Distributed Detection and Estimation in Wireless Sensor Networks:

Resource Allocation, Fusion Rules, and Network Security

UNIVERSITY OF LEEDS

Edmond Nurellari

Submitted in accordance with the requirements for the degree of
Doctor of Philosophy

The University of Leeds
School of Electronic and Electrical Engineering

February 2017

Declaration

The candidate confirms that the work submitted is his/her own, except where work which has formed part of jointly authored publications has been included. The contribution of the candidate and the other authors to this work has been explicitly indicated below. The candidate confirms that appropriate credit has been given within the thesis where reference has been made to the work of others. It is to assert that the candidate has contributed solely to the technical part of the joint publication under the guidance of his academic supervisors. Detailed breakdown of the publications is presented in the first chapter of this thesis.

Dedicated to

my family for their immense love and support.

Acknowledgements

Looking back at the years I spent at University of Leeds, I would like to express my deepest gratitude to my supervisors Dr. Des McLernon and Professor Mounir Ghogho. Without their support and guidance this thesis would have not been possible. It was their enthusiastic encouragement, professionalism, and their appreciation that led me to further successes in my academic career.

Many thanks to all the academic staff and personnel of the School of Electronic & Electrical Engineering for providing their help and support during my course of study and stay at the University of Leeds.

I am indebted to all of my friends, colleagues, and the academic staffs with whom I have been working with, for their presence and help during my stay at the University of Leeds. They have always motivated and encouraged me.

Lastly, I would like to thank my family. My parents taught me those most valuable "theorems of life" which I could not find them in any book or in any paper. Their love and support has been with me every moment of my life. I am deeply indebted to my wife for her sacrifice and being with me in both the tough and the good times. I also thank my brothers for their support and being close to the family while I have been away from home. I also do not forget my grandmother for caring so much for me while I was a baby. This thesis is dedicated to my family and to her as an inadequate but sincere expression of appreciation and love.

Abstract

This thesis addresses the problem of detection of an unknown binary event. In particular, we consider centralized detection, distributed detection, and network security in wireless sensor networks (WSNs). The communication links among SNs are subject to limited SN transmit power, limited bandwidth (BW), and are modeled as orthogonal channels with path loss, flat fading and additive white Gaussian noise (AWGN). We propose algorithms for resource allocations, fusion rules, and network security.

In the first part of this thesis, we consider the centralized detection and calculate the optimal transmit power allocation and the optimal number of quantization bits for each SN. The resource allocation is performed at the fusion center (FC) and it is referred as a *centralized* approach. We also propose a novel fully *distributed* algorithm to address this resource allocation problem. What makes this scheme attractive is that the SNs share with their neighbors just their individual transmit power at the current states. Finally, the optimal soft fusion rule at the FC is derived. But as this rule requires $a-priori$ knowledge that is difficult to attain in practice, suboptimal fusion rules are proposed that are realizable in practice.

The second part considers a fully distributed detection framework and we propose a two-step distributed quantized fusion rule algorithm where in the first step the SNs collaborate with their neighbors through error-free, orthogonal channels. In the second step, local 1-bit decisions generated in the first step are shared among neighbors to yield a consensus. A binary hypothesis testing is performed at any arbitrary SN to optimally declare the global decision. Simulations show that our proposed quantized two-step distributed detection algorithm approaches the performance of the unquantized centralized (with a FC) detector and its power consumption is shown

to be 50% less than the existing (unquantized) conventional algorithm.

Finally, we analyze the detection performance of $under-attack$ WSNs and derive attacking and defense strategies from both the Attacker and the FC perspective. We re-cast the problem as a minimax game between the FC and Attacker and show that the Nash Equilibrium (NE) exists. We also propose a new non-complex and efficient reputation-based scheme to identify these compromised SNs. Based on this reputation metric, we propose a novel FC weight computation strategy ensuring that the weights for the identified compromised SNs are likely to be decreased. In this way, the FC decides how much a SN should contribute to its final decision. We show that this strategy outperforms the existing schemes.

Contents

List of Figures

List of Tables

List of Acronyms and Symbols

Acronyms

AF	Attack free
AWGN	Additive white Gaussian noise
CSI	Channel state information
CSC	Compromised SNs (only) collaboration
ED	Energy detector
FC	Fusion center
GT	Game theory
HCSC	Honest and compromised SNs collaboration
i.i.d.	Independent identically distributed
IoT	Internet of things
K.K.T	Karush-Kuhn-Tucker
LMS	Least mean squares
LRT	Likelihood ratio test
LLRT	Log likelihood ratio test
MAC	Medium access control
MDC	Modified deflection coefficient
MFD	Match filter detector
MIMO	Mean squared error
MSE	Multiple input multiple output
NE	Nash equilibrium
OAFBB	Optimum Attack FC based belief
PAC	Parallel access channel

PDF	Probability density function
r.v.	Random variable
RHS	Right hand side
ROC	Receiver Operating Characteristic
RMSE	Root mean square error
SNR	Signal to noise ratio
SN	Sensor node
TSF	Test statistic falsification
WSNs	Wireless sensor networks
WAFBB	Weak Attack FC based belief

Mathematical Symbols

x or X, $\boldsymbol{x}$ or $\boldsymbol{X}$, $\mathbf{X}$	A scalar, a vector, and a matrix
$\mathbb{R}$	Set of real numbers
$\mathcal{H}_0$	Target absent hypothesis
$\mathcal{H}_1$	Target present hypothesis
M	Number of SNs
N	Number of samples
T_i	The test statistic at the i^{th} SN
P_d	Centralized global probability of detection
P_{fa}	Centralized global probability of false alarm
P_d^g	Distributed global probability of detection
P_{fa}^g	Distributed global probability of false alarm
Λ_f	FC detection threshold
K	Time window length
r_i	Reputation metric
$\mathbb{E}\{.\}$	Expectation operator
$\mathrm{Var}\{.\}$	Variance operator
$\mathrm{pr}(.)$	Probability of an event
$\mathbb{C}_{ij}$	Cost associated to each of the possible action
e_{ij}	The ij entry of matrix $\mathcal{E}$
Δ_i	The i^{th} SN neighbor set
$\lvert\Delta_i\rvert$	The number of neighbors for the i^{th} SN
P_T	The total power consumption
K_T	The total number of iterations
K_1	The first step number of iterations
K_2	The second step number of iterations
Υ	The link SNR threshold
d_{ij}	The physical distance between SN i and SN j
$\bigwedge$	Denotes the logical "*and*" operation
$\bigvee$	Denotes the logical "*or*" operation
γ	The path loss coefficient

$\mathcal{G}$	A graph
$\mathcal{V}$	The set of SNs
$\mathcal{E}$	The set of edges
$\mathbf{E}$	The adjacency matrix
$\mathbf{D}$	The degree matrix
$\mathbf{L}$	The Laplacian matrix
$\lambda_i(\mathbf{X})$	The i^{th} eigenvalue of $\mathbf{X}$
$\lambda_M(\mathbf{X})$	The smallest eigenvalue of $\mathbf{X}$ in magnitude
$\lambda_1(\mathbf{X})$	The largest eigenvalue of $\mathbf{X}$ in magnitude
$\mathcal{X}$	A finite nonempty set, the set of Player I
$\mathcal{Y}$	A finite nonempty set, the set of Player II
$\mathcal{X} \times \mathcal{Y}$	The product space
$x \in \mathcal{X}$	x belongs to set $\mathcal{X}$
$\mathcal{X} \subseteq \mathcal{Y}$	$\mathcal{X}$ is a subset of $\mathcal{Y}$
lim	The limit
max	The maximum
min	The minimum
$\text{diag}(\boldsymbol{x})$	A diagonal matrix whose entries are the element of vector $\boldsymbol{x}$
$\text{tr}(\mathbf{X})$	The trace of a matrix $\mathbf{X}$
$\mathbf{X}^T$	The transpose of matrix $\mathbf{X}$
$\mathbf{X}^{-1}$	The inverse of a square matrix $\mathbf{X}$
$\boldsymbol{x}^T$	The transpose of vector $\boldsymbol{x}$
P_t	Transmit power budget
h_i	Fading channel gains
σ_i^2	Sensing measurements noise variance at the i^{th} SN
ζ_i	Communication channel noise variance at the i^{th} SN
L_i	The i^{th} centralized SN quantization bits
q_i	The i^{th} distributed SN quantization bits
p_i	The i^{th} SN transmit power
$\sigma_{v_i}^2$	Quantization noise variance at the i^{th} SN
σ_e^2	The quantization error variance

$(\mathbf{a})_i$	The i^{th} element of vector $\mathbf{a}$
$(\mathbf{A})_{ij}$	The (i, j) element of matrix $\mathbf{A}$
$P_{fa}^{i}[k]$	The false alarm probability for the i^{th} SN at the k^{th} iteration
$P_{d}^{i}[k]$	The detection probability for the i^{th} SN at the k^{th} iteration
β	The fraction of compromised SNs
C_i	The attacker parameter at the i^{th} SN
P_{C}^{flip}	The attacker flipping probability
$\mathbf{1}$	The all-ones vector
$\mathbf{I}$	The identity matrix
$\boldsymbol{x} \bigodot \boldsymbol{y}$	The element-wise multiplication of vector $\boldsymbol{x}$ and $\boldsymbol{y}$
$\boldsymbol{x}_i$	The i^{th} column vector of matrix $\mathbf{X}$
$\mathbf{X}^c$	The logical complement of matrix $\mathbf{X}$
Λ	The local honest SN detection threshold
Λ^C	The local compromised SN detection threshold
I_i	The i^{th} honest SN's local decision
I_i^C	The i^{th} compromised SN's local decision
p_{fa}^{i}	The i^{th} honest SN local probability of false alarm
p_{d}^{i}	The i^{th} honest SN local probability of detection
$p_{fa}^{i,C}$	The i^{th} compromised SN local probability of false alarm
$p_{d}^{i,C}$	The i^{th} compromised SN local probability of detection
$P_{d}^{i,true}$	The probability that the i^{th} compromised SN has been truly detected
$P_{d}^{i,false}$	The probability that the i^{th} compromised SN has been falsely detected
δ	Reliability detection threshold
μ	The weight penalty
$\triangleq$	Defined as

Chapter 1

Introduction

IN THIS CHAPTER

The overview of the motivation behind the work presented in this thesis is described. The design challenges of a bandwidth-constrained/energy-constrained wireless sensor networks are stated. The consensus algorithm and the related-work literature are reviewed. Finally, the thesis outline and the contributions are presented.

1.1 Motivation

Wireless sensor networks (WSNs) spatially deployed over a field (see Fig. 1.1) can be designed to collect information and monitor many phenomena of interest. Because of their relatively low cost and robustness to sensor node (SN) failures they are receiving significant attention. WSNs are defined as one of the most important emerging technologies that together with Internet of Things (IoT) [1] will revolutionize the world. In fact, one of the most important component of the IoT paradigm is the WSN. They are playing an important role in several daily application scenarios such as health-care monitoring, home applications, smart farming, environment monitoring, and military [2–4]. Generally, the sensing process is orientated towards estimating various parameters of interest which can be employed to arrive at a cer-

tain decision. This decision can then be relayed in a pre-specified manner or can be employed for on-field actuation. We note that the reliable and continued operation of a WSN over many years is often desirable.

There are different WSNs architectures depending on how the SNs take decision and exchange information with other SNs in the network or with the fusion center (FC) (see Fig. 1.1). We briefly mention here three of the different architectures that we will be using in this thesis; 1) The *Centralized Architecture* (we consider this in Chapter 3, Chapter 4, and Chapter 6), where there are mainly spatially distributed SNs that report to the FC. There is no inter-sensors collaboration. 2) The *Distributed Architecture* (we consider this in Chapter 5), where there is no FC and the SNs collaborate with each other in achieving the common goal. 3) The *Hybrid Architecture* (we consider this in Chapter 3), where there is a FC and there is also inter-sensor nodes collaboration.

The SNs, depending on how are deployed and used, can vary from being extremely tiny devices [5] to relatively large embedded platforms [6]. In general, a SN consists of limited signal processing capabilities, sensing device(s), a transceiver, limited memory capacity, and on-board power [2]. These devices have wireless communications capability that makes them suitable in a variety of applications as described above. However, there are a numerous challenging problems in designing WSNs that we describe next in Section 1.2.

