially when the clock offset is higher. Most of today's aircraft use the GPS to synchronise the flight control systems in addition to synchronising with air-traffic control.

5.2.3 IEEE 1588 Precision Time Protocol (PTP)

PTP follows a server-client architecture wherein the server sends out a synchronisation message to all the clients in the network to start the synchronisation process. This seems to be a more realistic approach for real-time closed-loop control systems as these systems use a single master and multiple local control units in a distributed manner. In addition, it uses a delay measurement system that calculates the propagation delay in the network with high precision. IEEE 1588 PTP can offer synchronisation accuracy in sub-microseconds. Only few sync pulses are involved in the protocol which minimise the network overhead and security risks. Therefore, IEEE 1588 PTP is being actively researched [Neagoe, 2006] for its suitability in networked control, especially in wireless systems. The next challenge is to test the protocol's suitability in real-time closed-loop control systems. The mechanism of IEEE 1588 PTP is presented in Section 5.4.1. The next section describes the two major ways of implementing clock synchronisation algorithms in industrial systems.

5.3 Clock Synchronisation Modes

Clock synchronisation approaches for industrial systems are broadly classified into two types as external clock synchronisation and internal clock synchronisation. In external synchronisation, the clocks in a sensor network are synchronised to a global reference time such as an atomic clock that provides real-world time (UTC) or GPS. In internal synchronisation, the nodes in a given network are synchronised to a Master node within the network such that the drift between the clocks is kept to a minimum.

5.3.1 External Synchronisation

In this approach, synchronisation between the control systems is achieved using an external time source such as a global time base (Universal Co-ordinated Time (UTC)). This is a hardware-based synchronisation where the clock in a network is adjusted whenever timing information is received from the external source. A majority of today's industrial systems rely on external clock synchronisation approaches such as Networked Time Protocol (NTP) and Global Positioning System (GPS). However, in wireless sensor networks as sensors could be deployed remotely, it is not practically possible to have a global time base at all times. External synchronisation is a hardware-based synchronisation where the clock in a network is adjusted whenever timing information is received from the external source. External synchronisation cannot synchronise large networks due to energy consumption issues and availability of global time source.

In this section, the implementation of an external synchronisation is done using a wireless sensor network formed from Texas Instruments MSP430 eZ430-RF2500 wireless sensors. The hardware setup is shown in Fig.5.2.

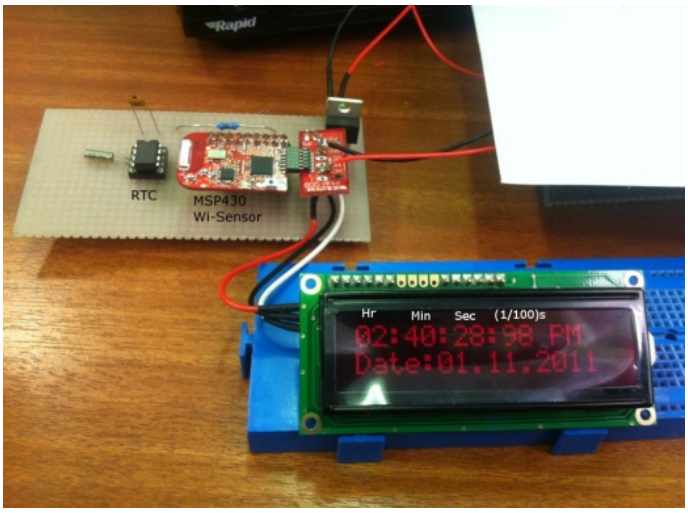

Figure 5.2: External clock synchronisation hardware setup

This consists of a MSP430 wireless sensor and a PCF8583 external real-time clock (RTC) chip. The RTC unit is sourced by a 32768 Hz quartz crystal. MSP430 in turn has an internal timer. The idea is to receive a time stamp from the external RTC and synchronise

the internal clock of the MSP430 appropriately. This setup will act as a Master module and now a time stamp will be sent to the slave nodes from the master, and the performance can be analysed for different transmission payloads. Therefore, this setup will provide a good platform to analyse the external synchronisation (RTC to MSP430) as well as internal synchronisation (MSP430 master to MSP430 slaves). The chosen RTC in turn provides options of getting an external clock signal from various other sources such as atomic crystal oscillators and AC sources. As explained earlier in Section 4.6.1, generally, four types of delay components need to be considered when implementing a synchronisation algorithm as shown in Fig.5.3.

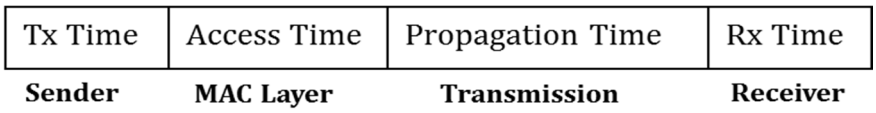

Figure 5.3: Delay components

- Send time (Tx) is the time taken by the master to construct the time stamp.
- Access time is the delay time encountered by the master in accessing the network (medium access control) to transmit.
- Propagation time is the delay due to transmission. It is the actual time taken for the physical transmission.
- Receive time (Rx) is the time taken by the receiver to decipher the time stamp and synchronise its own clock.

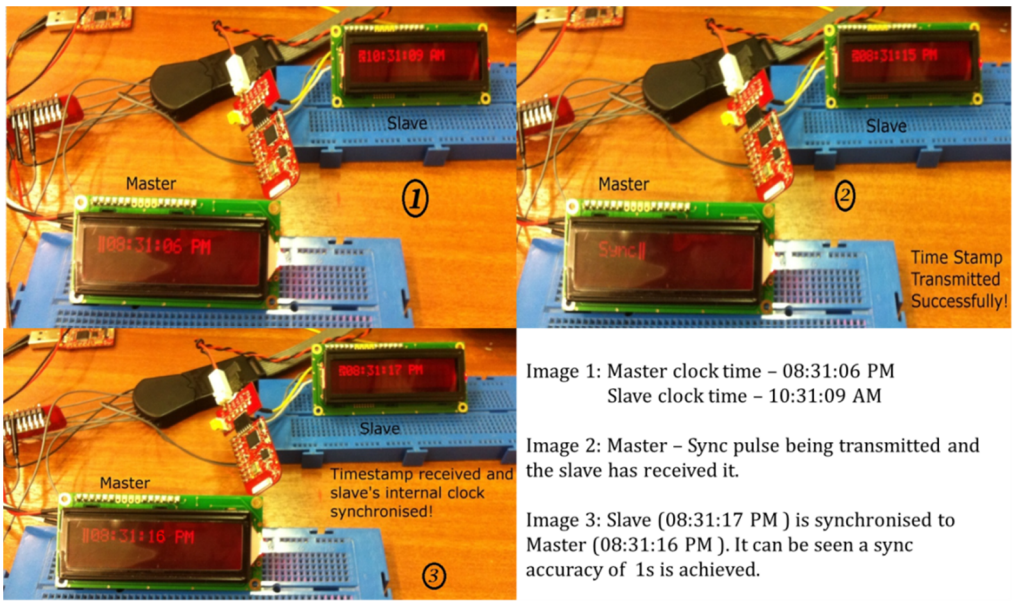

Figure 5.4: External clock synchronisation process

The send time, access time and receive time are negligible in small-scale and wide bandwidth networks. However, the propagation delay time may increase due to packet loss, interference issues, etc. Hence, this needs to be eliminated significantly to improve

the synchronisation process. The external synchronisation process is tested using the hardware implemented in Fig.5.2. The hardware setup acts as the external time source. A separate RF2500 radio module is used as a slave in the network and the synchronisation is tested in a single-master-single-slave environment (see Fig.5.4).

The master node receives a time stamp from the external RTC and sends a synchronisation beacon over the wireless channel to the slave node which is running a different time (see Fig.5.4(1) and (2)). The slave receives the timestamp and synchronises its internal clock as shown in Fig.5.4(3).

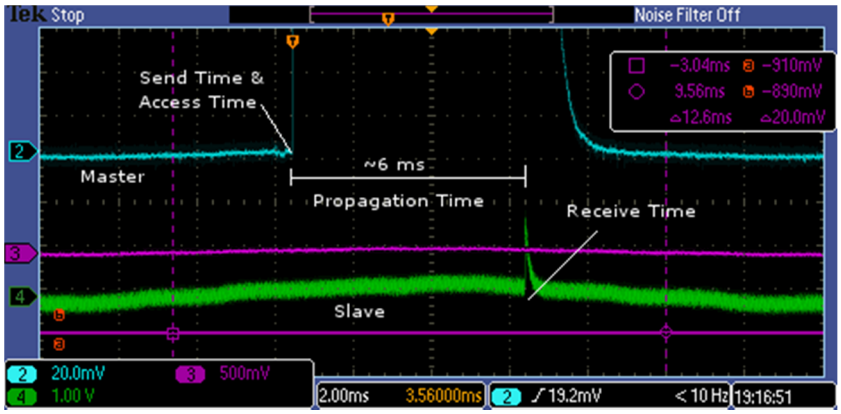

Figure 5.5: Delay components – Timing diagram

The timing response is shown in Fig.5.5. The send time and access time is almost negligible that occurs just before the transmission begins. It can be seen that the slave receives the time stamp at approximately 6 ms after the master has transmitted due to the propagation delay. The result depends on a lot of factors such as the proximity of the sensors, the amount of interference, power constraints, frequency agility of the master in case of packet loss, etc. The receive time duration is slightly greater than the send time due to the fact that receive time also incorporates the time taken to synchronise the slave clock.

It can be seen in Fig.5.4(3) a synchronisation accuracy of 1 second is achieved. Although external synchronisation methods using GPS aim synchronisation accuracy in ns, practically possible accuracy in many systems is in terms of seconds due to the internal clock oscillator variations. Therefore, for much better accuracy at least in milliseconds, internal synchronisation methods are used.

5.3.2 Internal Synchronisation

External synchronisation cannot synchronise large networks due to energy consumption issues and availability of global time source. This gave rise to the concept of internal clock synchronisation where nodes in a given network are synchronised to a master node within the network, which in turn synchronise itself to a global time source. The sensors in a given network are connected to the master using a peer-to-peer networked fashion and the synchronisation is achieved using client-server (the clients in a network requests for sync

pulse from the server) and server-client (server broadcasts sync pulse to the clients) architectures. The synchronisation process is achieved using software-based synchronisation techniques [Sundararaman, 2005]. The most frequently referred internal synchronisation techniques, especially in wireless sensor networks are Timing-sync protocol for sensor networks (TPSN), Reference broadcast synchronisation protocol (RBS), Flooding time synchronisation protocol (FTSP), Delay measurement time synchronisation (DMTS) and Time diffusion protocol (TDP). These protocols offer good synchronisation accuracy according to the needs of the wireless network. However, from a wireless control loop perspective, there is a need to evaluate the suitability of these protocols. Some of the features [Rhee, 2009] of these protocols are:-

- RBS requires a number of message exchanges, and hence it's computationally expensive.
- TPSN is more suitable for networks with a hierarchical infrastructure.
- FTSP is an extension of TPSN proposed for ad-hoc wireless networks.
- DMTS requires accurate local clocks so that the delay measurement can be done with high precision.
- TDP has high convergence time, and the clock value is instantly adjusted.

It is worth highlighting that most of the synchronisation protocols are designed to achieve the best possible synchronisation accuracy; however, there is no predetermined bound [Nielsen, 2014] on the synchronisation interval. Wireless real-time control loops, on the other hand, have tight real-time demands that synchronisation are expected to happen within a certain interval from the start of the synchronisation process.

A majority of today's industrial systems relies on external clock synchronisation approaches such as Networked Time Protocol (NTP) and Global Positioning System (GPS). In wireless closed-loop control systems, there is a need to choose a combination of external and internal synchronisation techniques. Since its launch, the IEEE 1588 PTP has been widely researched for its suitability in wireless sensor networks due to its delay estimation process and follow-up messages that ensure synchronisation accuracy. It is worth highlighting that PTP offers both hardware and software-based synchronisation. Therefore, the suitability of IEEE 1588 PTP for wireless closed-loop control systems is further discussed in this chapter.

5.4 Clock Synchronisation in Wireless Closed-loop Control

The clocks used in industrial systems are predominantly quartz crystal based clocks, which oscillate at a frequency of 32768 Hz. Over time, the clock's frequency changes thus introducing issues such as clock offset, clock drift, jitter, latency, etc. Clocks are also subjected to drift when there is a change in temperature, which is common in safety-critical applications such as aircraft control systems. Prolonged drifts in clocks and

uncorrected offsets can lead to jitter and latency in control response. Therefore, in this chapter the effects of clock offset and drift in wireless closed-loop control systems are considered. The wireless controlled BLDC motor modelled using the Truetime networked control system simulation tool explained in Chapter 4 is used for analysis (see Fig.5.6). The supervisory unit's clock (t) is considered as the reference clock and the local control unit's clock is considered to have an offset, $(\tilde{o})$. The delay in the forward path (τ_{ca}) and feedback path (τ_{ac}) in the wireless network is assumed to be symmetrical and within a known bound.

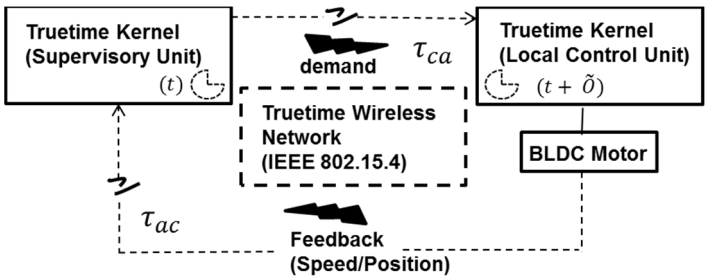

Figure 5.6: Truetime simulation model

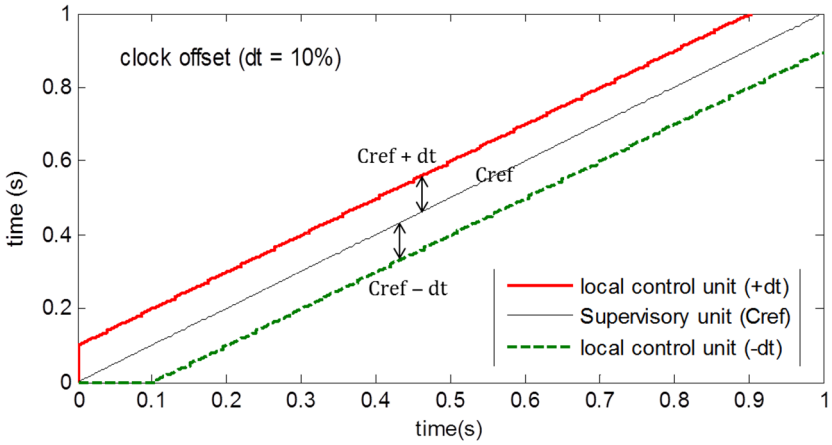

Figure 5.7: Clock offset

Clock offset: Clock offset is defined as the time offset of the local control unit from the supervisory unit's clock. It could either be a negative offset (-dt[4]) or a positive offset (+dt) (see Fig.5.7). Fig.5.8 (left side) shows how the control response (red dashed line) can deviate from the reference (blue solid line) when the local control unit's clock offset is 5% lower than the supervisory unit. It can be noticed that the local control unit's response lags behind the reference by 0.05s. The control response (green dashed line), where the local control unit's clock offset is 5% higher than the supervisory unit is shown on the right side of Fig.5.8. It can be noticed at 0.1s there is an overshoot as the local control unit identifies a delay in responding to the control demand, however, it settles over time with an offset to the ideal response.

[4] Offset $\tilde{O}$ is represented as dt in simulation results

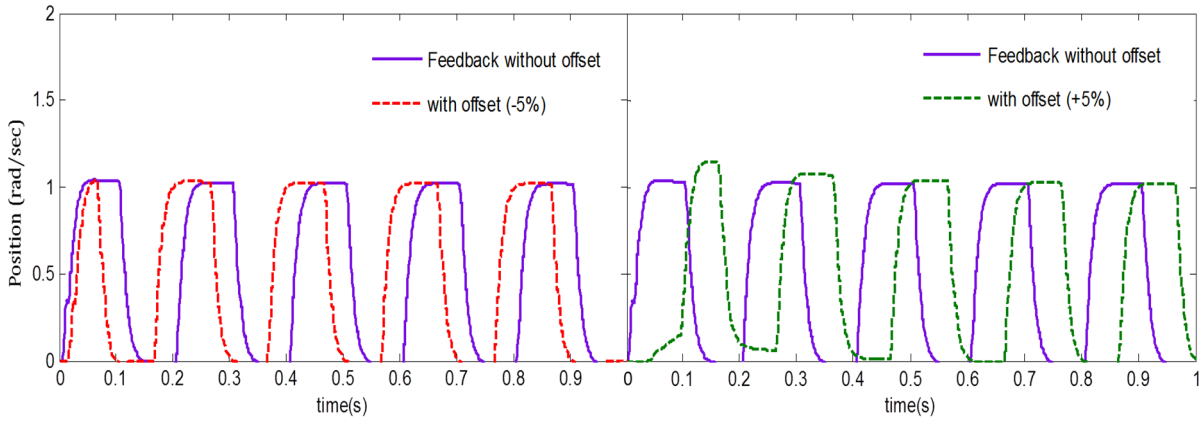

Figure 5.8: Wireless closed-loop control response with clock offset (Simulation)

Clock drift: Clock drift occurs when the frequency of the clock oscillator changes over time due to age of the clock's crystal or external factors such as temperature, harsh environments, etc. Fig.5.9 shows the clock drift of a local control unit in a wireless closed-loop control system for various drift levels and the feedback response is shown in Fig.5.10.

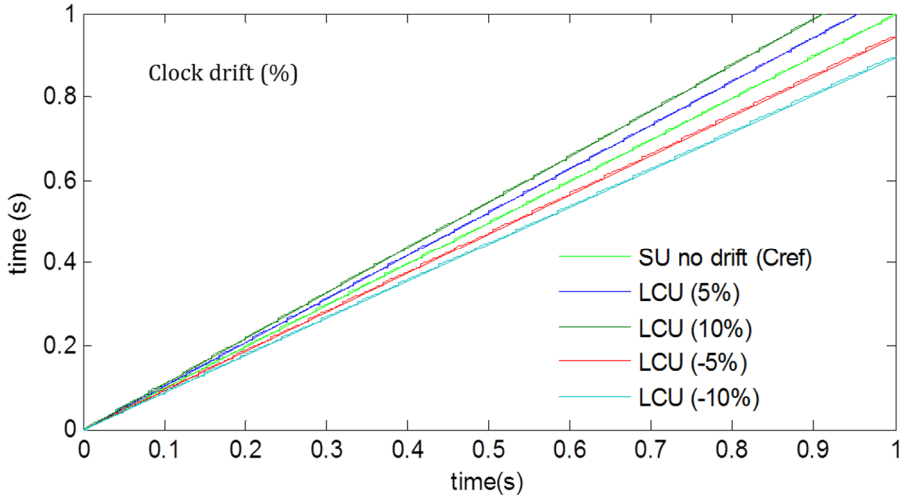

Figure 5.9: Clock drift

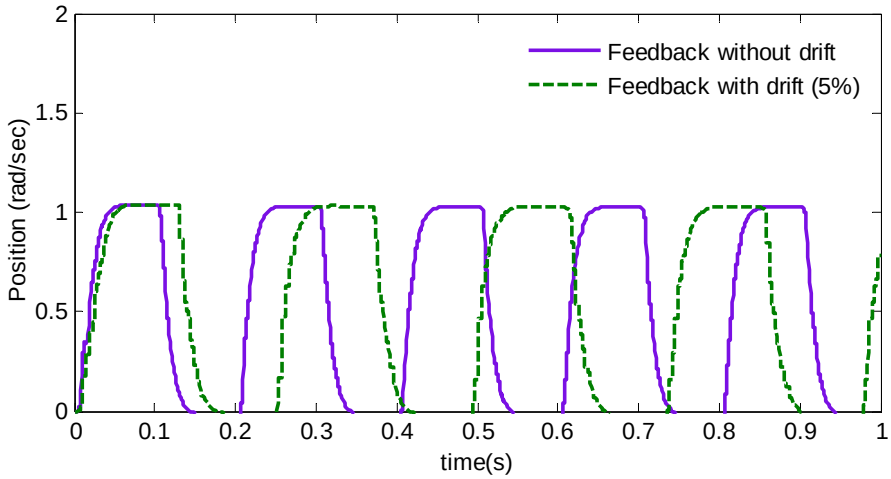

Figure 5.10: Wireless closed-loop control response with clock drift (Simulation)

It's evident from the above discussion that both clock offset and clock drift in the local control unit can cause a significant problem to the actuator response. In real-time and safety-critical systems, this will cause issues in maintaining deterministic tasks and adherence to deadlines. Therefore, to address these issues in a wireless closed-loop control, a synchronisation algorithm based on the IEEE 1588 PTP along with a clock discipline process is proposed in the next section.

5.4.1 Synchronisation process to estimate the clock offset

A clock synchronisation approach for wireless real-time closed-loop control systems based on IEEE 1588 PTP is presented in this section.

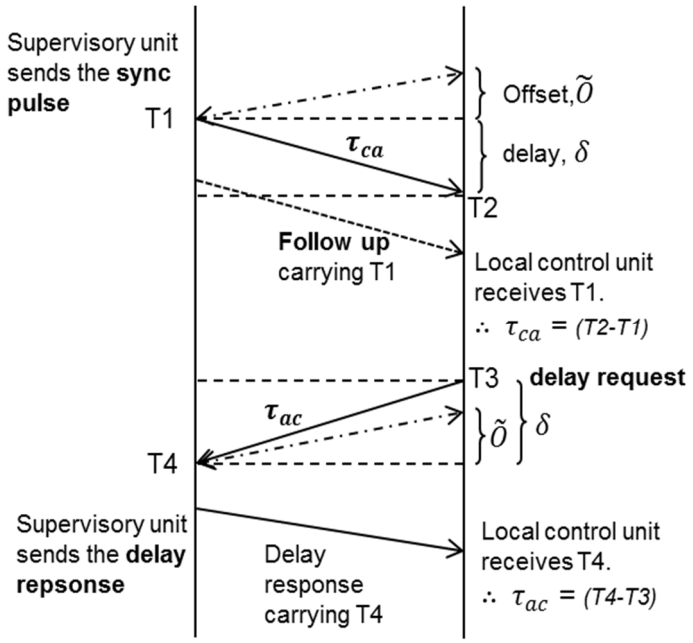

Figure 5.11: IEEE 1588 PTP for wireless closed-loop control

IEEE 1588 PTP uses a grandmaster clock that acts as the reference time source for the rest of the control units in the network. Therefore, the supervisory unit is used as the grandmaster clock whose clock is considered as reference time. IEEE 1588 PTP works (see Fig.5.11) as follows:

1. SYNC_PUL: The supervisory unit sends a synchronisation request pulse to the local control unit at time T1. This pulse is received by the local control unit at time T2. The time taken by the sync pulse to reach the local control unit is given by τ_{ca} which is the propagation delay due to the wireless network in the forward path between the supervisory unit and the local control unit.
2. FOLLOW_UP: The supervisory unit then sends a follow-up message to the local control unit containing the time stamp T1.
3. DELAY_REQ: After T1 is received, the local control unit sends a delay request

message at time T3 to the supervisory unit. The supervisory unit receives this message at T4. The time taken by the delay request message to reach the supervisory control unit is given by τ_{ac} which is the propagation delay due to the wireless network in the feedback path between the local control unit and the supervisory unit.

4. DELAY_RESP: Once the delay response is received, the supervisory unit records the reception time T4 and sends a delay response message to the local control unit containing the timestamp T4.

From Fig.5.11, if the local control unit's clock has an offset $\tilde{O}$ more than the supervisory unit's clock, then the time delay δ and offset $\tilde{O}$ can be calculated as follows:
Assuming a symmetric delay in the forward and feedback path,

Time delay, $$\delta = \tau_{ca} = \tau_{ac} \quad (5.3)$$

Round trip delay time, $$2\delta = \tau_{ca} + \tau_{ac} \quad (5.4)$$

From Step 1 and 3 in the PTP synchronisation mechanism,

$$\tau_{ca} + \tilde{O} = (T2 - T1) \quad (5.5)$$

$$\tau_{ac} - \tilde{O} = (T4 - T3) \quad (5.6)$$

Substituting Equation (5.5) and (5.6) in (5.4),

Time delay, $$\delta = ((T2 - T1) + (T4 - T3))/2 \quad (5.7)$$

Offset, $$\tilde{O} = (T2 - T1) - \delta \quad (5.8)$$

Drift, $$d = \frac{1}{n}\sum_{k=1}^{n}\frac{(T2 - T2_{k-1})}{(T1 - T1_{k-1})} - 1 \quad (5.9)$$

$$d = \frac{1}{n}\sum_{k=1}^{n}\frac{(\tilde{O} - \tilde{O}_{k-1})}{(T1 - T1_{k-1})} \quad (5.10)$$

Where, k is time step and n is synchronisation cycle.

5.4.2 Sampling Interval based Clock Synchronisation (SICS)

While IEEE 1588 PTP estimates the offset and delay in the network with high precision, it does not provide a methodology to correct the offset/drift. PI clock servo is generally used to correct the offset/drift estimated by the PTP protocol. A clock model's transfer function for a discrete-time system [Liu, 2014] is given by,

$$G(z) = \frac{K_c T_{sync}}{z - 1} \quad (5.11)$$

where K_c is the clock constant and T_{sync} is the synchronisation interval

PI clock servos are widely used [Correll et al., 2005] in correcting the clock inaccuracies in sensor networks and in general PI clock servos are used in a Master node. It is highlighted in [Liu, 2014] that due to the network delay the PI control may not converge to zero. However, this correction is made over multiple synchronisation intervals, due to no upper bound for synchronisation interval in the sensor networks.

As discussed earlier, a wireless closed-loop control has tight real-time demands; therefore, the clock offset correction must be done after the first synchronisation cycle. Hence, controlling the clock servo using T_{sync} (which happens over multiple synchronisation intervals) will render the system unstable over time. However, PI clock servo cannot correct the clock offset in a single synchronisation interval and running the clock servo until the offset is corrected will lead to an instant synchronisation issue (discussed later in Fig.5.14). In the case of closed-loop control systems, this will further affect the overall control system's performance.

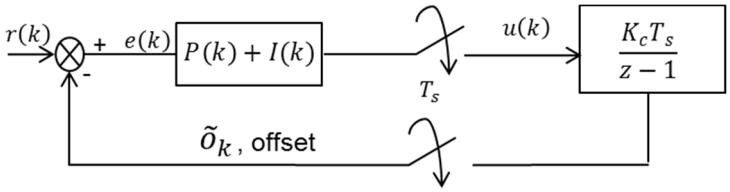

Figure 5.12: PI clock servo

Therefore, an alternative approach is proposed in this research where the PI clock servo is utilised at the local control unit (Slave) rather than the supervisory unit (Master). Based on the control algorithm explained in Chapter 4 (Fig.4.5), as the local control unit is time-driven, the interval at which the feedback is sampled can be used to control the PI clock servo instead of the synchronisation interval decided by the master. The proposed approach is termed as Sampling Interval based Clock Synchronisation (SICS) algorithm. Therefore, the clock servo's transfer function can be written as,

$$G(z) = \frac{K_c T_s}{z - 1} \tag{5.12}$$

where K_c is the clock constant and T_s is the sampling interval

From Fig.5.12, the error fed to the PI clock servo is given by,

$$e_k = r_k - \tilde{o}_k \tag{5.13}$$

where r_k is the ideal offset ($\cong 0$), $\tilde{o}_k$ is the actual offset and k is the current time step.
The integrated square error (ISE) in a PI clock servo can be given as,

$$\text{ISE} = \int_0^\infty e_k^2 = \int_0^\infty (r_k - \tilde{o}_k)^2 \tag{5.14}$$

The PI clock servo is used to control the transfer function such that the integrated square error (ISE) of the offset is kept to a minimum [Solis, 2006]. The proportional term tries to

reduce the clock offset while the integral term attempts to control the drift between the clocks. Therefore, the PI clock servo must satisfy the following conditions,

$$\frac{\mathrm{d(ISE)}}{\mathrm{dP}} = 0, \ \frac{\mathrm{d(ISE)}}{\mathrm{dI}} = 0 \tag{5.15}$$

Initially, the delay in the network and offset between the clocks are estimated in the first synchronisation interval. The PI clock servo is located in the local control unit. The PI controller is tuned based on equations (4.8) and (4.9). The values of the proportional and integral gains are chosen based on trial and error such that, $k_p = 0.0005, k_i = 45$. Here, the PI clock servo corrects the offset estimated based on its own sampling interval. After that as each data packet from the supervisory unit (master) is time stamped, the local control unit (slave) only has to estimate the offset based on its own timestamps, thereby eliminating the dependency on the master for further synchronisation intervals.

5.5 Results and Discussions

The performance of the clock synchronisation algorithm is tested using the wireless closed-loop control system modelled using the Truetime NCS tool described in Section 4.5.2 in Chapter 4. The network parameters are given in Table 5.1.

Network Parameters	Values
Network delay (one-way)	2.5 ms (milliseconds)
Offset (local control unit)	0.05s (5% of sim time)
Drift (local control unit)	0.10s (10% of sim time)
Time-driven sampling interval of local control unit	5 ms
Synchronisation accuracy	$\cong 6\ \mu s$ (microseconds)

Table 5.1: Network simulation parameters

5.5.1 Clock discipline process to correct clock offset using SICS

The effect of offset in the local control unit's clock on the position profile of the BLDC motor is shown in Fig.5.13. It can be seen that the output response (green dashed) leads the reference (black) by the given offset. There is an initial overshoot due to the disagreement between the supervisory and local control unit's clock. From Fig.5.15, it can be seen that the communication scheduler shows the disagreement between the controller and actuator in getting the network resource allocated due to the clock offset until 0.05s in the actuator.

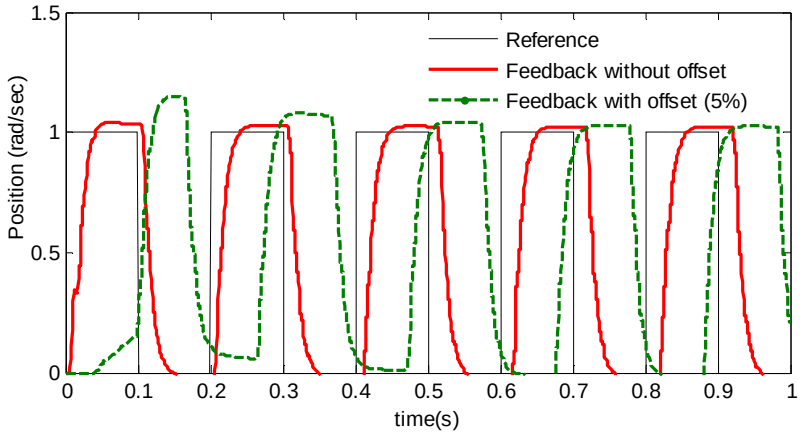

Figure 5.13: Position profile with offset

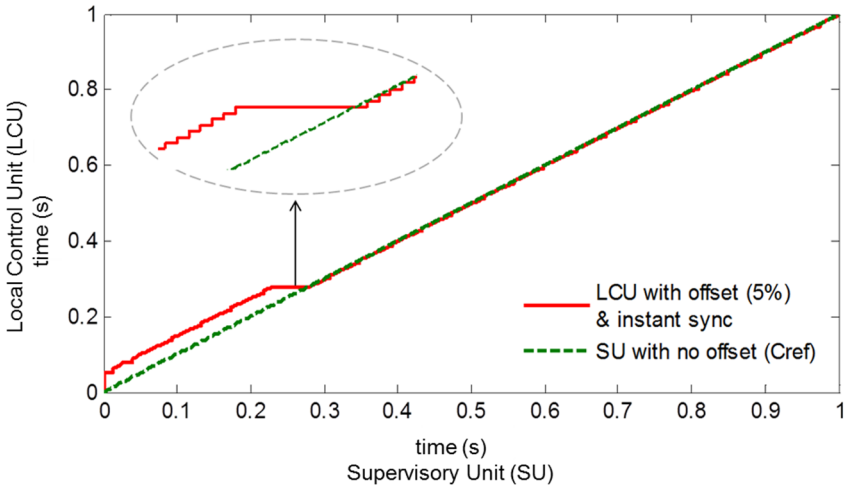

Figure 5.14: Instant clock synchronisation- clock offset

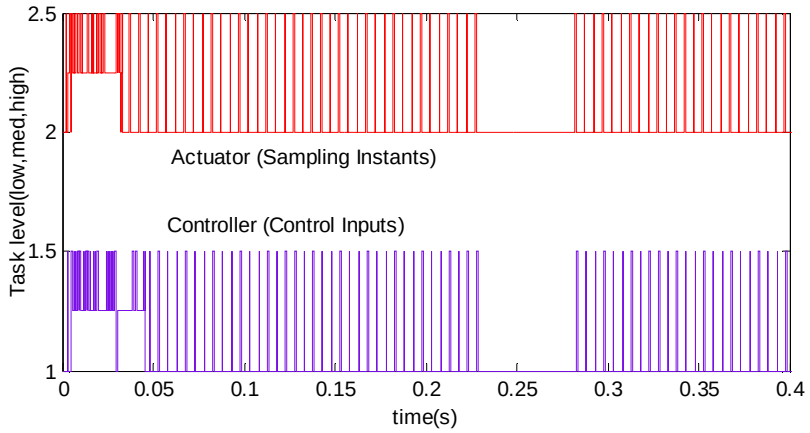

Figure 5.15: Network schedule- clock offset

Fig.5.14 shows the effects in clock offset when the PI clock servo is used in the local control unit without the SICS algorithm. It can be seen that as the PI controller controls the clock until the offset is corrected it results in an instant correction. The effect of this instant correction is shown using the wireless network scheduler. From Fig.5.15, it can be seen that the controller stops just after 0.2 sec at which the synchronisation is achieved. Due to the leading offset, the actuator cannot go back in time as soon as the offset is estimated.

Therefore, the actuator kernel (local control unit) stops the execution until the offset time has passed and resumes thereafter.

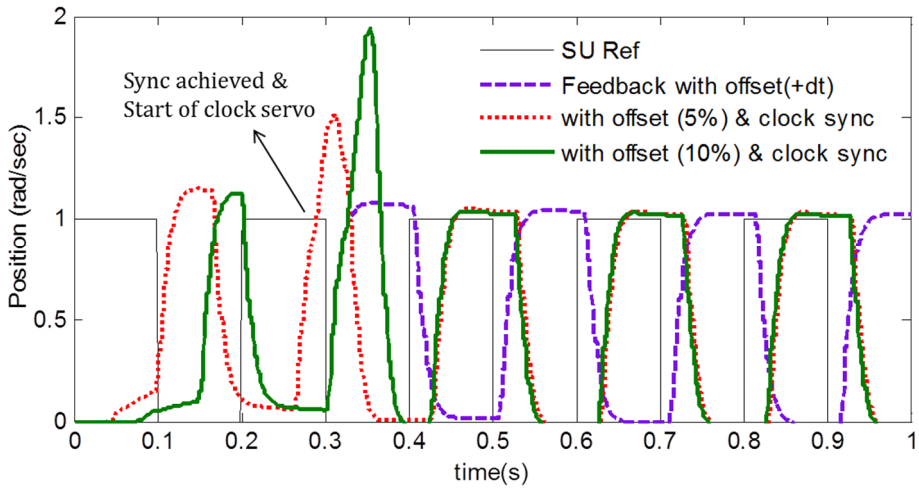

Figure 5.16: Position profile without SICS

The resulting control performance of the BLDC motor is shown in Fig.5.16. It is evident that stopping a kernel will result in overshoot (red dotted and solid green) and there will be a rise in overshoots as offset increases. Though the system is recovered in the simulation setup, such overshoots might render the system unstable in real-time even for a very short period of time.

Fig.5.17 shows the effects in clock offset when the PI clock servo is used in the local control unit based on the proposed SICS algorithm. As the PI controller corrects the clock based on the sampling interval it can be seen that the offset is corrected gradually. From the network scheduler (see Fig.5.18), it can be seen that due to the clock correction occurring based on the sampling interval; the scheduler does not stop abruptly and continues to sample the feedback data. Once the offset is completely corrected the sampling instants are resumed to the usual frequency.