1.2 Design Challenges in WSNs

While there are several design issues and challenges in WSNs, here we briefly discuss the three most important issues that are related to bandwidth/energy-constrained WSNs.

1. **Low Power Hardware**: Clearly, the biggest design constraint in WSNs still remains the power consumption. Even-though the SNs are being designed using low-power micro controllers, their power dissipation is still orders of magnitude too high. For a survey on hardware systems for WSNs, we refer the reader to [7] and see references therein.

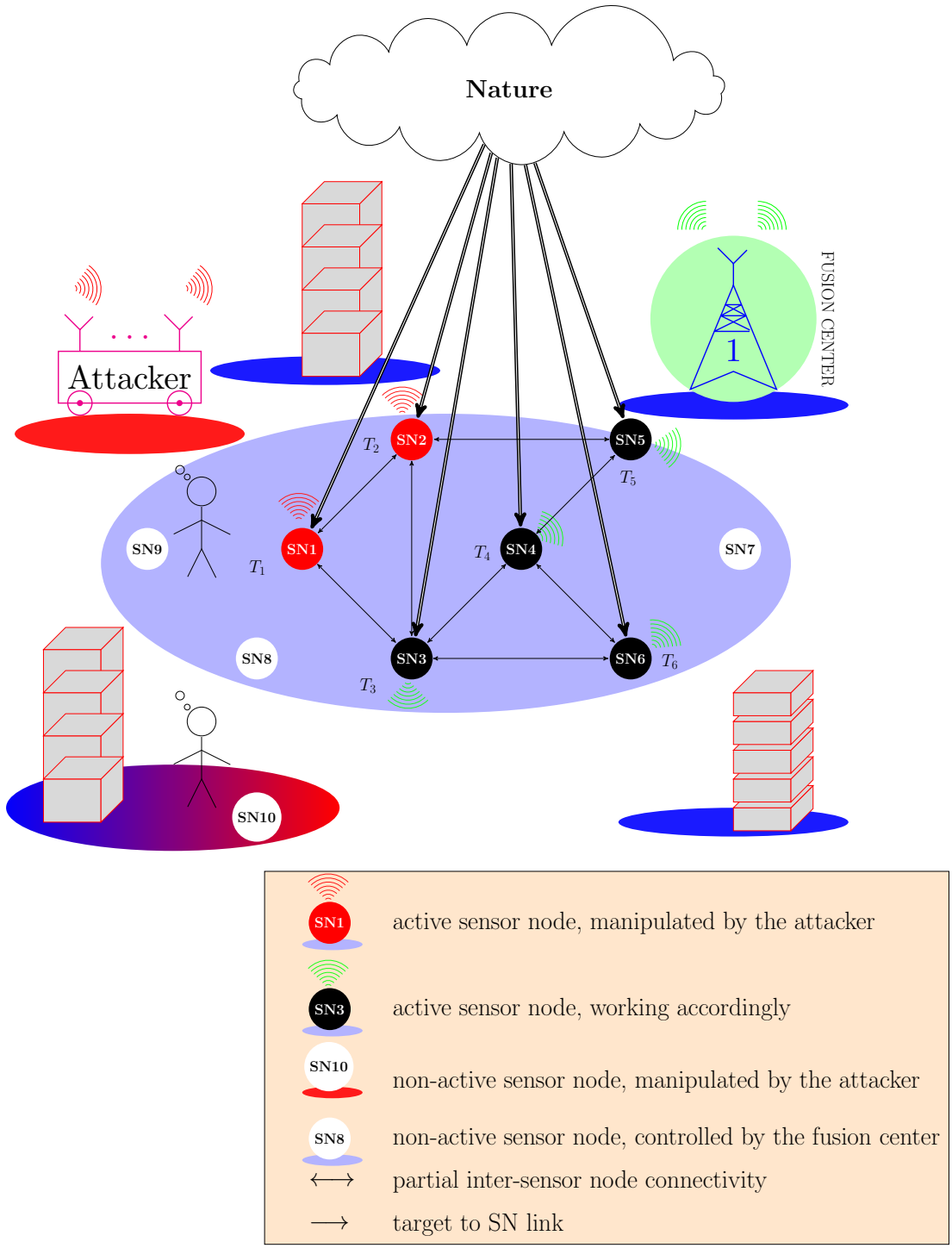

Figure 1.1: Schematic for a distributed communication architecture among peripheral SNs. Each SN generates a test statistic (T_i) by observing the target (thick lines). The SNs have partial connectivity (thin lines) among themselves (i.e., not a complete graph), but only over an energy-constrained/bandwidth-constrained network.

2. **Resource Constraints**: Because the SNs are battery operated devices with limited on-board energy, both the system lifetime and communication bandwidth (BW) are restricted. While designing the algorithms to be used by the SNs, both the signal processing and communication should be carefully designed to consume minimal energy in order to extend the lifetime and improve the overall reliability of the WSN. In this thesis, we consider several distributed detection and estimation problems with SNs reporting their local quantized observations to the FC or/and to their neighbors.

3. **Network Security**: Being geographically dispersed to cover large areas, the SNs are usually unattended and this makes them vulnerable to different types of attacks. The overall detection and estimation performance strongly depends on the reliability of these SNs in the network. While fusing the data received by the spatially deployed SNs allows the FC to make a reliable decision, it is possible that one or more SNs (compromised by an attacker) deliberately falsify their local observations to degrade the overall FC detection performance. While there are many types of security threats, in this thesis we focus on a single type of attack, which is the test statistic falsification (TSF) attack part of the Byzantine attacks family originally proposed by [8] and later widely used in the context of distributed detection (e.g., [9–11]). For further details on network security we refer the reader to [12] and references therein.

For other design issues such as SN localization, medium access control (MAC) protocols, time synchronization, hardware design and routing protocols in an energy constrained WSN, we refer the reader to [2].

1.3 Distributed Consensus Algorithm

In Chapter 3, we propose a fully distributed consensus-based algorithm that optimally allocates the SN to FC transmit power by using only local observations. Then, in Chapter 5, we develop and propose fully distributed quantized fusion rules (i.e., without a FC) via a consensus algorithm for distributed detection. Hence, herein we introduce the consensus algorithm.

Consensus algorithms are iterative low-complexity algorithms where multiple spatially distributed SNs across a network communicate with each other to agree on some relevant parameters. Upon an agreed consensus value, each SN in the network can use this global information to perform useful actions such as detecting or performing in-field actuation without necessary reporting their local observations to the FC. The simplest form of consensus algorithm is the average linear consensus algorithm [13] that converges to the average of initial states.

Investigated earlier by Tsitsiklis [14, 15] in the context of team decision problem with a group of agents, consensus algorithm under infinite energy-bandwidth WSNs has received a tremendous attention (see [16–19] and reference therein). But as the SNs are battery operated devices, these assumptions are not feasible in the contexts of WSNs. Recently, several publication considered practical WSNs that are restricted under limited power and bandwidth [20–23]. Consensus in the context of data fusion problems is also considered in [24–27]. However, in most of these papers, the proposed approaches either perform poorly at low bit rate and/or have high computational complexity. Therefore, the low complexity consensus-based algorithms designed under strict resource constraints of power and bandwidth are highly desirable.

1.4 Literature Overview

The *centralized solution* where noisy observations collected from spatially distributed local SNs are sent (inter-sensor collaboration is not considered) to a global FC for a final decision is considered in [28–37]. In the context of SN transmit power estimation, the effect of $inter-sensor\ collaboration$ was investigated in [38]. There are some recent publications [39, 40] (in the context of estimation) that considered the effect of $inter-sensor\ collaboration$ on the estimation performance. After the collaboration stage, the SNs (which in general can be a subset of all SNs) report to a FC where the final decision is made. Reference [39] proposes an $efficient$ collaboration strategy in a distributed fashion (as opposed to [41] where this optimal collaboration strategy is computed at a FC) by means of using only local SNs

observations.

These two *hybrid approaches* [36, 38] (a SN collaboration stage followed by reporting to a FC) and like the first approach (no collaboration stage and every SN reports directly to a FC), rely on the integrity of the FC. Now the limitation of the centralized approach is both the requirement of the FC to process a large amount of data (i.e., possible bottleneck) and the possible failure of the FC. Furthermore, collecting information at the FC lacks scalability, and may require large amounts of energy and communication resources [42].

The *fully distributed strategy* (i.e., without a FC) has been considered (e.g., in [43–56]) where the SNs exchange local information iteratively among their neighbors and are capable of reaching a global optimum decision. The authors of [43, 44] adopt the diffusion-based protocol and propose a new diffusion LMS algorithm while the authors of [45] design a bio-inspired algorithm for monitoring human activity in living conditions. References [18, 46] employ the iterative distributed consensus algorithm [19] for distributed inference. But these approaches consider ideal exchange of information among the SNs, and this assumption is unrealistic in the context of WSNs as discussed previously. Furthermore, practical WSN scenarios suffer from channel impairments such as fading and attenuation. Recently, to address the problem of consensus algorithms with quantized communications, a number of different approaches have been proposed, see [20–22, 52].

The framework of centralized detection under $attack - free$ WSNs has been extensively studied in [30, 34–36, 52, 57–65] to name but just a few references. While [32, 52, 58–60] consider centralized detection by assuming WSNs with unlimited bandwidth/resources, the latter assumption was relaxed in [30, 31, 34–36] by considering centralized detection over bandwidth-constrained/energy-constrained WSNs. But these approaches are vulnerable to some security attacks as some of the SNs reporting to the FC may be compromised. As a result, the FC is not robust against such attacks and its detection performance may be degraded.

Security problems in centralized detection using WSNs remain an open issue, see [9, 12, 66–74] and references therein. While there are many types of security threats, in this thesis we focus on a single type of attack, which is the test statistic

falsification (TSF) attack part of the Byzantine attacks family originally proposed in [8] and later widely used in the context of distributed detection (e.g., [9–11]).

In this thesis, we address the second design challenge discussed in Section 1.2 by proposing distributed detection and estimation schemes in WSNs that operates under limited SN transmit power and finite bandwidth. These schemes are shown to have low computational complexity and do not rely on doubly stochastic weight matrix assumption. The proposed schemes will be shown to outperform the existing schemes even at low bit rate. Then, we address the third design challenges discussed in Section 1.2 by examining $under-attack$ WSNs in the presence of falsified SNs, limited bandwidth fading channels, and quantization of test statistics. We also propose solutions and algorithms to cope with such scenarios and show that our proposed schemes outperform the existing approaches.

1.5 Thesis Outline and Contributions

This PhD thesis describes the research carried out on centralized and distributed detection (estimation) in practical WSN systems and, in particular, on the resource allocation, fusion rules, and network security.

Next, we describe the thesis organization, main contributions together with the publications list for each particular chapter. Throughout this thesis, we extensively use the detection theory, graph theory, and game theory concepts. Hence, for that reason, the next chapter is devoted to the theory preamble to introduce these concepts. The majority of the third chapter is devoted to resource allocations and in particular to quantization and power allocation for centralized detection (i.e., with a FC WSN). Chapter 4, considers also the centralized detection framework and is devoted to fusion rules design. The fifth chapter is devoted to fully distributed detection algorithms design (i.e., without any FC). Finally, Chapter 6 is devoted to WSN security and we propose algorithms to cope when compromised SNs are involved and Chapter 7 concludes the thesis and gives further future research directions.

Figure 1.2: Thesis organization.

Chapter 2: Theory Preamble

This chapter introduces the reader to the review of the fundamental concepts of detection theory, algebraic graph theory, and game theory as used in subsequent chapters. Notations and criteria used in detection theory, definitions and the terminology of connectivity for undirected and for directed graphs, and an overview of a zero-sum game are also presented. Some important graph related matrices with a special focus on the properties of the Laplacian matrix along with its spectral properties are described in some detail. Definitions of the strategic form zero-sum

game, the finite game, and the Nash Equilibrium are also provided.

Chapter 3: Optimal Quantization and Power Allocation

This chapter considers the centralized detection scheme, where the local SNs send quantized information to the FC. A simple linear fusion rule at the FC is adopted and we first propose a centralized optimal SN transmit power and quantization bits allocation scheme for each SN and investigate the detection performance over flat fading transmission links. Then, a fully distributed SN transmit power allocation algorithm is proposed. The algorithm is characterized in terms of convergence and data exchange rate and is shown to be efficient and simple to implement.

The work of this chapter has led to the publication of two articles in international conferences.

[1] E. Nurellari, D. McLernon, M. Ghogho and S. Aldalahmeh, "Optimal quantization and power allocation for energy-based distributed sensor detection," *Proc. IEEE EUSIPCO*, Lisbon, Portugal, 1-5 Sept. 2014.

[2] E. Nurellari, D. McLernon, M. Ghogho and S. A. R. Zaidi, "Distributed Optimal Quantization and Power Allocation for Sensor Detection Via Consensus," *Proc. IEEE VTC Spring*, Glasgow, United Kingdom, 11-14 May 2015.

Chapter 4: Centralized Quantized Fusion Rules

This chapter (similar to Chapter 3), also considers the centralized detection, but investigates the problem of quantized soft decision fusion. Using the likelihood ratio test (LRT), the optimal fusion rule at the FC has been derived. Then, we derive and analyze suboptimal fusion rules that require little or no $a-priori$ knowledge about the WSN system. Finally, we show how the effect of test statistics quantization can be mitigated by increasing the number of samples (i.e., bandwidth can be traded off against increased latency).

The work of this chapter has led to the publication of one article in an international conference.

[1] E. Nurellari, S. Aldalahmeh, M. Ghogho, and D. McLernon, "Quantized Fusion Rules for Energy-Based Distributed Detection in Wireless Sensor Networks," *Proc. IEEE SSPD*, Edinburgh, Scotland, 8-9 Sep. 2014.

A contribution [77] partially using the results of this chapter and included in Appendix D of this PhD thesis, is published in the proceedings of a journal.

[2] S. Aldalahmeh, M. Ghogho, D. McLernon, and E. Nurellari, "Optimal fusion rule for distributed detection in clustered wireless sensor networks", *EURASIP Journal on Advances in Signal Process.*, 2016:5, Jan. 2016.

Chapter 5: Distributed Two-Step Quantized Fusion Rules

The focus of this chapter is on a fully distributed detection framework via a consensus algorithm with quantized information exchange. We give a review of the related existing work and contributions and clearly provide the reasons behind the needs of developing new approaches. Based on the (unquantized) consensus algorithm, we provide a distributed consensus-based detection framework with (weight combining) quantized test statistics exchange. Each SN implements a low complexity uniform quantizer and the number of quantization bits is constrained to match the channel capacity of each link. Using the probability of detection and the probability of false alarm as metrics, we show that this approach does not converge across the network and does not approach the quantized centralized detector (i.e., with a FC) performance.

Because of this, we propose a novel two-step quantized distributed weighted fusion algorithm. The proposed two-step quantized fusion algorithm takes the advantage of the spatially distributed information across the WSN while combating fading. The proposed algorithm is analyzed in terms of detection performance as well as characterized in terms of convergence and data exchange rate. It converges to a global decision, approaches the centralized detector performance, and achieves the global decision in a finite number of iterations.

The technical contributions of this chapter have been published in the proceedings of one international conference and in one journal paper.

[1] E. Nurellari, D. McLernon, and M. Ghogho, "Distributed detection in practical wireless sensor networks via a two step consensus algorithm," in *Proc. IET Int. conf. on Intelligent Signal Process. (ISP)*, London, United Kingdom, 1-2 Dec. 2015.

[2] E. Nurellari, D. McLernon, and M. Ghogho, "Distributed Two-Step Quantized Fusion Rules via Consensus Algorithm for Distributed Detection in Wireless Sensor Networks," in *IEEE Transactions on Signal and Information Processing over Networks (TSIPN)*, vol. 2, no. 3, pp. 321-335, Sept. 2016.

Chapter 6: Sensor Detection in the Presence of Falsified Observations

This chapter considers again centralized detection, but now by an $under-attack$ WSN that operates over limited bandwidth fading channels and analyzes the network security.

In the first part, we consider that the attacker falsifies the local test statistics and it is assumed that it knows the true hypothesis. From the FC's perspective, we derive analytically the optimal weight combining, the optimal SN to FC transmit power and the number of quantization bits for each SN. It is shown that these expressions require the attacker parameters which cannot be estimated in practice. We also derive the attacker strategy that degrades the FC detection performance most and is shown to depend on the FC weight combining and SNs transmit power. We characterize the performance of sub-optimum strategies that do not require knowledge of the FC mechanism and attacker parameters. Finally, to identify the optimum behavior of both the FC and the attacker, we re-cast the problem as a minimax game between the FC and the attacker and show that the Nash Equilibrium exists.

In the second part, we relax the assumption of the true hypothesis knowledge by the attacker and introduce a different attacking model. Now, the SNs report to the FC their 1-bit local decisions instead of their quantized test statistics (like in the first part). The attacker manipulates this 1-bit local decision with a flipping probability.

We derive and characterize this optimum flipping probability and the minimum fraction of the compromised SNs that makes the FC incapable of detecting. Then, we propose a new non-complex and efficient reputation-based FC detection scheme to identify these compromised SNs. Based on this new approach, we also calculate the optimal weight combining at the FC and ensure that for the compromised SNs, their contribution toward the FC final decision is reduced proportionally. Numerical results show that this approach outperforms the existing schemes.

The technical contributions of this chapter have been published in two journal papers.

[1] E. Nurellari, D. McLernon, and M. Ghogho, "Distributed Binary Event Detection Under Data-Falsification and Energy-Bandwidth Limitation", in *IEEE Sensors Journal*, vol. 16, no. 16, pp. 6298-6309, Aug. 15, 2016.

[2] E. Nurellari, D. McLernon, and M. Ghogho "A Secure Optimum Distributed Detection Scheme in Under-Attack Wireless Sensor Networks", in *IEEE Transactions on Signal and Information Processing over Networks (TSIPN)*, vol. PP, no. , pp. , May 2017.

Chapter 2

Theory Preamble

IN THIS CHAPTER

Within this chapter, we illustrate the theoretical arrangement that is necessary for the comprehension of successive chapters. Additionally, this should serve as reference for notions subsequently mentioned. The subjects developed within this chapter are Detection Theory, Graph Theory, and Game Theory. Readers aquinted with these subjects may advance to Chapter 3 and refer here as needed. We assume the reader to be knowledgeable in linear algebra and dynamical systems theory.

2.1 Elements of Detection Theory

In this section, we introduce some detection theory concepts based on statistical signal detection theory that we will be using throughout this PhD thesis. In fact, the signal detection theory is used in many applications such as signal processing for communications, biomedicine, radar and sonar, and binary event detections. For instance, in statistical signal processing for communications, characterization and design of spatially distributed systems extensively involves detection and estimation in order to effectively provide a reliable and efficient system. For example, determining if the current bit received in the presence of channel disturbances was a zero or a one is clearly a detection problem.

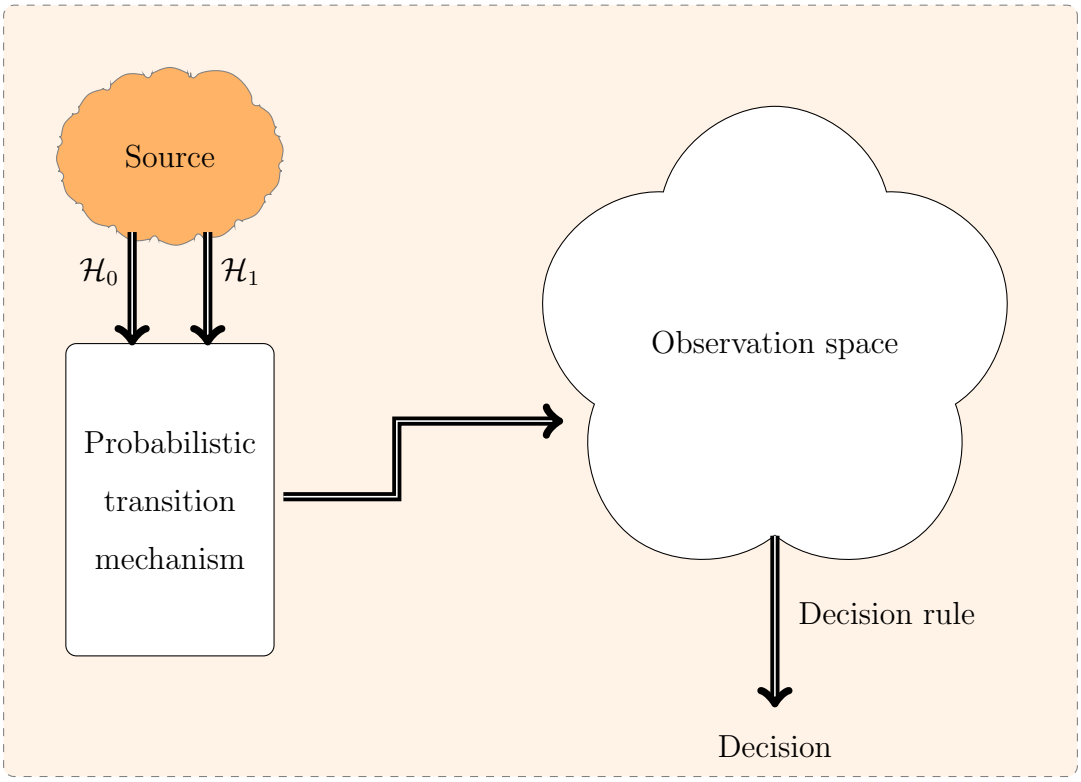

Figure 2.1: Components of a decision theory problem.

To this end, in Fig. 2.1 we capture some of the most fundamentals components of detection theory that includes:

1. The *source* (target)- Typically, it is a binary event that generates an output that is frequently assigned to one of the hypotheses, either $\mathcal{H}_0$ (absent) or $\mathcal{H}_1$ (present).

2. The *probabilistic transition mechanism*- It generates a point in the *observation space* based on the true hypotheses knowledge.

3. The *decision rule*- By observing the outcome in the *observation space*, we shall decide which hypothesis was true. To do that, we need to design an effective and reliable *decision* (fusion) rule based on some criteria that we define and elaborate in the coming chapters. General speaking, in one or another way, this PhD thesis will demonstrate a great deal of how these decision theory components fit together such that a binary hypothesis testing problem is effectively established.

2.2 Binary Hypothesis Testing

The main objective of this PhD thesis is to develop detection mechanisms and algorithms by means of multiple distributed sensor nodes (SNs) across the interested field. The i^{th} SN, based on its own observation, generates a local test statistics T_i. The statistical models of these SNs observations (test statistics), in a large number of detection problems, can accurately be modeled as Gaussian measurements. Furthermore, as we will see later in the following chapters, the assumption of a Gaussian model yields closed form solutions and gives insight into the system design parameters. Hence, throughout this work, we will focus particularly on Gaussian statistical observation models.

Binary detection is one of the simplest hypothesis tests that frequently finds applications in the real world scenarios. In this work, we assume that the statistical observations under $\mathcal{H}_0$ and $\mathcal{H}_1$ are completely known. The objective is to use this information (which is always buried in noise) to establish a suitable fusion (decision) rule by exploring different techniques for making a reliable decision. Essentially, we are to decide if the data generated by the *source* in Fig. 2.1 comes according to the (known) probability density functions (PDFs) under $\mathcal{H}_0$ or $\mathcal{H}_1$. While the complete knowledge of the PDFs yields a theoretically optimal solution (decision rule), often this solution is not mathematically tractable (as we will show in the later chapters). Hence, in this PhD thesis, while designing the decision rules we focus on those detectors that are particularly convenient from both theoretical and practical point of view.

Next, we discuss the Bayesan and the Neyman-Pearson's approach.