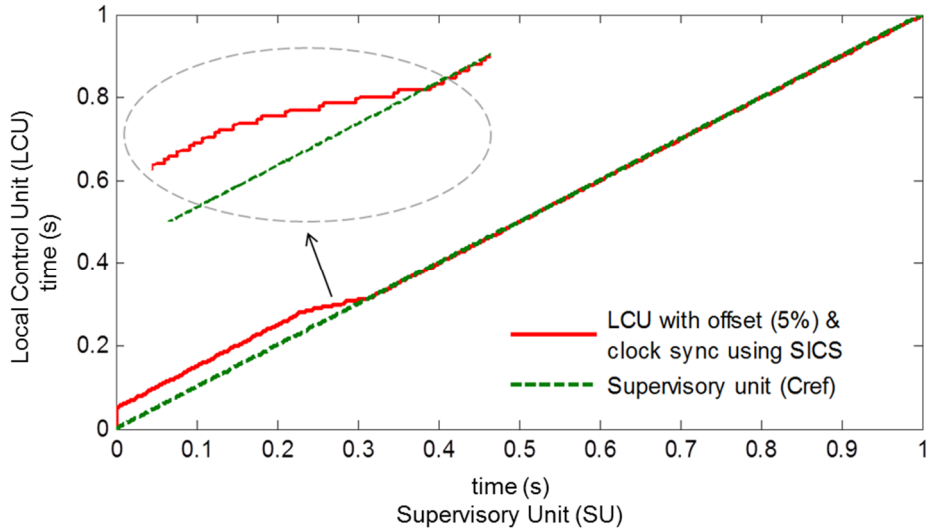

Figure 5.17: Clock synchronisation using SICS

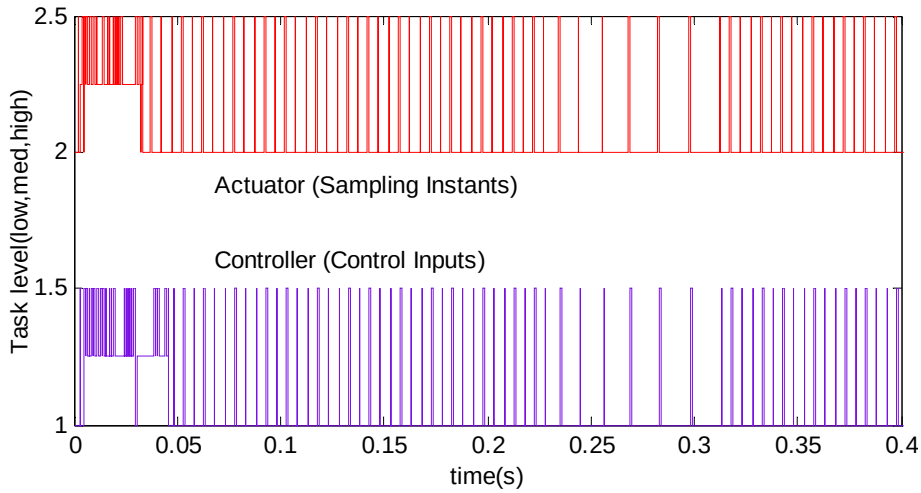

Figure 5.18: Network communication schedule with SICS

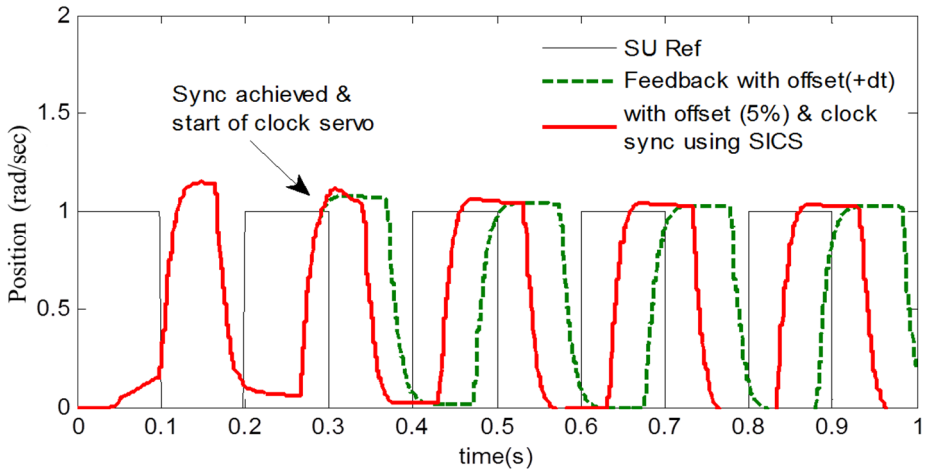

Figure 5.19: Position profile with SICS (Simulation)

Fig.5.19 shows the resulting control performance using the SICS algorithm. It can be seen that the overshoot is significantly reduced (red solid line), and the system response corrects itself for the offset and matches the ideal response in Fig.5.13, thereby keeping the system stable all the time. It can be noticed from the network scheduler (Fig.5.18) that the sampling frequency is reduced by the actuator during the clock correction. By increasing the sampling rate of the local control unit, the PI clock servo can correct the offset faster. However, changing sampling interval might result in unexpected behaviour in the control process, especially in the wireless control as the sampling interval depends on the network delay. This highlights the need to identify an optimal sampling rate to improve the PI clock servo's performance.

As the PI clock servo tries to minimise the integrated square error (ISE) of the offset, this in turn minimises the ISE in the position response induced by the clock offset. Fig. 5.20 shows the ISE of the position response. The synchronisation is achieved at 0.3s and therefore the ISE in the case of offset corrected by SICS (green dotted line) is significantly reduced as compared to the ISE in the case of offset without the SICS approach (blue dashed line). The ISE of the SICS approach remains higher than the ISE of the standard

clock synchronisation without any offset (red solid); however, this is due to the initial error accumulated before 0.3s.

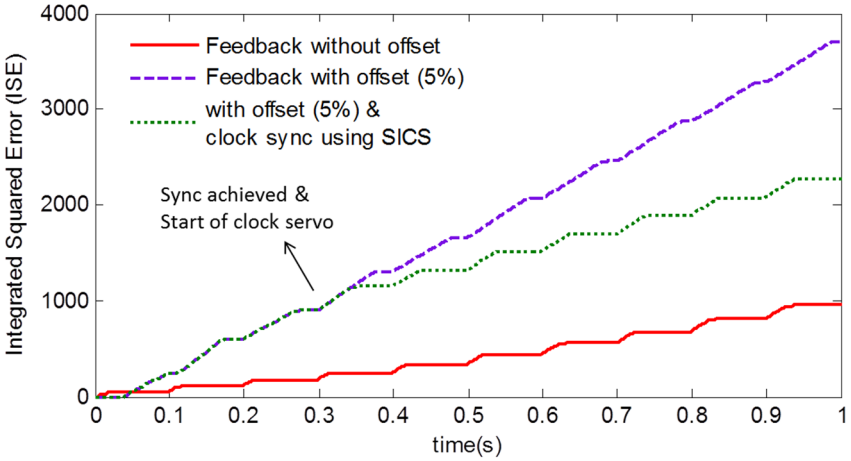

Figure 5.20: ISE of position profile (clock offset)

5.5.2 Clock discipline process to correct clock drift using SICS

Fig.5.21 shows the effects in clock drift when the PI clock servo is used in the local control unit without the SICS algorithm. It can be seen that the integral term in PI controller attempts to correct the clock drift; however, it results in an instant correction. In addition, it can be noticed the clock again starts to drift. This is due to the fact that as drift is a physical phenomenon that affects the clock crystal, even after the drift is corrected, the faulty clock may tend to drift again. Therefore, as compared to correcting a clock offset a clock drift must be corrected continuously until the drift is kept to a minimum.

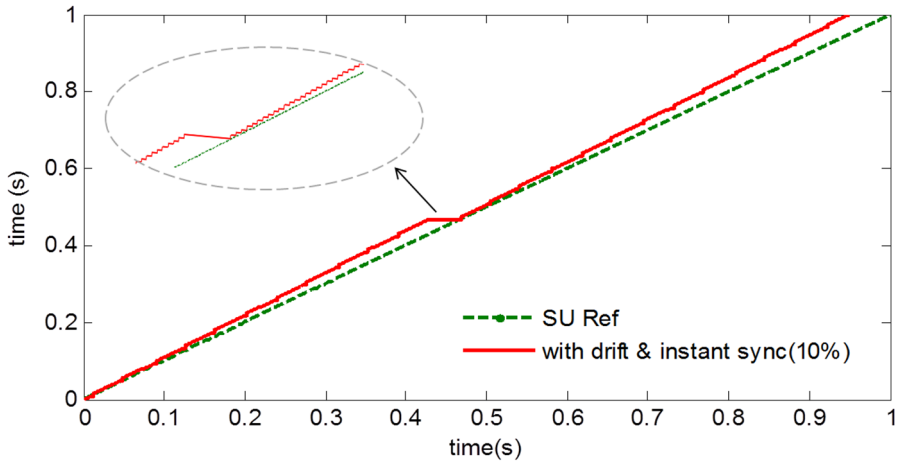

Figure 5.21: Instant clock synchronisation – clock drift

Fig.5.22 shows the effects in clock drift when the PI clock servo is used in the local control unit based on the proposed SICS algorithm. As the PI controller corrects the clock based on the sampling interval it can be seen that the offset is corrected gradually. In addition, it

can be noticed the clock tends to drift again (red solid line), however, the SICS algorithm corrects the drift again as it ensures the drift is corrected every sampling interval.

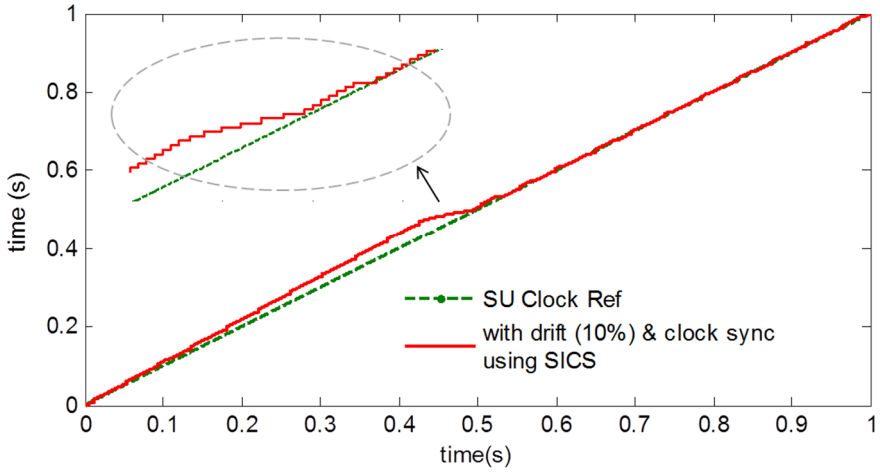

Figure 5.22: Clock synchronisation with SICS

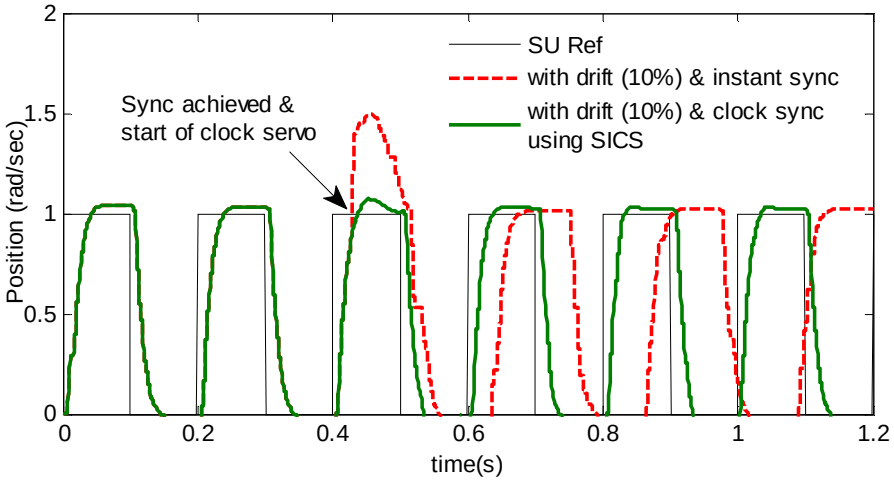

Figure 5.23: Position profile with SICS (clock drift)

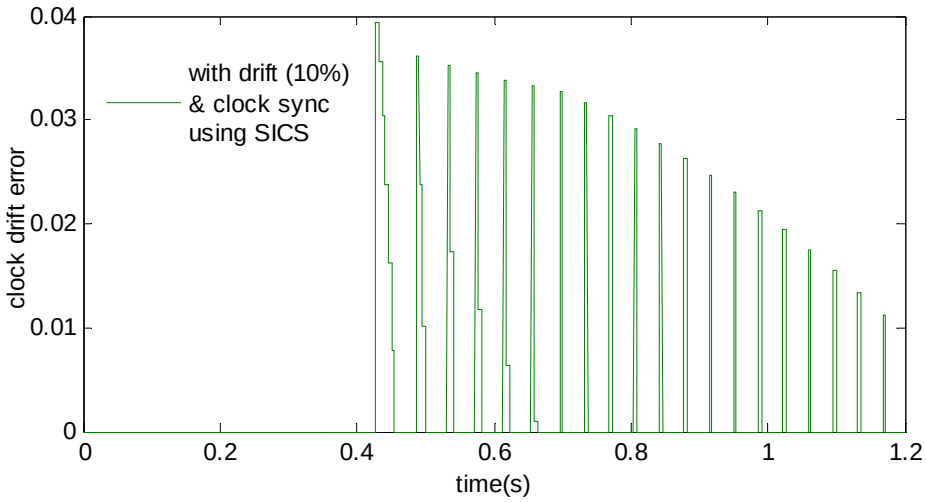

Figure 5.24: Clock drift error with SICS

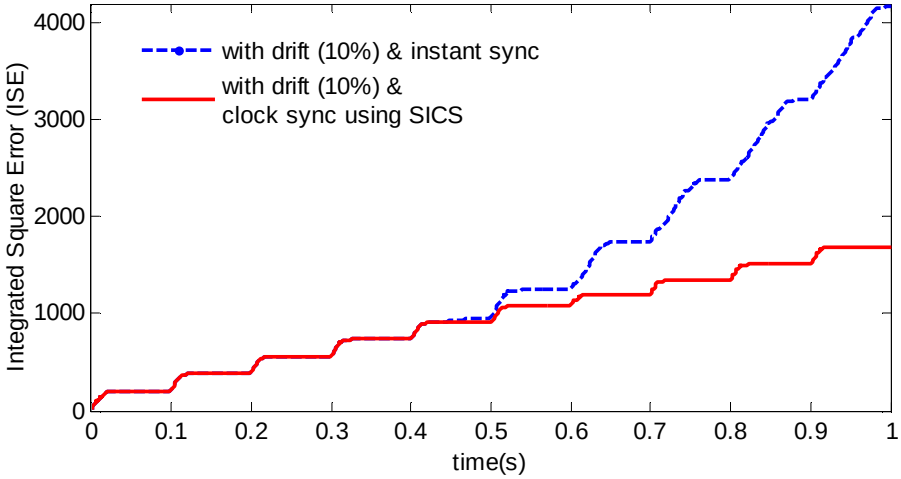

Figure 5.25: ISE of position profile (clock drift)

The resulting control performance of the BLDC motor is shown in Fig.5.23. It is evident that instant clock drift correction (red dashed line) results in overshoots. The performance of the clock drift correction using SICS algorithm (green solid line) shows that the drift is gradually corrected and tracks the reference. The clock drift error is shown in Fig.5.24. As the SICS algorithm continuously monitors the drift, it attempts to reduce the clock drift every time and keeps it to a minimum over time. Fig.5.25 shows the ISE of the position response. It can be seen that ISE in the case of drift corrected by SICS (red solid line) is significantly reduced as compared to drift without SICS (blue dashed line).

5.5.3 Hardware demonstration

This section explains the implementation of the proposed algorithm in the real-time wireless hardware demonstrator used in this research to achieve the best possible synchronisation accuracy. The proposed SICS approach is implemented in the local control unit in the hardware demonstrator to correct the offset (10%). Two additional slave nodes, in addition to the local control unit, are used to increase the overall network delay. The timing response for a control input transmission after the offset is corrected is shown in Fig.5.26.

It can be observed that the Master (Supervisory unit) takes 800 μs to transmit the control input. The slaves (next three graphs) receive the control input shortly after the transmission has begun and acknowledges the transmission after the data packet is completely received after which the master transmission is completed. The slave uses the synchronisation approach to estimate the offset to ensure the local clock is synchronised which takes a further 400 μs as observed from the lower three graphs. Therefore, the total time taken to transmit a clock pulse, receive it and subsequently correct the local control unit's clock using the proposed synchronisation approach requires only 1.3 milliseconds (±1%) (red

double headed arrow in Fig.5.26) while keeping the wireless control loop stable. This synchronisation accuracy is well suited for keeping most of the control loops stable in an industrial setup. This result is particularly good and compares with that claimed by industries. For example, Microstrain has demonstrated clock synchronisation within 5 milliseconds (ms) for industrial applications [Arms, 2009]. The resulting closed-loop system performance is shown in Fig.5.27 while the clock offset is corrected when the wireless control loop is in operation.

It should be noted that though the existing synchronisation algorithms ensure accuracy in ms, these are achieved in a sensor network setup. This research, on the other hand, has achieved synchronisation accuracy in ms in a wireless closed-loop control system while keeping the system stable.

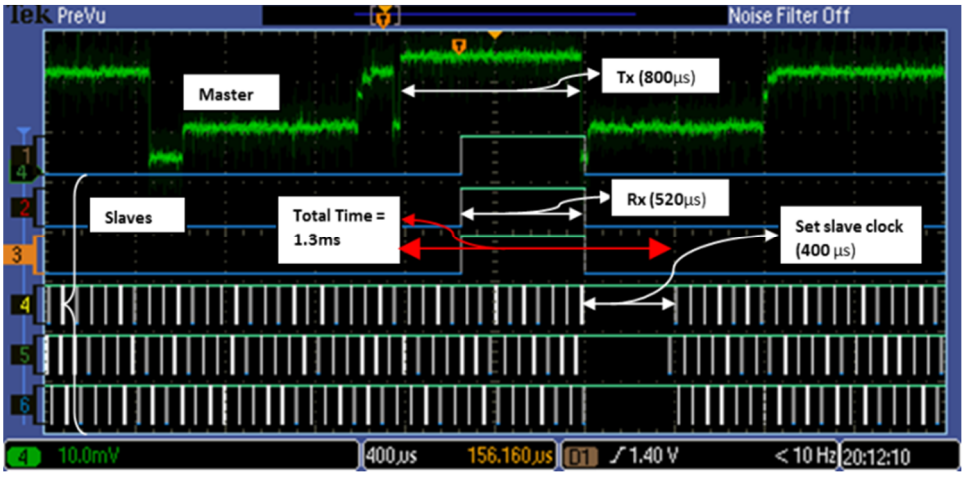

Figure 5.26: Clock synchronisation algorithm performance

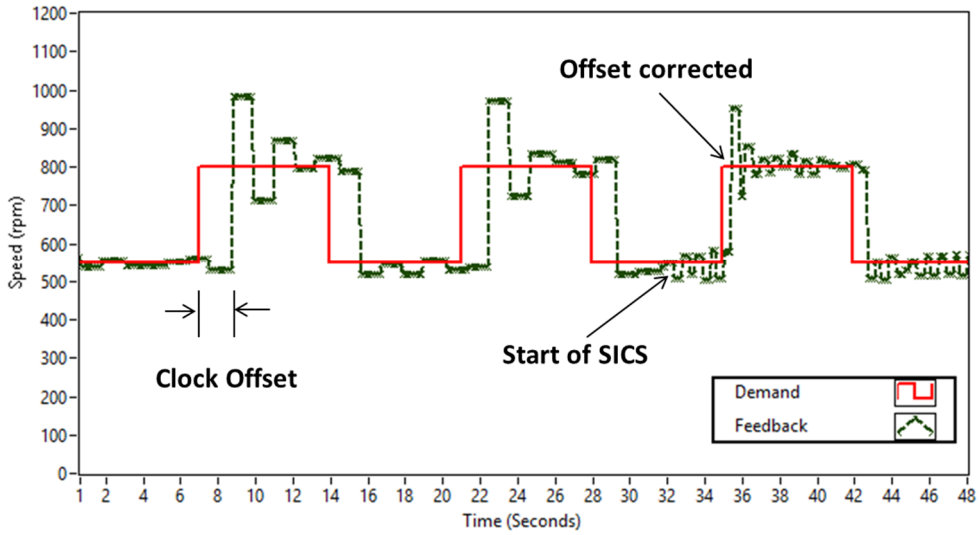

Figure 5.27 Wireless closed-loop control - clock offset correction (HW Demo)

5.6 Summary

There is an increasing interest to implement wireless communication in industrial control systems. Most of the existing research solutions in wireless networked control systems are based on the assumption that the control units are tightly synchronised. A sampling interval based clock synchronisation (SICS) approach for wireless closed-loop control system using the IEEE 1588 PTP protocol is proposed in this research. The SICS approach is suitable for wireless control loops as synchronisation is achieved using the sampling interval in the slave nodes rather than the synchronisation interval. It eliminates the need for multiple synchronisation intervals and the problem of instant clock synchronisation. The SICS approach assists the local controller in correcting its clock offset and drift. While the results are promising, it has been highlighted that an optimal sample rate can further improve the synchronisation accuracy. The proposed algorithm is then tested in a practical wireless control loop using an embedded microcontroller platform. While existing algorithms can achieve accuracy in less than 5 milliseconds, it does so in a pairwise sense without considering the overhead of transmitting control demand, feedback data and sync pulses. In this research work, a synchronisation accuracy of 1.3 milliseconds is achieved, while maintaining the stability of a wireless closed-loop control system in operation.

Chapter 6

Sensorless Supervisory Wireless Control under Intermittent Packet Loss

This chapter presents the issues and performance of a wireless closed-loop control system under lost data packets in a feedback loop. A novel sensorless supervisory wireless control approach that addresses the issue of intermittent packet loss in wireless feedback control loop is proposed. The proposed approach is then evaluated in an embedded hardware environment by introducing interference deliberately in the wireless feedback loop. The packet loss is deliberately introduced in the feedback loop by characterising the packet loss using the Gilbert-Elliott (GE) model. Therefore, the results based on hardware demonstrator are a typical representation of wireless closed-loop control performance under deliberate jamming. Finally, the effectiveness of the proposed algorithm is further evaluated using a simulation model of a wireless aircraft braking system (W-ABS).

6.1 Related Work

Packet loss is one of the major concerns in implementing wireless sensor networks in industrial automation [Gungor, 2013],[Delsing, 2010]. Most of the wireless standards available today including the industrial standards such as WirelessHART and ISA100.11a work in the 2.4 GHz ISM frequency band. Therefore, there is a high chance of devices operating on the same channel and hence leads to the problems like co-existence and channel interference. In wireless sensor networks, this can either increase the delay in the network or collisions of data packets eventually leading to the issue of lost data packets. Depending on the control application, corrupted or dropped data can result in anything from a disruptive glitch to a devastating failure [Poor and Hodges, 2004].

Among the industrial standards, Zigbee is considered to have the highest packet loss probability due to smaller strength of signal being transmitted in order to extend the battery life of the appliance [Kostadinovic, 2009]. Wi-Fi WLAN seems to have a better resilience towards packet loss due to a number of channels available to transmit and multiple frequency ranges. However, due to the number of devices used in the Wi-Fi spectrum, this may hamper the transmission rate and result in packet loss. WirelessHART

and ISA100.11a allows a TDMA based transmission slots so that each node gets a 10ms transmission slot in order to avoid collision with other nodes. However, it has been highlighted in [Petersen, 2011] that the packet loss rate of WirelessHART will increase when it has to coexist with IEEE 802.11 networks due to increase in network traffic load. An approach to reduce the latency and packet loss in WirelessHART networks by introducing deterministic and periodic downlink transmission to actuators is discussed in [Akerberg, 2010]. Moxa has proposed a concurrent dual-radio technology for packet loss issue in industrial WLAN's [Moxa, 2014]. The transmitted node uses two independent RF modules operating in two different frequency bands (2.4 GHz and 5 GHz) to transmit duplicate packets simultaneously. Therefore, if packet loss happens on one band, the duplicate packets from another band could be used.

The wireless control loop performance for a basic control problem using the IEEE 802.11b protocol is analysed in [Ploplys, 2004]. It is proved that the control loop was capable of closed-loop communication rates exceeding 250 Hz with little network data loss under the assumption that the nodes are tightly synchronised. An approach for compensating lost links in a wireless control network such that each node in the network updates its internal state to be a linear combination of the states of its neighbourhood nodes is discussed in [Pajic, 2011]. While this overcomes the drawback of single controller failure, it increases the network complexity. It is highlighted that sensor nodes must be capable of performing more complicated operations such as Kalman filtering in real-time.

In time-series analysis, packet loss is nothing but missing observations in a sequence of data received over a given period of time. Therefore, it is interesting to apply linear prediction techniques [Leborgne, 2007] for reconstructing the packet loss data in wireless control loops. Linear prediction techniques have been widely used in the area of wireless sensor networks to address the issue of intermittent packet loss and lost wireless links [Mostofi, 2009],[Liu & Goldsmith, 2004],[Sinopoli, 2003]. In wireless control systems, the research is fairly recent and early works [Schenato, 2009],[Henriksson, 2009],[Kawka, 2006] suggest approaches to use a stochastic 2-state Markov network model wherein the last received sample is used to estimate the control input during packet loss. An approach to predict the control input based on the previously received control inputs during packet loss over wireless networks is proposed in [Bin, 2008]. A simple solution to packet loss in wireless sensor and actuator networks (WSAN's) where the actuator produces an estimate of the sensed value based on the previous consecutive measurements to compute the control demand is proposed in [Xia, 2011]. A system identification based solution to compensate packet loss using ARMA modelling is proposed in [Short, 2011]. The drawbacks of such approaches are highlighted in Section 6.3.3.

In general, most of the literature dealing with packet drops in networked control considers two different strategies namely zero-order hold and first-order hold [Schenato, 2009]. In zero-order hold the control input/sensor data is set to the last received value whenever there is a packet loss whereas in first-order hold the control input/sensor data is estimated

using a set (usually the last two received samples) of data stored in a buffer to increase the credibility of the data. Model based predictive control [Ulusoy, 2011] (and references therein) methods are widely used to address the issue of burst packet loss in wireless networks. In these approaches, the controller predicts n future control signal estimates and sends it along with the current input. Whenever there is a packet loss, the actuator can use the input demand for the corresponding time instant stored in the buffer. While such approaches can keep the system stable under constant input demand, they may not perform well under varying input demand as in high dynamical systems.

It should be noted in all these approaches the idea is to move the controller action to the actuator end and thus control the actuator locally during packet loss. Evidently, this requires more computational capabilities in the actuator unit and network resources. The key issues due to intermittent packet loss in wireless closed-loop control systems are as follows:-

- In control systems, measured data is used as feedback to the controller to estimate the control input. Missing measurements could cause a large error in the control demand estimation.
- If the sensor data is lost for a significant period, then the new sensor data arriving could cause large overshoots while the controller tries to correct the accumulated error during the data loss period.
- The longer the data loss period it's more likely the system will reach an unstable state. For instance, for control systems that are divergent in nature such as Jet engines, the control system will rapidly diverge from a stable state if the feedback information is not provided.
- A control system may recover from short term random data loss as the controller corrects the error recursively. However, even in this scenario the system may become unreliable if the data loss happens during transient operation.

In addition, as explained in the literature review (Section 2.4), the existing results in this domain lack an experimental evaluation in a real-time wireless embedded hardware platform. In addition, in works that utilise wireless hardware units where the data transmission (sensing/demand) is sent over a wireless channel, the control algorithm is based on a computer-based simulation model that in turn depends on a general-purpose processor and operating system which may overlook many issues that become more obvious in embedded systems.

Therefore, in this research the stand-alone embedded wireless hardware demonstrator designed in Chapter 4 is used that incorporates the control algorithm as well as the radio transmission without any dependency on external processors. In addition to the existing hold (zero/first) strategies for packet loss in literature, in this research, a sensorless supervisory control approach for wireless real-time control for critical industrial applications is proposed. The advantage of the approach is that while a supervisory unit provides the adjustments to the control demands, a local control unit can take control of the critical loops.

6.2 Packet Loss model

Packet loss modelling is important in wireless control systems. If the loss status of a data packet in a wireless channel at time k depends on the preceding packets, then it is known as a kth order Markov chain model. Based on the order of the Markov model, the following two packet loss models are frequently used in networked control systems as they characterise the communication errors that occur in a wireless network.

6.2.1 Bernoulli packet loss model

Bernoulli packet (BP) loss is based on the Bernoulli property that is defined as, in a probabilistic event, the chances of failure and success are mutually exclusive, that is they are independent of each other. Therefore, a Bernoulli packet loss determines whether a packet is received or not. This is known as independent channel model or random loss model and it is the simplest approach to define packet loss in a wireless communication medium. Bernoulli packet loss model is a 0-th order Markov chain model (see Fig.6.1), as the probability of packet loss is independent. If the packet loss rate is represented as P_L, for a block of n consecutive data packets, the probability of j packet losses is given by the binomial distribution [Xunqi, 2005],

$$P(j,n) = \binom{n}{j} P_L^j (1-P_L)^{n-j}, n \geq 1, 0 \leq j \leq n \tag{6.1}$$

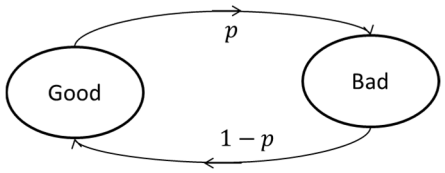

Figure 6.1: Bernoulli packet loss model

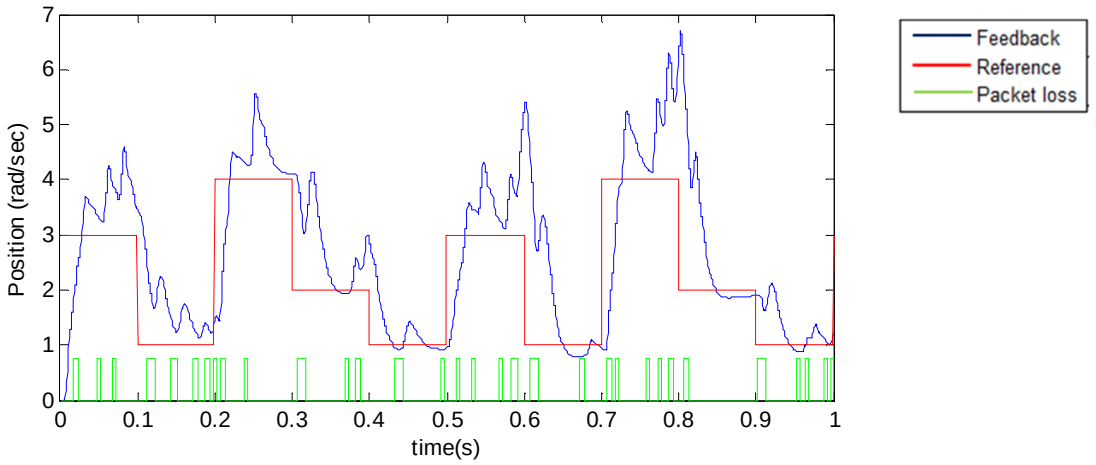

Figure 6.2: Wireless control performance under Bernoulli packet loss

The wireless closed loop control simulation model (designed in Section 4.5.2) is used to analyse the effects of the packet loss model. The effect of packet loss (40%) on the feedback data characterised by the BP model is shown in Fig.6.2.

6.2.2 Gilbert-Elliott model

In industrial systems, packet loss in wireless channel or any unreliable communication medium, the packet loss is identified to be of burst nature rather than of being random. Burst packet loss is defined as those where a series or a burst of contiguous data packets is lost over the communication channel. This scenario is more representative in wireless networks, especially when the packet loss is caused by interference or deliberate jamming. As burst error packets are contiguous, they are clearly depending on the preceding packets. Therefore, burst error packets are modelled using the Gilbert-Elliott (GE) packet loss model [Almstrom, 2009] which is a 1st order Markov chain model (see Fig.6.3). In GE model, there are two states, a good state and a bad state and two transition probabilities that represent the transfer from the good state to the bad state and vice-versa.

If the steady state probability of being in the reception state is given by $p(g|g)$ and the steady state probability of being in the loss state is $p(b|b)$,

The transition probability from reception state to loss state is given by,

$$p(g|b) = 1 - p(b|b) \tag{6.2}$$

and the transition probability from loss state to reception state is given by,

$$p(b|g) = 1 - p(g|g) \tag{6.3}$$

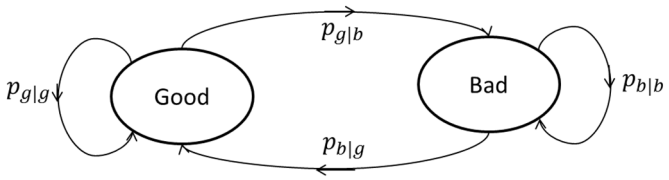

Figure 6.3: Gilbert-Elliott packet loss model

The effect of packet loss (40%) on the feedback data characterised by the GE model is shown in Fig.6.4. The bursty nature of the GE model can be noticed in comparison to the effect of BP model shown in Fig.6.2. As GE model characterises the packet loss in a wireless network more efficiently, the packet loss induced in all the experiments in this research is based on this model. The burst packet loss is induced for both simulation and hardware experiments. In case of the hardware demonstrator, the burst packet loss is deliberately introduced in the feedback loop by forcing the packet loss characterised by the GE model. Therefore, the results based on the hardware demonstrator are a typical

representation of wireless closed-loop control performance under deliberate jamming. For ease of analysis, the packet loss is introduced only in feedback loops, and the control demand is assumed to be received at all times. However, the control demand is still sent over the wireless channel to increase the network load.

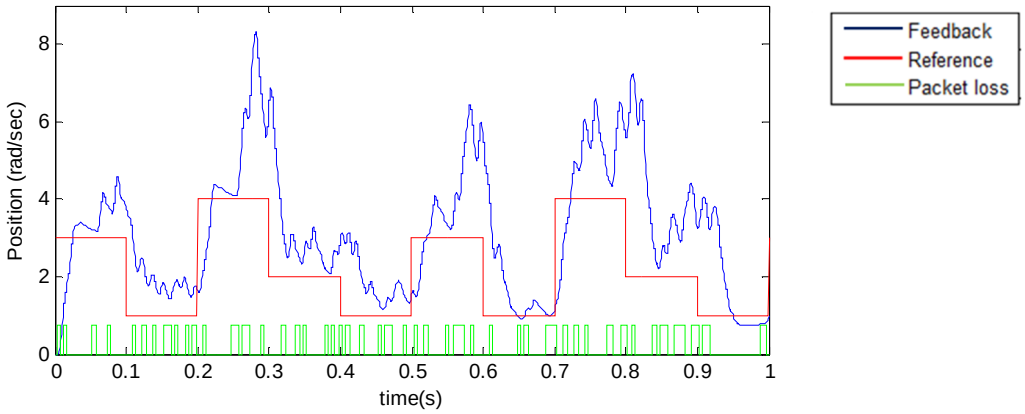

Figure 6.4: Wireless control performance under Gilbert- Elliott packet loss

6.3 Linear Prediction Techniques

Linear prediction is the process of estimating the future values of a discrete-time signal based on a linear combination of past values. The concept of linear prediction is widely used in the control domain for estimation of control parameters and in industrial applications for forecasting future system inputs based on previous values [Khan, 2011]. Wireless control systems are classified as discrete-time systems and the sampled signal is given as $x(kT)$, where kT is the sampling time interval. The measurement data (z_k) of a linear prediction model can be represented as:-

$$z_k = \sum_{i=1}^{p} a_i \, x_{k-i} \tag{6.4}$$

where, p is the linear prediction filter order, a_i is the filter co-efficient and x_{k-i} is the previous data samples. The zero-input strategy and hold-input strategy are widely used for packet loss compensation when a control system is closed over a network [Schenato, 2009]. Therefore, in this research, the performances of these two strategies are first analysed on a real-time wireless control loop. It then describes one step further than this, a sensorless supervisory control approach for industrial wireless closed-loop systems. The position of the BLDC motor is considered for the simulation result analysis. Speed data is used for analysis in the hardware demonstrator due to reduced complexity in speed computation in the embedded processors using Hall sensors.

6.3.1 Zero-order hold

In (6.4), if p=1, the equation becomes,

$$z_k = a_1 x_{k-1} \tag{6.5}$$

Considering the linear prediction coefficient a_1=1 (maximum weightage due to only one sample available at any time), the above equation becomes,

$$z_k = x_{k-1} \tag{6.6}$$

This is nothing but retaining the last received value as measurement data in case of data loss. Perhaps the simple way to support a controller with feedback data in case of data loss in a wireless feedback loop is to substitute the feedback data with the last received sensor value. This is known as the zero-order hold (ZoH) technique in literature. Zero-order hold technique can be quite efficient in wireless control systems where the sampling happens at long intervals or the dynamics of the systems changes in a slow manner.

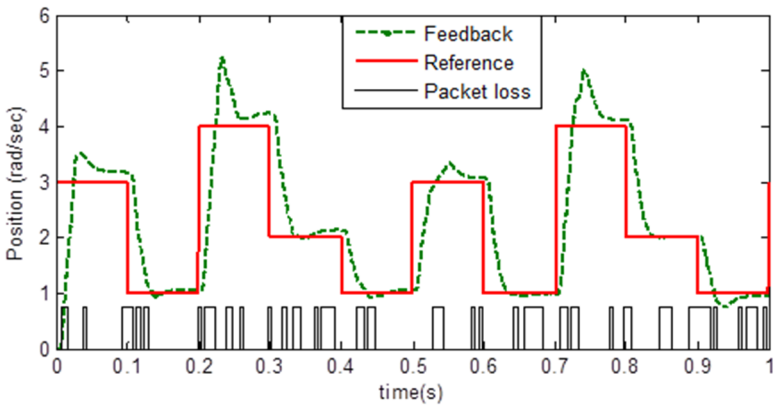

Figure 6.5: Case 1: Zero-order hold - wireless closed-loop control (simulation)

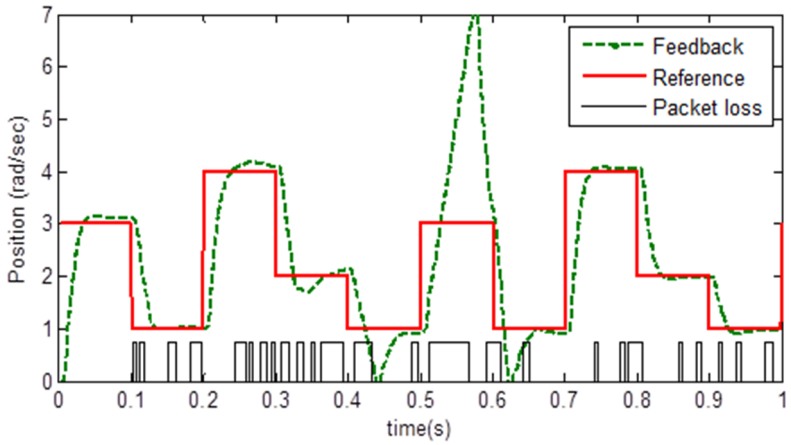

Figure 6.6: Case 2: Zero-order hold - wireless closed-loop control (simulation)

Fig.6.5 shows the position output of the BLDC motor controlled over the wireless channel with packet loss in the feedback loop, employing zero-order hold for missing data. Based on the Gilbert-Elliott packet loss model, the packet loss rate in the good state is chosen as 24% and the packet loss rate in the bad state is chosen as 40%. It can be seen that the zero-order hold technique performs sub-optimally if the packet loss rate is very low (in the good state) and if there is no change in the demand. However, if the packet loss rate is increased further (in the bad state) such that length of a burst error is significant, then the zero-order hold results in large overshoots and degraded system performance which can be seen at 0.5s in Fig.6.6.

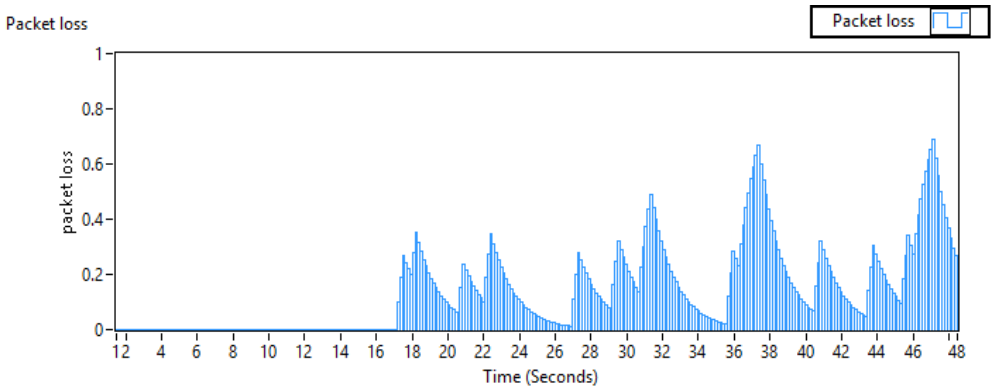

Figure 6.7: Zero-order hold – Packet loss (HW demo)

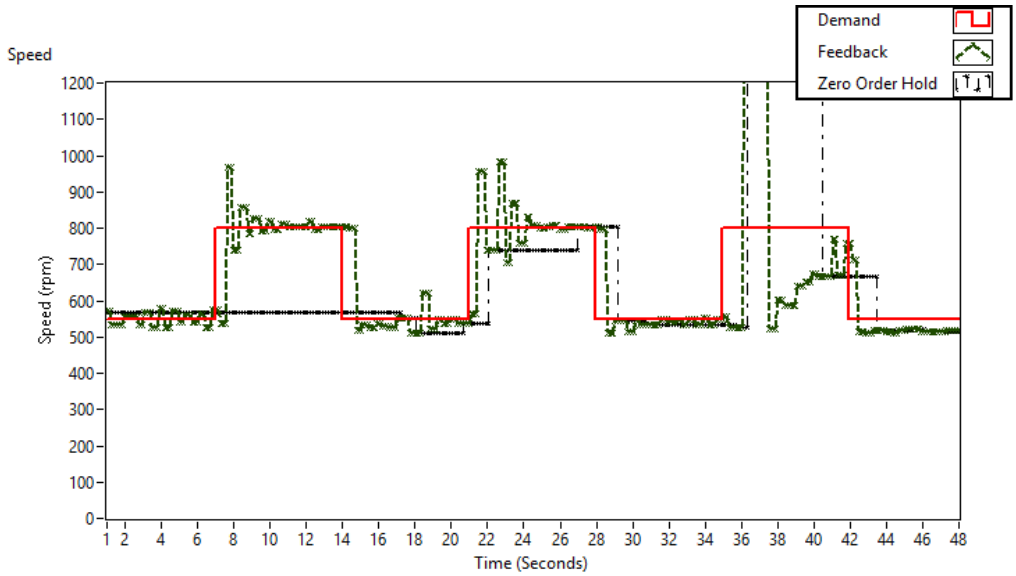

Figure 6.8: Zero-order hold – wireless feedback control (HW demo)

Fig.6.8 shows the speed of the BLDC motor controlled over wireless channel using the hardware demonstrator (HWD). It can be noticed that zero-order hold (black dot-dashed lines) supports the controller with the last held data for a packet loss rate of 10% (until 30s in Fig.6.7). However, the feedback response oscillates as the packet loss rate is increased and when the packet loss rate is over 40% (after 36s in Fig.6.7), the system exhibits large overshoots (see Fig.6.8) especially after a change in the demand. It is shown that the

response becomes very slow in reducing the steady state error after a large overshoot based on the zero-order hold data. In the case of the HWD, the feedback data is defaulted at 500 rpm so as to prevent any sudden surge in the current due to large control error. Therefore, the measurement resumes after significant packet loss, otherwise such a large overshoot may render the system unstable. In addition, zero-order hold may not hold good if the data is lost for a significant time period.

6.3.2 First-order hold

In first-order hold the last received two samples is utilised to estimate the measured data in case of missing data or lost sensor values. This gives more credibility to the estimated data as two received samples can give more information to the estimated data as compared to a single sample. If p=2, equation (6.4) becomes,

$$z_k = a_1 x_{k-1} + a_2 x_{k-2} \tag{6.7}$$

However, there is a need to calculate the linear prediction coefficients in order to weight the received samples. This can be classified as follows:

Case 1: Mean based approach (a_1= 0.5, a_2 = 0.5)

$$\therefore \quad z_k = \frac{x_{k-1} + x_{k-2}}{2} \tag{6.8}$$

If the linear prediction co-efficient are equal, that is, considering both the received samples with same credibility, then it is known as mean/average approach or equally weighted mean based approach. The control response for both simulation (Fig.6.9) and HWD (Fig.6.11) is given below. It can be noticed that the overshoot happens when a transient change happens in the input demand during the packet loss.

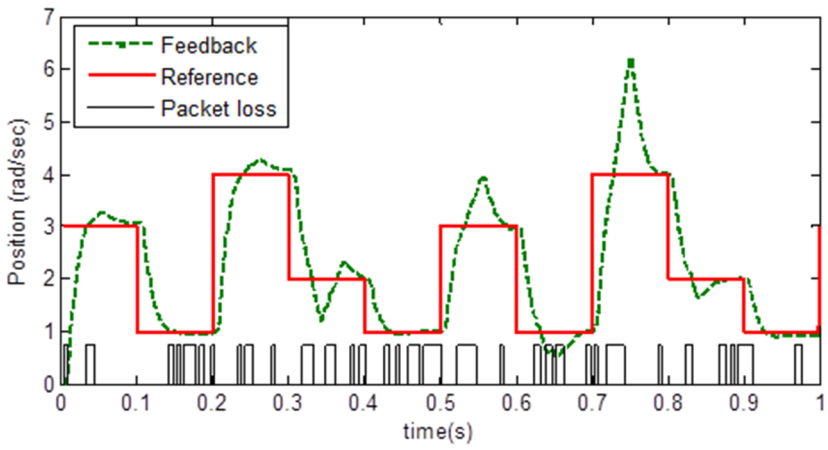

Figure 6.9: First-order hold - wireless feedback control (simulation)

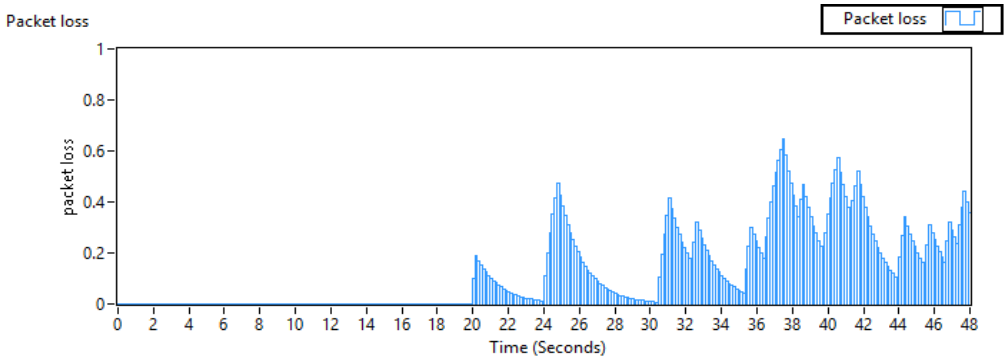

Figure 6.10: First-order hold – Packet loss (HW demo)

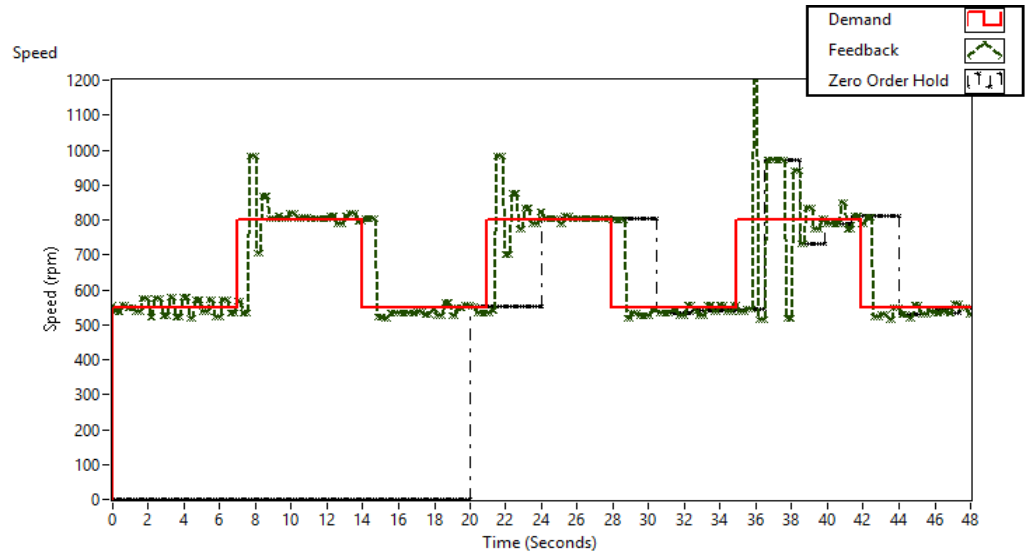

Figure 6.11: First-order hold – wireless feedback control (HW demo)

Case 2: In mean based approach, equally weighted samples may not be an optimal solution always. This is due to the fact that in linear prediction, for any given time step k, the most-recent sample has more credibility to the predicted data while the far most received data sample has less effect on the prediction. However, there is no set method to estimate the linear prediction coefficients as this depends on the characteristics of the given time-series data. Therefore, in linear prediction, the most recent sample needs to be given more weight as compared to the far most samples in the prediction series. This is known as the different weighted mean approach. As only two samples are considered in a first order hold, the linear prediction co-efficient can be calculated on an intuitive basis based on the received samples. The following two different cases are considered here. Fig.6.12 shows the case, where comparatively more weightage is given to the $(k-1)$ data as compared to the $(k-2)$ data. In this case, the system showed a sub-optimal response.

(i) a_1= 0.75, a_2 = 0.25

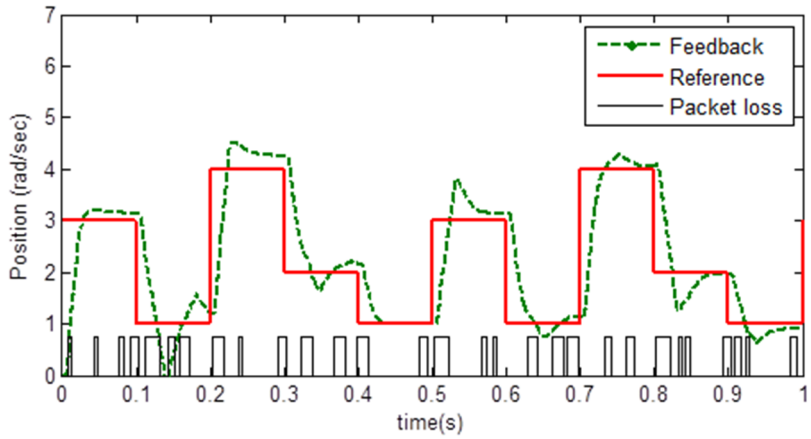

Figure 6.12: Case 1: First-order hold - wireless feedback control (simulation)

(ii) a_1= 0.90, a_2 = 0.10

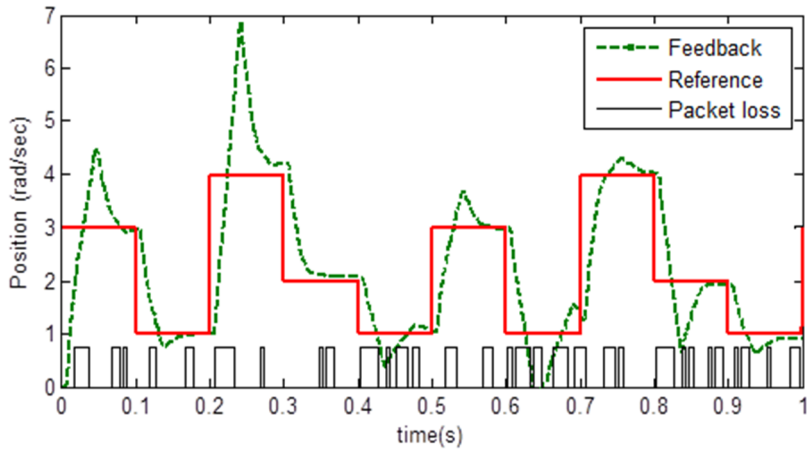

Figure 6.13: Case 2: First-order hold - wireless feedback control (simulation)

Fig.6.13 shows that the performance of a first-order filter is similar to a zero-order filter due to the fact that the last received sample $(k-1)$ is heavily weighted and the $(k-2)$ sample is weighted less. The hardware results showed a similar response to Fig.6.11.

Performance analysis:

The integrated absolute error (IAE) is used to analyse the performance of the linear prediction algorithms as shown in Fig.6.14. The increase in percentage error as compared to the feedback data (with no data packet loss) is given in Table.6.1. The first-order hold with different weighted mean technique offered a significant reduction in the overall percentage error (only 5%) as compared to the first-order mean based approach (15%) and the zero-order hold (24%).

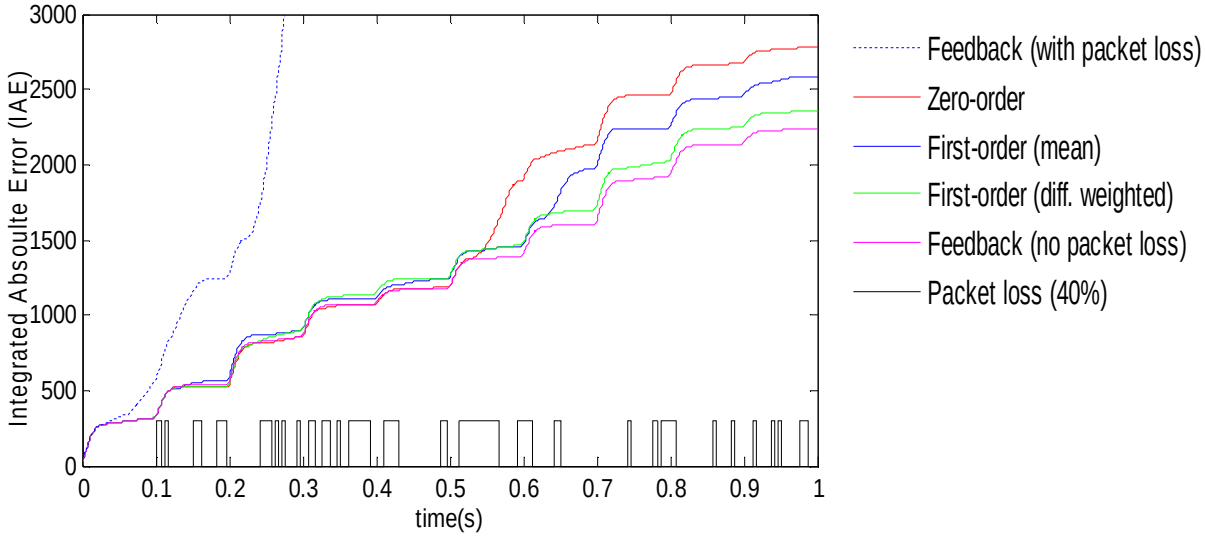

Figure 6.14: Performance analysis (Linear prediction)

Linear Prediction techniques	**Percentage increase in IAE compared to feedback data without packet loss**
Zero-order hold	24%
First-order hold (mean approach)	15%
First-order hold (different weighted mean)	5%

Table 6.1: Percentage increase in IAE of Linear prediction approaches

6.3.3 Sliding window / Moving average approach

For p>2, Equation (6.4) can be represented as,

$$z_k = \frac{1}{p}(a_1 x_{k-1} + a_2 x_{k-2} + \cdots a_p x_{k-p}) \tag{6.9}$$

This is known as moving average approach. As the number of sampled data in the linear prediction series increase, the computational complexity increases. In addition, data that is received well past in time may not be useful for future predictions. Therefore, there is a need to utilise the newly received samples and exclude the data received well past in time in (6.9). Hence, the averaging technique moves linearly over time and hence the name moving average approach. However, there is a need to select the optimal number of samples at any given time to perform the averaging efficiently. Since the maximum number of data received at any given time is limited by the linear prediction filter order, the number of samples required for a given averaging function can be decided using the sliding window approach.

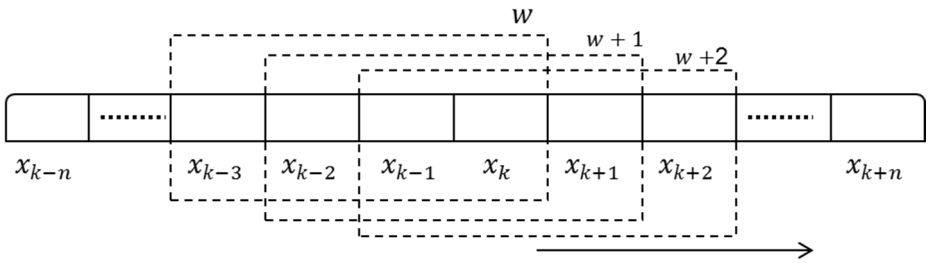

Figure 6.15: Sliding window / Moving average approach

However, the selection of linear prediction co-efficient becomes more difficult due to the fact that a set of co-efficient $[a_1, a_2, \dots a_p]$ for window (w) may not work well for window $(w + 2)$ in predicting the data. In such cases, the linear prediction coefficients can be calculated such that a cost function J that represent the mean or total squared error of the residual e_k (between the actual and the predicted data) is kept to a minimum.

$$\frac{\partial J}{\partial a_i} = 0 \qquad 1 \leq i \leq p \tag{6.10}$$

In addition, the linear prediction coefficients can be predicted using the autocorrelation or auto-covariance method. The underlying matrix equation is given by,

$$A_a = R_z^{-1} r_\gamma \tag{6.11}$$

where, A_a is the linear prediction coefficient matrix, R_z is a $p \times p$ autocorrelation matrix, and r_γ is autocorrelation column vector.

Calculation of the linear prediction coefficients (LPC's) through these methods involves O(p^3) additions, multiplications and inversion of the R_z matrix. In addition, as the linear prediction filter order (p) increases, the computational complexity increases. Various algorithms have been proposed in the literature such as Levinson-Durbin, Leorux-Gueguen and Schur algorithms to reduce the computational efforts in calculating LPC's. It has been shown that the Levinson-Durbin method for calculating the LPC's can reduce the computational effort from O(p^3) to O(p^2) [Khan, 2011].

Summary:

Linear prediction approaches offer solutions to estimate the feedback data in case of lost data packets and missing sample values in wireless closed-loop control. However, as the linear prediction filter order increase, a significant number of samples need to be stored, which increases memory requirements in embedded systems. In addition, these approaches purely depend on the measurement data observed over time. If there are frequent changes in the system control input, this will reflect in the measured feedback data and if the data is lost at irregular intervals, this might induce errors in averaging.

Therefore, there is a need to analyse approaches for data compensation under packet loss that will estimate data without the need for storing previous samples. In addition, for wireless control systems, if the prediction approach considers the system model, this will enable the prediction approach to incorporate any change in the control process and analyse the feedback data more efficiently. In the literature, this approach is widely classified as state estimation using filtering techniques.

6.4 State Estimation and Filtering

State estimation in control systems is the process of estimating the states of a control system based on the observed outputs from the control process. It is done using a state observer that contains the state-space model of the control system being observed. The inputs that are fed to the actual plant is also fed to the observer and based on the outputs received from the control process the future states of the system can be estimated. The error between the received measurements and the estimated state is weighted by an appropriate gain known as observer gain. This is termed as the residual or innovation which is then added to the state observer to estimate the states.

Filtering is the process of extracting an output signal corrupted by a noise source. The noise source can either be overlapping or non-overlapping with the signal. If the noise source is non-overlapping, then the signal can be extracted using a low-pass filter, high-pass filter or a band-pass filter. However, if the noise is overlapping with the signal, then it is difficult to separate the original signal from noise. Therefore, instead of extracting the signal from the noise source it can be reconstructed using linear filtering techniques. The linear filtering techniques can further be classified into three types as follows:-

Prediction: Prediction is the process of estimation of a particular state of the control system at a given time k, based on the measured output signal observed from the control process up to time $(k-1)$.

The mathematical representation is given as,

$$(x_{k-1}|z_{1:k-1}) \rightarrow (x_k|z_{1:k-1}) \tag{6.12}$$

Therefore, the system predicts the future state based on the previous state (system model) and the measurement data available until the last time instant $(k-1)$, where k- current time instant. Therefore, prediction can be defined as,

Given the measurements available until the last time instant, $(x_k|\, z_{1:k-1})$ *, what is the next state?*

Filtering: In discrete-time control systems based on state-space modelling, filtering can be defined as a process of extracting information about a particular state of the control system at a given time k, based on the measured output signal observed from the control process up to and including time k.

$$(x_k|z_{1:k-1}) \rightarrow (x_k|z_{1:k}) \tag{6.13}$$

Therefore, filtering can be defined as,

Given the measurements available until the current time instant, $(x_k|\, z_{1:k})$ *, what is the current state?*

Smoothing: Smoothing is the process of estimation of a particular state of the control system at a given time k, based on the measured output signal observed from the control process up to a time instant greater than k. Smoothing is a form of reconditioning the state estimates where data after the time of interest k is used for estimating a state at k.

The mathematical representation can be given as,

$$(x_{k+n}|z_{1:k+n}) \rightarrow (x_k|z_{1:k+n}) \tag{6.14}$$

For wireless real-time control systems, prediction and filtering are more applicable as smoothing is more of an offline process where n set of data including past, present and future samples is available for estimation. In wireless closed-loop control, compensation is only needed for the current packet dropout and there is no possibility of utilising future values. For robust control in wireless control systems, prediction and filtering can be utilised to estimate the systems states under packet loss and network disturbance. In literature, these two properties are utilised by the celebrated Kalman filter. Therefore, the Kalman filtering algorithm is used in this research to determine its suitability for wireless closed-loop control systems.

6.4.1 Kalman filter

The Kalman filter is a recursive estimation algorithm that can be used to predict unknown system states, in the case of noisy measurements, based on the underlying system dynamics. It was proposed by Kalman [Kalman, 1960] and since its inception, the Kalman filtering approach had proven beneficial for filtering noisy data in many industrial applications. Application of Kalman filtering in aerospace applications has been discussed in [Grewal, 2010],[Xue, 2010]. Issues such as intermittent observations and partial observation losses arising in wireless sensor networks have been addressed using a Kalman filter in [Liu & Goldsmith, 2004] and [Sinopoli, 2003]. In wireless real-time

control systems, the data transmitted and received are discrete in nature. Therefore, a discrete-time Kalman filter is considered in this research. The Kalman filter is used to estimate a discrete-time controlled process that is governed by the following difference equation:

Estimated State , $$x_k = Ax_{k-1} + Bu_{k-1} + m_{k-1} \quad (6.15)$$

Measurement Data , $$Z_k = Hx_k + n_k \quad (6.16)$$

where, u_{k-1} is the control input, H is the measurement matrix, m_k is the process noise and n_k is the measurement noise. x_k is the current state of the system, where k is the current time step. $A_{n\times n}$ is the state transition matrix and $B_{n\times m}$ represents input matrix (m is the number of inputs).

Both the process noise and measurement noise is assumed as a Gaussian, zero mean white noise with normal probability distribution. The discrete-time Kalman filter is implemented using a two-step approach [Welch and Bishop, 2014]. The first step, known as *a-priori* state estimation, predicts the system state and the estimation error co-variance for the next time step:

Predicted system state: $$\hat{x}_k^- = A\hat{x}_{k-1} + Bu_{k-1} \quad (6.17)$$

Predicted error co-variance: $$P_k^- = AP_{k-1}A^T + Q \quad (6.18)$$

Here $\hat{x}_k^-$ represents the a-priori state estimate, P_k^- is the *a-priori* error covariance estimate, Q is the process noise covariance matrix which represents the uncertainty in the predicted system states. The second step is known as the *a-posteriori* estimate or the measurement update. In this stage, the estimated state and the error co-variance are updated using the measurement feedback data. The measured data is weighted using the Kalman gain. The equations are given by:

Kalman Gain: $$K_k = P_k^- H^T (HP_k^- H^T + R)^{-1} \quad (6.19)$$

Updated system state: $$\hat{x}_k = \hat{x}_k^- + K_k(Z_k - H\hat{x}_k^-) \quad (6.20)$$

Updated error co-variance: $$P_k = (I - K_k H)P_k^- \quad (6.21)$$

The above process is repeated recursively. The time update equations can also be thought of as predictor equations, while the measurement update equations can be thought of as corrector equations. Indeed, the final estimation algorithm resembles that of a predictor-corrector algorithm. The Kalman filter is a recursive filter and therefore, relies on the measurement data for quick convergence. In equation (6.20), the difference between the measured data and the predicted data $(Z_k - H\hat{x}_k^-)$ is known as the residual. As long as the

measurement is received, based on the discrepancy in the residual, the Kalman gain weights it appropriately and updates the system state. It provides the following advantages as compared to the time-series based linear prediction approaches:-

- Only the current measured data is needed to update the system states as compared to traditional approaches where a large set of data is needed for a good estimate.
- As state estimation using Kalman filter uses a system model, it is easier to capture the change in system dynamics and incorporate any change in the input demand (which is the case in wireless control systems) whereas linear prediction approaches does not utilise a system model for estimation.
- A Kalman filter can be utilised for online estimation for missing data whereas, in linear prediction approaches where the filter order is greater than two, there is a need for analysing the trend offline. A linear prediction function is pre-determined using system dynamics and later utilised for missing sample estimation.
- Therefore, every time there is a change in the system dynamics the linear prediction based techniques have to repeat the entire offline based estimation process and apply the new linear prediction function for estimation [Short, 2011].

6.5 Sensorless Supervisory Wireless Control

A supervisory wireless control approach was proposed in the Chapter 4 for wireless real-time closed-loop control systems. A sensorless approach is proposed in this section to increase the robustness of the supervisory wireless controller and to ensure the system stability during packet loss. In wireless control systems, there is a need for prediction approaches compensating for lost data packets to consider the underlying system model. This will enable the prediction approach to incorporate any change in the control process and utilise the feedback data more efficiently.

Sensorless control has been an active area of research since the last decade. In the past, this approach has been widely applied to the control of DC and PMSM motors [Preindl, 2011],[Gamazo, 2010]. Utilising sensorless control to address issues in networked control systems [Ahmadi, 2014] is gaining interest in recent years. However, applying them to wireless real-time control is very much at its infancy. Therefore, in this research, a sensorless supervisory control algorithm based on a Kalman filter is proposed to predict the feedback data in the case of packet loss in the feedback loop.

6.5.1 Theory of operation

The supervisory unit identifies the lost data packets in the feedback loop as follows. The supervisory unit has an understanding of the round trip delay time t_{rtd} in the wireless network based on the clock synchronisation approach proposed in Chapter 5.

Round trip delay time: $t_{rtd} = t_{ca} + t_{ac}$ (6.22)

Time delay (actuator – controller): $\therefore\ t_{ac} = t_{rtd} - t_{ca}$ (6.23)

where, $t_{ca}$is the time delay between controller and actuator (sec), t_{ac} is the time delay between actuator and controller (sec).

Real-time control systems have tight deadlines, and therefore, the feedback data is expected within t_{ac} in order for the control loop to be stable. Whenever the data received exceeds this delay time it is deemed to be a data packet loss. Then the supervisor unit immediately resorts to the Kalman filter predicted state for that particular time instant. The supervisory unit uses the Kalman predicted states until it receives the next feedback data within the allowed delay time thereby guaranteeing the network stability. The architecture of the sensorless supervisory wireless control for industrial systems using a discrete-time Kalman filter is given in Fig.6.16.

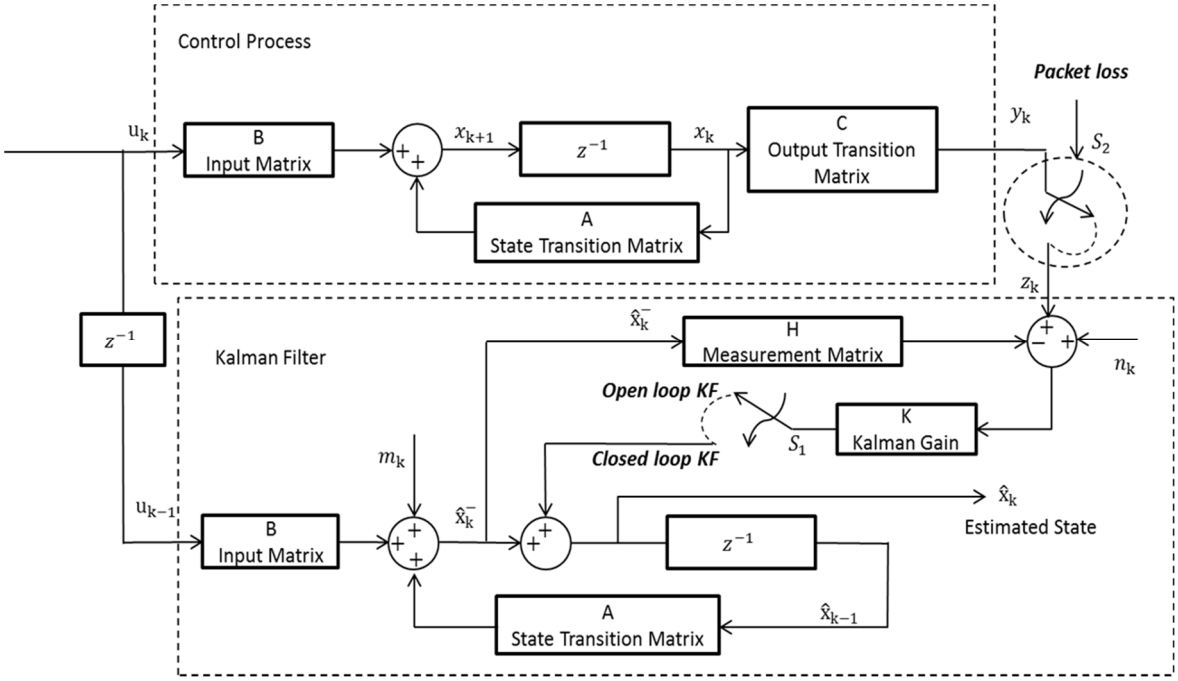

Figure 6.16: Sensorless supervisory wireless control – Methodology

The Kalman filter is designed such that it has an approximate model of the actual system being controlled with an initial estimation of process noise covariance and measurement noise covariance. The sampled feedback data y_k (represented by the switch S2 in closed position) is fed to both the controller as well as the Kalman filter. The packet loss in the feedback data is represented using the switch S2 in an open position.

As Kalman filter in turn depends on the measurement data for its correction step this is represented by the switch S1 in Fig.6.16. When the switch S1 is in a closed position, the Kalman filter is termed as closed-loop Kalman filter. As long as there is no packet loss, switch S2 and S1 will be closed and based on the discrepancy in the residual, the Kalman gain weights the measurement Z_k appropriately and updates the system state. The following cases are considered based on the states of switch S1 and S2.

Case (i):- S1 and S2 closed (No lost data)

The performance of the closed-loop Kalman filter for wireless closed-loop control under no packet loss is shown below for both simulation and HWD setup. The position feedback (rad/sec) is considered for analysis in simulation setup and the speed feedback (rpm) is considered for the hardware setup. Fig.6.17 shows the Kalman estimated state in a simulation setup.

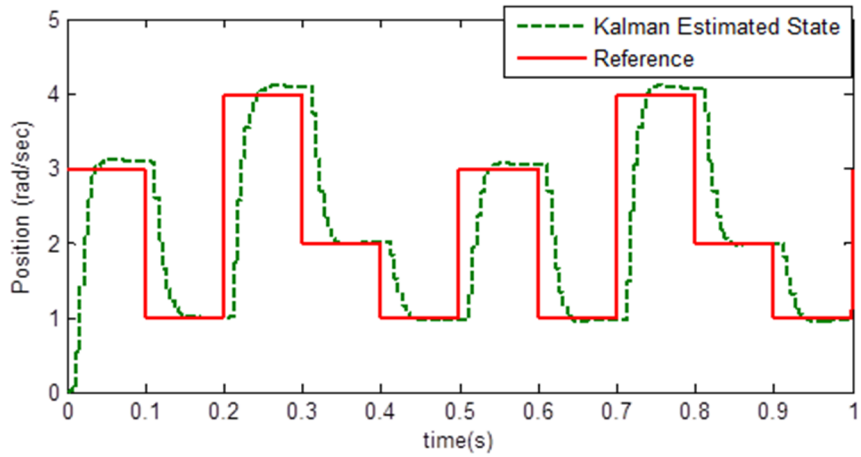

Figure 6.17: Kalman estimation under no packet loss (simulation)

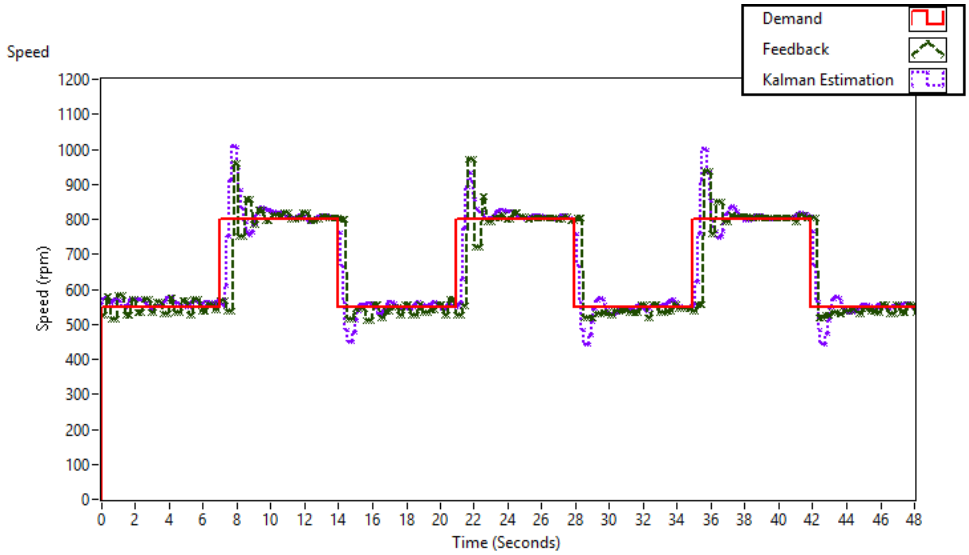

Figure 6.18: Wireless feedback control (WFC) under no packet loss (HW demo)

Fig.6.18 shows the Kalman estimation as well as the actual feedback from motor under no packet loss using the HWD setup. For clarity, Fig.6.19 shows the Kalman estimation and the reference data.

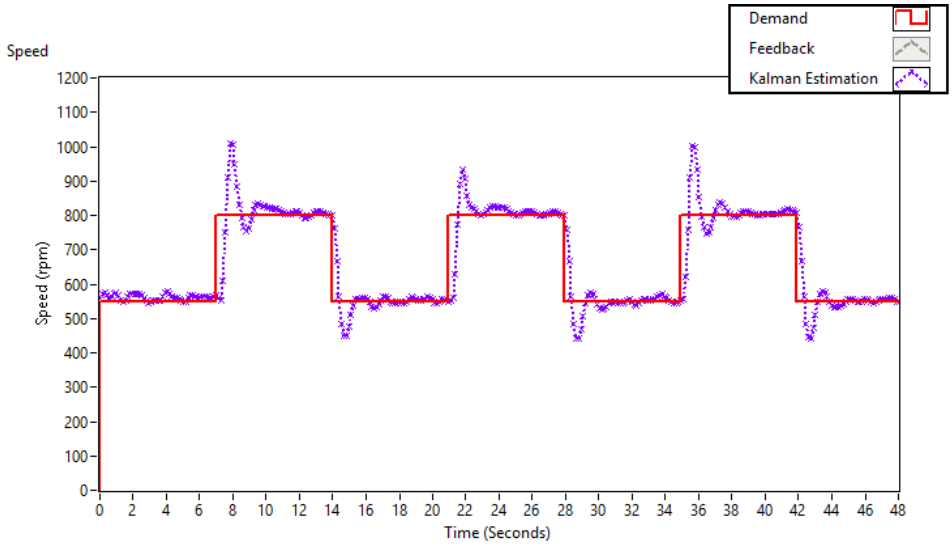

Figure 6.19: Kalman estimation for WFC under packet loss (HW demo)

Case (ii):- S1 open and S2 closed (Under intermittent data packet loss in feedback loop)

Fig.6.20 (simulation) and Fig.6.22 (hardware) shows the closed-loop Kalman filter's (CLKF) performance in supporting the controller under packet loss while transmitting the feedback information over wireless channel.