2.2.1 Bayes Criterion

There are mainly two approaches to hypothesis testing, the Bayesian and the Neyman-Pearson approach. The Bayesian approach depends on $a-priori$ known information about the source outputs and on the cost assigned to each possible action taken. In this case, the objective function to be optimized can be the *Bayes risk* $\mathcal{R}$ thats is

defined as follow [78]:

$$\mathcal{R} = \mathbb{E}(\mathbb{C}) = \sum_{i=0}^{1}\sum_{j=0}^{1} \mathbb{C}_{ij} \text{pr}\left\{\text{say } \mathcal{H}_i | \mathcal{H}_j \text{ is true}\right\} \text{pr}\left\{\mathcal{H}_j\right\} \tag{2.2.1}$$

where pr(.) denotes probability of an event and $\mathbb{C}_{ij}$ for $i = 0, 1,\ j = 0, 1$ are the costs associated to each of the possible action taken and are defined as follow:

$$\mathcal{H}_0 \text{ true} | \mathcal{H}_0 \text{ chosen} \quad \rightarrow \text{associated cost } \mathbb{C}_{00} \tag{2.2.2}$$

$$\mathcal{H}_0 \text{ true} | \mathcal{H}_1 \text{ chosen} \quad \rightarrow \text{associated cost } \mathbb{C}_{01} \tag{2.2.3}$$

$$\mathcal{H}_1 \text{ true} | \mathcal{H}_0 \text{ chosen} \quad \rightarrow \text{associated cost } \mathbb{C}_{10} \tag{2.2.4}$$

$$\mathcal{H}_1 \text{ true} | \mathcal{H}_1 \text{ chosen} \quad \rightarrow \text{associated cost } \mathbb{C}_{11.} \tag{2.2.5}$$

Suppose we are to design a security system to monitor a specific environment and detect any enemy/attacker in a region of interest. The result of the decision is for e.g., to raise an alarm and deploy/adapt other protection mechanisms if the enemy is declared to be present or do nothing (i.e., stay in the current mode) if no alarm is raised. Now, if we decide the enemy/attacker is not present but it proves to be present, the whole security system will fail (i.e., the enemy/attacker would be able to cause a greater system degradation) and we incur a larger cost ($\mathbb{C}_{10}$). If, however, we decide that the enemy/attacker is present but it proves the contrary, the false alarm will be raised and we incur a smaller cost ($\mathbb{C}_{01}$) associated only with the false alarm activation and precaution measurements to be taken in such a case.

Assuming that the cost of a wrong decision is higher than the cost of a correct decision (i.e., $\mathbb{C}_{10} > \mathbb{C}_{00}$ and $\mathbb{C}_{01} > \mathbb{C}_{11}$), the *Bayes* test that minimizes the risk $\mathcal{R}$ can be shown to be the *likelihood ratio test* (LRT):

$$\Lambda\left(\boldsymbol{T}\right) \triangleq LRT\left(\boldsymbol{T}\right) = \frac{\text{p}\left\{T_1, T_2, ..., T_M | \mathcal{H}_1\right\}}{\text{p}\left\{T_1, T_2, ..., T_M | \mathcal{H}_0\right\}} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \frac{(\mathbb{C}_{10} - C_{00})\text{pr}\left\{\mathcal{H}_0\right\}}{(\mathbb{C}_{01} - \mathbb{C}_{11})\text{pr}\left\{\mathcal{H}_1\right\}} = \gamma_{_B} \tag{2.2.6}$$

where $\text{p}\left\{T_1, T_2, ..., T_M | \mathcal{H}_j\right\}$ for $j = 0, 1$ is the joint probability density of the local soft decisions (T_i of the i^{th} SN for $i = 1, 2, \cdots, M$) under the j^{th} hypothesis. In general, T_i may represent the local SN's observation or processed SN's observation (i.e., can be the matched filter detector (MFD), the energy detector (ED) or other). Throughout the thesis, T_i represents the test statistic of the i^{th} SN defined later (see

for e.g., (3.2.3)). Now, the quantity on the left is the ratio of the two PDFs and that is why called the *likelihood ratio* while the right hand side is the threshold of the test denoted by $\gamma_{_B}$. Clearly, the optimum test using the *Bayes* criterion is the *likelihood ratio test* (LRT) given in (2.2.6). In the cases where the costs and the $a-priori$ probabilities can be estimated (for example from past history of the data), the optimum test in (2.2.6) can be implementable. However, in practice, situations where assigning realistic $a-priori$ probabilities and/or costs is not possible, frequently arises. For example, if detecting the presence of an enemy/intruder, the $a-priori$ belief in the likelihood of the hypothesis (i.e., the enemy/intruder is present or absent) is usually not possible. In such cases, the detection problem is tackled by means of Neyman-Pearson's approach. Throughout this PhD thesis, we assume that the $a-priori$ belief and the cost of course of actions cannot be determined and we use the Neyman-Pearson criterion to tackle the detection problems considered.

Next, we describe the Neyman-Pearson approach.

2.2.2 Neyman-Pearson Criterion

As we previously discussed, in real scenarios, situations where $a-priori$ belief in the likelihood of the hypothesis and assigning costs to each of the decision taken is not possible and/or practical. The Neyman-Pearson approach, which is based on the Neyman-Pearson Theorem, offers an alternative solution. That is, design an optimum detection rule that maximizes the probability of detection (P_d) for a given probability of false alarm (P_{fa}). We next state the Neyman-Pearson Theorem that can be defined as [78]:

Theorem 2.2.1 *(**Neyman − Pearson**). To maximize probability of detection (P_d) for a fixed probability of false alarm (P_{fa}) (i.e., $P_{fa}=\beta'$), the optimum test is the likelihood ratio test:*

$$\Lambda\left(\boldsymbol{T}\right) \triangleq LRT\left(\boldsymbol{T}\right) = \frac{\mathrm{p}\left\{T_1, T_2, ..., T_M|\mathcal{H}_1\right\}}{\mathrm{p}\left\{T_1, T_2, ..., T_M|\mathcal{H}_0\right\}} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \gamma_{_{NP}} \tag{2.2.7}$$

where $p\left\{T_1, T_2, ..., T_M|\mathcal{H}_j\right\}$ is the joint probability density of local soft decisions under the j^{th} hypothesis, and $\gamma_{_{NP}}$ is the threshold and can be found by defining a required

P_{fa} and solving for this threshold in:

$$P_{fa} = \Pr\left(\Lambda\left(\boldsymbol{T}\right) > \gamma_{NP} | \mathcal{H}_0\right) = \int_{\gamma_{NP}}^{\infty} \mathrm{p}\left(\Lambda\left(\boldsymbol{T}\right) | \mathcal{H}_0\right) d\Lambda = \beta'. \tag{2.2.8}$$

Usually, a transformation is required to further simplify the final expression $\Lambda\left(\boldsymbol{T}\right)$. However, as can be seen from (2.2.8), it is not easy task to implement the integration as $\Lambda\left(\boldsymbol{T}\right)$ might not posses a closed form distribution and does not allow mathematical tractability of the system design. So, the partial focus of this PhD thesis is to find and/or approximate a closed form distribution for $\Lambda\left(\boldsymbol{T}\right)$ that gives insight into the system designed parameters.

2.3 Performance Analysis Techniques

To evaluate the performance of the decision rules, different techniques are used in the literature. Typically, the probability of detection (P_d) and probability of false alarm (P_{fa}) metrics are evaluated. In this PhD thesis, we use the following performance analysis such as probability of detection (P_d) vs. probability of false alarm (P_{fa}) (i.e., *receiver operating characteristic* (ROC) curve), probability of mis-detection ($1 - P_d$) vs. SN transmit power budget, probability of detection vs. signal to noise ratio (SNR), and probability of detection vs. number of SNs. Because the above metrics can be evaluated from the *receiver operating characteristic* plot, we next introduce the ROC curve.

2.3.1 Receiver Operating Characteristic (ROC)

The two-dimensional plot P_d versus P_{fa}, gives the ROC curve which essentially describes each point (P_{fa}, P_d) for a given detection threshold γ_{NP}. Clearly, as γ_{NP} decreases, P_d increases. However, this also forces the P_{fa} to increase. By adjusting the detection threshold (i.e., for $-\infty < \gamma_{NP} < \infty$), any point on the curve is achievable. The ROC performance is frequently used and chosen as a metric for performance analysis in order to select the appropriate and most suitable detector.

In Fig. 2.2, we show some typical ROC curves. We can observe that the ROC curve of the *blind* detector (i.e., the detector that ignores all the SNs observations

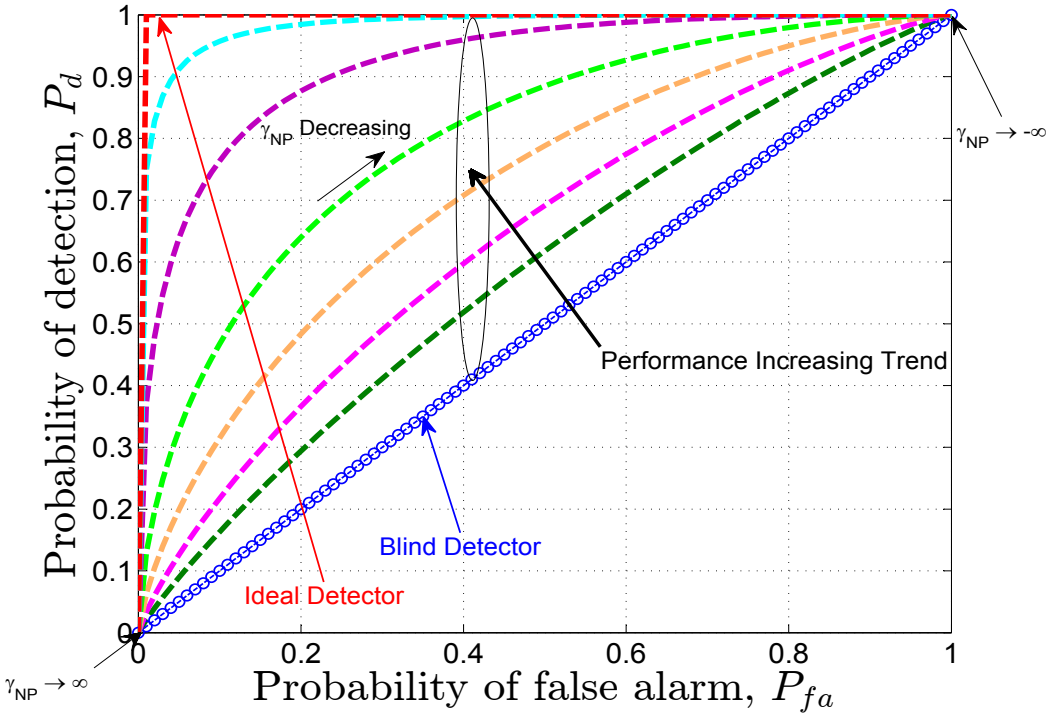

Figure 2.2: Typical family of Receiver Operating Characteristic curves and behavior.

and bases its decision on flipping a coin), is of no any use as $P_d = P_{fa}$, $\forall\gamma_{NP}$. What we require, is a detector with a (ROC) performance above the *blind* detector (ROC) curve. The (ROC) performance *upper* bound is the performance of the *ideal* detector (i.e., the detector which always makes the right decision $\forall P_{fa}$ and $\forall\gamma_{NP}$ values). In general, the achievable ROC performance of a good detector is between the ROC performance of these two (i.e., between *blind* and *ideal* detectors).

2.4 Graph Theory Preliminaries

In a Wireless Sensor Network (WSN), sensor nodes (SNs) are spatially deployed over a field to observe and collect relevant information about the nature of interest. Some of the features that these SNs possess are the sensing capability, limited communication capability, and some processing capability. The configuration of the WSN depends on different factors such as physical constraints (dictated by the available resources such as the power consumption to maintain reliable communication

links), applications (for instance, if deployed for detection purposes, maximizing the detection probability with respect to the communication topology and local SNs processing is of a great interest), and network security (for example if one or more SNs in the network are compromised or a SN failure occurs, is the network capable of performing a reliable decision?). There are mainly two network architectures used in the literature: the centralized architecture, where spatially deployed SNs report their local information to the fusion center (FC); and the distributed approach, where there is no FC and each of the SNs collaborate with each other in order to come up with a global decision. There are also hybrid architectures (i.e., there is a SNs collaboration and a FC). We elaborate more on the advantages and disadvantages of each architecture in the coming chapters but now we will focus on describing the interactions among these SNs and the FC.

The proper way to describe the information flow among these SNs in the network is to introduce a graph model of the network and the most useful approach to get insight into the properties of a graph is through *algebraic graph theory* [79]. Next, we review some important concepts of graph theory and recall important definitions (that we will be using later) to describe these concepts.