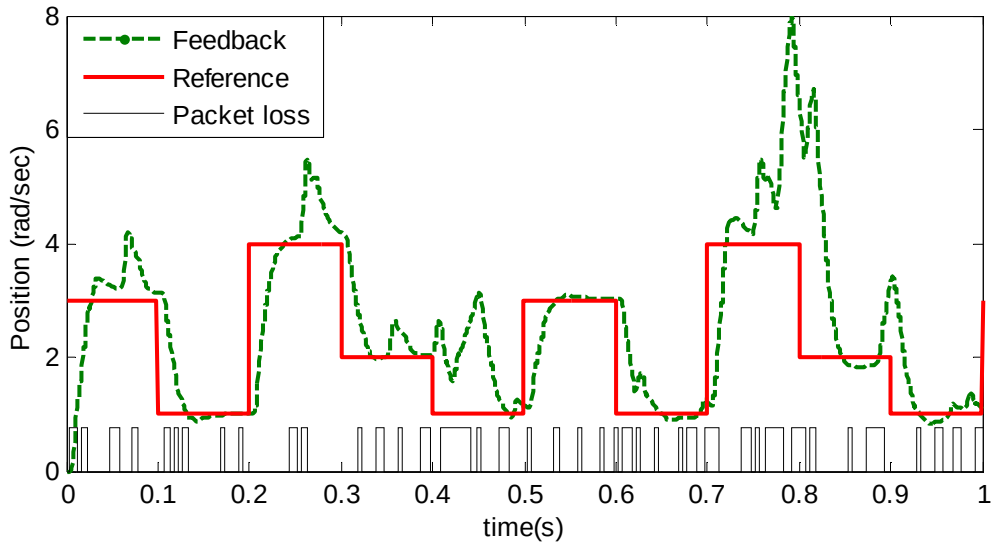

Figure 6.20: CLKF performance under packet loss (simulation)

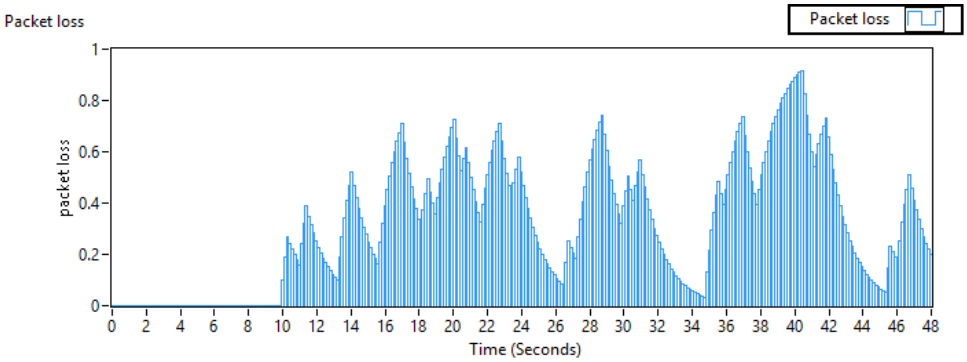

Figure 6.21: Packet loss (HW demo)

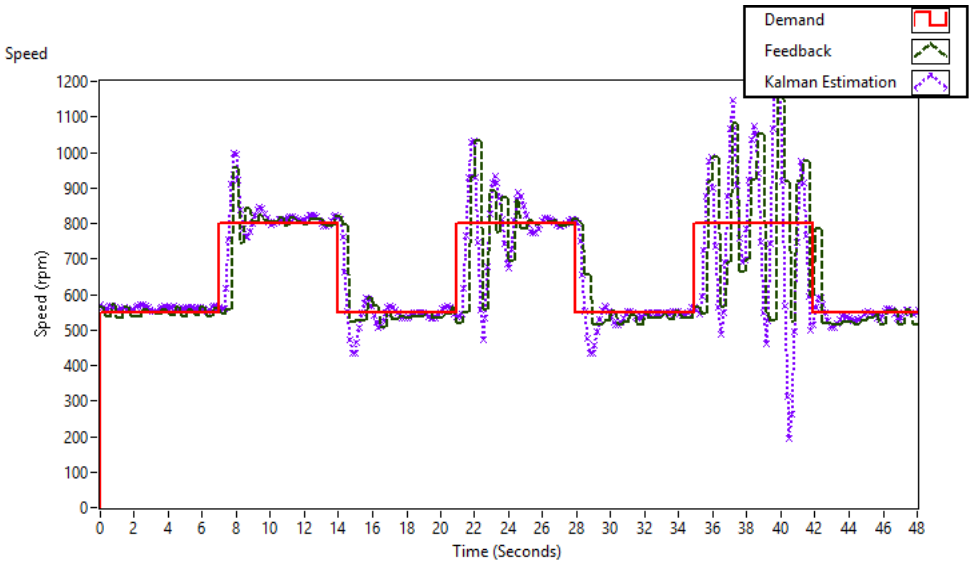

Figure 6.22: CLKF for WFC under packet loss (HW demo)

In Fig.6.22, the control performance is quite good for packet loss rate under 15%; however, as it is increased over 20% (around 20s in Fig.6.21), the system starts oscillating and when the packet loss is significantly raised over 40%, the system performance starts degrading. It can be seen the actual speed feedback (green dashed line) does not go to zero as it is defaulted at 500 rpm so as not to damage the power electronics with sudden current surge.

The reason behind the CLKF's poor performance under significant packet loss is explained below. It can be noticed from the block diagram in Fig.6.16, that the Kalman filter in itself depends on the measurements to update the predicted state. However, as the measurement data is lost frequently, the error discrepancy becomes abnormal. In addition, as Kalman gain depends on the measurement noise matrix, R declared initially, the estimated state might exhibit large divergence. Also, if the data is lost for a significant period, then whenever a new measurement arrives, this will result in oscillations in the estimated state as can be seen from Fig.6.22 after 34s.

Kalman filtering with missing measurements is an active area of research and various solutions have been discussed in [Khan, 2011],[Lu, 2009]. For industrial systems, due to

various constraints imposed by embedded microcontroller platforms, some of these solutions are computationally complex. In regard to the stability of the Kalman filter based estimation, the following holds, *if the system model upon which the Kalman filter is based is stochastically controllable, then the filter is uniformly asymptotically globally stable* [Rehbinder, 2004]. For proof see Appendix D. A sensorless Kalman filtering approach is considered to estimate the system states under packet loss in the next section.

6.5.2 Sensorless wireless feedback control

As Kalman filter is an observer of the real-time system, its error is induced in its estimation due to the missing observations. From equation (6.20), the residual is calculated by the difference between the measured data and the predicted data($Z_k - H\hat{x}_k^-$) and weighted by the Kalman gain. One straightforward and rapid approach during packet loss is to make the residual zero during packet loss. Therefore, whenever measurements are not received, the update step could be skipped by making the Kalman gain to zero. This is termed as open-loop Kalman filter (OLKF) estimation. As there is no feedback information used from the actual sensors a sensorless control methodology is implemented during intermittent packet loss.

According to the open-loop Kalman estimation, whenever measurement data is lost, only the first step a-priori estimate is performed. The a-posteriori step is skipped in order to avoid the divergence in the estimated state caused by the lost measurement data. Therefore, the Kalman gain is taken to be zero. This result in the system state and error covariance retains its current estimation without affecting them with the lost data. Therefore, under measurement data loss, equations, (6.19), (6.20) and (6.21) becomes,

Kalman Gain: $K_k = 0$ (6.24)

Updated system state: $\hat{x}_k = \hat{x}_k^-$ (6.25)

Updated error co-variance: $P_k = P_k^-$ (6.26)

As soon as a new measurement is received, the Kalman gain is estimated again, thereby, updating the state and error covariance. It is vital to tune the measurement noise matrix R in accordance with the significance of packet loss. From equation (6.19), increasing R will result in a low value of Kalman gain, K, and thereby enables the filter to trust its own prediction during packet loss.

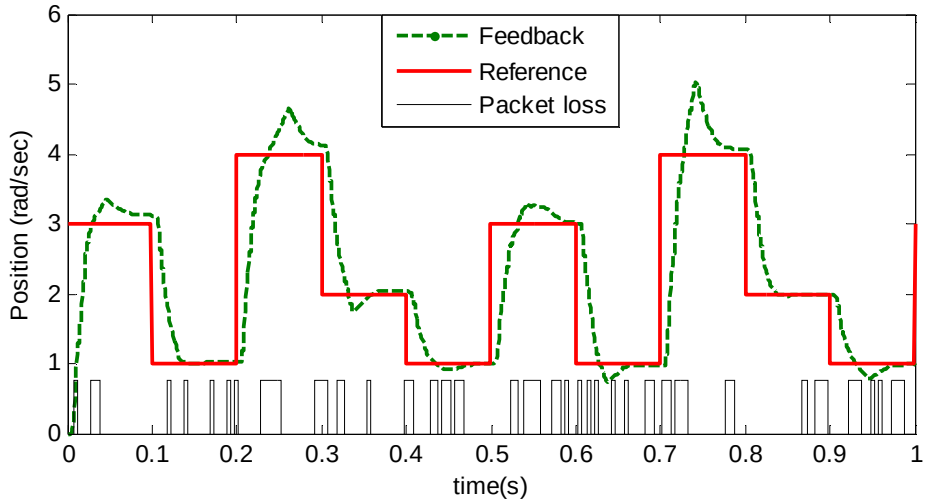

Figure 6.23: OLKF for WFC under packet loss (simulation)

Fig.6.23 shows the performance of OLKF in simulation setup. While the OLKF gives an optimal solution for low packet loss rate, for burst packet loss lasting for significant duration system exhibits overshoots. More interesting results are observed in the results using the hardware setup shown in Fig.6.24.

It can be seen (Fig.6.24) while the OLKF performs well for packet loss rate of 20% on average; it exhibits overshoots if the packet loss rate is increased over 40%. However, it performs much better than the CLKF under similar packet loss rate. The open-loop Kalman filter offers a simple and rapid approach for sensorless wireless control using embedded systems. While it works well for intermittent data loss in a wireless network, there is one drawback to the approach. It can be seen at about 36s, the packet loss reaches 75%, and therefore, a huge spike is seen in the Kalman estimation. This is typical of open-loop Kalman estimation, known as the sharp-spikes phenomenon. One way of reducing the overshoots is to ensure that the wireless network is synchronised and the overall time delay is under a known bound. In addition, if the measurement noise covariance matrix R is increased accordingly, the Kalman filter can make its next estimate closer to the demand.

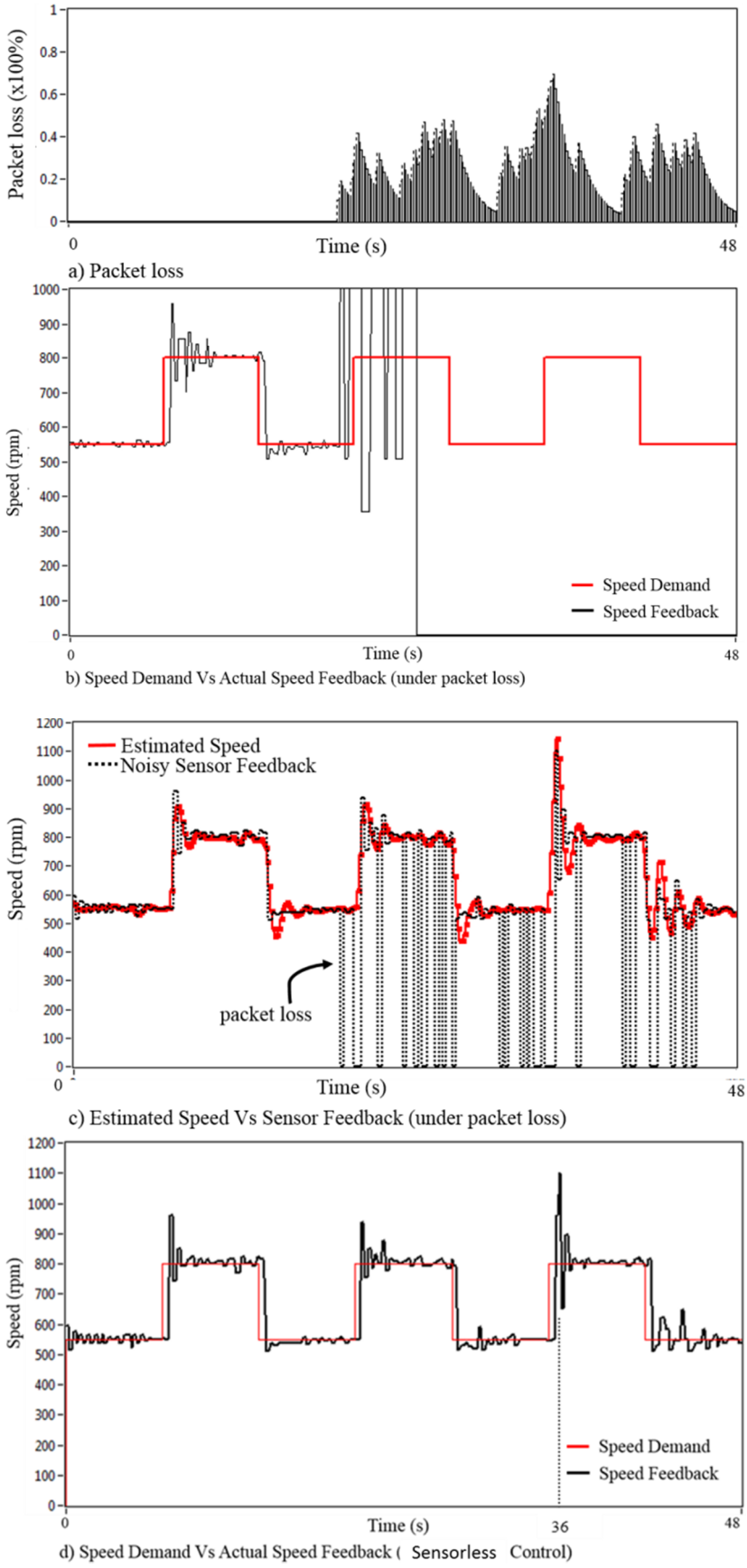

Figure 6.24: OLKF for WFC under packet loss (HW Demo)

Performance Analysis:

An overall performance analysis of the techniques used to compensate data packet loss in a wireless closed-loop control system is presented here. The IAE is used as a measure to compare the performance quantitatively. The feedback data without data packet loss (solid pink in Fig.6.25) is used as a reference to estimate the IAE for other approaches. It can be seen from Table.6.2 that, of all the approaches, the open-loop Kalman Filter approach offers the minimum IAE (3%). This is close to the first-order hold with different weighted mean approach (5%). However, it is to be noted that the first-order hold approaches just depend on the last received data samples and do not consider any system dynamics. In the open loop Kalman Filter approach, the estimated data is based on the system state, measurement noise and other disturbances. Therefore, the OLKF approach is more reliable than the traditional linear prediction approaches.

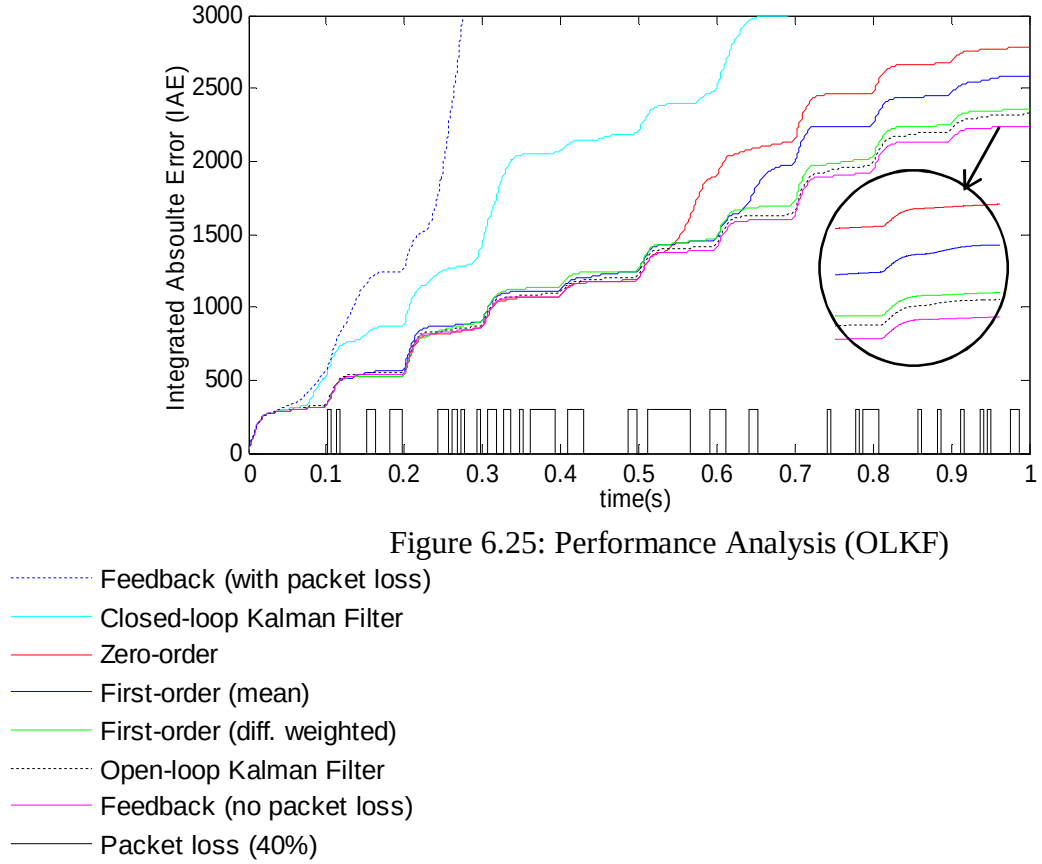

Figure 6.25: Performance Analysis (OLKF)

Linear Prediction techniques & Kalman Filter approach	Percentage increase in IAE compared to feedback data without packet loss
Zero-order hold	24%
First-order hold (mean approach)	15%
First-order hold (different weighted mean)	5%
Open-loop Kalman Filter	3%
Closed-loop Kalman Filter	76%

Table 6.2: Percentage increase in IAE (performance of OLKF)

6.6 Wireless Aircraft Braking System – Case Study

An aircraft's electric braking system [Venugopalan, 2014] is one of the potential applications where wireless links could be of benefit. For instance, Messier-Bugatti has developed a full wireless tyre pressure and brake temperature monitoring system for the A380 and Boeing jets. It uses a wireless link to transmit data from the wheel to the landing gear before being sent to the cockpit [Messier-Bugatti, 2006]. The aircraft-braking computer that receives input from the brake pedals usually resides in the avionics bay in an aircraft. From there, conventional wiring is used to transmit the information to the controller in the landing gear undercarriage. In addition, many sensors are involved in measuring the position and speed of the brake discs in order to regulate the braking action. By introducing wireless links to transmit the demand signal and the feedback information, a significant reduction in physical wiring quantity, weight and complexity can be achieved. Therefore, in this section, the proposed sensorless supervisory wireless control approach is evaluated on a wireless aircraft braking system.

The major aircraft manufacturing companies, Airbus and Boeing, have implemented electric braking systems in the A380 and Boeing 787 Dreamliner respectively. This research describes one step further than this, a case study of the design and implementation of a wireless feedback control system for an aircraft electric braking system.

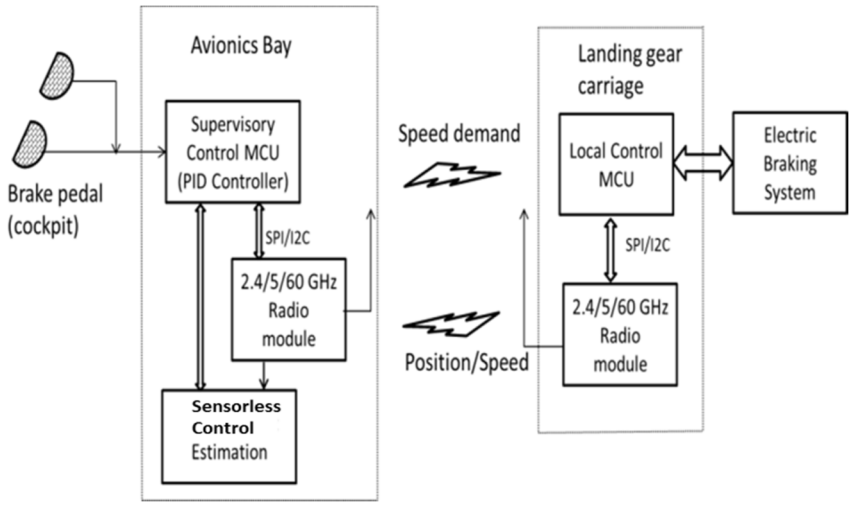

Figure 6.26: Wireless controlled aircraft braking system

This section explains the design of supervisory wireless control to test the braking performance in an aircraft. Fig.6.26 depicts the block diagram of a wireless braking system in an aircraft environment. The implementation is based on a supervisory wireless control strategy where both the demand and feedback are sent over the wireless channel. A supervisory unit is used as a master that sends the control demand over the wireless

channel to a local control unit. The supervisory unit can be located in the avionics bay in the aircraft. The demand is received from the brake pedal in the cockpit. The local control unit receives the control demand and controls the speed of a brushless DC motor which in-turn actuates the braking discs. The local control unit also computes the speed and position of the braking discs and sends them as feedback information back to the supervisory unit over the wireless channel.

6.6.1 Modelling of electro-mechanical actuation

The electro-mechanical actuation consists of two phases. The first phase involves the production of rotational motion using a brushless DC motor.

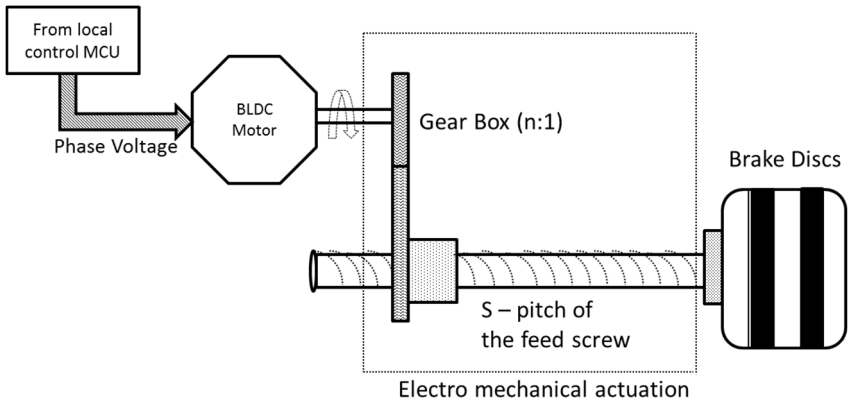

Figure 6.27: Electric braking system schematic [Venugopalan, 2010]

The second phase then transforms this rotational motion into linear motion that provides the desired mechanical action. This process of converting the rotational motion to linear motion is achieved using a gearbox. An aircraft braking system presents high performance issues and safety concerns. To provide consistent actuation and to avoid skidding the braking must be efficient. Therefore, the coupling mechanism involves both the gearing mechanism and a feed screw coupling to provide the linear motion required. Fig.6.27 shows the schematic of an electric braking system in an aircraft.

T_c	=	Gearbox coulomb frictional torque	(N-m)
B_{gear}	=	Viscous damping co-efficient	(N-m/s)
K_b	=	Brake stiffness	(N/m)
s	=	Pitch of the screw	(mm)
n	=	Number of turns on feed screw	

Mechanical Transmission:

Nut-to-motor transmission ration : 35:1
Thread Length : 5mm
Gearbox coulomb frictional torque reflected to motor side: 0.0355 Nm

Gearbox viscous damping reflected to motor side: 26×10^{-5} Nm/s

Brake Disc Characteristic:

Brake stiffness: 24×10^{6} N/m

Maximum force: $41kN$

6.6.2 Feed screw arrangement and gearing mechanism

Assuming the energy efficiency of the gear is 100%, the torque on two sides of the gear for a feed-screw drive can be expressed as,

$$\frac{T_m}{F_l} = \frac{V_l}{\omega_m} = \frac{x_l}{\theta_m} = \frac{s}{2\pi} = a \tag{6.27}$$

The gearbox arrangement has been modelled according to the governing equations below. From (6.27),

Force attained, $$F = x_l K_b \tag{6.28}$$

The linear displacement of the nut (x_l) is proportional to the nut position (θ_n):

$$x_l \propto \theta_n \qquad \therefore x_l = \frac{s}{2\pi}\theta_n \tag{6.29}$$

The rotor position (θ_m) and the nut position (θ_n) is related by $\theta_m = n\theta_n$,

$$\therefore x_l = \frac{s\theta_m}{2\pi n} \tag{6.30}$$

The torque developed in the nut is proportional to the force output.

$$T_n \propto F \qquad \therefore T_n = \frac{Fs}{2\pi} \tag{6.31}$$

where the rotor torque (T_m) and the nut torque (T_n) is related by

$$T_m = \frac{T_n}{n} \tag{6.32}$$

Substituting (6.27), (6.28), (6.30) and (6.31) in (6.32),

$$T_m = \frac{Fs}{2\pi n} = \frac{x_l K_b s}{2\pi n} = \frac{s\theta_m}{2\pi n} K_b \frac{s}{2\pi n}$$

$$\therefore T_m = \left(\frac{s}{2\pi n}\right)^2 \theta_m K_b \tag{6.33}$$

The brushless DC motor sees the load (braking demand) as a torque requirement. In other words, the motor rotates at its rated speed to achieve the required torque. This required torque to the motor is given as load torque. Therefore, the load torque equation can be given as,

Load Torque, $$T_L = T_m + T_c + B_{gear} \tag{6.34}$$

Electromagnetic Torque,

$$T_{em} = J\frac{d\omega_m}{dx} + b\omega_m + T_L \quad (6.35)$$

The Electromagnetic Torque of the motor is given by (6.35) which is repeated from (4.3) in Chapter 4. Substituting (6.33) and (6.34) in (6.35), given that ($T_{em} \cong T_m$), the motor speed ω_m can be calculated. The speed along with the rotor position θ_m(obtained by integrating ω_m) is sent as feedback data using the Truetime Wireless Network as shown in Fig.6.28.

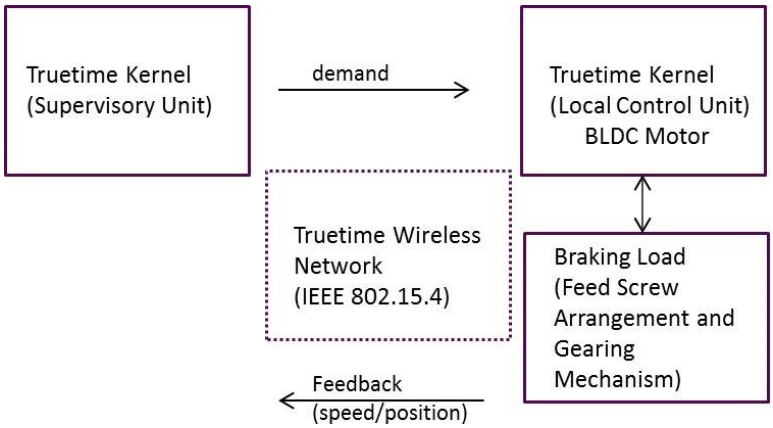

Figure 6.28: Truetime simulation model

In a safety-critical system such as an aircraft braking control system, the frequent loss of feedback data over the wireless communication channel may induce conditions that may affect the stability of system and may result in dangerous scenarios. The wireless braking system performance is tested using an anti-skid aircraft braking profile [Venugopalan, 2010]. Fig.6.29 shows the anti-skid braking demand profile (red solid) and the achieved braking profile (blue dashed) over the wireless communication channel without packet loss.

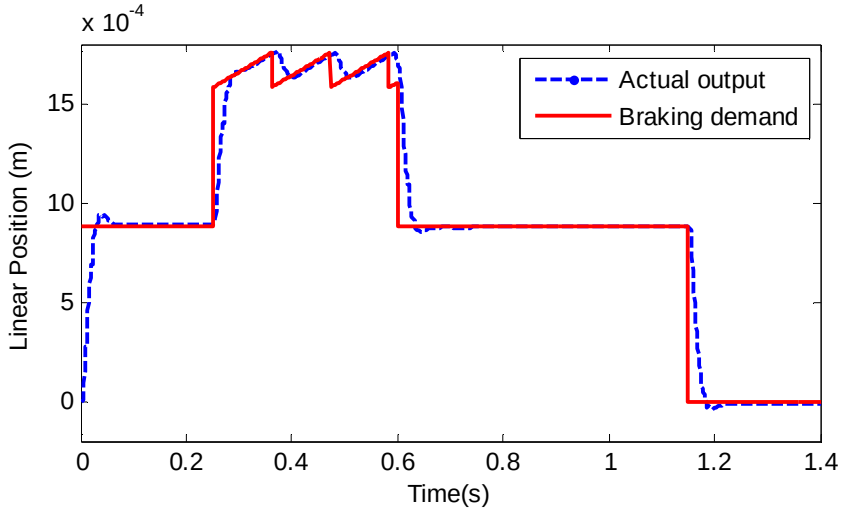

Figure 6.29: Anti-skid braking position profile [Venugopalan, 2010]

The wireless braking system is then tested by deliberately introducing packet loss into the feedback loop using the Truetime network. The packet loss was introduced from 0.39s to 0.425s and from 0.68s to 0.74s of the simulation time. Fig.6.30 shows that the position feedback has high overshoots due to the packet loss in the wireless network thus degrading the system performance. In the simulation model, the overshoots are reduced once the packet loss is removed; however, in a real-time system such overshoots can cause drastic effects, eventually rendering the system unstable.

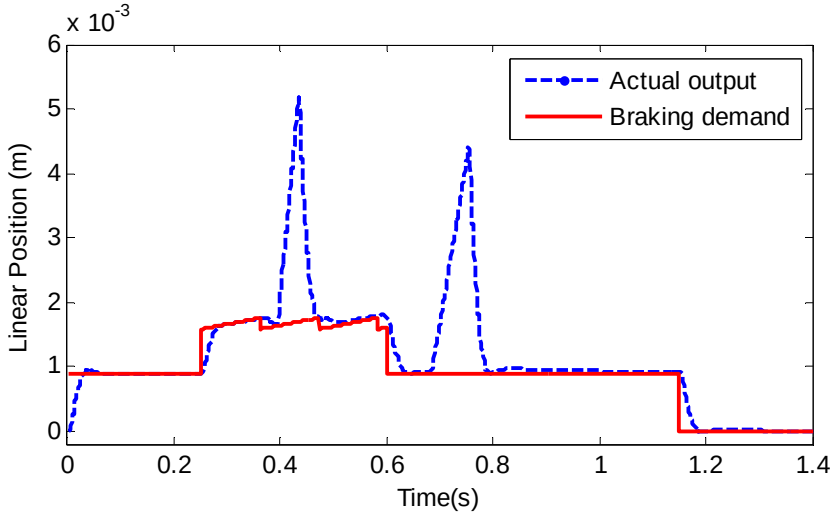

Figure 6.30: Wireless braking system under packet loss

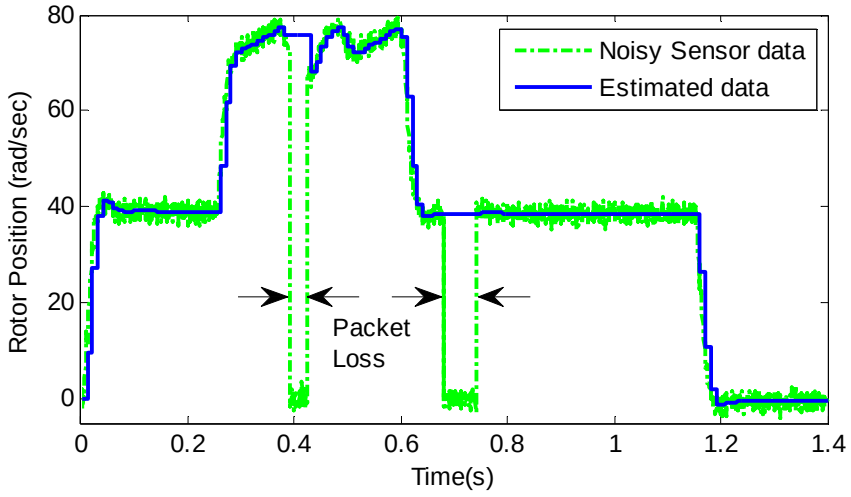

Figure 6.31: Estimation algorithm performance

Fig.6.31 shows how the implemented sensorless supervisory control algorithm helps the controller to decide the control demand during packet loss. The dashed plot shows the noisy sensor data. It can be noticed that at 0.4s and 0.7s, the rotor position feedback is lost over the feedback channel. The solid plot shows the rotor position as predicted by the Kalman filter. It can be noticed that the Kalman prediction due to its open loop nature retains the last predicted value until the next measurement is available. Also, by increasing

the measurement noise covariance matrix, R dynamically, the Kalman filter makes its estimation much closer to the expected demand once a new measurement is available. Once the sensor data is available after the packet loss duration, the controller switches to actual sensor data from the estimator block. Fig.6.32 shows the aircraft braking profile under data packet loss with the sensorless supervisory control mechanism. It can be seen that the braking profile is well controlled using the implemented estimation algorithm. The advantage of the proposed approach over traditional zero/first-order hold approaches is that, it utilises the estimated data obtained by the Kalman Filter based on the system dynamics. In traditional linear prediction approaches (zero-order, first-order hold), the data estimated is just based on the last received samples which could include data that is delayed or corrupted and does not consider the system state under poor network conditions.

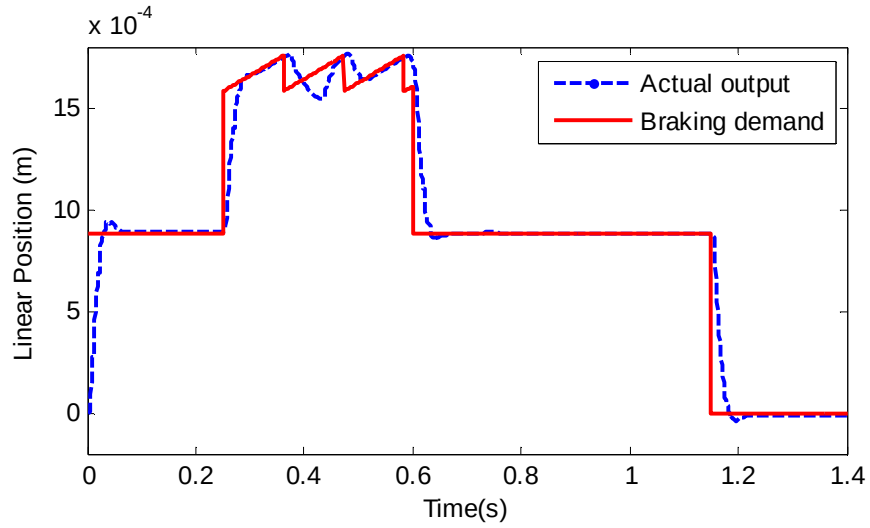

Figure 6.32: Braking profile under packet loss with sensorless control

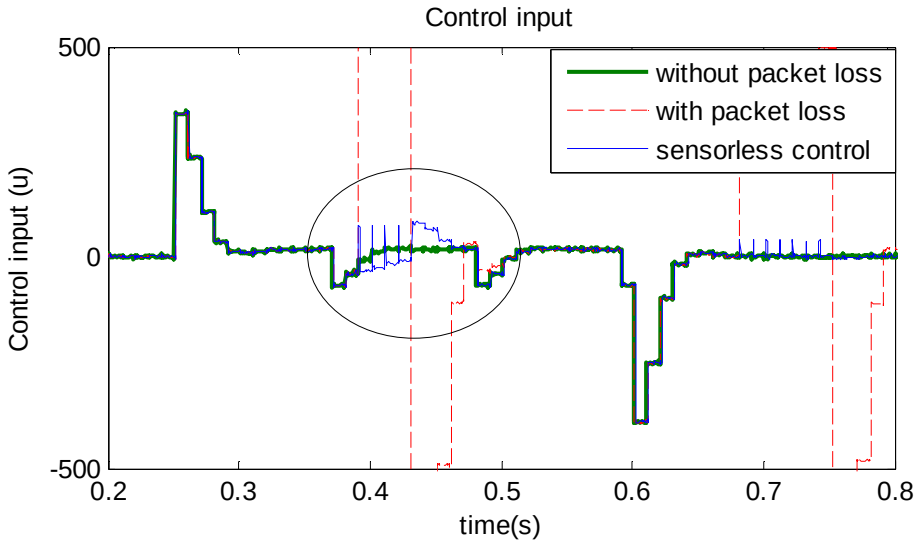

Figure 6.33: Performance analysis of the proposed algorithm

The effectiveness of the approach is analysed using the control demand generated by the supervisory control in Fig.6.33. The green solid line shows the control demand input without packet loss. The red dashed line shows the large error in the control demand during packet loss duration due to lack of feedback. The blue thin line shows how the proposed sensorless supervisory control significantly reduces the large error in the control demand, thereby keeping the system stable during packet loss.

6.7 Summary

A sensorless supervisory control algorithm is proposed in this chapter to address the issue of intermittent data packet loss in the wireless feedback loop. It is shown that the algorithm assists the supervisory controller in deciding the control demand during packet loss caused by interference in a wireless network. Intermittent packet loss causes significant error in determining the control demand thereby rendering the system unstable. The proposed algorithm significantly reduces this error and ensures the reliability of the wireless closed-loop control system. The proposed algorithm is then tested in a practical wireless control loop using an embedded microcontroller platform. The performance is assessed by deliberately introducing packet loss and radio interference. While the results show the effectiveness of real-time control in wireless systems, it is highlighted that there is scope for improvement, as estimated data may exhibit overshoots if the data is lost more than a certain bounded delay in the network. The effectiveness of the proposed approach on a critical system is further evaluated using a simulation model of a wireless aircraft braking system.

Chapter 7

Time-Varying delay in Industrial Wireless Closed-loop Control Systems

This chapter presents an adaptive compensation method for time-varying delays in the industrial wireless closed-loop control systems. It highlights the issues and challenges associated with wireless closed-loop control when time delay exceeds the sampling rate. A Kalman filter based modified Smith predictor for wireless closed-loop control is presented and is also extended with an adaptive sliding window compensation (SWC) technique to tackle the drawbacks of conventional Smith predictor when the delay exceeds the sampling interval.

7.1 Time Delay Issues in Industrial Wireless Control Systems

Time delay in a wireless network poses several challenges for industrial wireless control applications. There is a growing interest in utilising wireless sensor and actuator networks (WSAN) in cyber physical control systems. However, the current trends in deploying the sensors and actuators in a decoupled manner across the network make the whole system vulnerable to time-varying delay [Yoo, 2012],[Körber, 2007]. Communication latency is defined as the time taken by the wireless sensor right from the point it senses the data to the point where the controller receives the data successfully. Although wireless networked control systems can tolerate constant time delay that is less than a sampling interval, varying delay is not desirable for time critical systems. Table 7.1 provides an analysis of latency that can occur in the wireless standards that could be used for industrial control.