2.4.1 Basic Definitions and Terminology

The interaction among SNs is according to the communication topology which is given by a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{1, 2, \ldots, M\}$ represents the set of M SNs and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the set of edges $\{i, j\}$. The graph properties can be represented by an *adjacency matrix* $\mathbf{E} \in \mathbb{R}^{M \times M}$ whose entries $e_{ij} = 1$ if the pair of SNs (i, j) is connected, otherwise $e_{ij} = 0$. If the graph is *undirected* (see Fig. 2.3), then $e_{ij} = e_{ji}$ and clearly $\mathbf{E} \in \mathbb{R}^{M \times M}$ is symmetric. If the graph is *directed* (see Fig. 2.4), then for the communication link (i, j), we say SN i transmits to SN j (i.e., j is called the *head* and i is called the *tail* of the edge $\{i, j\}$). In this case, the *adjacency* matrix $\mathbf{E} \in \mathbb{R}^{M \times M}$ is asymmetric. This property (i.e., $\mathbf{E} \in \mathbb{R}^{M \times M}$ being symmetric or asymmetric) will have practical consequences when we design distributed detection algorithms. To this end we give some more definitions.

We denote the i^{th} SN neighbor set as Δ_i and $|\Delta_i|$ is the number of neighbors.

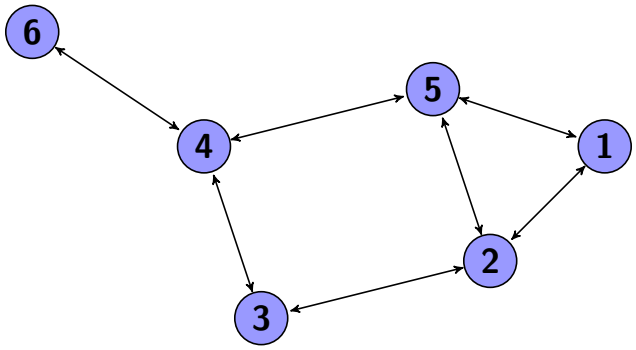

Figure 2.3: Undirected graph with $M = 6$ sensor nodes (SNs)/vertices and seven (communication) links/edges.

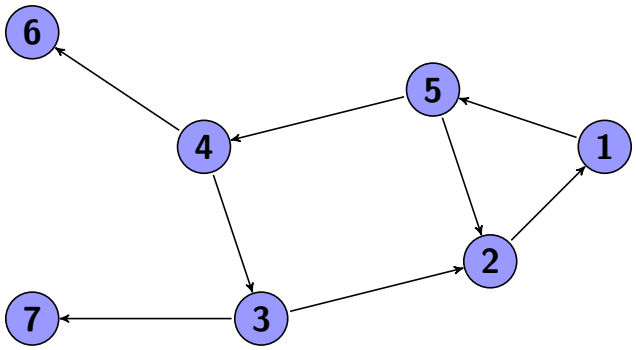

Figure 2.4: Directed graph with $M = 7$ sensor nodes (SNs)/vertices and eight (communication) links/edges.

The definition of the graph *Laplacian* matrix ($\mathbf{L} \in \mathbb{R}^{M\times M}$) is $\mathbf{L} = \mathbf{D} - \mathbf{E}$ with $\mathbf{D} = \text{diag}(|\Delta_1|, \ldots, |\Delta_M|)$. Next we recall some properties of the *Laplacian* matrix.

The Laplacian matrix

The connectivity of a WSN, usually is described by the *Laplacian* matrix of its underlying graph model. The spectral properties of the *Laplacian* matrix play an important role on the design and the convergence analysis of distributed detection algorithms. For an (undirected) graph $\mathcal{G}$, its corresponding *Laplacian* matrix $\mathbf{L}$ with eigenvalues $\lambda_M \leq \lambda_{M-1} \leq \cdots < \lambda_1 = 1$, possesses the following properties:

Property 1 The *Laplacian* $\mathbf{L}$ has a null eigenvalue (i.e., $\lambda_M = 0$) corresponding to the eigenvector $\boldsymbol{v}^r = [1, 1, \ldots, 1]^T$.

By construction, we have that every row sum and column sum of $\mathbf{L}$ is zero. Hence, clearly $\lambda_M = 0$ because $\boldsymbol{v}^r$ satisfies $\mathbf{L}\boldsymbol{v}^r = \mathbf{0}$.

Property 2 The number of times that this null eigenvalue appears corresponds to the number of connected components in the graph $\mathcal{G}$.

Clearly, for a connected graph $\mathcal{G}$, the null eigenvalue has multiplicity one (i.e., appears only once).

Property 3 The second smallest eigenvalue (λ_{M-1}) of $\mathbf{L}$ is defined as the *algebraic connectivity* [80].

The second smallest eigenvalue has many interesting properties and was named by Fiedler (1973), the *algebraic connectivity* of a graph [80]. The *algebraic connectivity* and the Fielder vector (i.e., the eigenvector associated with this eigenvalue) is one of the most powerful concepts in *graph theory*. One of the most important properties (that we will be focusing on here) is the capability of yielding important information about the communication topology of the network. For instance, the *algebraic connectivity* is monotonically increasing when more communication links are established among the SNs. However, establishing more communication links means more resources (such as the power budget) should be allocated. This trade-off will be discussed later when we develop the distributed detection algorithm and effectively allocating these available (limited) resources while maintaining the overall objectives aims satisfied, will constitute a significant part of this PhD thesis.

2.4.2 Connectivity in Undirected Communication Topologies

The relations among SNs are described by edges (communication links) between pairs of SNs (vertices). This section provides some important definitions and terminologies regarding the connectivity in a graph that we will be using in the coming chapters.

Definition 2.4.1 (*Path*) A sequence of distinct vertices (SNs) starting with vertex

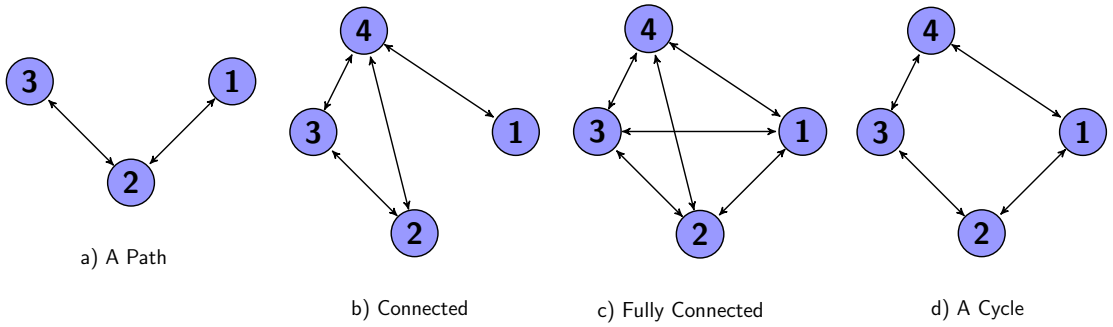

Figure 2.5: **Graph examples.** a) Describing a path with two communication links; b) Describing a connected graph with 4 SNs; c) Describing a fully connected (complete) graph with 4 SNs; d) Describing a cycle involving 4 SNs.

(SN) i and ending with vertex (SN) j such that consecutive vertices (SNs) are adjacent is defined as a *path* from vertex (SN) i to a vertex (SN) j. For unity link weight, the *shortest path* is the *path* with fewest links.

Definition 2.4.2 (*A connected graph*) When there is a path between every pair of vertices (SNs), the graph $\mathcal{G}$ is called *connected*. In a *connected graph*, each vertex (SN) is reachable from any other vertex (SN) via a *path*. A graph that is not *connected* is called a *disconnected* one.

Definition 2.4.3 (*A fully connected graph*) When there is an (edge) link between every pair of vertices (SNs), the graph is called *fully connected*. For a given number of vertices (SNs), there is a unique *fully connected graph*, which is often written as $\mathcal{G}_M$, where M is the number of vertices (SNs).

Definition 2.4.4 (*Diameter of a graph*). The geodesic distance between two SNs in a (connected) graph is the number of the edges (i.e., links) in the *shortest path* connecting these two SNs. The *diameter of a graph* is the maximum geodesic distance taken over all possible pairs of SNs in the graph.

Definition 2.4.5 (*Cycle*) A closed path that starts and ends at the same vertex (SN), and visits each other vertex (SN) only once is called a *cycle*.

The above definitions are illustratively described in Fig. 2.5. The path with two links and three SNs is shown in part a). For example, part b) shows a connected SN

network with four SNs and four communication links. For example, SN 2 communicates with SN 1 via two different paths. The first path is the sequence involving SNs $\{2, 3, 4, 1\}$ and the second path is the sequence involving SNs $\{2, 4, 1\}$. This second *path* is the *shortest path* connecting these two SNs and the number of communication links is two. This *path* (i.e., the sequence involving SNs $\{2, 4, 1\}$) happens to be the *diameter of the graph* at the same time which in this case is three. Part c) shows a *fully connected* graph (complete graph) with $M = 4$ SNs. For this case, the *diameter of the graph* is one and the number of links is $\frac{M(M-1)}{2} = 6$. Finally, part d) describes a *cycle* that involves SNs $\{1, 2, 3, 4\}$.

2.5 Game Theory Preliminaries

Game theory (*GT*) is a mathematical tool that helps to describe the phenomenon of conflict and interaction between intelligent decision-makers. Games are optimization problems that involve more than one decision maker and in general having conflicting goals. In general, the theory of games is complicated, but some games are closely related to convex optimization and posses nice theory and properties.

The fundamental volume *Theory of Games and Economic Behavior* by von Neumann and Oskar Morgenstern established *GT* in 1944. The basic terminology and the problem setup that are still in use today were provided in this monumental book. The theory of Neumann and Morgenstern is most complete for the two-players zero-sum games (i.e. games with only two players in which one player wins what the other player loses). In this PhD thesis (more specifically in Chapter 6), we make use of *GT* tools to describe, optimize, and characterize the behavior of a non-cooperative two-players zero-sum game while aiming to maximize their respective outcomes from the game.

2.5.1 A Zero-Sum Game

Games with two players with conflicting objectives (i.e., two-players zero-sum games) that are independently acting (i.e., no collaboration or communication among players is established) are with a particular focus of this PhD thesis. Let $(\mathcal{X} \times \mathcal{Y}, \mathcal{K}(x, y))$

denote a game played by 2 players where $\mathcal{K}(x, y)$ is a pay-off function defined on the product space of $\mathcal{X}$ by $\mathcal{Y}$, and $\mathcal{X}$ and $\mathcal{Y}$ are the sets of strategies for the first and the second player respectively. The first player is the fusion center (FC) which tries to maximize the performance metric ($\mathcal{K}(x, y)$) (see Chapter 6 for an exact definition). The second player is the Attacker which tries to minimize this performance metric (pay-off function) (i.e., maximize its negative). Next, we introduce some basic definitions and theorems in game theory that we will be using in Chapter 6.

Definition 2.5.1 *The strategic form, or normal form, of a two-person zero-sum game is given by a triplet ($\mathcal{X}$, $\mathcal{Y}$, $\mathcal{K}$), where*

1. *$\mathcal{X}$ is a nonempty set, the set of strategies of Player I*
2. *$\mathcal{Y}$ is a nonempty set, the set of strategies of Player II*
3. *$\mathcal{K}$ is a real-valued function defined on $\mathcal{X}$ by $\mathcal{Y}$. In other words, $\mathcal{K}(x, y)$ is a real number for every $x \in \mathcal{X}$ and every $y \in \mathcal{Y}$.*

Definition 2.5.2 (Finite Game) *A two-person zero-sum game $(\mathcal{X} \times \mathcal{Y}, \mathcal{K}(x, y))$ is said to be finite if both strategy sets $\mathcal{X}$ and $\mathcal{Y}$ are finite set.*

Definition 2.5.3 (Nash Equilibrium) *A Nash equilibrium, is a set of strategies, one for each player, such that no player has the incentive to unilaterally change its action. Players are in equilibrium if a change in strategies by any one of them would lead that player to earn less than if it remained with its current strategy.*

Definition 2.5.4 (Pure and Mixed Strategies) *The elements of $\mathcal{X}$ or $\mathcal{Y}$ are defined as pure strategies. Randomly choosing among the pure strategies $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ in various proportions is called a mixed strategy. Every pure strategy, $x \in \mathcal{X}$, can be considered as the mixed strategy that chooses always the pure strategy x.*

Theorem 2.5.1 *(**Nash** [81]). Every finite game in a strategic (normal) form has a Nash Equilibrium (NE) in either pure or mixed strategies.*

Chapter 3

Optimal Quantization and Power Allocation

IN THIS CHAPTER

Within this chapter, we address the optimal transmit power allocation problem (from the sensor nodes (SNs) to the fusion center (FC)) for the centralized detection of an unknown deterministic spatially uncorrelated signal. The overview of the motivation behind this work is presented. The assumptions made and the problem formulation by describing the target sensing and the WSN architecture are stated. The same problem formulation is used in Chapter 4. Part of the theory stated and the derivations developed will be used in the next Chapter. The core sections are mainly those two that describe the centralized and the distributed SNs power allocation schemes proposed.