	Latency	Network Size	Data Rate
ZigBee	~15 ms	Very Large	250 Kbps
WirelessHART	~10 ms	Large	250 Kbps
Bluetooth	up to 100 ms	Small	> 1 Mbps

Table 7.1: Latency in wireless standards for industrial control [LaJoie, 2014]

More research needs to be done into identifying the network latency for industrial wireless standards in the case of harsh environments and in the case of high-traffic load. Latency depends upon various factors, such as the practical throughput of a wireless standard, network size and possible sources of interference. This can lead to analysing the trade-off between the network latency and how far delays can be mitigated. In the wireless closed-loop control systems, the communication latency should be kept within a certain limit as sensor reading reaching the controller after the specified deadline is of no use, and it will be rejected by the controller thus wasting valuable network resources. The industrial wireless protocols such as WirelessHART, ISA100.11a are based on the IEEE 802.15.4 standard and the most frequently used Wi-Fi is based on the IEEE 802.11b. In these standards, the sensor, actuator and control node's access for data transmission will be handled equally as they are not intended for safety-critical control operations. For instance, the WirelessHART has a time slot of 10ms for each node and therefore the minimum latency will be at least 10 ms. (see Table 7.1). The standards can be extended to critical applications that are more deterministic with improvement in Quality of Service (QoS) metric; however, the priority is handled based on network traffic [Gungor, 2013]. Therefore, there is a need to explore solutions that can explicitly compensate the communication latency or the time delay in a wireless closed-loop system in addition to the methods, the wireless standards can offer. Time delay in industrial wireless systems can be classified as intrinsic delays and extrinsic delays.

7.1.1 Intrinsic delays

Intrinsic delays are delays induced by the medium access control (MAC) in the wireless protocol. The MAC layer in a communication protocol is responsible for scheduling the transmission of data packets across the network [Park, 2011]. As the name indicated MAC is responsible for deciding how the network medium is accessed by the sensor nodes in the wireless network. The MAC layer addresses the channel contention methods for senor nodes within a network to transmit and receive data. The channel contention methods in turn contributes to the time delay in getting the data packet queued up for transmission to the point it is sent over the physical medium of transmission. This is known as medium access delay. Likewise, at the sensor node that receives the data packet, the time taken by the receiver to send the message to the application layer where the message has to be processed is known as reception delay.

Wireless protocols are half duplex as compared to wired networks, which can be both half duplex and full duplex networks [Willig, 2008]. Therefore, wireless sensors can communicate in only one direction at any given time, and hence it is impossible to detect any collision that happens due to multiple sensor nodes trying to transmit at the same time. This is the reason why the channel contention methods applied to wired networks cannot be applied to wireless networks. Channel contention methods such as Token ring, token

bus, CSMA/CD are frequently used in wired protocols such as Ethernet while wireless protocols predominantly follows the TDMA, CSMA/CA and CDMA based techniques with few protocols using ALOHA based contention methods. As mentioned earlier, the MAC layer induces two types of delays, the access delay and the reception delay. Table 7.2 presents the channel contention methods of industrial wireless standards. Almost all of them use the CSMA-CA in addition to other techniques to avoid collisions that can contribute to time delay in the network. (see Appendix B for the mechanism of MAC contention methods).

Wireless protocols	Channel Contention Method
IEEE 802.11b (Wi-Fi)	CSMA- CA
Bluetooth	FH-TDD-TDMA
ZigBee	CSMA-CA
WirelessHART	TDMA (Fixed) /CSMA-CA
ISA100.11a	TDMA (Flexible) /CSMA-CA

Table 7.2: Channel contention methods of wireless standards

7.1.2 Extrinsic delays

Extrinsic delays are caused by factors that influence the wireless network once the data packet is in air for transmission. These factors are otherwise known as Quality of Service (QoS) parameters such as high network traffic, network congestion, bandwidth availability, throughput, etc.

The delay that is caused by these factors while the packet is being transmitted is known as transmission delay or propagation delay. It is defined as the time taken by the data packet right from the moment it was physically transmitted in the wireless channel to the moment it was successfully received by the receiver. In wireless closed-loop control systems, propagation delay consists of two components as follows:

t_{ca} = Time delay between controller and actuator
t_{ac} = Time delay between actuator and controller

Therefore, the round-trip delay time t_{rtd} for transmitting a control demand and receive a feedback is given by,

Round trip delay time: $$t_{rtd} = t_{ca} + t_{ac} \quad (7.1)$$

Round trip delay time is defined as the average time taken to transmit a message and receive an acknowledgment between master and slave over a wireless channel. In wireless networks with symmetric network delays, propagation delay is half of round trip delay

time. However, in systems with asymmetric network delays, propagation delay has to be estimated separately.

In the wireless hardware demonstrator designed in Chapter 4, in order to process the demand and feedback data efficiently two separate radio modules are used in the local control unit. Therefore, the propagation delay has to be measured separately for sending the demand and the feedback data. The propagation delay for transmitting a message from the supervisory control unit to the radio module in the local control and vicevera is shown in Fig.4.16 and Fig.4.17 (Chapter 4). On an average a delay of 2.4 ms is observed. It can be noticed that the average delay in the network is symmetric (i.e., the onward and feedback wireless links experience the same amount of delay across the wireless channel.)

7.1.3 Related work

Time delay in networked control systems has been investigated widely over the last few decades. Early works [Halevi, 1988] analysed the effects of time delay, jitter, and transient errors in distributed control for a single control-actuator-control delay. The same was extended to multiple sensor-controller-actuator delays [Wittenmark, 1995]. An attempt to represent a time delayed system using augmented state vectors, which has the knowledge of past and present outputs as well as inputs thereby considering the system time-invariant is presented in [Cho, 2006]. However, in these studies the network delay is assumed to be bounded by the sampling interval. Much research [Gonzalez, 2012],[Cloosterman, 2009], [Nilsson, 1998] have been dedicated to analysis and modelling of the networked control systems by considering the time delay as an uncertainty in the modelled system. In these works, the stability of the system is analysed by assuming a maximum upper bound for time delay as worst case, however, such assumptions might not be valid in all industrial applications. Therefore, an online estimation of time delay and compensation is considered in this research which is more suitable for industrial scenarios. Time delays in industrial control systems can be classified as follows:

- Constant time delay networks
- Markov chain based time delay networks
- Time-varying or random delay networks

Stabilisation with constant delay in networked control systems is fairly straight forward where time buffers could be introduced to achieve the optimum delay in the networks. Such an approach for networked control is proposed in [Luck and Ray, 1990] where input buffers and output buffers longer than the worst-case time delay are used in the controller and actuator respectively to store the received delayed data. However, the drawback of such systems is that at times it may make the control delay longer than necessary as the buffer is decided based on the worst-case delay.

A special case of analysing the Markov chain based time delay is done using the Markov Jump Linear Systems (MJLS). A significant amount of work in literature [Han, 2009] (and references therein) has been dedicated to the study of systems under time delay, especially those in networked control by modelling the system as MJLS and derive its stability under time-varying conditions. However, there is a need to have a prior knowledge of time delay in the network and appropriate system states which has to be estimated offline.

As explained earlier, time-varying delay occurs when the network QoS parameters keep changing according to the network conditions. As wireless network load depends on the QoS parameters much work in literature [Luan, 2011],[Tas, 2011] is dedicated in analysing the time-varying delay. Such networks are known as delay sensitive networks (DSN) where the delay is affected by the QoS parameters.

A gain scheduler middleware to compensate the controller under varying network conditions such as time delay and packet loss is considered in [Tipsuwan, 2004]. A time delay compensation for wireless networked based control with time-varying delay using the IEEE 802.11 time synchronisation function (TSF) is presented in [Uchimura, 2008]. It has been highlighted that t_{ca} and t_{ac} should be measured separately in a wireless networked control system for delay compensation methods to work efficiently. Instead of estimating the time delay directly, a pade approximation of the time delay function that is observed using the network disturbances is used for delay compensation in [Natori, 2008].

A design of networked control systems with explicit time delay compensation using system identification methods is discussed in [Martins, 2010],[Uchimura, 2008]. In these works the time delayed packet is assumed to be a lost packet as it becomes stale for the current time instant and suitable estimated data using an ARMAX model of the system is substituted. However, it should be noted the time delayed data still consumes network resources as unlike lost data, time delayed data would still be received by controller/actuator. Another drawback is that the system identification has to be done offline and needs a prior assumption of delay. In addition identifying system states for varying delay and sampling rates becomes computationally complex.

One of the most commonly used approaches to compensate time delay in wireless sensor networks is to use adaptive sampling rates. IEEE 802.11b WLAN networks utilises the Automatic Rate Fallback (ARF) algorithm for the efficient performance of the wireless network during time-varying conditions affecting the QoS parameters [Colandairaj, 2007]. Though adjusting sampling rates during periods of high traffic reduces the number of samples in the transmitting queue it does not eliminate the packets arriving in error, which had to be retransmitted thus reducing the throughput. Adaptive sampling rate techniques have also been widely discussed in the literature specific to wireless feedback control [Xia, 2007],[Ploplys, 2003],[Lian, 2001]. These works show that the control path delays must be less than the maximum time delay determined for various benchmark sampling rates for an acceptable system performance.

The Smith predictor is a time delay compensation approach proposed by O.J.M.Smith [Smith, 1957] and since its inception, it has been discussed [Abe, 2003] and modified in various ways to be utilised in compensating time delays in various applications. The implementation of a time delay compensation scheme using a Smith predictor for networked control systems that communicates over a UDP network is discussed in [Vardhan, 2011]. A modified Smith predictor for wireless networked control systems is proposed in [Feng, 2009]. The proposed approach eliminates the need for time delay estimation in Smith prediction; however, it does so by moving the controller to co-exist with the controlled plant. A Smith predictor based time delay compensation is proposed in [Cheng, 2007] for studying the time delay effect of NCS based on Ethernet, CAN and wireless LAN networks. While the Smith prediction is applied directly to compensate the delay in networked control loops, the effect of dynamic change in control inputs is not considered. Time delay has been widely addressed in the literature in different aspects. However, as explained in the next section time delay exceeding the sampling rate is a significant issue in wireless closed-loop control systems. The gaps identified in the existing literature with respect to wireless closed-loop control systems are as follows:-

- Solutions based on system identification methods can offer a predicted packet in place of delayed data. However, the system needs to rely on the predicted data until the data without delay is received. In addition, system identification needs to be done offline.
- While adaptive sampling rate based solutions can be utilised in situations where time delay exceeds sampling interval, changing sampling rate frequently in wireless closed-loop control systems may not be desirable in all situations. In addition, the network traffic needs to be estimated at all times to change the sampling rate accordingly.
- Smith predictor based solutions can compensate constant/invariant time delay. However, its performance in wireless closed-loop control systems when both time delay and input demand is changing need to be studied further. In addition, Smith predictor relies on the time delay estimated initially and there is a need for a dynamic time delay estimation algorithm in wireless closed-loop control systems.
- Time delayed data is still transmitted/received over the wireless channel consuming network resources. Therefore, there is a need for solutions that can let the controller incorporate the delayed data in computations.

.

Therefore, in this research, a sliding window based adaptive compensation approach for time-varying delay in wireless closed-loop control systems is proposed. The proposed approach utilises the delayed data in a novel way, such that the information in the delayed data is used for estimation and at the same time the lag introduced by the delay is eliminated using a Smith predictor. While delay compensation methods based on Smith predictor for networked control performed in [Vardhan, 2011],[Feng, 2009],[Cheng, 2007] consider only constant input demand, the proposed approach highlights the issues in utilising Smith compensation for varying input demand and under delay exceeding sampling interval.

7.1.4 Sampling rate issues

In the wireless networked control systems, the time delay is unavoidable because of the data being routed through a network. Apart from the transmission delay, there could be a number of unknown parameters that constitutes towards the total time delay in the network. The immediate expected response of an uncompensated delayed system is an oscillatory behaviour in the output response [Andrews, 2001] (also see Fig.7.14). The block diagram of a discrete-time delayed system is shown in Fig.7.1.

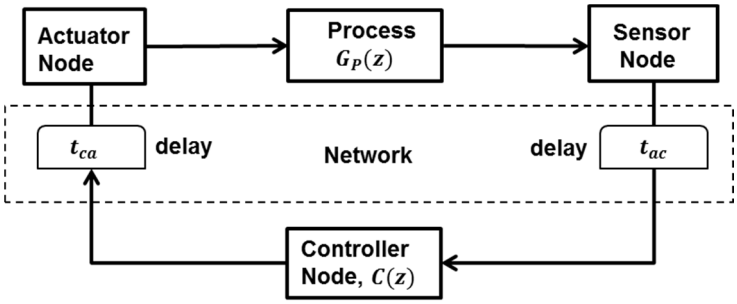

Figure 7.1: Discrete-time delayed networked control system

If the controller is given by $C(z)$, the plant is represented by $G_p(z)$, (e^{-kT}) is the time delay, kT is the sampling instant, then the closed-loop transfer function of a discrete-time delayed system is given by,

$$\frac{y_k}{r_k} = \frac{C(z)G_p(z)e^{-kT}}{1 + C(z)G_p(z)e^{-kT}} \tag{7.2}$$

The closed-loop characteristic equation of the system is given by,

$$1 + C(z)G_p(z)e^{-kT} = 0 \tag{7.3}$$

The delay term e^{-kT} in the characteristic equation will produce a phase lag in the system which might render the system unstable. In a wireless closed-loop control system, the delay term e^{-kT} is equal to the round-trip delay time.

Asymmetric time-varying delay $(t_{ca} \neq t_{ac})$ occurs in cases where there is a possibility that the actuation and sensing action are decoupled or happens separately (chemical plants, medical applications, etc.) or the control input could be sent over a different channel from the sensing information and therefore, different network conditions can contribute to time-varying delay [Lian, 2001]. However, as far as the wireless closed-loop control is concerned, the actuators and sensors will co-exist in most cases, and the system is expected to respond quickly. Therefore, the control demand and feedback are transmitted in the same or adjacent channels and therefore, the forward and feedback delay will usually be symmetric $(t_{ca} = t_{ac})$.

Time delay in wireless closed-loop control systems can be distinguished as follows:-

- Total round trip delay time less than the sampling rate of the system ($t_{rtd} < T_s$)
- Total round trip delay time greater than the sampling rate of the system ($t_{rtd} > T_s$)

The two cases are represented in Fig.7.2.

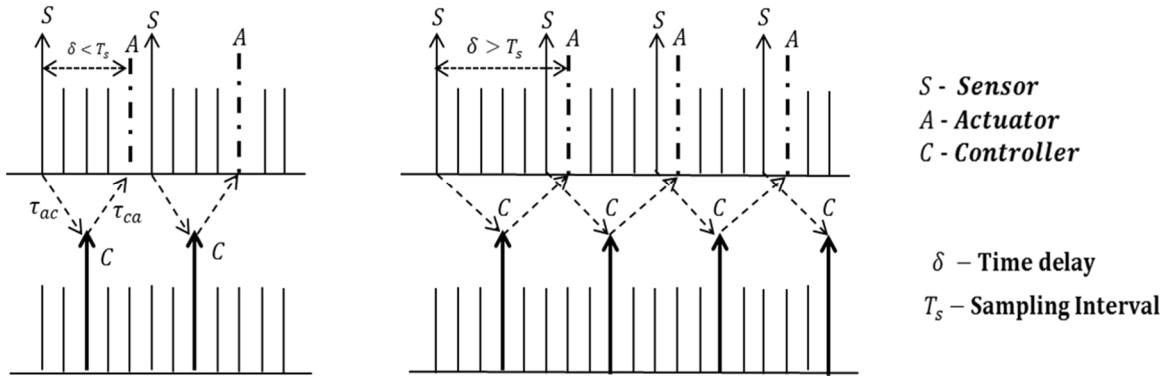

Figure 7.2: Sampling rate analysis in wireless closed-loop control

When the time delay is less than the sampling rate of the system (left side of Fig.7.2), the system may still perform well, as the control and the actuation tasks would still be completed before the next sampling interval. On the other hand, the real challenge is posed by systems where the delay exceeds the sampling interval (right side of Fig.7.2). It can be seen that each time a sensing data is received the controller estimates the control input, however, delivers it to the actuator after the next sampling interval due to the time delay.

If there is a change in the input before the next controller action, then the controller will use the sensing data that was taken before the actuation happened. This will introduce a significant error, and this error will get propagated as each time the actuation will happen after its corresponding sensing event resulting in a oscillatory behaviour.

7.2 Modified Smith Predictor

The Smith Predictor for a wireless closed-loop control system is shown in Fig.7.3. The Smith predictor has two components. The outer feedback loop estimates the control error from the reference and the received delayed sample data. However, as the received data is delayed it gets reflected in the control error. Therefore, the Smith predictor uses an inner feedback loop that actually cancels out the delay component by simply adding the delayed prediction. The output will be the reference data without the delay component to which the prediction from the Smith predictor is given as feedback thereby estimating the control error without delay. Therefore, the delay is completely eliminated from the error fed to the controller which then transmits the control input to the actuator. While the Smith predictor is efficient in compensating the delay instantly, its performance depends on various factors.

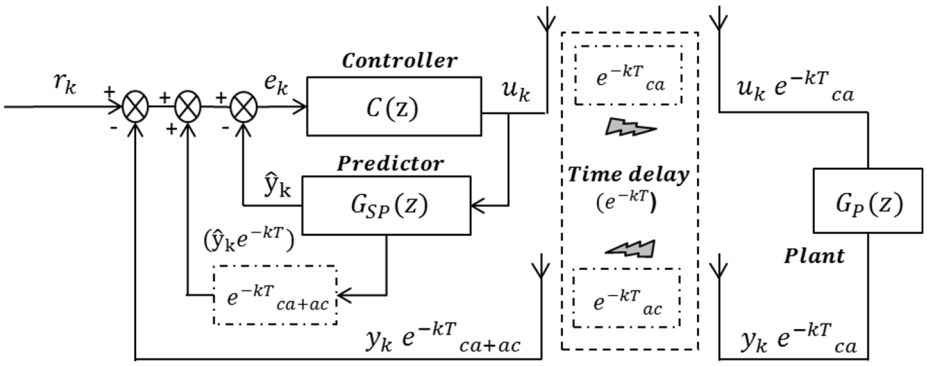

Figure 7.3: Smith predictor for industrial wireless control

- It needs an exact representation of the control plant for a good estimation, and this is not practically possible.
- The delay estimated needs to be close to the actual delay in the network. There is a need to estimate the delay in the network as the Smith predictor needs this data updated often.
- The Smith predictor does not consider any external disturbances or noise and therefore, the effects of these are not reflected in the estimated data.

In order to eliminate the above disadvantages one optimal approach is to use a Kalman filter in place of a traditional Smith predictor. One of the salient features of Kalman filter is that it corrects the system every time based on the received measurement data, and this is vital in time delayed systems where the system representation used for estimation should be updated regularly (see Section 6.4.1 for Kalman filter algorithm).

However, there is one challenge in utilising a Kalman filter for compensating time delay in wireless closed-loop control. A Kalman filter depends on the measurement data (y_k) to correct its estimated data $(\hat{y}_k)$. If (y_k) is delayed and this is used by Kalman filter in its correction step, it will in turn propagate the delay in the Kalman estimated data as well. In traditional Smith prediction approach (see Fig.7.3) the actual received data with time delay is cancelled out, and only the predicted data $(\hat{y}_k)$ is used as feedback for calculating the control input. However, when the predictor is replaced by a Kalman filter, the estimated data by the Kalman filter $(\hat{y}_k)$ can be applied as feedback data to the controller, however, the same data cannot be utilised as measurement data for the correction step in the Kalman filter.

Kalman filtering with time delayed measurements have been extensively researched [Lu, 2009],[Tasoulis, 2007] in the past. In addition to the regular Kalman filter the above approaches utilise a parallel Kalman filter that has the covariance and measurement matrix according to the delayed measurement and hence prior knowledge of error covariance and measurement noise for varying delays is needed. In addition, the above approaches may increase the computational overhead, especially in a resource constrained environment such as wireless closed-loop control systems.

Therefore, a revised architecture of the Smith predictor based on a Kalman filter is proposed for its suitability in wireless closed-loop control in this section. The proposed architecture is termed as Modified Smith Predictor (MSP). A schematic representation of the proposed MSP architecture is given in Fig.7.4. In the proposed architecture, the inner feedback loop is divided into two steps. The time delay compensation is performed as follows:-

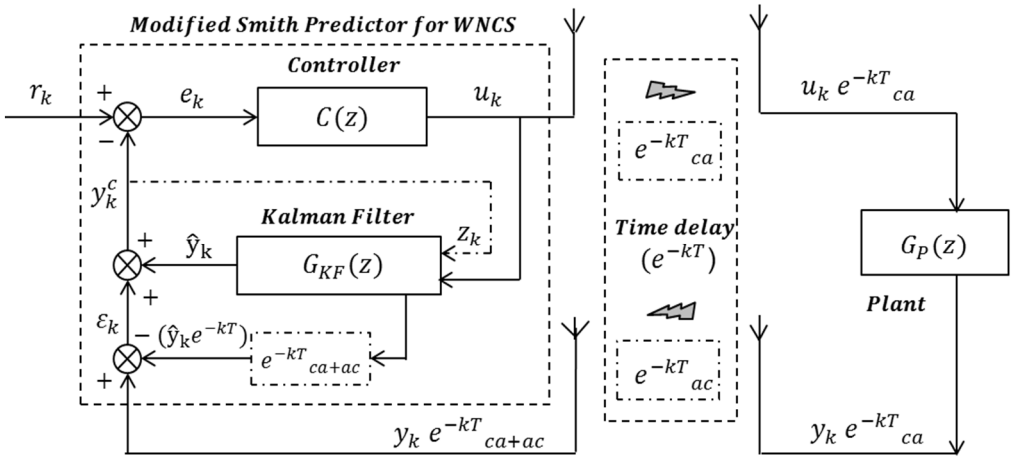

Figure 7.4: Modified smith predictor for industrial wireless control

- In the outer loop, the received feedback data with time delay $(y_k\, e^{-kT}{}_{ca+ac})$ is compared with the predicted data $(\hat{y}_k)$ from the Kalman filter which is also delayed $(\hat{y}_k e^{-kT})$ by an equivalent delay in the network $(e^{-kT} = e^{-kT}{}_{ca+ac})$.
- The output of this loop will be an error difference $(\varepsilon_k = (y_k - \hat{y}_k)\, e^{-kT})$ between the predicted data and the received data with the time delay (e^{-kT}) cancelled out.
- In the inner loop, this error is added to the actual predicted data $(\hat{y}_k)$ from the Kalman filter with no delay. The output (y_k^c) of this loop will be equivalent to the actual received data (y_k) free from both the delay and the error (if any) between the actual measured data and the Kalman filter estimated data in the previous loop.
- Finally, the delay compensated feedback data (y_k^c) which is equivalent to the actual measured data (y_k) is fed to the reference for the control input estimation. As this data is now free of delay, this is further used as measurement data (z_k) by the Kalman filter for future estimation.

If the controller is given by $C(z)$, the plant is represented by $G_p(z)$, the Kalman filter is given by $G_{KF}(z)$, then the closed-loop transfer function of the above system (Fig.7.4) can be derived as follows:

The control demand before being transmitted over the wireless channel is given by,

$$u_k = \mathrm{C(z)}.\, e_k \text{ (where } e_k = r_k - z_k) \tag{7.4}$$

From Fig.7.4.,

$$y_k^c = y_k\, e^{-kT}{}_{ca+ac} + [\hat{y}_k - \hat{y}_k e^{-kT}] \tag{7.5}$$

$$e_k = r_k - (y_k\, e^{-kT}{}_{ca+ac} + [\hat{y}_k - \hat{y}_k e^{-kT}]) \tag{7.6}$$

If $e^{-kT}{}_{ca+ac} = e^{-kT}$ and $y_k = \hat{y}_k$ then the delayed term gets cancelled with the delayed Kalman estimation and any error is added to the Kalman estimated data which in turn is used as the feedback data for control demand estimation.

The closed-loop transfer function of the delay compensated system can be derived as follows,

Rearranging (7.6) and from Fig.7.4, substituting $\hat{y}_k = u_k G_{KF}(z)$ (From Fig.7.4)

$G_{KF}(z)$ represents the following Kalman Filter equations (Refer Section 6.4.1 for details)

Predicted system state: $\hat{x}_k^- = A\hat{x}_{k-1} + Bu_{k-1}$

Updated system state: $\hat{x}_k = \hat{x}_k^- + K_k(Z_k - H\hat{x}_k^-)$

Z_k represents the measurement data (dot-dashed line) in Fig.7.4.

$$e_k = \left(r_k - y_k\, e^{-kT}{}_{ca+ac}\right) - [u_k G_{KF}(z) - u_k G_{KF}(z) e^{-kT}] \tag{7.7}$$

Substituting (7.7) in (7.4),

$$u_k = \left(\left(r_k - y_k\, e^{-kT}{}_{ca+ac}\right) - u_k G_{KF}(z)[1 - e^{-kT}]\right).C(z) \tag{7.8}$$

Considering $E_k = r_k - y_k\, e^{-kT}{}_{ca+ac}$ and substituting in (7.8),

$$u_k = (E_k - u_k G_{KF}(z)[1 - e^{-kT}]).C(z) \tag{7.9}$$

$$u_k = E_k.C(z) - u_k G_{KF}(z).[1 - e^{-kT}].C(z) \tag{7.10}$$

$$u_k(1 + C(z).G_{KF}(z)[1 - e^{-kT}]) = E_k.C(z) \tag{7.11}$$

From Fig.7.4, the transfer function of the modified Smith predictor is given by,

$$G_{MSP}(z) = \frac{u_k}{E_k} = \frac{C(z)}{(1+C(z).G_{KF}(z)[1-e^{-kT}])} \tag{7.12}$$

Here $(G_{KF}(z) \cong G_p(z))$ depending on good equivalence. Considering (7.12) as $C(z)$ in (7.2) and simplifying, the overall transfer function of the delay compensated system is given by,

$$\frac{y_k}{r_k} = \frac{C(z).G_{KF}(z)e^{-kT}}{1+C(z).G_{KF}(z)} \tag{7.13}$$

Therefore, the characteristic equation of the Smith compensated system is given by,

$$1 + C(z).G_{KF}(z) = 0 \tag{7.14}$$

Comparing with (7.3), it can be seen the delay term is eliminated. Therefore, the system becomes stable and thus the control performance can be improved significantly.

7.2.1 Merits

The advantages of the proposed architecture as compared to traditional Smith prediction approach are as follows:

- As the proposed architecture works based on a Kalman filter, it will work well for systems where exact representation of the actual plant being controlled is not available. Therefore, it is highly suitable for industrial wireless closed-loop control systems.
- As wireless feedback control involves transmission and reception of data packets every sampling interval, the clock synchronisation messages can easily be added to these packets without any significant overhead.
- Utilising the IEEE 1588 PTP based time delay estimation process explained in Chapter 5, the time delay can be estimated as needed and the supervisory controller can be kept updated.
- As the corrected feedback data z_k, which is equivalent to the actual feedback data received is used for control demand estimation this eliminates all the strict assumptions made with respect to the predicted data in the traditional Smith prediction approach.
- The Kalman filter utilises the noise and disturbance information, and as it is also fed with the actual measured data, Kalman filter can track the original system efficiently and keep the system stable whenever there is a time delay in the wireless network.

7.2.2 Drawbacks

The modified Smith predictor for wireless closed-loop control will provide an efficient control over time delay in the wireless network. However, it can do so only if the time delays in the network remains constant and within a certain known bound. The known bound should basically be within the maximum sampling interval beyond which the system may go unstable. The key advantage of a wireless network over a wired network is its flexibility. Whenever a wired network needs to be extended a high-maintenance cost is involved whereas in a wireless network it's only a matter of adding another sensor to the existing network. However, this increase in nodes in turn contributes to the overall network load and hence the QoS parameters are time-varying. Therefore, time delay in wireless networks will exhibit a time-varying behaviour.

As the delay is varying there is a high probability that the Kalman filter will start utilising stale data for future prediction. For instance, assume the network delay is initially of less than one sampling interval and gets changed over time to more than three sampling interval. The modified Smith predictor will compensate the time delay in the received data, assuming that it is less than one sampling interval; however, the data is actually delayed by three sampling intervals now. Therefore, though the data arrived is compensated for the network delay it is still delayed by three sampling intervals or in other words, if the delay is less than a sampling interval, then a more recent sensor data will be available rather than the one compensated. Therefore, for each time instant, a delay compensated data which is actually a stale data for the current time instant (due to inconsistent sampling intervals) will be utilised by the controller.

7.3 Adaptive Time Delay Compensation

It is evident from the above discussion that the modified Smith predictor cannot be used as it is for time-varying delay in a wireless network. Therefore, a sliding window based adaptive compensation for time-varying delay in industrial control is proposed in this section. In a delayed system, the measurement is not completely lost; however, it is received after a certain time period. Therefore, the measurement could still be credible as long as the delay can be compensated. For cases, where the total time delay exceeds the sampling interval, the delay can be compensated, however, the controller needs this data for the previous sampling instant, and therefore, it becomes stale data for the current sampling instant. In order to eliminate this issue the modified Smith predictor in Fig.7.4 is replaced using the sliding window based adaptive delay compensator as shown in Fig.7.5.

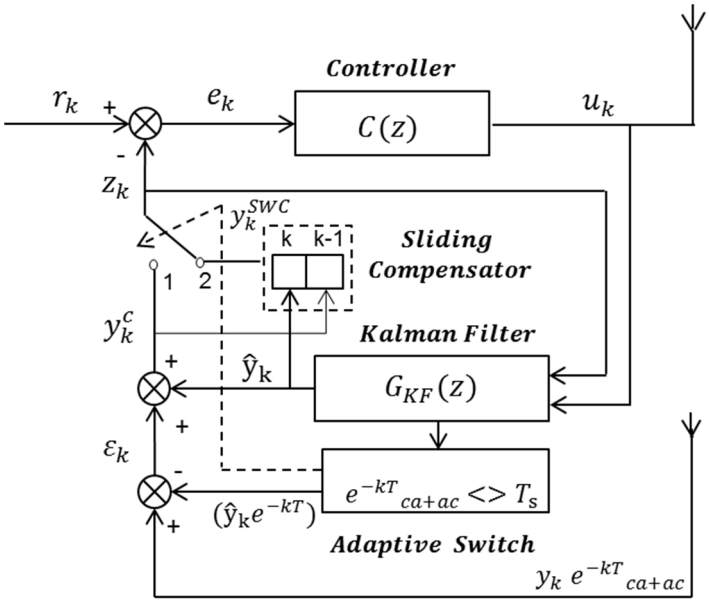

Figure 7.5: Sliding Window Compensator (SWC)

7.3.1 Adaptive switch

An adaptive switch is used to track the time delay in the network and determine if it exceeds the sampling interval. The adaptive switch is used to estimate the time delay in the wireless network using the IEEE 1588 PTP based clock synchronisation approach for industrial wireless closed-loop control systems as proposed in Chapter 5. Once the network is synchronised, the time delay can be estimated periodically using the IEEE 1588 PTP based time delay estimation.

7.3.2 Sliding window compensator

A sliding compensator is used to cancel the delay between the inconsistent arrivals of measurement. The idea of sliding compensator is shown in Fig.7.6. In time-series analysis the measurement data at any given time k is an auto regression on the measurement data available until $(k-1)$. It can be represented as,

$$Z_k = a_1 x_{k-1} + a_2 x_{k-2} + a_3 x_{k-3} + \cdots + a_n x_{k-n} + m_k \tag{7.15}$$

where, Z_k is measured signal, x_k is state variables, m_k is measurement noise, $a_1 - a_n$ is constant parameter. Therefore, in a discrete-time sampled system, where the time delay exceeds the sampling rate (h), the measurement arrives with a lag equivalent to the number of sampling rate (nh) the time delay has exceeded,

$$Z_k = a_1 x_{(k-i-nh)} \tag{7.16}$$

As long as the data is delayed greater than one sampling interval and less than n sampling interval, the delay (δ) between two consecutive measurements will be equal to n sampling interval and the round trip delay time.

$$\delta = nh + e^{-kT}{}_{ca+ac} \tag{7.17}$$

In the MSP approach, while the $(e^{-kT}{}_{ca+ac})$ term is compensated using the Smith predictor, it will not cancel the (nh) term. Therefore, the compensated measurement will still have a delay term of (nh).

In the proposed approach named Sliding Window Compensation based Modified Smith Predictor (SWC-MSP), whenever the delay exceeds the sampling rate, a $nh + 1$ window compensator is used where n is the number of sampling intervals the time delay has exceeded. A two window compensator where the delay exceeds one sampling interval $(\delta \geq nh, n = 1)$ is explained in Fig.7.6.

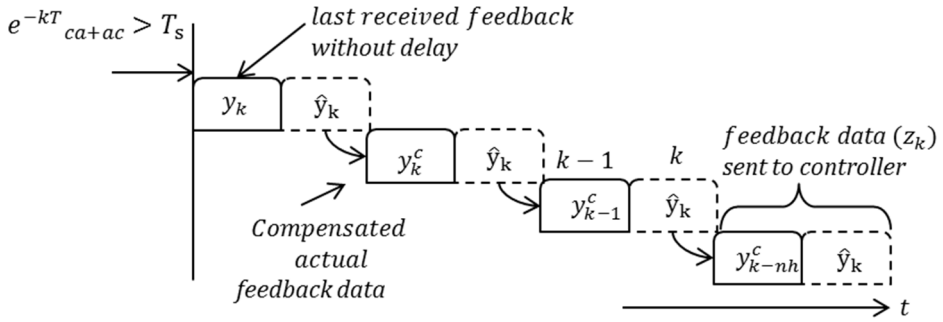

Figure 7.6: Sliding window compensator workflow ($h \leq e^{-kT}{}_{ca+ac} \leq 2h$)

When the time delay exceeds the sampling interval, the sliding compensator uses two windows where the (k) window uses the Kalman estimation$(\hat{y}_k)$, which was obtained using the last received feedback data without delay (y_k). The $(k-1)$ window uses the delay compensated data (y_k^c) based on the data received at current time instant k, which is nothing but the data that should have arrived in the previous sampling interval. An appropriate exponentially weighted mean of these two data will be utilised for the control input estimation.

The window slides over each time with current Kalman estimation in k window and the compensated data in the $(k-1)$ window. If the data is delayed by two sampling intervals but less than three sampling intervals $(2h \leq e^{-kT}{}_{ca+ac} \leq 3h)$ then the sliding window is increased to three windows as shown in Fig.7.7.

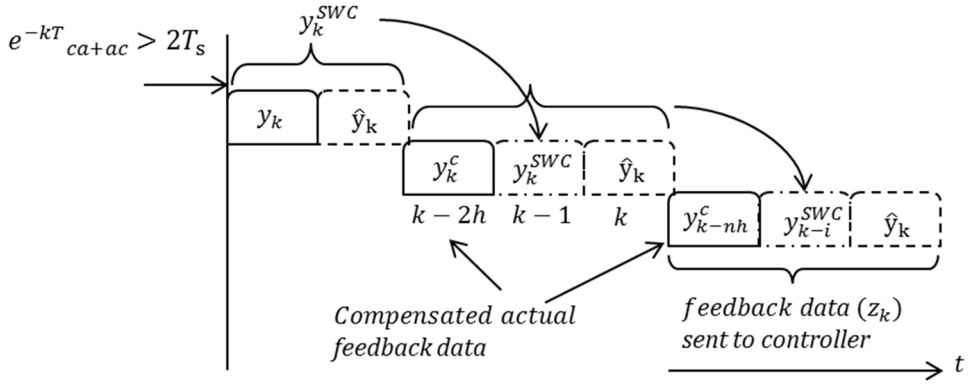

Figure 7.7: Sliding window compensator workflow ($2h \leq e^{-kT}{}_{ca+ac} \leq 3h$)

As long as the delay is greater than two sampling interval but less than three sampling interval, the delay between two consecutive measurement should be at least two sampling interval delayed $(\delta \geq nh,\ n = 2)$. Therefore, in the sliding compensator, the $(k-2)$ window is updated with the current delay compensated data (y_k^c) while the $(k-1)$ window will have the previous compensated measurement (y_k^{swc}) estimated using the SWC approach, and k window will have the Kalman filter estimation $(\hat{y}_k)$ for the current

time instant k. Therefore, based on the SWC approach the measurement data can be obtained as follows,

$$y_k^{swc} = a_1 \hat{y}_{k-1} + a_h y_{k-nh}^c \qquad (if\ \ h \le e^{-kT}{}_{ca+ac} \le 2h) \tag{7.18}$$

$$y_k^{swc} = a_1 \hat{y}_{k-1} + \sum_{i=2}^{nh-1} a_i y_{k-i}^{swc} + a_h y_{k-nh}^c \qquad (if\ \ 2h \le e^{-kT}{}_{ca+ac} \le nh) \tag{7.19}$$

Where, y_k^{swc} is the measurement data estimated using the proposed SWC approach, $\hat{y}_k$ is the Kalman estimated data, y_k^c is the delay compensated data by Smith principle, and $a_{i \to h}$ is the weighting factor. The adaptive controller controls the switch 1 and 2 as shown in Fig.7.5 to decide the measurement data (z_k) based on the estimated delay as below,

$$z_k = \begin{cases} y_k^c, & if\ e^{-kT}{}_{ca+ac} \le h, \quad S1 \\ y_k^{swc}, & if\ \ h \le e^{-kT}{}_{ca+ac} \le nh, \quad S2 \end{cases} \tag{7.20}$$

Therefore, the sliding window compensator is extended according to the delay exceeding the sampling interval which can be detected using the delay estimator block. The flow diagram of the proposed approach is shown in Fig.7.8.

It can be observed that the Kalman filter in addition to filtering also performs a Kalman smoothing action where a data is updated for a previous time instant given the future data values. However, there are three design considerations for the above proposed approach to work effectively.

- The Kalman filter and controller have to be time-triggered (similar to sampling interval), and the Smith compensation part will be event-triggered (event being the received data) as shown in Fig.7.8. In the Kalman filter based modified Smith predictor, as the Kalman filter in turn depends on the measurement for updating the states, this approach will also carry forward the delay between the inconsistent arrival of measurements in its estimation and filtering process. Therefore, the Kalman filter and the controller are decoupled from the Smith compensator as the latter depends on the sampled data.
- Another consideration is increasing the sampling rate of control demand more than the feedback data [Luck and Ray, 1990]. As the time delay is observed as a total network phenomenon, increasing the control input sampling rate will increase the arrival rate of the control input at the actuator end. Therefore, the actuator can be updated as soon as a change in control input is detected.
- Selection of weighting factors $(a_{i \to h}, a_1)$ such that more weight is given to the recently received data.

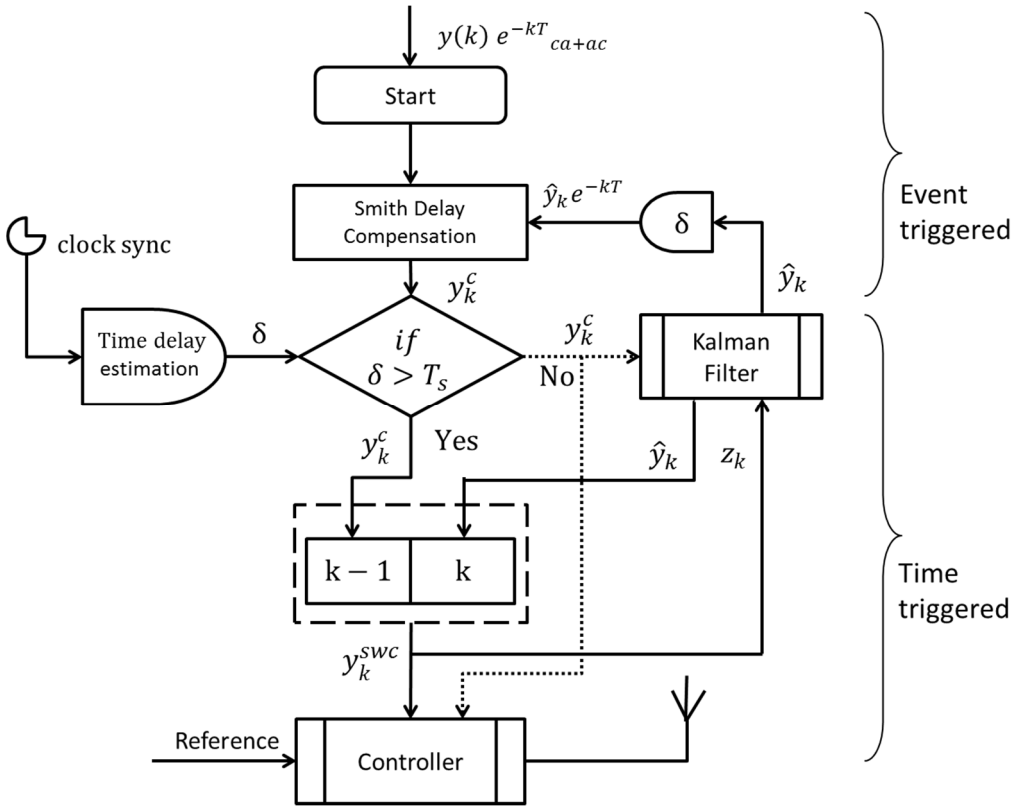

Figure 7.8: Sliding window compensator – Flow diagram

The idea of sliding compensator stems from the fact that in situations where the delay exceeds the sampling interval, the Kalman filter can actually be decoupled from the Smith predictor so that the Kalman filter can work as a time-triggered system whereas the Smith predictor can only work as an event-triggered system the event being the sampled feedback data. However, the advantage of a Kalman filter as a linear predictor can be utilised in the sense that the Kalman filter can operate without any dependency on the delayed measurement as long as the Kalman filter error covariance is within a controllable bound (see Appendix D for more details).

7.4 Results and Discussions

The wireless closed-loop control system modelled using the Truetime networked control system simulation tool in Chapter 4 is used to study the effects of time delay exceeding the sampling interval. The results consider the position response of the BLDC motor for analysis where the round trip time delay is increased gradually. The results will highlight the importance of the relation between sampling rate (nh), sampling interval (T_s) and increasing round trip time delay(t_{rtd}).

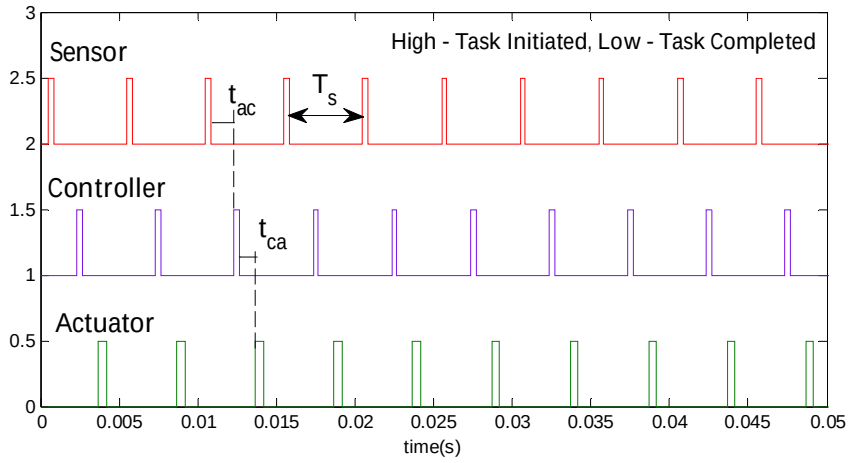

Figure 7.9: Wireless closed-loop control - Network schedule

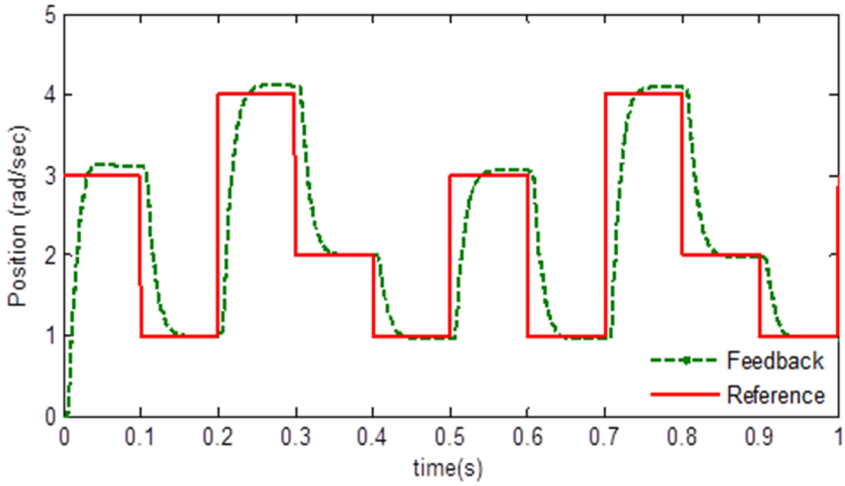

Figure 7.10: Wireless closed-loop control performance – Position profile

Fig.7.9 shows the wireless network scheduler for time delay less than a sampling interval. As long as the delay is less than a sampling interval (T_s =5 ms), the sensor, controller and actuator tasks are scheduled in sync with each other, and thus a tightly coupled deterministic behaviour is observed in the wireless closed-loop control system. The corresponding position response of the BLDC motor (simulation model) without time delay is shown in Fig.7.10.

Fig.7.11 shows the wireless network scheduler when the time delay exceeds one sampling interval. It can be seen, the sensing (red), control (blue) and actuation (green) schedule has started to overlap and become inconsistent. When a task reaches high (0.5,1.5,2.5) it indicates the transmission is successful. When a task reaches a medium level (1.25,2.25) it indicates that the scheduler waits for a back-off time as it senses another node is utilising the channel which in this case is due to inconsistent sampling interval.

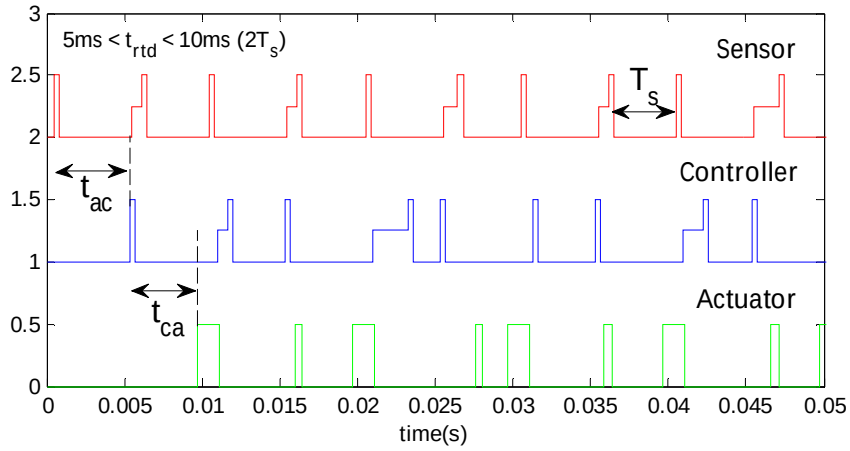

Figure 7.11: Wireless closed-loop control - Network schedule ($t_{rtd} < 2T_s$)

Fig.7.12 to Fig.7.15 shows the control performance of the implemented wireless control loop for time-varying delay exceeding the sampling interval. Fig.7.16 to Fig.7.19 shows the performance of the proposed approach as compared to the delayed feedback (FB) response and the modified Smith predictor (MSP) using the integrated squared error (ISE).

It can be seen in Fig.7.12 to Fig.7.15, as time delay varies over different sampling interval, the system response (red dashed line) tends to become oscillatory, and by the time it exceeds nearly five sampling intervals (Fig.7.15) the system goes completely unstable. In order to compensate the delay, the modified Smith predictor for WNCS is applied first. Though the Smith predictor reduces the overshoot (green dot-dashed line), the response lags each time as it is compensating the feedback data delayed by the number of sampling interval (nh) the time delay has exceeded. This behaviour warrants the use of a suitable time delay compensation approach before the system goes unstable eventually.

For instance, in Fig.7.13, the sensor data is delayed by two sampling intervals. It can be seen in Fig.7.13, the response with delay (red dashed line) shows high oscillatory behaviour. The modified Smith predictor (dot-dashed green line) fails to achieve a satisfactory response. In this case, the sliding window has three windows $(k, k-1, k-2)$. Considering the current time instant as k, windows $(k-2)$ and $(k-1)$ are updated with the delay compensated data (z_k^c) and (z_{k-1}^c), respectively. Window (k) is updated with the Kalman Filter estimated data at k. The response (black solid line) shows the efficiency of the proposed approach while the delay is under three sampling interval.

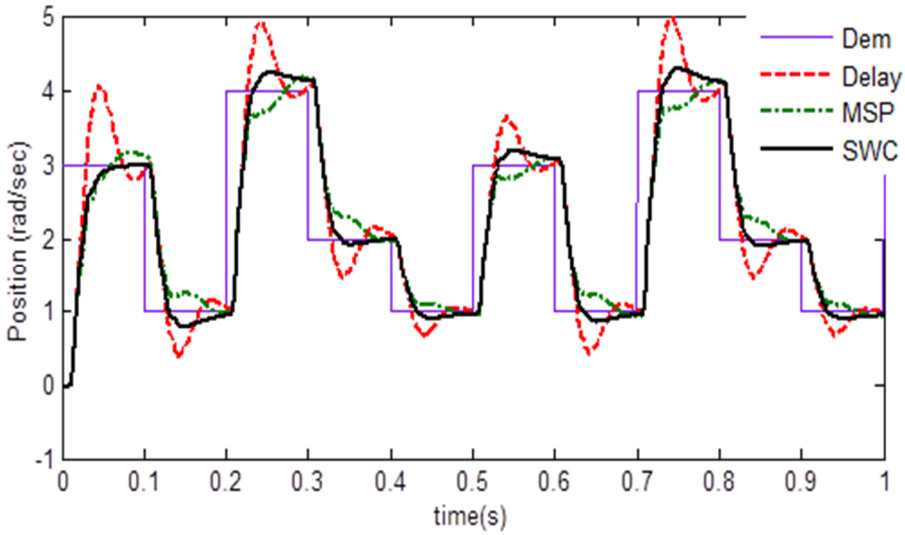

Figure 7.12: Wireless control performance ($1T_s < t_{rtd} < 2T_s$ (2h))

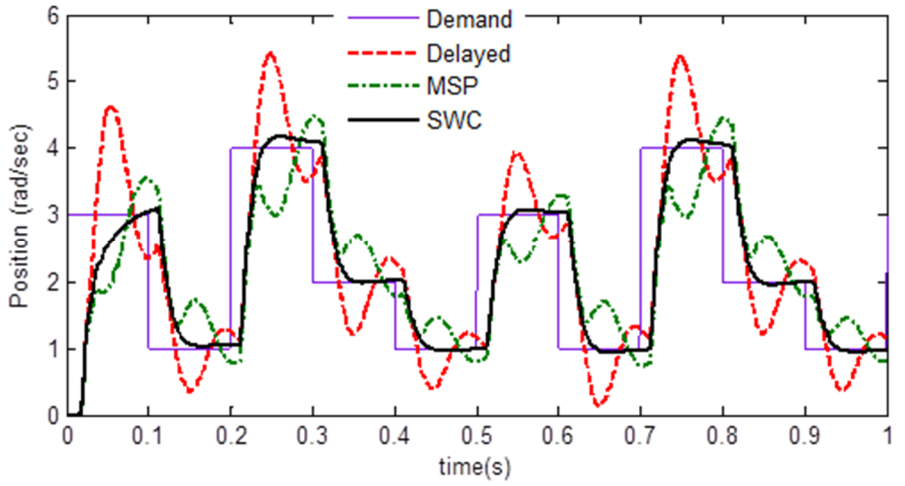

Figure 7.13: Wireless control performance ($2T_s < t_{rtd} < 3T_s$ (3h))

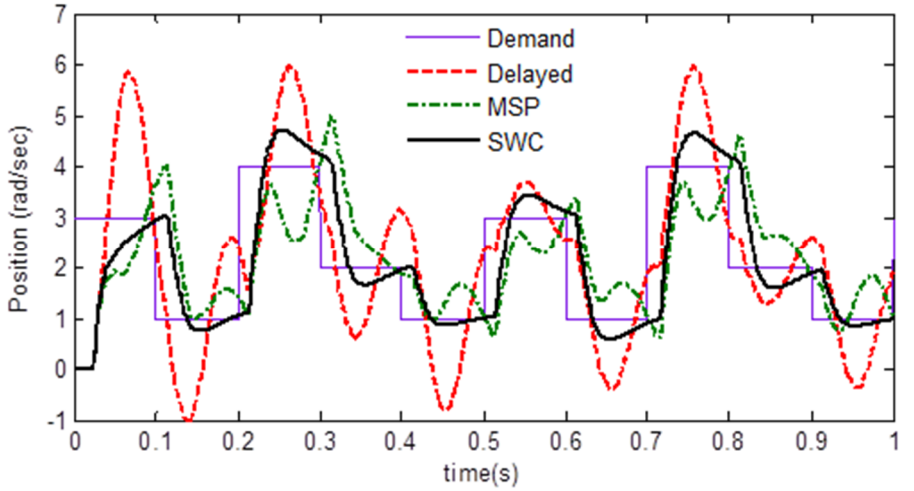

Figure 7.14: Wireless control performance ($3T_s < t_{rtd} < 4T_s$ (4h))

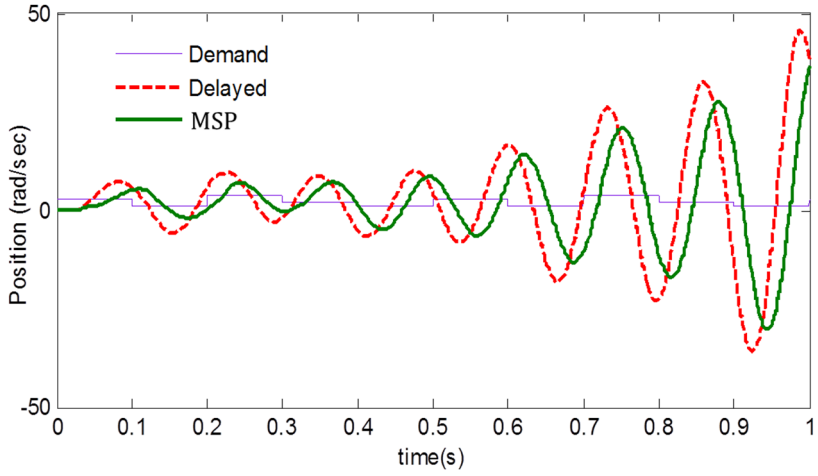

Figure 7.15: Wireless control performance ($4T_s < t_{rtd} < 5T_s$ (5h))

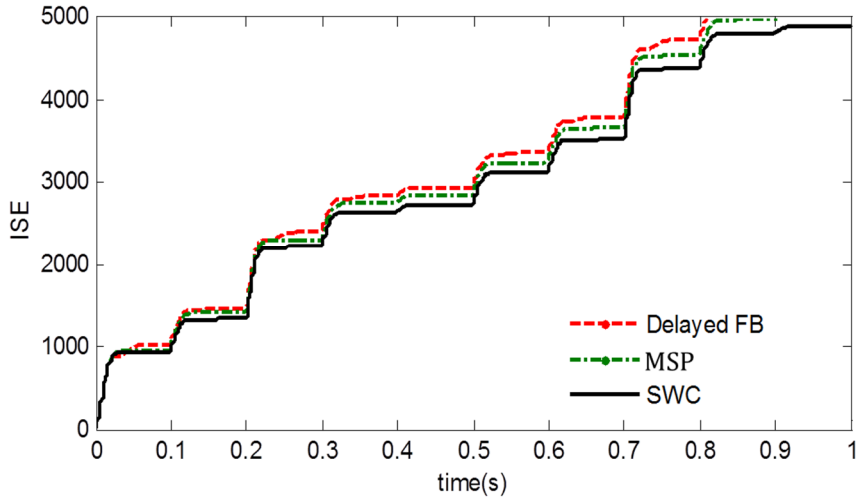

Figure 7.16: ISE based performance of SWC ($1T_s < t_{rtd} < 2T_s$ (2h))

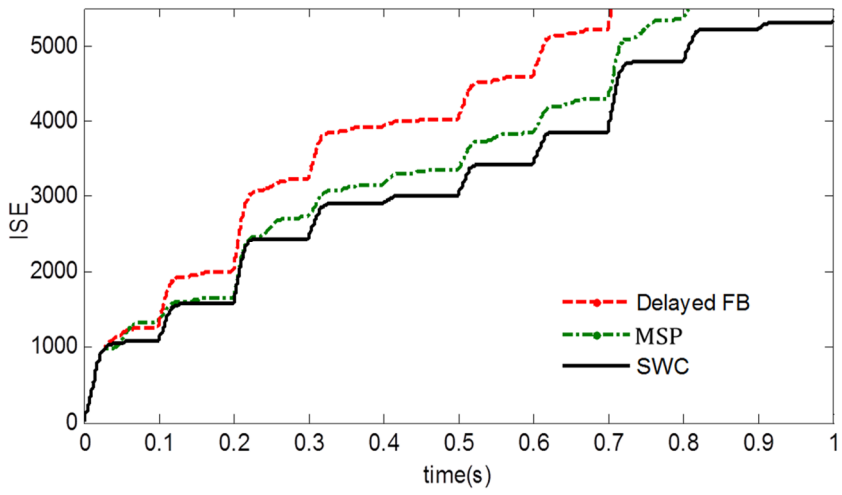

Figure 7.17: ISE based performance of SWC ($2T_s < t_{rtd} < 3T_s$ (3h))

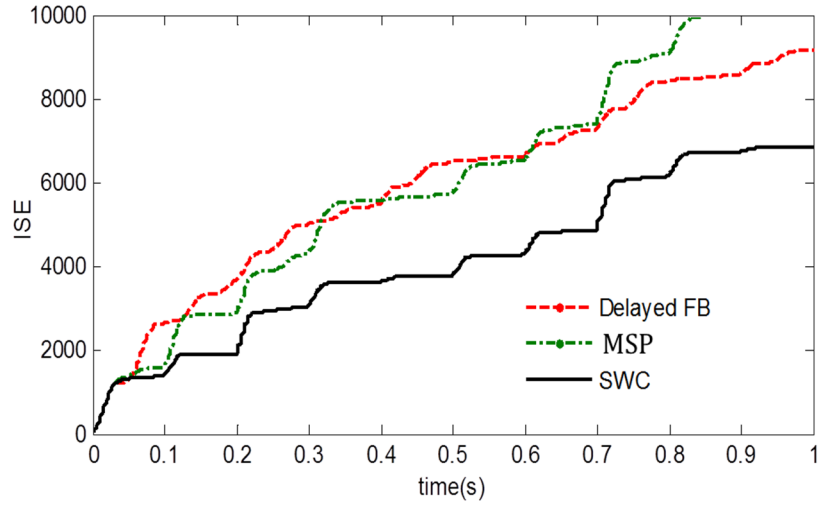

Figure 7.18: ISE based performance of SWC ($3T_s < t_{rtd} < 4T_s$ (4h))

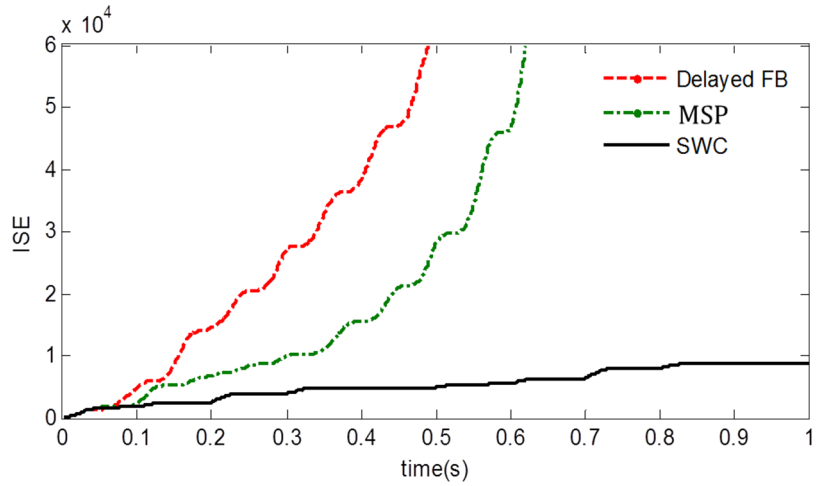

Figure 7.19: ISE based performance of SWC ($4T_s < t_{rtd} < 5T_s$ (5h))

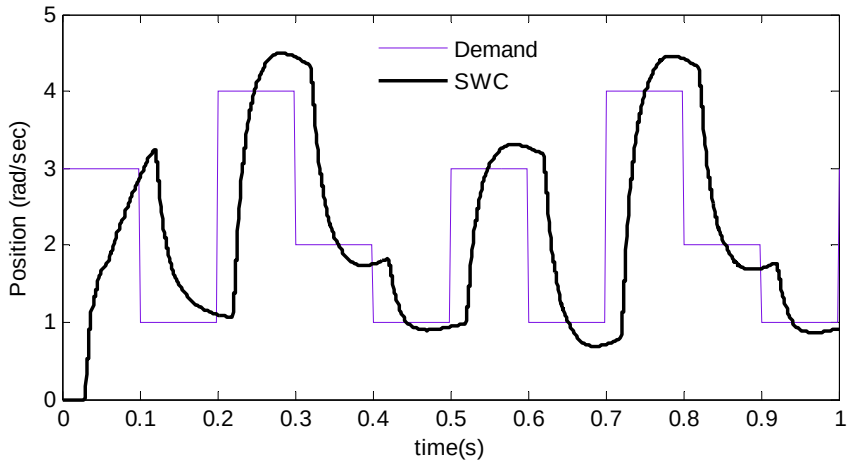

Figure 7.20: Wireless control performance - SWC ($4T_s < t_{rtd} < 5T_s$ (5h))

For all the scenarios, it can be seen from the results, the response (black solid line) of the proposed SWC approach significantly reduces the overshoot, and the response is better than the modified Smith predictor. When sensor data is delayed by nearly five sampling intervals, the system goes unstable (see Fig.7.15). At a sampling rate of 5 ms, for every second 200 samples are needed for an efficient performance of the wireless controller. This in turn translates to 20 samples per 100 ms. Therefore, if the data is delayed for five sampling interval (25 ms), it nearly contributes to one-quarter of the samples being delayed for every 100 ms. Therefore, the controller is unable to regain the system from the delayed samples and thus renders the system completely unstable.

It is interesting to notice that even the modified Smith predictor response goes unstable as each time it compensates the data delayed by nearly five sampling interval, and this is not credible enough for the controller to keep the system under control. The response (black solid line) of the proposed SWC approach is shown in Fig.7.20. In this case, the sliding window is increased to five windows, with (k) holding the Kalman estimated data, $(k-1, k-2, k-3)$ holding $(z_{k-1}^{c},\ z_{k-2}^{c},\ z_{k-3}^{c})$ respectively and $(k-4)$ gets updated with the compensated data (z_{k}^{c}) by SWC approach which is originally delayed by 4 sampling intervals. Since the SWC approach utilises the delayed data in their respective time window, it can be seen in Fig.7.20 that the system performance is stable.

One other interesting observation that can be made from Fig.7.20 is that the system response has started shifting from the reference and results in mild overshoots. This is due to the fact that while the time delay compensation approaches are aimed at compensating the delayed data to keep the system stable, their purpose is not to remove the delay from the network. Therefore, the output response while stable will remain delayed with respect to the demand by the amount of delay experienced in the wireless medium unless the original external source of time delay is removed. This is due to the fact that in an event-triggered control, the feedback data that triggers the controller is delayed initially by the amount of delay experienced in the network. However, SWC approach can keep the system stable as long as this time shift in response is acceptable in industrial systems. Most of the industrial systems are designed such that they can tolerate certain delay in the output response known as the maximum tolerated delay as long as the delayed response does not render the system unstable.

7.5 Summary

There is an increasing interest to implement wireless communication in industrial control systems. Time delay in a wireless closed-loop control system can lead to the controller using stale data and render the system unstable. A sliding window based adaptive compensation (SWC) method is explained in this chapter for time-varying delay exceeding the sampling interval in a wireless closed-loop control system. The proposed approach incorporates the delayed measurement as well in its prediction process to increase the credibility of the predicted data thereby ensuring the control stability. The stability of the system is evaluated during dynamic change in input demand under varying time delay. In approaches where adaptive sampling rates are used to accommodate the time delay the sampling rate cannot be increased over a certain bound. The proposed approach can ensure stability in such systems when the adaptive sampling rate has reached its maximum bound and cannot be increased further. While the results are promising it is highlighted that in cases where time delay causes a significant amount (a quarter in this case) of sampled data to be delayed, there will be a natural shift in the system response as the initial feedback data that triggers the controller is delayed. Therefore, the shift in system response will be exhibited unless the original external source of time delay in the wireless network is removed. However, the proposed approach could still keep the system stable under such scenarios as long as this shift is within a tolerated limit in industrial wireless closed-loop control systems.

Chapter 8

Conclusions

This chapter summarises the research contributions and provides suggestions for future research work. There is increasing interest in the use of wireless communication for industrial control systems. Wireless closed-loop control systems for critical industrial applications need a co-design approach between communication, computing and control systems. Therefore, the aim of this research is to investigate the open research problems in these three domains from an industrial wireless closed-loop control perspective and address the gaps identified in order to deliver communication reliability and control stability.

8.1 Main Contributions

Fig.8.1 depicts the key areas investigated in the domain of wireless control and the main contributions (Chapters 5 to 7) of this research work.

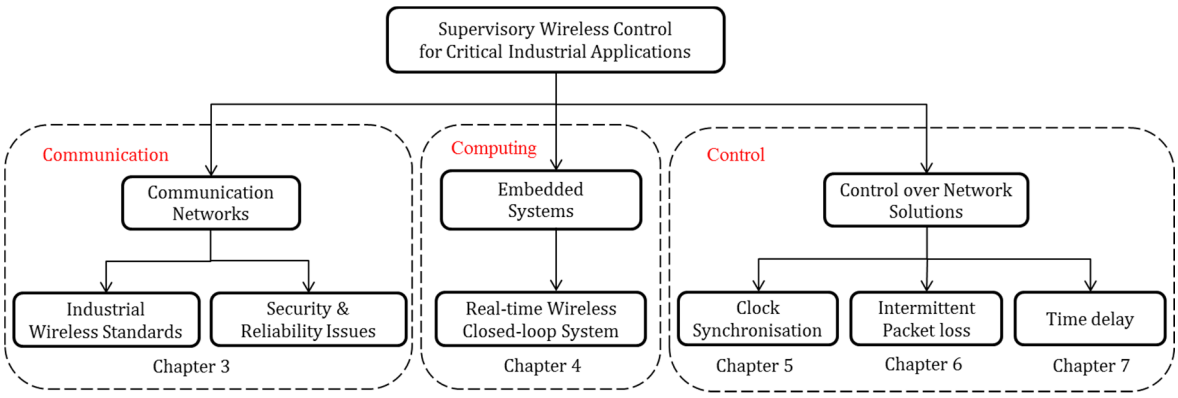

Figure 8.1: Illustration of key areas and main contributions in the thesis

The research was initiated by a number of potential areas identified for wireless control across Rolls-Royce businesses such as Aerospace, Installations, Marine and Energy. The highest ranked application was for backup control lanes for improved availability and redundancy. As the control systems that will be closed over the wireless network in these business areas are considered to be safety-critical, addressing the underlying issues is clearly a research priority. When a control system is closed over a shared communication

medium network, there is a need to understand the complexity and integration issues. In addition, the limitations of embedded systems in supporting such integration need to be analysed. The key issues investigated in this research are as follows:

- A state-of-the-art analysis of industrial wireless standards was performed and a case for their suitability for wireless closed-loop control in critical industrial applications is presented.
- A novel supervisory wireless real-time control approach for real-time closed-loop wireless control was proposed, and the effectiveness of the proposed approach was evaluated in a stand-alone wireless embedded hardware environment.
- Novel and pragmatic solutions from an industrial perspective were discussed for the *control over network* issues as listed below:
    - clock synchronisation,
    - time delay exceeding sampling rates, and
    - intermittent packet loss in feedback control loops

8.1.1 Communication Networks

Industry is hesitant to introduce wireless technologies in critical control due to safety regulations and certification limitations. However, it should be noted that there are historical parallels with respect to concerns in introducing communication technologies in critical control applications. For instance, the first version of safety standards ISA/ANSI 884 prohibited the implementation of critical control systems over communication networks. However, due to the development of proven communication protocols such as Fieldbus, Profibus, industrial automation is now actively using these protocols for control systems. As highlighted in Chapter 2, the CAN network is predominantly used by major aircraft companies to implement the Fly-by-Wire communication networks across various control systems and the flight computer. There is a growing interest to utilise fly-by-wireless technologies and a few airlines have already started utilising the 2.4 GHz Wi-Fi for internal wireless communications and in-flight entertainment networks. Early experiments where flight control systems are controlled using wireless networks is highlighted in Section 2.1.1.

Due to certification and marketing issues, industrial applications need standardised wireless protocols that can be used across various control systems. Chapter 3 presented an analysis of industrial wireless standards and their suitability for critical control applications; a case for a wireless standard for critical industrial applications is discussed. While various works in literature discuss the merits and drawbacks of industrial wireless standards, this chapter focuses, in particular, on the suitability of these standards for wireless closed-loop control.

Wi-Fi, due to various issues, is definitely not a candidate for safety-critical control. However, Wi-Fi becomes the obvious choice when it comes to COTS products, worldwide usage, availability of technical support, etc. Therefore, Wi-Fi has a potential to be used in

proof-of-concept studies and in maintenance and test bed environments. The WirelessHART standard proves to be the most promising for industrial control in the short term but does not address critical applications. ISA 100.11a specifically addresses industrial process monitoring and control and it has additional features and flexibility over WirelessHART. However, currently it is focused on non-critical applications and its performance may be extended to critical applications in the future.

Chapter 3 further analysed the effectiveness and application impacts of security protocols in industrial wireless standards with respect to wireless closed-loop control. The implementation of a specific security protocol requires analysis of the level of protection it provides, e.g. potential loopholes and security threats versus the effects it has on the controlled system. A summary of open research problems and a list of key findings are highlighted. The issues that arise when a control loop is closed over a control network are classified as *Control over Network* issues and the identified issues are further addressed in this research to produce a reliable wireless control loop.

8.1.2 Computing (Embedded Systems)

Having analysed the issues with communication standards in industrial wireless closed-loop control systems, the next step was to investigate the issues with computing. Chapter 4 explained the design considerations and issues in implementing a wireless closed-loop control using embedded firmware. Wireless real-time control systems are classified as embedded control systems wherein the entire control operation and other components are handled by an embedded processor. Control stability depends on how the sampling and actuation are done in a wireless control system. Defining an event-driven or time-driven approach for sampling/actuation depends on what the application demands. Event-driven approaches can save bandwidth as sensor readings are processed only when required. Time-driven approaches can save data loss and avoid collisions as each node is permitted to transfer only in their allocated time. Therefore, a supervisory closed-loop control approach using a hybrid time-triggered and event-triggered control strategy over a wireless channel is proposed. The effectiveness of the proposed approach is demonstrated using an embedded wireless hardware demonstrator.

Most of the solutions in the literature are evaluated using simulation models or hardware-in-the-loop setups. In such experiments while the data is transmitted using radio modules, the core computation is done using a general processor such as a PC or laptop. As these are highly capable processors, they may overlook a few issues that become more obvious when the implementation is done using an embedded setup. One such issue with interrupt latency and deadlock is clearly highlighted in Chapter 4. It was found that when a single microcontroller is used to handle both the control algorithm and the wireless protocol, it performed well when operated on a time-triggered basis. However, the same processor was not able to handle both control processing and wireless transmissions when implemented

on an event-triggered setup due to the interrupt latency when the events overlap. Such issues may not be evident on general-purpose processors that have multithreading capabilities. As event-triggered control is more applicable to industrial systems (due to power saving, less consumption of network resources, etc.) a parallel processor approach is proposed to overcome this issue.

One drawback to parallel processors is the increase in complexity (in multiple sensor and actuator networks) and power consumption. However, radio units can be optimised using various channel hopping techniques as discussed in Section 3.4.4. Such optimisation will result in reduced power consumption. In addition, development in embedded processors has resulted in low power processors that utilise a sleep mode when not in use.

Another issue that was highlighted concerns utilising adaptive sampling rates in an embedded environment. A sampling policy was proposed for wireless closed-loop control systems where the sampling rate of the controller should always be higher than the sampling rate of the feedback data. While adaptive sampling rates have been widely discussed in the literature for addressing lost data packets and to overcome time delay in the feedback loop, the studies do not consider the effects of embedded processors in implementing such solutions. Most of the studies suggest an approach to vary the sampling rates on the feedback loop to overcome time delay, however, the effects this will have on the embedded processor in sampling the control demand are not considered. Using the wireless hardware demonstrator, it was observed that the control demand must always be higher than the feedback as it affected the control demand transmission if it is equal to or less than the feedback sampling rate. In addition, this improves the chances of keeping a control loop stable during interference in control demand transmission as suggested in [Luck and Ray, 1990].

8.1.3 Control over Network Issues: Clock Synchronisation

Chapter 5 discussed the clock synchronisation issues such as clock offset and clock drift and their effects on a wireless closed-loop control system. Clock synchronisation is essential in wireless networked control systems to guarantee sample rates and prevent time skewing. Current clock synchronisation methods that are utilised in industrial automation such as NTP and GPS are discussed and it is highlighted that they are not suitable for networks due to energy consumption issues and availability of global time. Therefore, there is a need for internal clock synchronisation algorithms that can guarantee the synchronisation between wireless nodes in a network and update its time stamp whenever a global time base is available.

The key issues identified from the literature in utilising these algorithms in wireless closed-loop control are discussed. While a few synchronisation algorithms address the pair-wise synchronisation process they do not explicitly address the stability of the

controlled system. On the other hand, control system stability is ensured by using an event-triggered control and time-triggered sampling thus eliminating the need for synchronising the clocks. This chapter highlights the effects of clock offset and clock drift on a wireless closed-loop system's stability under an event-triggered control and time-triggered sampling system.

A sampling interval based clock synchronisation (SICS) approach is proposed for utilising the IEEE 1588 precision time protocol (PTP) for correcting clock offset/drift in wireless closed-loop control systems. The SICS approach is suitable for wireless control loops as synchronisation is achieved using the sampling interval in the slave nodes rather than the synchronisation interval decided by the master node. It eliminates the need for multiple synchronisation intervals and the problem of instant clock synchronisation. The SICS approach assists the local controller in correcting its clock offset and drift thereby keeping the control process stable. While synchronisation algorithms using PTP for wireless sensor networks concentrate on correcting the clock offset, the SICS approach corrects the clock drift and keeps the drift error to a minimum as clock drift is a recurring phenomenon. While the results are promising it is also highlighted that choosing an optimal sampling rate for feedback controllers can further improve the synchronisation accuracy. The proposed algorithm is then tested in a practical wireless control loop using an embedded microcontroller platform. An accuracy of 1.3 ms is achieved which is comparable to recent findings in clock synchronisation in industrial control and monitoring.

It is to be noted, the existing synchronisation mechanisms for industrial systems that claims accuracy in milliseconds are defined for wireless sensor networks using pairwise synchronisation. While synchronisation accuracy is achieved in milliseconds in previous works, the suitability of such mechanisms while a wireless closed-loop control system is in operation is not known. However, the proposed technique in this research work achieves such accuracy while maintaining the stability of a wireless closed-loop control system.

8.1.4 Control over Network Issues: Intermittent packet loss

Chapter 6 describes the issues associated with packet loss in wireless feedback control. Packet loss is an unavoidable phenomenon in wireless sensor networks, especially those operating in harsh industrial environments. The rate of packet loss depends on many different factors such as co-channel interference, deliberate jamming, network traffic load, power consumption of the sensor nodes and transmitting distance, etc. In addition, sensor faults and failures could also contribute to complete packet loss in distributed control systems. While there are various solutions available for addressing lost data packets utilising them for wireless real-time control are fairly an emerging research area and therefore, a comprehensive study from a wireless control loop perspective is presented in this thesis. While the data link, network and the transport layer of the wireless standards

guarantee the stability of the network, to a certain extent, there is a need for further work to guarantee the control stability in critical systems.

A novel sensorless supervisory wireless real-time control approach that addresses the issue of packet loss in wireless feedback control loops is proposed. The proposed solution can keep the wireless control loop stable and at the same time provide a methodology with ease of implementation in real-time industrial systems. Results and discussion are presented using a MATLAB Simulink model of a wireless control system as well as using the wireless hardware demonstrator. In the hardware demonstrator, the burst packet loss is deliberately introduced in the feedback loop by characterising the packet loss using the Gilbert-Elliott (GE) model. Therefore, the results based on the hardware demonstrator are a typical representation of wireless closed-loop control loop performance under deliberate jamming. The effectiveness of the proposed supervisory control algorithm is further evaluated using a Wireless Aircraft Braking System (W-ABS) simulation model.