3.1 Introduction

3.1.1 Motivation

Wireless sensor networks (WSNs) spatially deployed over a field can monitor many phenomena. Because of their relatively low cost and robustness to node failures they are receiving significant attention. Generally, the sensing process is orientated towards estimating various parameters of interest which can be employed to arrive

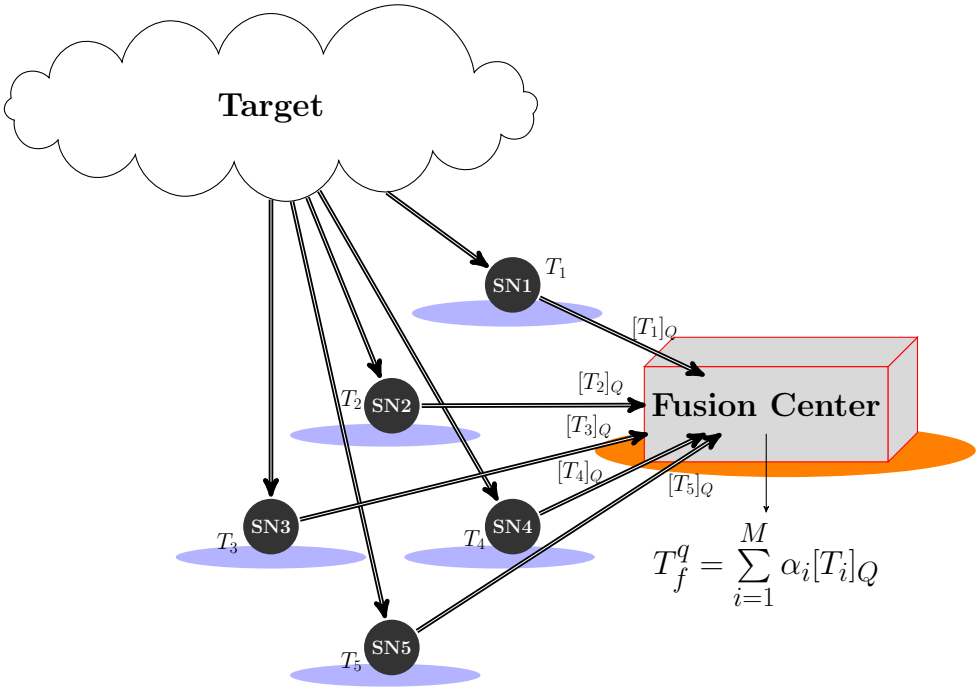

Figure 3.1: Schematic communication architecture between peripheral SNs and the fusion center (FC). Each SN generates a test statistic (T_i) by observing the target and can communicate (using $[T_i]_Q$) with the FC only over an energy-constrained/bandwidth-constrained link.

at a certain decision. This decision can then be relayed in a pre-specified manner or can be employed for on-field actuation. We note that the reliable and continued operation of a WSN over many years is often desirable. This is due to the operational environment in which post-deployment access to a sensor node (SN) is at best very limited. Unfortunately, SNs suffer from constrained bandwidth and limited available on-board power. Moreover, due to the locality of the observed process, cooperation amongst SNs is often required to derive an inference. However, such a cooperation comes at the expense of high bandwidth requirements and signalizing overhead. For instance, a WSN (with decentralized architecture) formed by M sensor nodes would require transmission of $O(M^2)$ message exchanges to attain full cooperation. Consequently, designing distributed detection algorithms that efficiently utilize the scarce bandwidth and cope with the impairments in a wireless channel is very important. A typical wireless sensor network consists of a fusion center (FC) and a number of

geographically distributed SNs (see Fig. 3.1). Each individual SN makes an estimate of a particular quantity (in our case, the energy of the received signal, T_i), and then sends a quantized version to the (FC) $[T_i]_Q$, where all the SNs outputs are optimally combined to arrive at a global detection decision.

WSNs have been considered for different applications such as localizing and tracking acoustic targets, voice activity detection, and spectrum sensing for cognitive radios (e.g., see [16], [49], [82–84] and references therein). In such applications, accurate distributed observations are fundamental to reduce detection errors.

In the first part of this chapter (see Section 3.3 and Section 3.4), we show how by maximizing the modified deflection coefficient we can calculate the optimal transmit power allocation for each SN and the optimal number of quantization bits to match the channel capacity. The resource allocation is performed at the FC and is called a *centralized* resource allocations and detection approach. The FC then informs back to each SN their allocated SN transmit power and number of quantization bits that maximizes the detection probability.

In the second part (see Section 3.5), we propose a novel fully distributed algorithm, in order to calculate the optimal transmit power allocation for each sensor node (SN) and the optimal number of quantization bits for the test statistic in order to match the channel capacity. What makes this scheme attractive is that the SNs share with their neighbours just their individual transmit powers at the current states. As a result, the SN processing complexity is further reduced. The final detection decision is again taken at the FC. This is called a *hybrid* architecture where there is a collaboration among SNs and there does exists a FC.

3.1.2 Related Work

The problem of decentralized detection (and estimation) in a WSN assuming error-free communication has been extensively tackled in [31], [85,86] to name but just a few. For a target MSE performance, the authors in [85] proposed the minimization of the summation of sensor transmit powers, while [86] suggested minimization of the Euclidean norm of the transmit powers. In both [85] and [86] the number of bits used for quantization to transmit data from each sensor to the FC is constrained to

be less than channel capacity. In [30] asymptotic results are provided for distributed detection on a joint power constraint in wireless sensor networks while in [34] a finite number of sensors with both individual and joint power constraints is considered for distributed detection over MIMO channels. A decentralized strategy for optimizing the estimation MSE subject to a network rate constraint is presented in [33]. A more recent work in [87] proposed optimum training and data power allocation with inhomogeneous sensors using binary phase shift keying modulated decisions at the FC for distributed detection.

Recent publications [50, 51] propose a distributed algorithm for in-network estimation of algebraic connectivity. Interestingly, [51] uses an estimation strategy to adapt the SN transmit power in order to maximize the connectivity of the network, while in this chapter we take advantage of the objective function structure and develop a novel distributed algorithm to allocate the SN to FC transmit power.

3.1.3 Chapter Contributions

In this chapter, we consider the *centralized* detection of an unknown deterministic signal in a spatially uncorrelated distributed WSN. For a finite number of SNs, we derive analytically the optimal transmit power and number of quantization bits for each SN, and investigate the detection performance of the sensor network over flat fading transmission links. Our work differs from [85] in that instead of sending the quantized version of the SN observations, we propose to send the quantized local test statistics (i.e., the sample energy) to the FC. We employ a simple linear fusion rule at the FC and adopt the modified deflection coefficient (MDC) [32] as the detection performance criterion, while [85] uses a matched filter. When minimum *a priori* information about the useful signal is available at the FC, our proposed scheme is superior to that in [85], as just the local SNR at each individual SN is used (no need to know the entire signal at the FC) in order to be able to detect the target. We also propose a fully distributed algorithm where we allocate the SN transmit power for each individual SN using only local information. The algorithm is very efficient in terms of convergence and data exchange, also accurate and simple to implement.

3.1.4 Chapter Outline

This chapter is organized as follows. Section 3.2 describes the system model and the WSN communication architecture. In Section 3.3, we derive an approach that utilizes the SN to FC channel capacity. An optimum linear combining rule is adopted at the FC with the combining weights optimized in Section 3.4. Section 3.5 presents the derivation of the decentralized optimum SN transmit power allocation and our proposed algorithm. Finally, simulation results are given in Section 3.6 and conclusions in Section 3.7.

3.2 Problem Formulation

In this section, we formulate the problem by first introducing and modeling the target as well as the WSN architecture adopted in this chapter. Then, the *centralized* detection set up is described.

3.2.1 System Model

Here we describe the target sensing, communication channel, and the WSN architecture.

Target Sensing

Consider the problem of detecting the presence of an unknown single target, which emits a deterministic signal $s(n)$, by a sensor network consisting of M spatially distributed SNs. N samples of the observed signal are gathered and the energy estimation is performed by each SN. The measurement at each sensor $s_i(n)$ is further corrupted by AWGN $w_i(n) \sim \mathcal{N}(0, {\sigma_i}^2)$. the received signal takes one of the following forms, depending upon the underlying hypothesis:

$$\mathcal{H}_0 : y_i(n) = w_i(n) \tag{3.2.1}$$

$$\mathcal{H}_1 : y_i(n) = s_i(n) + w_i(n) \tag{3.2.2}$$

for $i = 1, 2, \ldots, M$ and $n = 1, 2, \ldots, N$. The i^{th} sensor evaluates

$$T_i = \sum_{n=1}^{N} (y_i(n))^2, \ i = 1, 2, \ldots, M \tag{3.2.3}$$

which for large N can be approximated by a Gaussian distribution [88]. It is not difficult to show that

$$\mathbb{E}\left\{T_i|\mathcal{H}_0\right\} = N\sigma_i^2, \mathrm{Var}\left\{T_i|\mathcal{H}_0\right\} = 2N\sigma_i^4 \tag{3.2.4}$$

$$\mathbb{E}\left\{T_i|\mathcal{H}_1\right\} = N\sigma_i^2\left(1+\xi_i\right), \mathrm{Var}\left\{T_i|\mathcal{H}_1\right\} = 2N\sigma_i^4\left(1+2\xi_i\right) \tag{3.2.5}$$

where $\xi_i = \sum_{n=1}^{N} s_i^2(n) / N\sigma_i^2$.

Communication Channel

The communication between the local SNs and the FC are modeled as error-free[1] (the SNs exchange quantized information matched to the channel capacity of each link) orthogonal flat fading channels and additive white Gaussian noise (AWGN) with a known variance ζ_i. The assumption of flat fading (see for e.g., [52]) is reasonable and valid in many WSN applications operating at both short distances and low bit rate (hence large symbol interval) due to resource limitations. Furthermore, the fact that they are (densely) spatially deployed across an open field result in a small delay spread. Each SN then sends (through single-hop) its information (quantized to L_i bits (defined later)) to the FC for soft decision combining.

The communication among SNs is modeled by using the *graph theory* tools and we assume that the communication topology is not *fully connected*. Furthermore, in this chapter, ideal exchange of information between SNs that are connected is also assumed and there are no "overhearing SNs" across the WSN.

WSN Architecture

In this chapter we use two different WSN architectures. The first one is called the *centralized* architecture where there is a FC that communicates (through single-hop) with spatially distributed SNs. The FC broadcasts a periodic pilot signal that is used for channel state information (CSI) estimation and this is used for synchronization by the local SNs. Based on this CSI and on the limited available SNs' resources, the FC

[1] We match the information rate among SNs to the corresponding channel capacity of each communication link. Hence, from Shanon's theorem, there exists a coding technique such that information can be transmitted over the channel with arbitrarily small error probability.

should allocate the optimum SNs transmit power and the test statistics quantization bits. For example, if at any particular instant, the communication link between a SN and the FC is deeply faded, the contribution from this SN received at the FC may be irrelevant and degrade the overall FC performance. The communication link can be reactivated when the fading conditions improve. Now, the communication links between the SNs and the FC are time-varying and may require multiple handshaking throughout the WSN operation depending on the variation periodicity. Dealing with the handshaking minimisation is out of this thesis scope. To deal with handshaking burden, we propose a distributed power allocation scheme (see Section 3.5). Finally, upon receiving the contributions from all the SNs and assuming a delay-constrained[2] network, the FC should fuse all these local test statistics to yield a reliable global detection decision. In the case when a particular SN's observation is not available to the FC upon a maximum delay period (which is application dependent), the FC takes the final decision based on the available test statistic at that time.

The second architecture used is called the *hybrid* architecture. Similar to the first architecture, there is a FC that communicates to the geographically dispersed SNs across the field. However, in this case, the SNs can establish communication among each other and we don't make any assumption on the communication topology (e.g., mesh topology) but only require to be "connected" (see later Chapter 5). In this way, using knowledge of the CSI (estimated by the FC), each SN collaborates with its neighbors (single-hop and no "overhearing" is assumed) and will be able to allocate its own SN to FC transmit power using only local information (see Section 3.5). As before, the FC is tasked to perform a reliable global detection decision based on the SNs' reported test statistics.

3.3 Quantized Soft Decision Combining

Here we will investigate linear soft decision combining at the FC. This has superior performance to the hard decision approach (e.g., [89] and see references therein),

[2]In delay-constrained networks, all the test statistics collected during the sensing phase must be communicated to the FC in the transmission phase of that particular time-slot

but it entails additional complexity at the FC. Soft decision combining also puts additional demands on both the limited power resources of the sensors and effective utilization of the SN to FC channel capacity. So here we propose a scheme, where each individual SN has to quantize its observed test statistic (T_i) to L_i bits. To satisfy the capacity constraint on each SN to FC channel, we require:

$$L_i \leq \frac{1}{2}\log_2\left(1+\frac{p_i h_i^2}{\zeta_i}\right) \text{ bits/sample} \tag{3.3.1}$$

where p_i denotes the transmit power of sensor i, h_i is the flat fading gain between sensor node i and the FC, and ζ_i is the variance of the AWGN at the FC. The quantized test statistic ($\hat{T}_i$) at the i^{th} sensor can be modeled as

$$\hat{T}_i = T_i + v_i \tag{3.3.2}$$

where v_i is quantization noise independent of $w_i(n)$ in (3.2.1) and (3.2.2). Assuming uniform quantization with $T_i \in [0, 2U]$, then

$$\sigma_{v_i}^2 = \frac{U^2}{3\times 2^{2L_i}}. \tag{3.3.3}$$

Linearly combining $\left\{\hat{T}_i\right\}_{i=1}^{M}$ at the FC gives

$$T_f = \sum_{i=1}^{M}\alpha_i \hat{T}_i \tag{3.3.4}$$

where the weights $\left\{\alpha_i\right\}_{i=1}^{M}$ will be optimized in Section 3.4.1. Again, for large M, T_f will be approximately Gaussian and we can show that:

$$\mathbb{E}\left\{T_f|\mathcal{H}_0\right\} = \sum_{i=1}^{M}\alpha_i\left(N\sigma_i^2+U\right) \tag{3.3.5}$$

$$\mathbb{E}\left\{T_f|\mathcal{H}_1\right\} = \sum_{i=1}^{M}\alpha_i\left(N\sigma_i^2(1+\xi_i)+U\right) \tag{3.3.6}$$

$$\mathrm{Var}\left\{T_f|\mathcal{H}_0\right\} = \sum_{i=1}^{M}\alpha_i^2\left(2N\sigma_i^4+\sigma_{v_i}^2\right) \tag{3.3.7}$$

$$\mathrm{Var}\left\{T_f|\mathcal{H}_1\right\} = \sum_{i=1}^{M}\alpha_i^2\left[2N\sigma_i^4(1+2\xi_i)+\sigma_{v_i}^2\right]. \tag{3.3.8}$$

The FC makes the following decisions:

$$\left.\begin{array}{l}\text{if } T_f < \Lambda_f, \text{ decide } \mathcal{H}_0\\ \text{if } T_f \geq \Lambda_f, \text{ decide } \mathcal{H}_1\end{array}\right\} \tag{3.3.9}$$

where Λ_f is the FC detection threshold. The probabilities of false alarm and detection at the FC are respectively:

$$P_{fa} = \Pr\left(T_f \geq \Lambda_f | \mathcal{H}_0\right) = Q\left(\frac{\Lambda_f - \mathbb{E}\left\{T_f|\mathcal{H}_0\right\}}{\sqrt{\mathrm{Var}\left\{T_f|\mathcal{H}_0\right\}}}\right) \tag{3.3.10}$$

$$P_d = \Pr\left(T_f \geq \Lambda_f | \mathcal{H}_1\right) = Q\left(\frac{\Lambda_f - \mathbb{E}\left\{T_f|\mathcal{H}_1\right\}}{\sqrt{\mathrm{Var}\left\{T_f|\mathcal{H}_1\right\}}}\right) \tag{3.3.11}$$

where $Q(.)$ is the Q-function. And from (3.3.10) and (3.3.11) we can write [78]

$$P_d = Q\left(\frac{Q^{-1}\left(P_{fa}\right)\sqrt{\mathrm{Var}\left\{T_f|\mathcal{H}_0\right\}} - \Psi}{\sqrt{\mathrm{Var}\left\{T_f|\mathcal{H}_1\right\}}}\right) \tag{3.3.12}$$

where

$$\Psi = \mathbb{E}\left\{T_f|\mathcal{H}_1\right\} - \mathbb{E}\left\{T_f|\mathcal{H}_0\right\} = N\sum_{i=1}^{M}\alpha_i\left(\sigma_i^2\xi_i\right). \tag{3.3.13}$$

So using (3.3.1), (3.3.3) and (3.3.5) in (3.3.12) we get

$$P_d = Q\left(\frac{Q^{-1}\left(P_{fa}\right)\sqrt{\sum_{i=1}^{M}\alpha_i^2\left(2N\sigma_i^4 + \frac{U^2}{3\left(1+\frac{p_i h_i^2}{\zeta_i}\right)}\right)} - \Psi}{\sqrt{\sum_{i=1}^{M}\alpha_i^2\left[2N\sigma_i^4\left(1+2\xi_i\right) + \frac{U^2}{3\left(1+\frac{p_i h_i^2}{\zeta_i}\right)}\right]}}\right). \tag{3.3.14}$$

The formula in (3.3.14) imposes a relationship between the probability of detection, the power allocated to each transmission (SN to the FC) link and the weight (α_i in (3.3.4)) for each individual link.

3.4 Centralized Optimum Weight Combining and Power Allocation

In this section, we would like to find the optimum weighting vector ($\boldsymbol{\alpha}_{opt}$) and the optimum power allocation vector ($\boldsymbol{p}_{opt}$) that maximize (3.3.12) (see definiton later), under the constraint of a maximum transmit power budget (P_t). However, maximizing (3.3.12) w.r.t. $\boldsymbol{\alpha}$ and $\boldsymbol{p}$ is difficult and no closed form solution can be found. So we will approximate the optimal solution by adopting the modified

deflection coefficient [32] as an alternative function to be maximized. This is given as:

$$\tilde{d^2}\left(\boldsymbol{\alpha},\boldsymbol{p}\right)=\left(\frac{\mathbb{E}\left\{T_f|\mathcal{H}_1\right\}-\mathbb{E}\left\{T_f|\mathcal{H}_0\right\}}{\sqrt{\mathrm{Var}\left\{T_f|\mathcal{H}_1\right\}}}\right)^2=\frac{\left(\boldsymbol{r}^T\boldsymbol{\alpha}\right)^2}{\boldsymbol{\alpha}^T\mathbf{G}\boldsymbol{\alpha}} \tag{3.4.1}$$

where

$\boldsymbol{r}=[N\sigma_1^2\xi_1, N\sigma_2^2\xi_2, ..., N\sigma_M^2\xi_M]^T$

$\boldsymbol{\alpha}=[\alpha_1,\alpha_2,\ldots,\alpha_M]^T$, $\boldsymbol{p}=[p_1,p_2,\ldots,p_M]^T$

$\mathbf{G}=2N\mathrm{diag}\left(\sigma_1^4\left(1+2\xi_1\right)+\frac{\sigma_{v1}^2}{2N},\ldots,\ \sigma_M^4\left(1+2\xi_M\right)+\frac{\sigma_{v_M}^2}{2N}\right).$

Note that the dependence of $\tilde{d^2}\left(\boldsymbol{\alpha},\boldsymbol{p}\right)$ on the transmit power vector $\boldsymbol{p}$ enters (3.4.1) through the $\left\{\sigma_{v_i}^2\right\}_{i=1}^M$ terms via (3.3.1) and (3.3.3). Now, our optimization problem is:

$$\begin{aligned}\left(\boldsymbol{\alpha}_{opt},\boldsymbol{p}_{opt}\right)=&\ \arg\ \max_{\boldsymbol{\alpha},\boldsymbol{p}}\left(\tilde{d^2}\left(\boldsymbol{\alpha},\boldsymbol{p}\right)\right)\\ \text{subject to}&\sum_{i=1}^{M}p_i\le P_t\ \text{for}\ \ p_i\ge 0,\ i=1,2,\ldots,M.\end{aligned} \tag{3.4.2}$$

We assume that the fusion center (FC) has full knowledge of quantities such as the channel gains (h_i) from sensors to FC, sensing noise variances (σ_i^2) at the different sensors, and prior information about the signal's energy. In the case where the conditions affecting the network do not change fast, the above assumptions are realistic. Furthermore, in the cases where we know the position of the target (i.e., we know where the phenomenon to be detected happens), the assumption for the knowledge of the ξ_i is a valid assumption. Our proposed scheme can be used to detect a spatial resonance in a bridge, to detect a fire event in a factory to name just a few.

3.4.1 Weight Combining Optimisation

Further, via the transformation $\boldsymbol{\beta}=\mathbf{G}^{1/2}\boldsymbol{\alpha}$, the deflection coefficient (3.4.1) becomes:

$$\tilde{d^2}\left(\boldsymbol{\beta},\boldsymbol{p}\right)=\frac{\boldsymbol{\beta}^T\mathbf{M}\boldsymbol{\beta}}{||\boldsymbol{\beta}||^2},\ \mathbf{M}=\mathbf{G}^{-T/2}\boldsymbol{r}\boldsymbol{r}^T\mathbf{G}^{-1/2}. \tag{3.4.3}$$

So $\boldsymbol{\alpha}_{opt} = \mathbf{G}^{-1/2}\boldsymbol{\beta}_{opt} = k\mathbf{G}^{-1}\boldsymbol{r}$, where $\boldsymbol{\beta}_{opt} = k\mathbf{G}^{-1/2}\boldsymbol{r}$ is the normalized eigenvector corresponding to the maximum eigenvalue of $\mathbf{M}$. Also, we can easily show that:

$$\boldsymbol{\alpha}_{opt} = k \begin{bmatrix} \frac{N\sigma_1^2\xi_1}{2N\sigma_1^4(1+2\xi_1)+\sigma_{v_1}^2} \\ \frac{N\sigma_2^2\xi_1}{2N\sigma_2^4(1+2\xi_1)+\sigma_{v_2}^2} \\ \vdots \\ \frac{N\sigma_M^2\xi_M}{2N\sigma_M^4(1+2\xi_M)+\sigma_{v_M}^2} \end{bmatrix}. \tag{3.4.4}$$

So now (3.4.4) establishes a relationship between the optimum weighting vector ($\boldsymbol{\alpha}_{opt}$) and the sensor transmit power ($\boldsymbol{p}$) through the $\sigma_{v_i}^2$ quantity (see definition (3.3.1) and (3.3.3)).