The traditional linear prediction approaches used to estimate data under packet loss conditions do not consider the system dynamics and are prone to have corrupted data due to time delay and other security issues. The proposed approach in this research work estimate the data based on the system dynamics thereby producing a more reliable data under packet loss and poor network conditions. In addition, it assists in maintaining the system performance from degrading during intermittent packet loss. While the results show the effectiveness of real-time control in wireless systems, it is highlighted that there is scope for improvement, as estimated data may exhibit overshoots if the data packet loss is lost for a significant time period.

8.1.5 Control over Network Issues: Time delay

Chapter 7 presented the issues and major challenges due to time delay in forward and feedback path in wireless closed-loop control systems. Time delays bounded by the sampling interval generally is not a cause for concern in discrete-time systems. However, delays exceeding the sampling interval will lead to stale data being processed by the controller and will eventually lead to instability issues. Time-varying delays bounded by the sampling interval can still cause problems to a discrete-time system if the system has a long sampling interval. Existing research addressing time-varying delay is discussed and the gaps identified in the existing literature with respect to wireless closed-loop control systems are highlighted.

Constant time delays in wireless networks can be compensated using a Smith Predictor. However, the Smith predictor is not suitable for time-varying delays in wireless control loops as pointed out in Section 7.2. Therefore, a modified Smith predictor based on a Kalman filter that is suitable for wireless closed-loop control systems is proposed. However, there is one drawback with the proposed approach for time-varying delays

exceeding the sampling interval. Though the data arrived is delay compensated it has arrived one sampling interval later or, in other words, if there is no delay, then more recent sensor data would be available rather than the one compensated.

Another issue with time delayed networked control is that time delayed data is still transmitted/received over the wireless channel consuming network resources. Therefore, a sliding window based adaptive compensation approach is proposed to incorporate the delayed data in the estimation process and to tackle the drawbacks of the modified Smith predictor. In the proposed approach, the delayed data that is compensated is incorporated in the Kalman filter estimated data in a novel way such that stale data is not used by the controller. Therefore, it is ensured that the delayed data is not completely ignored and as a result the estimated system states can closely track the actual system states.

The results showed that the proposed approach can keep the wireless closed-loop control system stable even when the time-varying delay has rendered the system completely unstable otherwise. In approaches where adaptive sampling rates are used to accommodate the time delay the sampling rate cannot be increased over a certain bound. The proposed approach can ensure stability in such systems when the adaptive sampling rate has reached its maximum bound and cannot be increased further. While the results are promising it is highlighted that in cases where time delay causes a significant number of sampled data to be delayed, there will be a proportionate natural shift in the system response unless the original external source of time delay is removed. However, the proposed approach can keep the wireless closed-loop system stable as long as this time shift is within an acceptable range or the maximum tolerated delay for a given control system.

8.2 Suggestions for Future Work

Future work might consider the analysis of such issues over a real-time operating system (RTOS). An RTOS can ensure a tight scheduling policy to overcome the interrupt deadlock issues. For instance, pre-emptive scheduling will force the controller to exit a particular interrupt service routine (ISR) if it exceeds its scheduled timing. However, in wireless closed-loop control with tight real-time constraints, skipping a control operation may not be a desirable solution. For instance, forcing a controller to exit from an ISR that handles Hall sensor events will result in incorrect speed estimation. Therefore, such issues need to be further analysed against the processing capability of the embedded processors.

While some research in the literature shows the possibility of implementing a networked control system over a RTOS using general-purpose processors, in this research, the possibility of a wireless closed-loop control using a stand-alone low-cost low-power embedded system with real-time scheduling is demonstrated. The next step is to demonstrate the experiment using an RTOS on an embedded processor to overcome the

issues highlighted. However, COTS embedded processors that support fully-fledged RTOS have just started to appear in the market, and they might lack a wireless interface readily available in addition to power consumption and cost issues.

While this work considers the round trip time delay t_{rtd} as a QoS metric to detect packet loss, possible extensions to the supervisory wireless control approach would be to build a framework considering the suitability of other QoS metrics. Currently, this is done through exhaustive simulation and theoretical studies, which are unlikely to produce optimal solutions in embedded systems. Therefore, future work could take the form of the sensorless supervisory control approach proposed in this work to make the system more robust and fault tolerant.

The majority of wireless systems in today's industrial systems are widely used for data transfer and monitoring. In terms of closed-loop control systems, wireless transmitters can be used as input devices for transmitting sensor data. However, there are no industrial wireless analog output devices such as valve positioners as yet [Verhamme, 2011]. As highlighted in section 3.4.3, one of the key challenges in implementing wireless output devices is the required power when these devices operate on batteries. Therefore, future research work should consider the effectiveness of the control over network solutions while improving the battery life of the wireless devices.

Although air provides huge possibilities for message transmission using different frequencies and robust modulation techniques, the available frequencies are already determined for specific applications and most of them are not license-free. Issues such as resource constraints, unpredictability of wireless standards, real-time problems and security issues are important hurdles that need to be resolved for implementing wireless technology in critical control. When it comes to safety-critical applications, wireless communication links do not introduce any new failure modes. It is just that existing issues in wired communication networks are exacerbated due to the unreliable nature of the wireless medium. Though research has just started for extending wireless services to safety-critical applications, some of the early experiments, as shown in this research, suggest that there is definite scope for the use of wireless systems in critical real-time closed-loop control applications.

Appendix A

Industrial Benefits

The main benefits of using wireless sensor networks (WSN's) in aerospace applications as listed by Consultative Committee for Space Data Systems [CCSDS, 2010] are:-

Benefit	Feature
Mobility of crew, sensors and instrumented systems	Enables operational communications capabilities that could not be accomplished otherwise.
Harness complexity reduction/elimination	Wireless communication enables the elimination of complex, expensive, cable harnesses.
Eases retro-fit activities	Wireless technologies facilitate add-on capabilities to existing vehicles without significant engineering (e.g., mechanical, electrical) effort.
Mass and volume reduction	Wireless communication enables the elimination of cables and supporting infrastructure (cable runs, cable ties, which can amount to 10 percent of total vehicle mass).
Lowers cost of distribution	Broadcast mechanism provides a relatively low cost of content distribution; can add users and systems in a cost-effect manner (point-to-multipoint).
Reduced cost through flexible infrastructure	Elimination of infrastructure associated with wired systems.
Simplification of AIT activities	Wireless communications simplifies and eliminates any wired-biases associated with functional ground testing of the complex systems of modern spacecraft in addition to minimizing contamination issues and simplifying structural considerations.
Common network for onboard and off board communications	A single transceiver may be used for both onboard (intra-spacecraft) and off-board (inter-vehicle or surface) communications.
Rotating mechanisms and articulated structures	Wireless technologies are the easiest and sometimes the only way to implement contact-less data communications and acquisition systems.
Layout independence	Wireless techniques may bring additional flexibility when implementing fault tolerance and system reconfigurations.
Convenience	Allows access to network communications from anywhere within the range of the network, reduce complexity of operation and associated risk.
Ease of deployment	Set-up of a infrastructure-based wireless network requires only an access point.
Flexibility	Within radio coverage the wireless nodes cans communicate without restriction. RF radio waves can penetrate non-conductive walls so it is feasible that a sender or receiver could be hidden within or behind a physical wall.
Ad-hoc networking	Wireless ad hoc networks enable communication between compliant devices without the need of a planned system as would be required with a wired network.
Small form factor	Wireless devices are engineered to low mass, power and volume requirements, all three of which are fundamental constraints in spacecraft design.
Fault tolerance	Wireless devices can survive disasters, such as a catastrophic event of nature or even the common occurrence of a power loss (blackout). As long as the wireless devices are intact, all-important communications still exist.

Table A.1: Industrial wireless benefits [CCSDS, 2010]

Appendix B

Radio Spectrum and Channel Contention

B.1 Radio Frequency Spectrum

Radio frequency interference issues pose serious problems for wireless communications. Therefore, it is important to have a fundamental understanding of the radio frequency spectrum in order to evaluate the wireless technologies. This section provides a brief overview of the radio frequency range of the electromagnetic spectrum and the interference issues. The electromagnetic spectrum is a continuum of a range of possible frequencies that can provide electromagnetic radiation. It is defined as a range of frequencies starting from the lowest frequency and moving towards the highest frequency between which an electromagnetic wave can exhibit radiation (see Fig B.1). An EM wave can be described in terms of its wavelength, frequency and energy. Bandwidth is defined as the difference between the highest and the lowest cut-off frequency of a particular communication band.

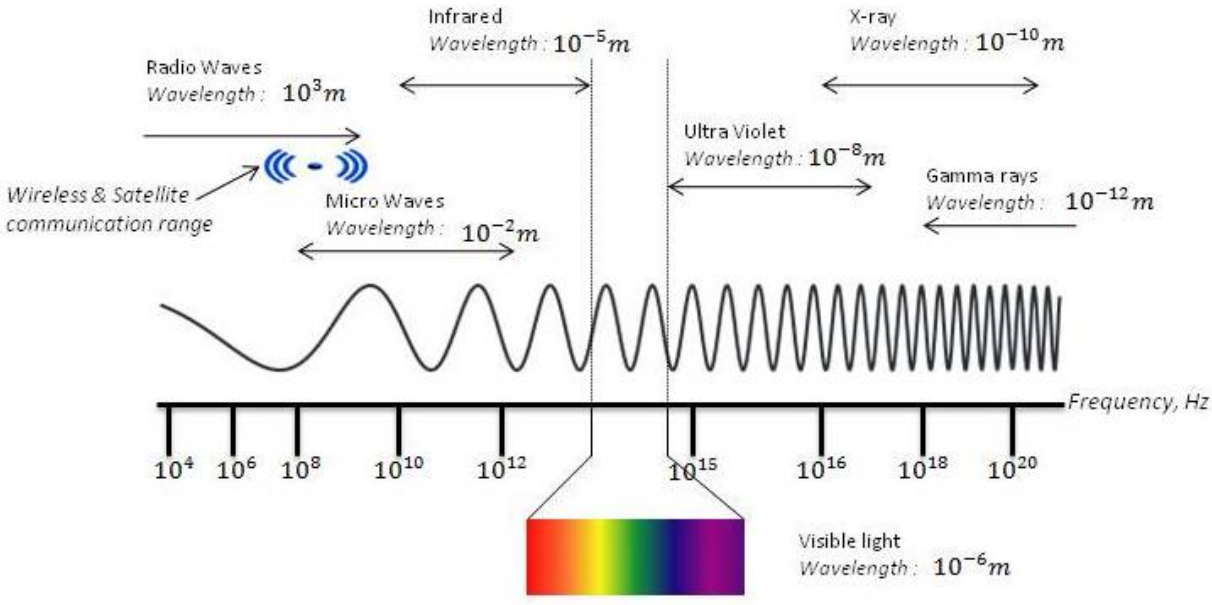

Figure B.1: Electromagnetic spectrum

Low frequency bands have less bandwidth and hence they carry only low data rates. Hence, theoretically, higher frequency bands can provide higher bandwidths and hence high data rates.

The extremely high frequency waves beyond the visible light range are difficult to modulate. In other words, encoding a carrier signal with information is highly difficult at these frequency ranges. Also, gamma rays and x-rays provide ionisation effects and hence these are undesirable for communication purposes.

The radio frequency spectrum offers frequencies less than 300 GHz which is suitable for communication purposes. Above 300 GHz, the absorption effect of atmosphere is very high and electromagnetic radiation becomes difficult. In order to utilise the radio spectrum efficiently and to avoid interference issues, ITU (International Telecommunication Union) has split the radio spectrum into different frequency ranges that should be used for various communication purposes. This prevents signal overlapping. Some of these ranges may differ slightly among different countries based on the purpose of usage. Table B.1 provides a list of available radio frequency bands utilised for communication purposes and their applications.

Frequency	Band Name	Applications
< 3 kHz	Extremely Low Frequency (ELF)	Submarine communications
3 kHz - 30 kHz	Very Low Frequency (VLF)	Marine communications
30 kHz - 300 kHz	Low Frequency (LF)	AM Radio
300 kHz - 3 MHz	Medium Frequency (MF)	AM Radio
3 MHz - 30 MHz	High Frequency (HF)	AM Radio
30 MHz - 300 MHz	Very High Frequency (VHF)	FM Radio, TV
300 MHz - 3 GHz	Ultra High Frequency (UHF)	TV, cellular, wireless systems
3 GHz - 30 GHz	Super High Frequency (SHF)	Satellites
30 GHz - 300 GHz	Extra High Frequency (EHF)	Satellites, radars

Table B.1: Common radio frequency bands and typical applications [CCSDS,2010]

Wireless communication is targeted at the ultra-high frequency range of the radio spectrum. Various consumer electronics such as TV, cordless telephones, Wi-Fi systems operate in this range. The advantage of UHF is that it can oscillate with short wavelength and this leads to smaller transmitting and receiving antennas. However, the transmitter and receiver are expected to have a line-of-sight for better transmission and reception.

B.2 Channel Contention Methods

When real-time systems are connected over a wireless communication network, time delays and packet loss are inevitable. When a supervisory controller has to control multiple local control units, there will be more wireless sensors in the network and it is likely that there will be issues due to channel contention by these sensors over the available bandwidth. The supervisory controller then has to decide how to allocate the bandwidth

based on which local control unit has high priority. The key issue here is how to achieve this in real-time as there is a need to identify what can be missed (soft real-time) and what cannot be missed (hard real-time). However, an industrial wireless standard does offer methods to tolerate time delays and interference in a communication network. The OSI layer (explained in Chapter 3) governs the workflow of any communication standard. The second layer of the OSI model known as the data link layer incorporates a Medium Access Control (MAC) protocol.

MAC protocol is responsible for sharing the available bandwidth to the sensors in a given network and ensures successful delivery of the data packets. The MAC protocol depends on the Physical layer (PHY) which is the first layer of the OSI model that decides whether the communication medium is wired or wireless. As the wireless medium introduces various issues such as packet loss, time delay, interference, attenuation, etc. the MAC protocol has to ensure that the data packets are delivered overcoming these issues. Therefore in order to address these issues the MAC protocol uses the channel contention methods to tell each sensor when it can transmit and when it is expected to receive the data. Over the last few decades, numerous algorithms have been proposed to address channel contention in a network. However, only few of them address the needs of a wireless real-time control loop and these are discussed below.

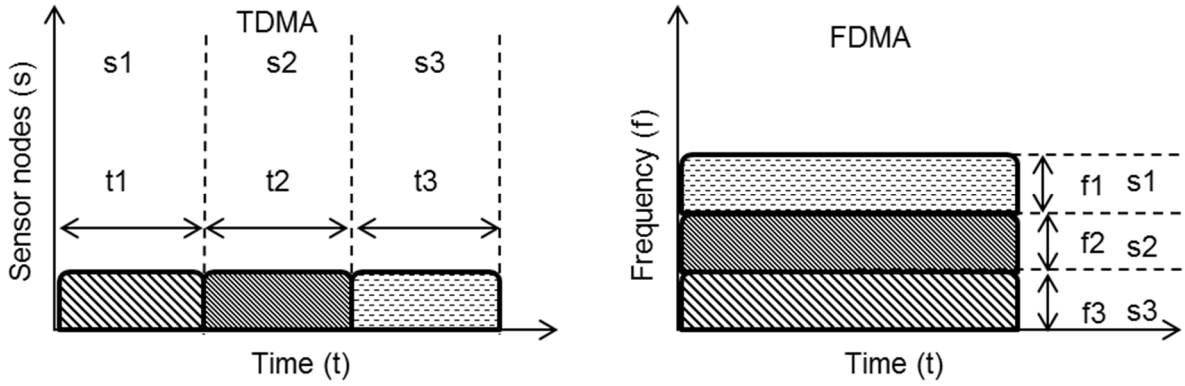

Figure B.2: Channel contention methods

Time division multiple access (TDMA)

In time division multiple access (TDMA), sensor nodes are allocated a specific time slot to transmit and receive the data. The MAC protocol divides the available bandwidth into fixed size time slots and allocates them to the sensors in an organised pattern. A sensor can transmit in more than one available slots but this should be allowed by the MAC protocol based on priorities. Packet collisions are greatly reduced in TDMA protocol due to the dedicated time slots. Due to its reliability and robustness TDMA has been widely adopted in industrial wireless standards such as WirelessHART and ISA100.11a. WirelessHART utilises a TDMA protocol that allocates a 10ms time slot for the sensor nodes in the network. However, even if a particular sensor does not have any data to transmit the time slots are still allocated to the sensor and therefore the bandwidth could be wasted. For

wireless real-time control loops TDMA is a suitable approach given that each sensor will have a dedicated time slot to transmit and receive data without any interruption. However, the protocol should allocate these slots based on priority so that a sensor data does not become stale data.

Frequency division multiple access (FDMA)

In Frequency division multiple access (FDMA), the available bandwidth is divided into slots based on individual frequencies and the sensor nodes are allowed to transmit and receive data in their allocated frequency. The advantage of this scheme is to allow sensors to transmit and receive simultaneously whereas in TDMA each sensor has to wait for its allocated time slot. However, in FDMA, there are various issues such as co-channel interference, spectral spreading due to Doppler Effect, and channel noise. FDMA can offer good network throughput in distributed wireless sensor networks with soft real-time requirements, however, it may be unsuitable for real-time control loops as any interference issues would lead to undesirable results. Solutions such as frequency hopping and channel blacklisting could help in addressing some of the issues in FDMA.

Carrier sense multiple access with collision avoidance (CSMA-CA)

CSMA-CA as the name indicates looks out for a clear carrier medium before it starts transmission in order to avoid collision of data packets. It is a special case of MAC protocol used for wired Ethernet communication which uses carrier sense multiple access with collision detection (CSMA-CD). In Ethernet communication the MAC protocol has the ability to listen to packets colliding while the sensor nodes transmit and receive as they all have the same signal strength. However, in radio communication, a sensor node's signal strength during transmission is high enough that it masks the rest of the signals nearby. Therefore, radio nodes lack the ability to detect collision like Ethernet. Therefore, for radio communication CSMA-CA offers an alternative where instead of listening to collisions it tries to avoid it at the first instance. Therefore, a radio node before transmitting checks if the network medium is busy or available using a contention timer. The node waits for a random time and at the end of the timer it checks if the network is idle and transmits the message. The timer is statistically built so that it offers equal chance to the rest of the sensors in the network to access the channel. This mechanism is currently used by many industrial wireless standards in the ISM band. At the moment, there is no industrial wireless standard for specific use of wireless in aerospace applications. However, in such a standard, a combination of TDMA and CSMA-CA would offer significant advantages for channel contention mechanisms and minimise the risk of collisions.

Appendix C

Industrial Wireless Standards

C.1 Security in IEEE 802.15.4

The IEEE 802.15.4 standard defines various security suites as given in Table C.1 to implement the security for the transmitted data. All the security keys used in the various suites are computed using the Advanced Encryption Standard (AES) cipher and hence prefixed to all security suites.

Name	Description
Null	No Security
AES-CTR	Encryption only, CTR Mode
AES-CBC-MAC-128 AES-CBC-MAC-64 AES-CBC-MAC-32	128 bit MAC 64 bit MAC 32 bit MAC
AES-CCM-128 AES-CCM-64 AES-CCM-32	Encryption & 128 bit MAC Encryption & 64 bit MAC Encryption & 32 bit MAC

Table C.1: Security suites supported by IEEE 802.15.4

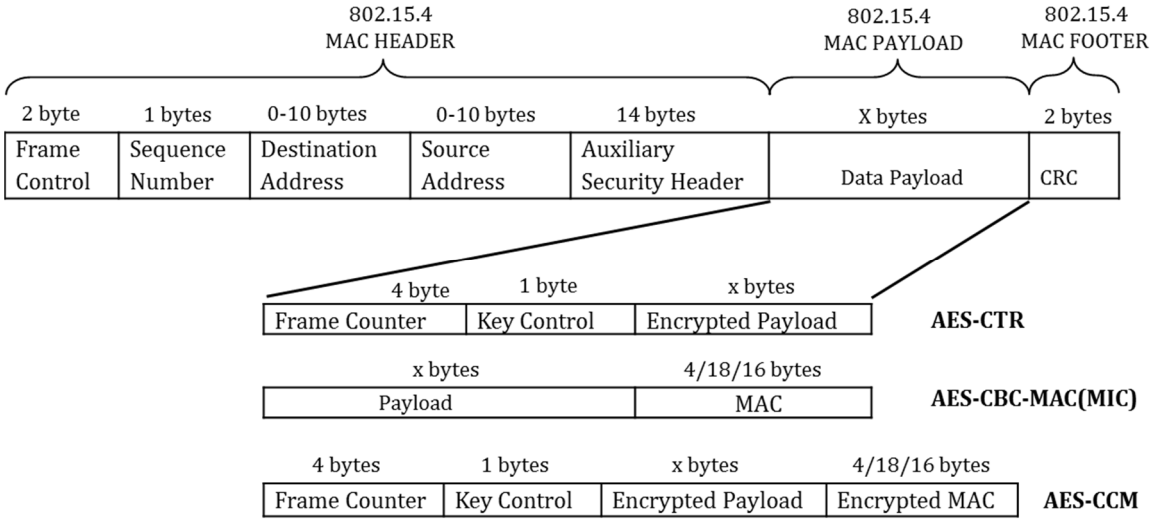

Figure C.1: Security in the IEEE802.15.4 MAC frame [Gascon, 2014]

Encryption only mode (AES-CTR)

In order to ensure integrity of the transmitted data the IEEE 802.15.4 standard specifies the encryption only mode Advanced Encryption Standard Counter (AES-CTR) as shown in Fig.C.1. In this mode, the sender divides the data packet into 16-byte blocks $(p_1, p_2, \ldots p_n)$ and calculates $c_i = p_i \oplus E_k(x_i)$. c_i is the encrypted text, p_i is the plain text, E_k is the encryption mode and x_i is the nonce. The recipient recovers the received data using $p_i = c_i \oplus E_k(x_i)$. Therefore, the recipient needs the value of counter x_i which is termed as cryptographic nonce or IV [Sastry, 2004]. The structure of a nonce is shown in Fig.C.2.

1 byte	8 bytes	4 bytes	1 bytes	2 bytes
Flags	Source address	Frame Counter	Key Counter	Block Counter

Figure C.2: Structure of a cryptographic Nonce (IV)

It consists of a 4 byte frame counter which is incremented at the radio hardware after each data packet is encrypted. If the frame counter reaches the maximum value then no further encryptions are possible and therefore the counter is reset by incrementing the 1 byte key counter. The 2 byte block counter numbers the 16 divided blocks of data. The idea is that each time a data packet is encrypted a nonce should never be re-used which is ensured by the unique combination of frame counter and key counter.

Authentication only mode (AES-CBC-MAC (MIC))

In order to avoid tampering of data by an outsider and for the receiver to identify that the packet received is from the intended sender, IEEE 802.15.4 offers MAC (Message Authentication Code) based security suite known as cipher block chaining (CBC-MAC). MAC is otherwise termed as MIC (Message Integrity Check) in the protocol definition in order to avoid confusion with Medium Access Control (MAC) layer. The message authentication code is computed for each encrypted message using a unique key which is shared by all legitimate nodes in the network. The MIC data is then sent along with the encrypted data packet as shown in Fig.C.1. The receiver in turn will compute the MIC using the unique key and matches with the MAC found in the received message. The data packet will be accepted if the MAC matches else would be rejected.

Encrypted – Authenticated mode (AES-CCM)

This security suite offers both encryption and authentication by combining the above two methods. It first applies integrity check using the AES-CBC-MAC and the encryption is done using the AES-CTR process. This method is more secure as in addition to the frame counter and key counter in AES-CTR process, the AES-CCM (counter with CBC-MAC) utilise the MAC key to make the nonce more robust and preventing it from being reused. The 4 byte frame counter can go up to 2^{32} encrypted frames before the MIC key is "used up" after which a new key need to be redeployed [Zach, 2009]. Thus the above mechanism

is very secure and efficient as long as the same nonce value is not used twice for the same key.

C.2 Network Reliability

In a wireless closed-loop control system, the sensor nodes transmit the data packets using the uplink graph route and the control demand from the controller is transmitted using the downlink graph route on their allocated time slots as shown in Fig.C.3.

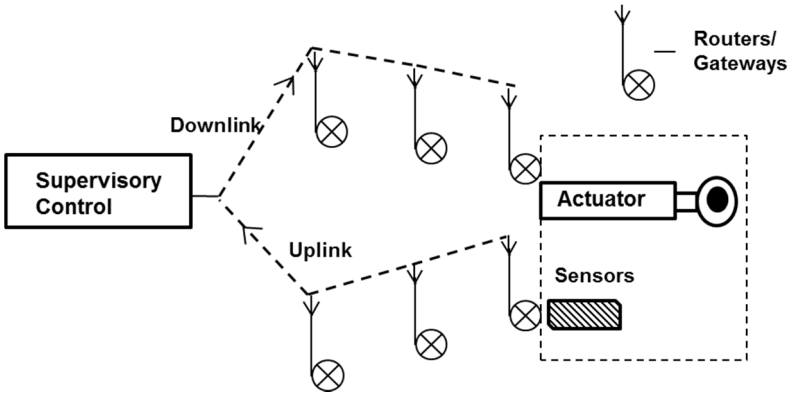

Figure C.3: Link quality in wireless closed-loop control

WirelessHART can utilise up to 15 RF channels to transmit as prescribed by the IEEE 802.15.4 standard. The end-to-end reliability is ensured as follows. For each data being transmitted from the sensor to controller along the uplink graph route the Network scheduler allocates a time slot for the sensor data packet and a follow-up time slot for any retransmissions in case of lost or corrupted data transmission. There are known as dedicated links. In addition, the scheduler allocates a third time slot on separate channels in case both the transmissions in the dedicated links are lost. These links on separate channels are known as shared links. The control demand from the controller to the actuator is transmitted through the downlink routing using similar dedicated and shared links.

A group of time slots is known as a superframe and the network manager manages the transmission of the superframes. In case of a given channel affected by heavy traffic or interference the WirelessHART has the ability to blacklist that channel (Channel blacklisting) and choose another channel for further transmission (Frequency hopping)

ISA100.11a follows the IEEE 802.15.4 standards at its PHY and MAC layer and hence similar to the WirelessHART mechanisms in addressing the network reliability, however, it has made many amendments across various OSI layers to differ itself from the WirelessHART networks. ISA100.11a offers the network reliability at both data link and network layers similar to WirelessHART protocol. In WirelessHART networks, the data link layer offered the communication reliability between neighbouring nodes whereas the end-to-end link reliability between two nodes across the network was determined by the network layer. However, in ISA100.11a the data link layer ensures end-to-end delivery at

the data link layer level across neighbouring nodes in a given subnet up to the backbone network. Communication reliability beyond backbone networks (gateway, network manager, etc.) is taken care of by the Network layer.

In ISA100.11a the wireless field devices (sensors, actuator nodes) and all the routing nodes are grouped together as a subnet. The subnet in turn links to a backbone network for further communication with gateway (see Fig.3.2b in Chapter 3). Therefore, the routing algorithms are implemented at the data link layer and the subnets are known as DL subnet.

In WirelessHART networks the management of frequency hopping across different channels is not explicitly defined. The network manager defines this based on its observation of network load. ISA100.11a specifically defines five pre-programmed hopping patterns [Sen, 2014] for the network manager to choose from as shown in Fig.C.4.

In addition, ISA100.11a offers slotted hopping patterns where k time slot from a given superframe can be used in channel n and k+1 time slot form the same superframe can be used in n+1 channel. ISA100.11a supports hopping between different time slots in the same superframe as well as between consecutive superframe whereas WirelessHART supports only the latter. ISA100.11a also supports slow hopping patterns for event based data transmission and a hybrid between slotted and slow hopping algorithms.

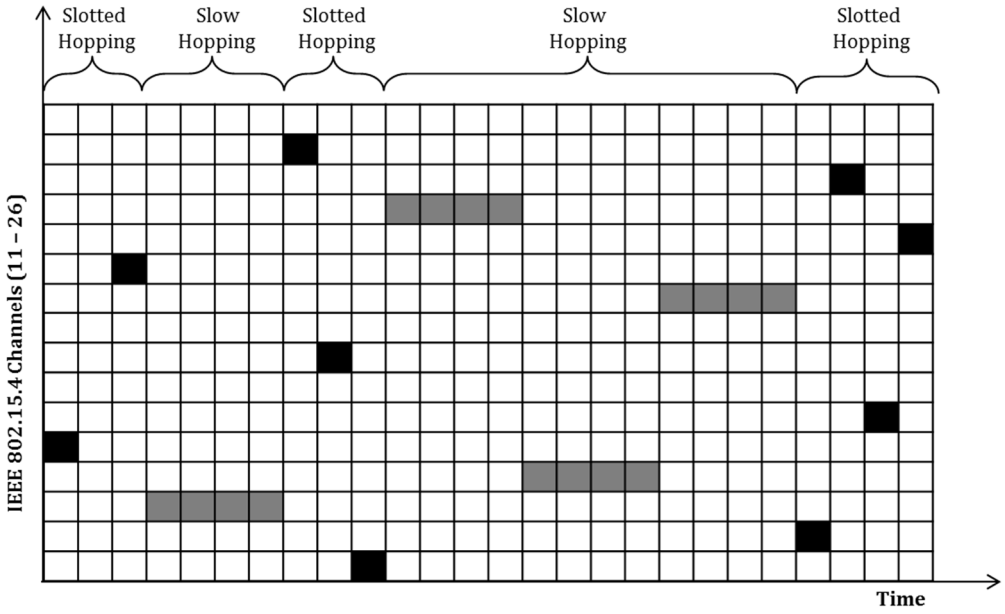

Figure C.4: Channel hopping patterns in ISA100.11a [Gungor, 2013]

In ISA100.11a as the Mesh routing is performed at the data link layer level, the network layer is responsible for source and destination addressing (16 bit or 128 bit) for end points and backbone networks. In addition, it performs fragmentation of data packets of length greater than that handled by data link layer.

C.3 Transport Layer in Wireless Stack

Lost wireless links and missed data packets are usually detected using acknowledgement (ACK) signals by the Transport layer. ACK and NACK signals are mandatory requirements of any wireless standards as the sender decides retransmission of data packets based on the reception of the ACK/NACK signals. ACK signals are known as positive acknowledgement where the ACK is transmitted as a normal packet to the sender as soon as the receiver receives the data packet and the CRC is validated. NACK known as negative acknowledgment is utilised where the receiver records the sequence of the received data packets. The sequence number is then transmitted to the sender to detect any lost packets. This is useful for control operations where a large number of data packets are grouped together and sent as a single packet for optimised consumption of network resources.

However, in Wireless closed-loop control with tight real-time constraints the reception of an ACK/NACK signal is not sufficient for reliable operation. As long as the ACK is received the sender will assume a successful transmission however in sampled systems the ACK should be transmitted before the next sampled data. In order to ensure this wireless controlled system utilise the Round-trip delay time to detect the reception of ACK/NACK signal within a certain interval as explained in Section 7.1.2 (Chapter 7).

The WirelessHART standard supports the ACK signals at the Transport layer. It supports both acknowledged signals for applications requiring confirmation of transmitted signals and unacknowledged signals for those applications where explicit acknowledgement is not needed (data publishing) to save network resources. ISA100.11a does not support ACK at the transport layer and WIA-PA does not explicitly define this in its specification.

C.4 WIA-PA (IEC 62601)

WIA-PA (see Section 3.1.4.2) makes use of the beacon mode of the IEEE 802.15.4-2006 standard. In contrast to the super frames used by the WirelessHART and ISA100.11a networks WIA-PA's superframe structure is based on its network architecture. WIA-PA uses a hybrid star-mesh network routing where mesh networking is implemented between the gateway and routing devices and the star topology is followed for links between routing devices and wireless field devices. A star network comprising of a group of field devices is termed as a cluster and based on this a superframe structure is as follows:-

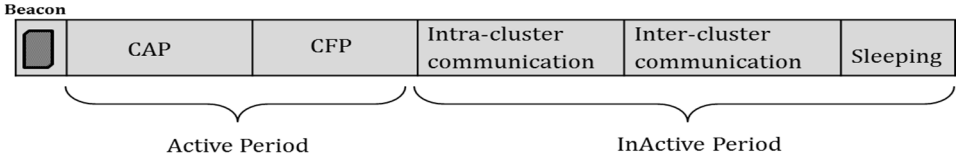

Figure C.5: WIA-PA superframe structure (inherited from IEEE 802.15.4-2006)

The data link layer of a WIA-PA offers various features compared to both WirelessHART and ISA100.11a. It employs both TDMA and CSMA-CA simultaneously within a superframe for better network reliability. The CSMA-CA is used for the contention access period (CAP) which addresses the device joining and retires. TDMA is used for the contention free period (CFP) as well as inactive period to support the respective functions.

As WIA-PA is based on the beacon-enabled mode of the IEEE 802.15.4 standard it offers the guaranteed time slot (GTS) mechanism during the contention free period of the superframe for applications with tight time constraints. WIA-PA ensures hop-by-hop network reliability between neighbouring nodes at the data link layer. WIA-PA offers a range of hopping techniques for robust transmission of data packets. It follows the adaptive frequency switch (AFS) at the beacon, CAP and CFP communication, Adaptive Frequency Hopping (AFH) for the intra-cluster period and Time hopping (TH) for the inter-cluster period. At the network layer level WIA-PA offers similar services as ISA100.11a such as fragmentation and reassembly of data packets, and source and destination addressing of routing and gateway devices.

WIA-PA offers two types of synchronisation mechanism to ensure the robust implementation of the TDMA contention method. In the inter-cluster communication the router devices are synchronised with the gateway devices and in the intra-cluster period the field devices are synchronised with the router devices. As WIA-PA follows the beacon frame model of IEEE 802.15.4-2006 standard the synchronisation messages are passed as beacon frames. Another type of synchronisation is done using keep-alive messages to ensure the neighbouring nodes in the cluster are always synchronised. The router devices send keep-alive messages in the inter-cluster period to ensure connection between neighbouring devices while the field devices send it in the intra-cluster period.

Data packets aggregation is a special feature of WIA-PA which is not available in ISA100.11a and WirelessHART devices. When a field device has multiple data objects they can be aggregated to a single data packet at the application layer known as data aggregation. Likewise the network layer can aggregate data packets received from different clusters (comprised of field devices) known as packet aggregation. This minimise energy consumption in WIA-PA networks, however, under interference there is a risk of losing all the aggregated packets at once.

Appendix D

Asymptotic Stability of Kalman Filter

Asymptotic stability of the Kalman Filter means that its solution will gradually become insensitive to its initial condition, provided that the norms of the noise covariance Q, R are bounded [Terejanu, 2014].

The Kalman Filter equations are given as (from Section 6.4.1),

Predicted system state: $$\hat{x}_k^- = A\hat{x}_{k-1} + Bu_{k-1} \quad (6.17)$$

Predicted error co-variance: $$P_k^- = AP_{k-1}A^T + Q \quad (6.18)$$

Kalman Gain: $$K_k = P_k^- H^T (HP_k^- H^T + R)^{-1} \quad (6.19)$$

Updated system state: $$\hat{x}_k = \hat{x}_k^- + K_k(Z_k - H\hat{x}_k^-) \quad (6.20)$$

Updated error co-variance: $$P_k = (I - K_k H)P_k^- \quad (6.21)$$

The corresponding discrete-time algebraic Ricatti equation (DARE) [Khan, 2011] from (6.18), (6.19) and (6.20) is given by,

$$P_{k+1|k} = AP_{k|k-1}A^T - AP_{k|k-1}H^T\left(HP_{k|k-1}H^T + R_k\right)^{-1}HP_{k|k-1}A^T + Q_k \quad (D.1)$$

Considering the system model in (6.17) is linear, time-invariant, observable, controllable and symmetric and Q, R, A are bounded matrices, the algebraic Ricatti equation in (D.1) will yield a constant solution $\bar{P}$ known as the steady-state prediction error covariance for constant values of Q and R matrices, therefore, (D.1) becomes,

$$\bar{P} = A\bar{P}A^T - A\bar{P}H^T(H\bar{P}H^T + R)^{-1}H\bar{P}A^T + Q \quad (D.2)$$

And the constant Kalman gain also known as the steady-state Kalman gain is given as,

$$\bar{K} = \bar{P}H^T(H\bar{P}H^T + R)^{-1} \quad (D.3)$$

In addition, if the system under consideration is an unforced discrete-time linear system, Equation (6.20) can be written as,

$$\hat{x}_{k|k} = [I - \bar{K}H]A\hat{x}_{k|k-1} + Kz_k \tag{D.4}$$

$$\hat{x}_{k|k} = [A - A\bar{K}H]\hat{x}_{k|k-1} + Kz_k \tag{D.5}$$

If $|\lambda_i(A)| < 1$, then $|\lambda_i[A - A\bar{K}H]| < 1$, where λ_i are the eigenvalues of the closed-loop matrix $[A - A\bar{K}H]$, then the designed Kalman filter is asymptotically stable [Assimakis, 2003].

Theorem 1: [Khan, 2011] Given that the designed filter is time-invariant and asymptotically stable, for any non-negative symmetrical initial condition($P_{k_{0|0}} = P_0$), of error co-variance matrix P, it can be obtained that,

$$\lim_{k\to\infty} P_{k+1|k} = \bar{P}$$

Theorem 2: [Simon, 2006] The DARE has a unique positive semi-definite solution P_∞ if and only if both of the following conditions hold:

1. (A, H) is detectable
2. $(A - A\bar{K}H, G)$ is controllable on and inside the unit circle

   Where, $GG^T = Q$

   Furthermore, the corresponding steady-state Kalman filter is stable. That is, $|\lambda_i[A - A\bar{K}H]| < 1$

Proof: Refer to Theorem 23, [Simon, 2006].

From (D.5), the following can be observed in regards to Kalman Filter stability [Polavarapu, 2004],

- In cases, where there are abundant measurement data, $KH \cong I$. Therefore, the Kalman Filter becomes stable even for unstable dynamics.
- If the system model is very stable, even if there is no measurement data such as in open loop Kalman filtering where the Kalman gain,$K = 0$, the Kalman Filter eventually loses memory of the initial condition.
- In order to keep errors from exceeding a certain bound, sufficient measurement data is needed if the system model becomes unstable.

References

Abdul-Aziz, A., & Woike, M. (2013). Turbine Rotor Disk Health Monitoring Assessment Based on Sensor Technology and Spin Tests Data. In *The Scientific World Journal* (Vol. 2013, Article ID 413587).

Abe, N., & Yamanaka, K. (2003). Smith predictor control and internal model control - a tutorial. In *SICE 2003 Annual Conference* (Vol. 2, pp. 1383–1387).

Abed, A., Alkhatib, A., & Baicher, G. S. (2012). Wireless Sensor Network Architecture. In *International Conference on Computer Networks and Communication Systems* (Vol. 35, pp. 11–15).

Abubakari, H., & Sastry, S. (2008). IEEE 1588 style synchronization over wireless link. *2008 IEEE International Symposium on Precision Clock Synchronization for Measurement Control and Communication*, 127–130.

Ahmadi, A. A., Salmasi, F. R., Noori-Manzar, M., & Najafabadi, T. A. (2014). Speed sensorless and sensor-fault tolerant optimal PI regulator for networked DC motor system with unknown time-delay and packet dropout. *IEEE Transactions on Industrial Electronics, 61*, 708–717.

Aircraft wiring incidents persisting in aging systems. (2004). Flight Safety Foundation, Aviation Mechanics Bulletin, Sep-Oct issue.

Akerberg, J., Gidlund, M., Neander, J., Lennvall, T., & Björkman, M. (2010). Deterministic downlink transmission in WirelessHART networks enabling wireless control applications. In *IECON Proceedings (Industrial Electronics Conference)* (pp. 2120–2125).

Albertos, P., Crespo, A., Vallés, M., & Ripoll, I. (2005). Embedded Control Systems: Some Issues and Solutions. *16th IFAC World Congress*.

Alcaraz, C., & Lopez, J. (2010). A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 40*.

Ali, Q., Khuder, E. (2012). Analysis of Industrial Networks using different WLAN standards. *Information Engineering (IE)*, Vol.1, Issue 1.

Almström, P., Rabi, M., & Johansson, M. (2009). Networked state estimation over a Gilbert-Elliot type channel. In *Proceedings of the IEEE Conference on Decision and Control* (pp. 2711–2716).

Andrews, M., Kumaran, K., Ramanan, K., Stolyar, A., Whiting, P., & Vijayakumar, R. (2001). Providing quality of service over a shared wireless link. *IEEE Communications Magazine*, *39*.

Araujo, J., Anta, A., Mazo, M., Faria, J., Hernandez, A., Tabuada, P., & Johansson, K. H. (2011). Self-triggered control over wireless sensor and actuator networks. *International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, 1–9.

Arms et al. (2009). Synchronized System for Wireless Sensing, RFID, Data Aggregation & Remote Reporting. *American Helicopter Society Forum 65*, Grapevine.

Arzen, K.-E., Bicchi, A., Hailes, S., Johansson, K. H., & Lygeros, J. (2006). On the Design and Control of Wireless Networked Embedded Systems. In *2006 IEEE Conference on Computer-Aided Control Systems Design* (pp. 440–445).

Assimakis, N.D., Psarakis, E.Z., and Lainiotis, D.G. (2003). Steady State Kalman Filter: A new Approach. *Journal of Neural, Parallel and Scientific Computations,* Vol. 11, No. 4, pp. 485-490.

Astrom, K., and Hagglund, T. (1995). PID Controllers: Theory, Design and Tuning, 2nd Edition, Instrument Society of America.

Auburn, C., Simon, D., Song, Y.Q. (2010). Co-design Approaches to Dependable Networked Control Systems. ISTE Ltd and John Wiley & Sons Inc.

Baillieul, J., & Antsaklis, P. J. (2007). Control and communication challenges in networked real-time systems. *Proceedings of the IEEE*, *95*, 9–28.

Becker, A. (2007). Bluetooth Security & Hacks. Ruhr-Universitat, Bochum.

Bin, L., Wang, F. Y., Qingming, Y., and Hui, G. (2008). Closing the control loop in intelligent spaces systems: control over wireless networks with a packet loss perspective. *In International Conference on Mechatronics and Embedded Systems and Applications, MESA 2008* (pp. 186–191).

Björkbom, M., Nethi, S., Eriksson, L. M., & Jäntti, R. (2011). Wireless control system design and co-simulation. *Control Engineering Practice*, *19*, 1075–1086.

Bluetooth. [Online]. (cited Sep 2014). http://www.bluetooth.com/

Bond, A. (2006). My View…Wireless Offers. *The IEE Seminar on Industrial Networking and Wireless Communications in Control*.

Boughanmi, N., Song, Y., & Rondeau, E. (2008). Wireless networked control system using IEEE 802.15. 4 with GTS. *2nd Junior Researcher Workshop on Real-Time Computing (JRWRTC 2008), 2008*, 4–7.

Bourke, T. (2010). ISA 100.11a. Honeywell Analytics, United Kingdom.

CC2500, Low-Cost Low-Power 2.4GHz RF Transceiver, Texas Instruments, Literature Number: SWRS040C, [Online], [cited Sep 2014]. http://www.ti.com/lit/ds/symlink/cc2500.pdf

CCSDS. (2010). Wireless Network Communications Overview for Space Mission Operations. Informational Report, CCSDS 880.0-G-1.

Chamaken, A., & Litz, L. (2010). Joint design of control and communication in wireless networked control systems: A case study. *American Control Conference (ACC), 2010*.

Chen, D et al. (2004). Wireless Process Control Products from ISA. Austin, USA.

Cheng, C. W., Lai, C. L., Wang, B. C., & Hsu, P. L. (2007). The time-delay effect of multiple-network systems in NCS. In *Proceedings of the SICE Annual Conference* (pp. 929–934).

Chilakala, S. K. (2008). Development and Flight Testing of a Wireless Avionics Network Based on the IEEE 802 .11 Protocols. *Master's thesis in Aerospace Engineering*, University of Kansas

Cho, C et al. (2006). A Random Backoff Algorithm for Wireless Sensor Networks. Next Generation Teletraffic and Wired/Wireless Advanced Networking, *Lecture Notes in Computer Science*, Volume 4003, pp 108-117, Springer.

Cloosterman, M. B. G., Wouw, N. van de, Heemels, W. P. M. H., & Nijmeijer, H. (2009). Stability of Networked Control Systems With Uncertain Time-Varying Delays. *IEEE Transactions on Automatic Control*, *54*.

Colandairaj, J., Irwin, G. W., & Scanlon, W. G. (2007). A co-design solution for wireless feedback control. *In 2007 IEEE International Conference on Networking, Sensing and Control, ICNSC'07* (pp. 404–409).

Colandairaj, J., Irwin, G. W., & Scanlon, W. G. (2007). Wireless networked control systems with QoS based sampling. *IET Control Theory Applications.*, 1, 430–438.

Correll, K., Barendt, N., & Branicky, M. (2005). Design considerations for software only implementations of the IEEE 1588 precision time protocol. *Proc. Conference on IEEE 1588*, Switzerland.

DeepSpace Atomic Clock (DSAC). [Online]. [cited Sep 2014]. http://www.nasa.gov/mission_pages/tdm/clock/#.VBWbT_ldV1Y

Delsing, J., Eliasson, J., & Leijon, V. (2010). Latency and packet loss of an interferred 802.15.4 channel in an industrial environment. In *Proceedings - 4th International Conference on Sensor Technologies and Applications*, (pp. 33–38).

Ding, S. X., Zhang, P., Yin, S., & Ding, E. L. (2013). An integrated design framework of fault-tolerant wireless networked control systems for industrial automatic control applications. *IEEE Transactions on Industrial Informatics*, *9*, 462–471.

Douglas, B.P., (2009). Real-Time Agility: The Harmony/ESW Method for Real-Time and Embedded Systems Development, Addison-Wesley.

Eidson, J. C., & Lee, K. (2003). Sharing a common sense of time. *IEEE Instrumentation and Measurement Magazine*, *6*, 26–32.

Feng, D., & Wencai, D. (2009). A novel Smith predictor for wireless networked control systems with uncertainty delay. In *Proceedings - International Conference on Environmental Science and Information Application Technology*, (Vol. 3, pp. 552–555).

Flammini, A., and Ferrari, P. (2010). Clock Synchronization of Distributed, Real-Time, Industrial Data Acquisition Systems, Data Acquisition, Michele Vadursi (Ed.), ISBN: 978-953-307-193-0, InTech.

Flärdh, O., Johansson, K. H., & Johansson, M. (2005). A new feedback control mechanism for error correction in packet-switched networks. In *Proceedings of the 44th IEEE Conference on Decision and Control, and the European Control Conference, CDC-ECC '05* (Vol. 2005, pp. 488–493).

Gaderer, G., Holler, R., Sauter, T., & Muhr, H. (2004). Extending IEEE 1588 to fault tolerant clock synchronization. *Proceedings of IEEE International Workshop on Factory Communication Systems.*

Gamazo-Real, J. C., Vázquez-Sánchez, E., & Gómez-Gil, J. (2010). Position and speed control of brushless dc motors using sensorless techniques and application trends. J. *Sensors.*

Gascon, D. [Online]. (cited Sep 2014). Security in the IEEE802.15.4 MAC Frame http://www.sensor-networks.org

Gonzalez, A., Garcia, P., Albertos, P., Castillo, P., and Lozano, R. (2012). Robustness of a discrete-time predictor-based controller for time-varying measurement delay. *Control Engineering Practise.*, vol. 20, pp. 102–110.

Graham, S., & Kumar, P. R. (2003). The convergence of control, communications, and computation. *Lect. Notes Comput. Sci.*, *2275*, 458–475.

Greco, K. (2013). FAA to Allow Airlines to Expand Use of Personal Electronics. *Press Release*, Federal Aviation Administration. http://www.faa.gov/news/press_releases/news_story.cfm?newsId=15254

Grewal, M. S., & Andrews, A. P. (2010). Applications of Kalman filtering in aerospace 1960 to the present. *IEEE Control Systems Magazine*, *30*, 69–78.

Gulfstream demonstrates fly-by-wireless aircraft control system (dated 2008). [Online]. (cited Sep 2014). http://gulfstreamnews.com/news/gulfstream-demonstrates-fly-by-wireless-aircraft-control-system

Gungor, V.C., and Hancke, G.P. (2013). Industrial Wireless Sensors Networks. CRC Press, Taylor and Francis Group.

Gupta, R. A. (2010). Networked control system: overview and research trends. *IEEE Transactions on Industrial Electronics*, *57*, 2527–2535.

Halevi, Y., & Ray, A. (1988). Integrated Communication and Control Systems: Part I—Analysis. *Journal of Dynamic Systems, Measurement, and Control*, Vol. 110, p. 367.

Han, C., & Zhang, H. (2009). Optimal estimation for continuous-time Markovian jump linear systems with delayed measurements. *International Journal of Control, Automation and Systems*, *7*, 871–881.

Han, S., Zhu, X., Mok, A. K., Nixon, M., Blevins, T., & Chen, D. (2010). Control over WirelessHART network. In *IECON Proceedings (Industrial Electronics Conference)* (pp. 2114–2119).

Hedlund, M., Aronson, F. (2002). Evaluation of real-time operating systems for safety-critical systems. *Thesis Report,* School of Electronics and Embedded Systems, University of Jonkoping.

Heemels, W. P. M. H., Johansson, K. H., & Tabuada, P. (2012). An introduction to event-triggered and self-triggered control. In *Proceedings of the IEEE Conference on Decision and Control* (pp. 3270–3285).

Henriksson, D., Cervin, A., Andersson, M., & Årzén, K. E. (2006). Truetime: Simulation of networked computer control systems. In *Analysis and Design of Hybrid Systems 2006* (pp. 272–273).

Henriksson, E. (2009). Compensating for Unreliable Communication Links in Networked Control Systems, Licentiate Thesis, Stockholm, Sweden

Henzinger, T. A., Horowitz, B., & Kirsch, C. M. (2003). Giotto: A time-triggered language for embedded programming. *Proceedings of the IEEE*, *91*, 84–99.

Hernandez, A., Faria, J.F., Araújo, J., Park, P. G., Sandberg, H., & Johansson, K. H. (2011). Inverted Pendulum Control over an IEEE 802.15.4 Wireless Sensor and Actuator Network. In *European Conference on Wireless Sensor Networks.*

Hespanha, J. P., Naghshtabrizi, P., & Xu, Y. (2007). A Survey of Recent Results in Networked Control Systems. *Proceedings of the IEEE, 95*, 138–162.

Horjel, A., (2001). Bluetooth in Control. Master's thesis, Department of Automatic Control, Lund Institute of Technology, Sweden.

Horvath, P., Yampolskiy, M., Xue, Y., Koutsoukos, X. D., & Sztipanovits, J. (2012). An integrated system simulation approach for wireless networked control systems. In *2012 5th International Symposium on Resilient Control Systems* (pp. 118–123).

Hou, I. H., & Kumar, P. R. (2012). Real-time communication over unreliable wireless links: A theory and its applications. *IEEE Wireless Communications, 19*, 48–59.

IEEE 1588 Precision Time Protocol (PTP). IEEE Std 1588-2008, *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, (1 –269).

Irwin, G.W., Colandairaj J., Scanlon, W.G. (2006). An overview of wireless networks in control and monitoring. Springer. *Lecture Notes in Computer Science*. 4114, 1061-1072.

ISA-100. [Online]. (cited Sep 2014). http://www.isa100wci.org/

Junior, E. and Souza, M. (2010). Effects of Offset and Clock Drift on Clock Synchronization of NCS. *12th Brazilian Workshop on Real-Time and Embedded Systems*.

Kalman, R. E. (1960). A New Approach to Linear Filtering and Prediction Problems. *Transactions of the ASME-Journal of Basic Engineering, 82*, 35–45.

Kawka, P. A., & Alleyne, A. G. (2006). Stability and performance of packet-based feedback control over a Markov channel. *2006 American Control Conference*.

Khan, N. (2011). Linear Prediction Approaches to Compensation of Missing Measurements in Kalman Filtering. PhD Dissertation, Control and Instrumentation Research Group, University of Leicester, Leicester, UK.

Kim, W., Ji, K., & Ambike, A. (2006). Real-time operating environment for networked control systems. *IEEE Transactions on Automation Science and Engineering, 3*, 287–296.

Kline, P. (1997). Atomic clock augmentation for receivers using the global positioning system. PhD Thesis.

Knight, J. (2002). Safety Critical Systems: Challenges and Directions. In *International Conference on Software Engineering* (pp. 547–550).

Kopetz, H. (1993). Should responsive systems be event-triggered or time-triggered? *IEICE Transactions on Information and Systems, E76-D*, 1325.

Körber, H. J., Wattar, H., & Scholl, G. (2007). Modular wireless real-time sensor/actuator network for factory automation applications. *IEEE Transactions on Industrial Informatics, 3*, 111–118.

Kostadinovic, M et al. (2009). Problem of Packet loss in WirelessHART Network. *13th International Research/Expert Conference, TMT 2009,* Tunisia. (pp.16-21)

LaJoie, A. [Online]. (cited Sep 2014). Wireless Sensor Technology for Real-Time Applications. http://www.techbriefs.com/

Lau, R. & Fuhr, P. (2014). The Realities of Dealing with Wireless Mesh Networks. (Cited Sep 2014). [Online]. http://www.sensorsmag.com/networking-communications

Leborgne, Y., Santini, S., & Bontempi, G. (2007). Adaptive model selection for time series prediction in wireless sensor networks. *Signal Processing*, *87*, 3010–3020.

Lee, E et al. (Cited Sep 2014). [Online]. Cyber-Physical Systems – a Concept Map. http://cyberphysicalsystems.org/

Li, T et al. (2012). Stabilisation of wireless networked control systems with packet loss. IET Control Theory & Applications, 6, 2362–2366.

Lian, FL., Moyne, J., & Tilbury, D. (2001). Time delay modelling and sample time selection for networked control systems. In *Proceedings of ASME-DSC, International Mechanical Engineering Congress and Exposition*.

Lian, FL., Moyne, J., & Tilbury, D. (2002). Network design consideration for distributed control systems. *Control Systems Technology, IEEE Transactions on*, *10*, 297–307.

Lian, FL., Yook, J.K., Tilbury, D.M., Moyne, J. (2006). Network architecture and communication modules for guaranteeing acceptable control and communication performance for networked multi-agent systems, *IEEE Transactions on Industrial Informatics*, vol.2, no.1, pp.12-24.

Liu, J. (2014). A New Design of Clock Synchronization Algorithm. *Advances in Mechanical Engineering*. Hindawi Publishing Corporation, Article ID 958686.

Liu, X., & Goldsmith, A. (2004). Wireless network design for distributed control. In *Proceedings of the IEEE Conference on Decision and Control* (Vol. 3, pp. 2823–2829).

Liu, X., & Goldsmith, A. (2004). Wireless Medium Access Control in Networked Control Systems. *Proceedings of American Control Conference*, *4*, 3605–3610.

Liu, X., & Goldsmith, A. (2004). Kalman filtering with partial observation losses. In *Proceedings of the IEEE Conference on Decision and Control* (Vol. 4, pp. 4180–4186).

Liu, X., Ding, H., Lee, K., Sha, L., & Caccamo, M. (2006). Feedback Fault Tolerance of Real-Time Embedded Systems–Issues and Possible Solutions. *ACM SIGBED Review*, *3*, 23–28.

Lopez, J., Roman, R., & Alcaraz, C. (2009). Analysis of Security Threats , Requirements , Technologies and Standards in Wireless Sensor Networks. *Foundations of Security Analysis and Design V*, *5705*, 289–338.

Lorand, C., & Bauer, P. H. (2006). On synchronization errors in networked feedback systems. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *53*, 2306–2317.

Lu, X. (2014). Supervisory Control and Data Acquisition System Design for CO_2 Enhanced Oil Recovery. Technical Report, University of California, Berkeley.

Lu, X., & Guo, B. (2009). Kalman filtering for wireless networks systems with delayed-missing measurements. In *2009 Chinese Control and Decision Conference, CCDC 2009* (pp. 4682–4686).

Luan, X., Shi, P., & Liu, F. (2011). Stabilization of networked control systems with random delays. *IEEE Transactions on Industrial Electronics, 58*, 4323–4330.

Luck, R., & Ray, A. (1990). Delay Compensation in Integrated Communication and Control Systems: Part II -- Implementation and Verification. *1990 American Control Conference*.

Luo, J., Keusgen, W., Kortke, A., & Peter, M. (2008). A design concept for a 60 GHz wireless in-flight entertainment system. *In IEEE Vehicular Technology Conference*.

Lynch, J. P et al. (2008). Implementation of a closed-loop structural control system using wireless sensor networks. *Structural Control and Health Monitoring* 15(4): 518-539.

Marti, P et al. (2008). Clock Synchronization for Networked Control Systems Using Low-Cost Microcontrollers. *Research Report: ESAII-RR-08-02*, 2008.

Martins, E. C., & Jota, F. G. (2010). Design of networked control systems with explicit compensation for time-delay variations. *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews, 40*, 308–318.

McKernan,A. (2010). Co-design of Wireless Feedback Control. *PhD thesis*, Queen's University, Belfast.

McKernan, A. D., & Irwin, G. W. (2010). Event-based sampling for wireless network control systems with QoS. *American Control Conference (ACC), 2010*.

Messier-Bugatti, a global player in aircraft braking. (2006). White Paper. [Online]. (cited Sep 2014) http://www.safranmbd.com/IMG/pdf/pressfile2006en.pdf.

Micheli, M., Jordan, M.I. (2002). Random sampling of a continuous-time stochastic dynamical system. *In Proceedings of 15th International Symposium on the Mathematical Theory of Networks and Systems (MTNS)*. University of Notre Dame, South Bend, Indiana.

Mifdaoui, A., and Gayraud, T. (2012). Fly-By-Wireless for next generation aircraft: Challenges and potential solutions. *In 2012 IFIP Wireless Days*, pp. 1–8.

Mills, D. L. (1991). Internet time synchronization: the network time protocol. *IEEE Transactions on Communications, 39*.

Minghu, Z., Senzu, S., Jian, S., & Ting, Z. (2008). Simple clock synchronization for distributed real-time systems. In *Industrial Technology, 2008. ICIT 2008. IEEE International Conference on* (pp. 1–5).

Mitchell, R., & Chen, I.-R. (2014). A survey of intrusion detection in wireless network applications. *Computer Communications*, *42*, 1–23.

Mock, M., Frings, R., Nett, E., & Trikaliotis, S. (2000). Continuous clock synchronization in wireless real-time applications. *Proceedings 19th IEEE Symposium on Reliable Distributed Systems SRDS-2000*.

Mostofi, Y., & Murray, R. M. (2009). To drop or not to drop: Design principles for Kalman filtering over wireless fading channels. *IEEE Transactions on Automatic Control*, *54*, 376–381.

Moxa. [Online]. (cited Sep 2014). Zero Packet Loss in Wireless Mission-Critical and Safety-Critical Systems. Concurrent Dual-Radio Technology, http://www.moxa.com/Event/IW/2013/Zero/index.htm

MSP430x5xx and MSP430x6xx Family User's Guide. (2013). Texas Instruments, Literature Number: SLAU208M.

Naghshtabrizi, P., & Hespanha, J. P. (2011). Implementation considerations for wireless networked control systems. In *Wireless Networking Based Control* (pp. 1–27).

Naman, A. T., Abdulmuin, M. Z., & Arof, H. (2000). Implementation and performance evaluation of a wireless feedback loop for water level control. *TENCON Proceedings of Intelligent Systems and Technologies for the New Millennium*, *2*.

Natori, K., & Ohnishi, K. (2008). A design method of communication disturbance observer for time-delay compensation, taking the dynamic property of network disturbance into account. *IEEE Transactions on Industrial Electronics*, *55*, 2152–2168.

Neagoe, T., Cristea, V., & Banica, L. (2006). NTP versus PTP in computer networks clock synchronization. In *IEEE International Symposium on Industrial Electronics* (Vol. 1, pp. 317–322).

Nielsen, B. (2014). Time in distributed systems. Distributed and embedded systems research group, Aalborg University, Denmark.

Nilsson, J. (1998). Stochastic analysis and control of real-time systems with random time delays. *Automatica*, *34*, 57–64.

Ofcom. Mobile phone jammers and cellular enhancers. [Online]. (cited Sep 2014) http://stakeholders.ofcom.org.uk/enforcement/spectrum-enforcement/jammers/

Oh, S., & Sastry, S. (2006). Distributed Networked Control System with Lossy Links: State Estimation and Stabilizing Communication Control. *Proceedings of the 45th IEEE Conference on Decision and Control*.

Ong, M., & Thompson, H. A. (2011). Challenges for wireless sensing in complex engineering applications. *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, 2106–2111.

Ong, M., Thompson, H.A. (2013). Hybrid Wireless RF Controller Area Network (CAN) for Wireless Monitoring and Control with Energy-efficient Self-Powered Sensor Systems. THHINK Wireless Technologies Ltd, Sheffield, UK.

Pacner, J., Ryavy, O., Veda, M. (2013). On the Evaluation of Clock Synchronization Methods for Networked Control Systems. *Eastern European Regional Conference on Engineering of Computer Based Systems (EERC- ECBS)*, pp.161-162, 29-30.

Pajic, M., Sundaram, S., Pappas, G. J., & Mangharam, R. (2011). The wireless control network: A new approach for control over networks. *IEEE Transactions on Automatic Control*, *56*, 2305–2318.

Pajic, M., Chernoguzov, A., & Mangharam, R. (2012). Robust architectures for embedded wireless network control and actuation. *ACM Transactions on Embedded Computing Systems*, *11*, 1–24.

Park, P., Araujo, J., & Johansson, K. H. (2011). Wireless networked control system co-design. *2011 International Conference on Networking, Sensing and Control*, 486–491.

Petersen, S., & Carlsen, S. (2009). Performance evaluation of WirelessHART for factory automation. In *2009 IEEE Conference on Emerging Technologies and Factory Automation*.

Petersen, S., & Carlsen, S. (2011). WirelessHART versus ISA100.11a: The format war hits the factory floor. *IEEE Industrial Electronics Magazine*, *5*, 23–34.

Ploplys, N. J., & Alleyne, A. G. (2003). UDP network communications for distributed wireless control. Proceedings of the 2003 American Control Conference, 4.

Ploplys, N. J., Kawka, P. A., & Alleyne, A. G. (2004). Closed-loop control over wireless networks. *IEEE Control Systems Magazine*, *24*, 58–71.

Polavarapu, S. (2004). The Linear Kalman Filter. *Atmospheric Data Assimilation*. The University of Toronto, Canada.

Poor, R., and Hodges, B. (2004). Reliable Wireless Networks for Industrial Applications. Ember Corporation, White paper.

Preindl, M., & Schaltz, E. (2011). Sensorless model predictive direct current control using novel second-order PLL observer for PMSM drive systems. *IEEE Transactions on Industrial Electronics*, *58*, 4087–4095.

Ralph, K. (2012). Standardization of CAN networks for airborne use through ARINC 825. Airbus Operations GmbH, iCC, Bremen, Germany.

Ramamurthy, H et al. (2007). Wireless Industrial Monitoring and Control Using a Smart Sensor Platform. *Sensors Journal*, IEEE, 7, 611–618.

Ramanathan, P., Shin, K. G., & Butler, R. W. (1990). Fault-tolerant clock synchronization in distributed systems. *Computer*, 23, 33–42.

Raouf, A. Minimize Frequency Drift in Crystals. [Online]. [cited Sep 2014]. http://electronicdesign.com/analog/minimize-frequency-drift-crystals

Raza, S., Slabbert, A., Voigt, T., & Landernäs, K. (2009). Security considerations for the wirelessHART protocol. *In IEEE Conference on Emerging Technologies and Factory Automation (ETFA'09).*

Rehbinder, H., & Hu, X. (2004). Drift-free attitude estimation for accelerated rigid bodies. *Automatica*, *40*, 653–659.

Rhee, I.-K., Lee, J., Kim, J., Serpedin, E., & Wu, Y.-C. (2009). Clock synchronization in wireless sensor networks: an overview. *Sensors* (Basel, Switzerland), 9, 56–85.

Ristaino, A. (2014). ISA100.11a Approved as IEC 62734. [Online]. http://www.isa100wci.org/en-US/Documents/Presentations/2014-Oct-15-ISA100-Wireless-IEC62734-Approval.aspx

Road, C.N. (2014). Testing and troubleshooting of WiFi 802.11 embedded design. RF 2014 Technology Days. Leiden.

Rolls-Royce Gas turbine programmes, [Online]. [cited Sep 2014], Sustainable and Green Engine (SAGE) ITD, http://www.rolls-royce.com/about/our-technology/research/research-programmes/sustainable-and-green-engine-sage-itd.aspx

Saifullah, A et al. (2010). Real-time scheduling for WirelessHART networks. *In Proceedings - Real-Time Systems Symposium*, (pp. 150–159).

Sastry, N., & Wagner, D. (2004). Security considerations for IEEE 802.15.4 networks. In *Proceedings of the 2004 ACM workshop on Wireless security - WiSe '04* (p. 32).

Schenato, L., Sinopoli, B., Franceschetti, M., Poolla, K., & Sastry, S. S. (2007). Foundations of control and estimation over lossy networks. *Proceedings of the IEEE*, *95*, 163–187.

Schenato, L. (2009). To zero or to hold control inputs with lossy links? *IEEE Transactions on Automatic Control*, *54*, 1093–1099.

Sen, S.K. (2014). Fieldbus and Networking in Process Automation. CRC Press.

Seth, S., Lynch, J. P., & Tilbury, D. M. (2005). Wirelessly networked distributed controllers for real-time control of civil structures. *Proceedings of the 2005, American Control Conference, 2005.*

Seuret, A., K.H. Johansson. (2012). Networked control under time-synchronization errors. Time Delay Systems: Methods, Applications and New Trends, Sipahi, R et al, 369-383.

Short, M., Abrar, U., French, I., & Abugchem, F. (2011). Real-time implementation of a burst error compensator for wireless control systems. *The 17th International Conference on Automation and Computing*, 104–109.

Sichitiu, M. L., & Veerarittiphan, C. (2003). Simple, accurate time synchronization for wireless sensor networks. *In IEEE Wireless Communications and Networking*. (Vol. 2, pp. 1266–1273).

Simon, D. (2006). Optimal State Estimation: Kalman, H∞, and Nonlinear approaches. John Wiley & Sons.

SimpliciTI, Low-power RF Protocol, Texas Instruments, [Online]. [cited Sep 2014]. http://www.ti.com/lit/ml/swru130b/swru130b.pdf

Sinopoli, B., Schenato, L., Franceschetti, M., Poolla, K., Jordan, M.I., and Sastry, S.S. (2003). Kalman Filtering with Intermittent Observations. *Proceedings of 42nd IEEE Conference on Decision and Control*, pp. 701-708.

Smith, O.J.M. (1957). Closer control of loops with dead time. *Chem. Eng. Progress*, vol.53, no.5, pp. 217–219.

Solis, R., Borkar, V.S., Kumar, P.R. (2006). A New Distributed Time Synchronization Protocol for Multihop Wireless Networks. *In Proceedings of 45th IEEE Conference on Decision and Control*.

Song, J et al. (2008). WirelessHART: Applying wireless technology in real-time industrial process control. *In Proceedings of the IEEE Real-Time and Embedded Technology and Applications Symposium, RTAS,* (pp. 377–386).

Song, J., Han, S., Mok, A. K., Chen, D., Lucas, M., Nixon, M., & Pratt, W. (2008). WirelessHART: Applying wireless technology in real-time industrial process control. In *Proceedings of the IEEE Real-Time and Embedded Technology and Applications Symposium, RTAS* (pp. 377–386).

Sundararaman, B., Buy, U., Kshemkalyani, A. D., Street, S. M. (2005). Clock Synchronization for Wireless Sensor Networks : A Survey. *Ad Hoc Networks*, 3, 281–323.

Suri, A., Baillieul, J., Raghunathan D.V. (2005). Control using feedback over wireless Ethernet and Bluetooth. Handbook of Networked and Embedded Control Systems, *Control Engineering*, Springer, (pp. 677-697).

Tabbara,M., Ne,D., Teel,A.R. (2007). Stability of wireless and wireline networked control systems. *IEEE Transactions on Automatic Control*, 52, 1615–1630.

Tahoun, A. H. (2011). Output-feedback MRAC of networked systems with network-induced delays and packet dropout. *In Proceedings of International Conference on Computer Engineering and Systems* (pp. 91–96).

Tas, N.C., Mesrob, V., Genc, Y. (2011). Wireless sensor networks in the control loop: Delay-sensitive networks. *Consumer Communications and Networking Conference (CCNC)*, pp. 575-579.

Tasoulis, D. K., Adams, N. M., & Hand, D. J. (2007). Should delayed measurements always be incorporated in filtering? In *2007 15th International Conference on Digital Signal Processing, DSP 2007* (pp. 264–267).

Taylor, J. H., & Ibrahim, H. M. S. (2010). A new, practical approach to maintaining an efficient yet acceptably-performing wireless networked control system. In *2010 International Conference on System Science and Engineering*, (pp. 269–274).

Terejanu A.G. [Online]. (cited Sep 2014). Discrete Kalman Filter, University of Buffalo. http://www.cse.sc.edu/~terejanu/files/tutorialKF.pdf

Thompson, H. A. (2004). Wireless and Internet communications technologies for monitoring and control. *Control Engineering Practice*, *12*, 781–791.

Thompson, H. A. (2009). Wireless sensor research at the Rolls-Royce Control and Systems University Technology Centre. In *Proceedings of the 2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2009* (pp. 571–576).

Tipsuwan, Y., & Chow, M. Y. (2004). Gain scheduler middleware: A methodology to enable existing controllers for networked control and teleoperation - Part II: Teleoperation. *IEEE Transactions on Industrial Electronics*, *51*, 1228–1237.

Uchimura, Y. (2008). Wireless network based identification and control with variable time delay. *10th IEEE International Workshop on Advanced Motion Control*.

Uchimura, Y., & Shimano, H. (2009). Network based control with compensation of time-varying delay and modeling error. In *IECON Proceedings (Industrial Electronics Conference)* (pp. 3013–3018).

Ulusoy, A., Gurbuz, O., & Onat, A. (2011). Wireless model-based predictive networked control system over cooperative wireless network. *IEEE Transactions on Industrial Informatics*, *7*, 41–51.

Vardhan, S., & Kumar, R. (2011). An implementation of time-delay compensation scheme for networked control systems using MATLAB/simulink. In *Proceedings - 2011 International Conference on Computational Intelligence and Communication Systems*, (pp. 149–153).

Venugopalan, V. (2010). Modelling and design of Electric Braking System for Civilian Aircraft," *Master's Thesis*, Electronic and Electrical Engineering Dept., The University of Sheffield, Sheffield, UK.

Venugopalan, V., Relan R., Thompson H.A., Ong, M., Fleming, P.J. (2014). Sensorless Supervisory Wireless Control: Aircraft Braking System Case Study. *Journal of Unmanned Systems Technology (JUST)*. Vol.2, Issue 2.

Venugopalan, V., Relan R., Thompson H.A., Ong, M., Fleming, P.J. (2015). A Sampling Interval based Clock Synchronisation approach for Wireless Closed-loop Control. In proceedings of *IEEE Indian Control Conference*, Chennai, India, pp.316 - 321.

Verhamme, I. (2011). Wireless Control for Process Automation using ISA100.11a. *Industrial Ethernet Book*, Issue 64/30.

Wagner, R.S. (2010). Standard-Based Wireless Sensor Networking Protocols for Spaceflight Applications. NASA Johnson Space Centre, Texas.

Wang, F., Liu, D. (2008). Networked Control Systems – Theory and Applications. Springer.

Wang, X., and Lemmon, M. D. (2011). Event-triggering in distributed networked control systems. *IEEE Transactions on Automatic Control*, 56, 586–601.

Weibel, H. (2005). High precision clock synchronization according to IEEE 1588 implementation and performance issues. *The Embedded World 2005 Conference*.

Welch, G., and Bishop, G. (2006). An Introduction to the Kalman filter. [Online]. (cited Sep 2014). http://www.cs.unc.edu/~welch/media/pdf/kalman_intro.pdf

Werb, J., Amidi, S. (2012). Control over Wireless: Current Applications and Future Opportunities. ISA Automation week 2012.

WICAS (Wireless Interconnectivity and Control of Active Systems). (2011). [Online]. http://www.sheffield.ac.uk/systemsutc/projects/wicas

Willig, A., Matheus, K., & Wolisz, A. (2005). Wireless Technology in Industrial Networks. *Proceedings of the IEEE, 93*.

Willig, A. (2008). Recent and emerging topics in wireless industrial communications: A selection. *IEEE Transactions on Industrial Informatics, 4*, 102–122.

Wi-Fi Alliance. [Online]. (cited Sep 2014). http://www.wi-fi.org/

Wireless Avionics Intra-Communications (WAIC). (2012). Presentation for ICAO Regional Meeting, Lima, Peru. [Online]. (cited Sep 2014) http://www.icao.int/SAM/Documents/ITU-WRC-15

Wireless Control in the Industries: Blasphemy or Common Sense. (2010). [Online] http://www.automationworld.com/

WirelessHART. [Online]. (cited Sep 2014). http://en.hartcomm.org/

WiTNESS (Wireless Technologies for Novel Enhancement of Systems and Structures Serviceability). (2009). [Online]. (cited Sep 2014). http://www.geaviation.com/press/systems/systems_20090528.html

Wittenmark, B., Nilsson, J., & Torngren, M. (1995). Timing problems in real-time control systems. *Proceedings of 1995 American Control Conference - ACC'95, 3*.

Wu, J., & Chen, T. (2007). Design of networked control systems with packet dropouts. *IEEE Transactions on Automatic Control, 52*, 1314–1319.

Wu, F.-J., Kao, Y.-F., & Tseng, Y.-C. (2011). From wireless sensor networks towards cyber physical systems. *Pervasive and Mobile Computing*, Vol 7.4, 397-413

Xia, F et al. (2011). Cyber-physical control over wireless sensor and actuator networks with packet loss. Springer. *In Wireless Networking Based Control* (pp. 85–102).

Xia, F., and Zhao, W. (2007). Flexible Time-Triggered Sampling in Smart Sensor-Based Wireless Control Systems. *In Sensors Journal*, vol.7, no.11, pp. 2548-2564.

Xue, W., and Guo, Y.Q. (2010). Application of Kalman Filters for the Fault Diagnoses of Aircraft Engine. *Intech open*.

Xunqi,Yu., Modestino, J.W., Xusheng T. (2005). The accuracy of Gilbert models in predicting packet-loss statistics for a single-multiplexer network model. *In Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies*. vol.4, (pp.2602-2612)

Yang, T.C. (2006). Networked control system: a brief survey. *Control Theory and Applications, IEE Proceedings, 153*, 403–412.

Yedavalli, R.K., Belapurkar, R.K. (2011). Application of wireless sensor networks to aircraft control and health management systems. *Journal of Control Theory & Applications*, Vol. 9(1), 28-33.

Yoo, J., Zhou, Y., Lee, S., Joo, M., Park, J. (2012). An Adaptive Delay Compensation Technique for Wireless Sensor and Actuator Network. *International Journal of Smart Home*. Vol. 6, Issue 4, pp.187.

Zach, S. (2009). 6LowPAN: The Wireless Embedded Internet. *Wiley Series in Communications networking & Distributed Systems*. John Wiley & Sons Ltd.

Zaidan, M. A., Mills, A. R., & Harrison, R. F. (2013). Bayesian framework for aerospace gas turbine engine prognostics. In Proceedings of IEEE Aerospace Conference.

Zhang, W.A., and Yu, L. (2007). Output Feedback Stabilization of Networked Control Systems with Packet Dropouts. *IEEE Transactions on Automatic Control*, Vol.52, pp.1705-1710.

Zhang, D., Wang, X. (2012). Static output feedback control of networked control systems with packet dropout. International Journal of Systems Science, Vol.43, 4, 2012.

Zhong, T et al. (2010). Real-time communication in WIA-PA industrial wireless networks. *3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2*, (pp.600-605).

ZigBee Alliance. [Online]. (cited Sep 2014). http://www.zigbee.org/

60 GHz Technology Overview. [Online]. (cited Sep 2014). http://www.bridgewave.com/products/tech_overview.cfm