3.4.2 Centralized Optimum Power Allocation

We now substitute $\boldsymbol{\alpha}_{opt}$ ($k = 1$) back into (3.4.1) and we then have the following optimization problem to obtain $\boldsymbol{p}_{opt}$:

$$\begin{aligned} \boldsymbol{p}_{opt} &= \arg \max_{\boldsymbol{p}} \left(\tilde{d}^2 \left(\boldsymbol{\alpha}_{opt}, \boldsymbol{p} \right) \right) \\ &\text{subject to} \sum_{i=1}^{M} p_i \leq P_t \text{ for } \; p_i \geq 0, \; i = 1, 2, \ldots, M \end{aligned} \tag{3.4.5}$$

which is easily shown to be equivalent to (3.4.6):

$$\begin{aligned} &\underset{\boldsymbol{p}}{\text{maximize}} \left(\sum_{i=1}^{M} \frac{N^2\sigma_i^4\xi_i^2}{2N\sigma_i^4\left(1+2\xi_i\right) + \frac{U^2}{3\left(1+\frac{p_i h_i^2}{\zeta_0}\right)}} \right) \\ &\text{subject to} \quad \sum_{i=1}^{M} p_i \leq P_t, \; p_i \geq 0, \; i = 1, 2, \ldots, M. \end{aligned} \tag{3.4.6}$$

The aim of solving the above optimization problem is to distribute in an optimum way the total SN transmit power[3] budget among M distributed SNs such that the probability of detection is maximized. We consider the total transmit power budget constraint in order to investigate the following: given a constant total transmit

[3]Here we only consider the power dissipation due to the test statistics transmission from the SNs to FC.

power budget (fixed transmission cost of our network) how we can maximize the probability of detection at the fusion center by controlling the SN transmit power (i.e., the number of active SNs)? As it will be shown later in the simulations results by controlling the transmit power in an optimum way we can select a number of active SNs while keeping those that have very poor SN to FC channels in sleeping mode. In this way, the SNs that require very high power will not transmit and so provide longer battery life. After justifying our constrain choice, (3.4.6) can be solved analytically using the Lagrangian function:

$$f(\boldsymbol{p},\lambda_0,\mu)=\sum_{i=1}^{M}\frac{N^2\sigma_i^4\xi_i^2}{2N\sigma_i^4\left(1+2\xi_i\right)+\frac{U^2}{3\left(1+\frac{p_ih_i^2}{\zeta_i}\right)}}-\lambda_0\left(\sum_{i=1}^{M}p_i-P_t\right)+\sum_{i=1}^{M}\mu_ip_i \tag{3.4.7}$$

and imposing the Karush-Kuhn-Tucker (K.K.T) conditions [90]:

$$0\in\frac{N^2\sigma_i^4\xi_i^2}{\left(2N\sigma_i^4\left(1+2\xi_i\right)+\frac{U^2}{3\left(1+\frac{p_ih_i^2}{\zeta_i}\right)}\right)^2}\times\frac{U^2\times\frac{h_i^2}{\zeta_i}}{3\left(1+\frac{p_ih_i^2}{\zeta_i}\right)^2}-\lambda_0+\mu_i \tag{3.4.8}$$

$$\lambda_0\left(\sum_{i=1}^{M}p_i-P_t\right)=0 \tag{3.4.9}$$

$$\sum_{i=1}^{M}p_i-P_t\leq 0 \tag{3.4.10}$$

$$\lambda_0\geq 0,\ \mu_ip_i=0,\ i=1,2,\ldots,M \tag{3.4.11}$$

$$\mu_i\geq 0,\ p_i\geq 0,\ i=1,2,\ldots,M. \tag{3.4.12}$$

Solving the K.K.T conditions in (3.4.8)-(3.4.12) gives:

$$p_{i,opt}=\left[\frac{1}{\sqrt{\lambda_0}}\left(\frac{\xi_iU\sqrt{3}}{6\sigma_i^2\left(1+2\xi_i\right)\sqrt{\frac{h_i^2}{\zeta_0}}}\right)-\frac{U^2}{6N\sigma_i^4\left(1+2\xi_i\right)\frac{h_i^2}{\zeta_0}}-\frac{\zeta_0}{h_i^2}\right]^+ \tag{3.4.13}$$

where $[x]^+$ equals 0 if $x < 0$, otherwise it equals x, and λ_0 can be evaluated in similar way as in [86] by imposing equality in the constraint $\sum_{i=1}^{M} p_i = P_t$ in (3.4.6).

3.5 Distributed Optimal Quantization and Power Allocation via Consensus for Centralized Detection

The straightforward solution to (3.4.6) is to obtain it in a centralized manner (i.e., at a FC), where the FC has full knowledge of the channel gains (h_i) which might change over time and need to be updated. In this section, we propose a distributed solution, where the SNs are limited to use local information to be able to decide if they should transmit any information to the FC or stay in sleeping mode.

3.5.1 Decentralized Optimum Power Allocation

We now propose a novel algorithm aimed at allocating the SN transmit power to the FC in a fully decentralized fashion. The Lagrangian function in (3.4.7) can be rewritten as follows:

$$f(\boldsymbol{p}, \lambda_0, \mu) = \sum_{i=1}^{M} f_i(p_i, \lambda_0) = \sum_{i=1}^{M} \left(\frac{N^2 \sigma_i^4 \xi_i^2}{2N\sigma_i^4 (1+2\xi_i) + \frac{U^2}{3\left(1+\frac{p_i h_i^2}{\zeta_i}\right)}} - \lambda_0 p_i + \frac{\lambda_0}{M} P_t \right). \tag{3.5.1}$$

Now, (3.5.1) is converted into M separable problems that can be solved in parallel using the dual ascent algorithm:

$$p_i[k+1] = \arg \min_{p_i} f_i(p_i, \lambda_0[k]) \tag{3.5.2}$$

$$\lambda_0[k+1] = \lambda_0[k] + \epsilon[k] \left(\sum_{i=1}^{M} p_i[k+1] - P_t \right). \tag{3.5.3}$$

For this formulation, we can see that step (3.5.2) can be evaluated in a closed form for SN i at iteration k by using only its own local information and shown to be:

$$p_i[k+1] = \left[\frac{1}{\sqrt{\lambda_0[k]}} \left(\frac{\xi_i U \sqrt{3}}{6\sigma_i^2 (1+2\xi_i) \sqrt{\frac{h_i^2}{\zeta_i}}} \right) - \frac{U^2}{6N\sigma_i^4 (1+2\xi_i) \frac{h_i^2}{\zeta_i}} - \frac{\zeta_i}{h_i^2} \right]^+. \tag{3.5.4}$$

The only step that requires an exchange of values among the SNs is the (3.5.3) step which requires the computation of the $\sum_{i=1}^{M} p_i[k+1]$ quantity at each SN. Because of the communication topology for the M SNs (i.e., not fully connected), we will use the average consensus algorithm [19] to ensure the availability of this term at each SN. In this chapter, we assume ideal exchange of information between the SNs that are connected and we assume there are no "overhearing" SNs.

As mentioned before, the centralized solution at the FC requires full knowledge of the channel gains (h_i) which might be time-varying and need to be always updated. It also requires the variance of AWGN (ζ_i) and each of the local SNRs (ξ_i). Moreover, the FC has to broadcast back to each SN the allocated SN transmit power which might be decoded with error due to fading. Furthermore, when the FC is battery operated, the centralized solution (at the FC) becomes inefficient and not scalable as the number of SNs increases. On the other hand, the proposed distributed algorithm (**Algorithm 3.6.1**) is fully scalable in terms of data exchange and SN processing complexity. We now define $\epsilon[k]$ to be the positive user defined step size and $\overline{p_i[k+1]} = \frac{1}{M}\sum_{i=1}^{M} p_i[k+1]$. The proposed algorithm is described in the next page.

3.6 Simulation Results

In this section, the proposed algorithm is evaluated numerically and compared to its centralized counterpart. Also, we choose $\lambda_0[0] = 10^{-8}$, $\forall i$, $\kappa = 10^{-7}$ and $\epsilon[k] = \lambda_0[k]/k$. We let all the σ_i^2 terms at each SN be different, such that $\xi_a = 10\log_{10}\left(\frac{1}{M}\sum_{i=1}^{M}\xi_i\right)$ = -3 dB, unless otherwise stated. In addition we let $\zeta_i = 0.1$ $\forall i$.

We compare the results with the matched filter detector[4] (MFD) and use this as a benchmark. The derivation of the optimum fusion rule and the optimum weights in (3.3.4) when the MFD local test statistics are used is given in Appendix A. We

[4]The test statistic is taken as: $T_i = \sum_{n=1}^{N} x_i(n)s_i(n)$, $\forall i = 1, 2, \ldots, M$. The global test statistic (T_f) at the FC has the same structure as (3.3.4) with $\alpha_i = \frac{\sum_{n=1}^{N} s_i^2(n)}{\sigma_i^2 \sum_{n=1}^{N} s_i^2(n) + \sigma_{v_i}^2}$, $\forall i = 1, 2, \ldots, M$. The optimum weights have been derived through the Likelihood Ratio Test (LRT) in Appendix A.

Algorithm 3.6.1: Optimizing the sensor nodes to fusion center transmit powers

STEP 1: Set $k = 0$, κ equal to a small positive value
and initialize $\lambda_0[0]$, $\forall i$;

STEP 2: Compute $p_i[1]$, $\forall i$ using (3.5.2);

STEP 3: Run consensus over $p_i[1]$ to get $\overline{p_i[1]}$;

STEP 4: Compute $\lambda_0[1]$ using (3.5.3);

STEP 5: Set $k = 1$;

STEP 6: Repeat until convergence

$$p_i[k+1] = \left[\frac{1}{\sqrt{\lambda_0[k]}}\left(\frac{\xi_i U\sqrt{3}}{6\sigma_i^2(1+2\xi_i)\sqrt{\frac{h_i^2}{\zeta_i}}}\right) - \frac{U^2}{6N\sigma_i^4(1+2\xi_i)\frac{h_i^2}{\zeta_i}} - \frac{\zeta_i}{h_i^2}\right]^+$$

Run consensus over $p_i[k+1]$ until convergence

$$\lambda_0[k+1] = \lambda_0[k] + \epsilon[k]\left(M\overline{p_i[k+1]} - P_t\right)$$

Set $k = k+1$, if convergence criterion is satisfied stop, otherwise go to step 6.

will also refer to "equal linear combining" in (3.3.4) (i.e., $\alpha_i = \frac{1}{\sqrt{M}}, \forall i$) and "equal power allocation" in (3.3.1) (i.e., $p_i = \frac{P_t}{M}, \forall i$). Finally, we choose L_i with equality in (3.3.1).

In Fig. 3.2, the two lower plots show the sensor transmit power p_i and the number of bits allocated to quantize T_i for the i^{th} sensor to the FC channel respectively. The actual channel coefficients (randomly chosen for $M = 10$) are in the upper plot. Clearly with optimum linear weighting in (3.3.4) we allocate more power and bits to the best channels unlike the non-optimum equal weighting. In the case of the optimum combining, SNs that have very bad channels (i.e., SNs that require very high power to transmit) will be censored (i.e., will not transmit even one bit).

In Fig. 3.3, as expected, increasing either the number of received samples (N) or the maximum power budget (P_t), improves the detection probability P_d. Furthermore, for large N, we can observe that detection probability improvement against P_t is negligible.

In Fig. 3.4, we illustrate how the detection probability P_d improves with increasing the number of SNs (M). And in Fig. 3.5, we re-examine Fig. 3.4 for $M = 10$ and compare optimal and non-optimal weighting, showing the advantage of optimal weighting over equal weighting in (3.3.4).

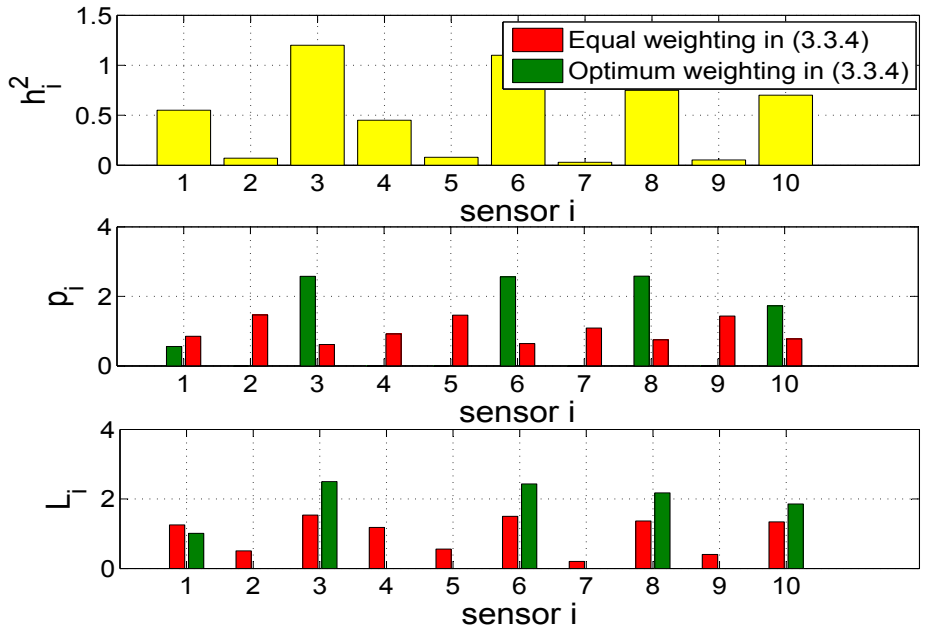

Figure 3.2: Equal weight ($\alpha_i = \frac{1}{\sqrt{M}}, \forall i$) and optimal weight combining ($\boldsymbol{\alpha} = \boldsymbol{\alpha}_{opt}$ in (3.4.4)) transmit power and channel quantization bits allocation for $P_{fa} = 0.1$, $P_t = 10$, $U = 0.1$, and $M = 10$.

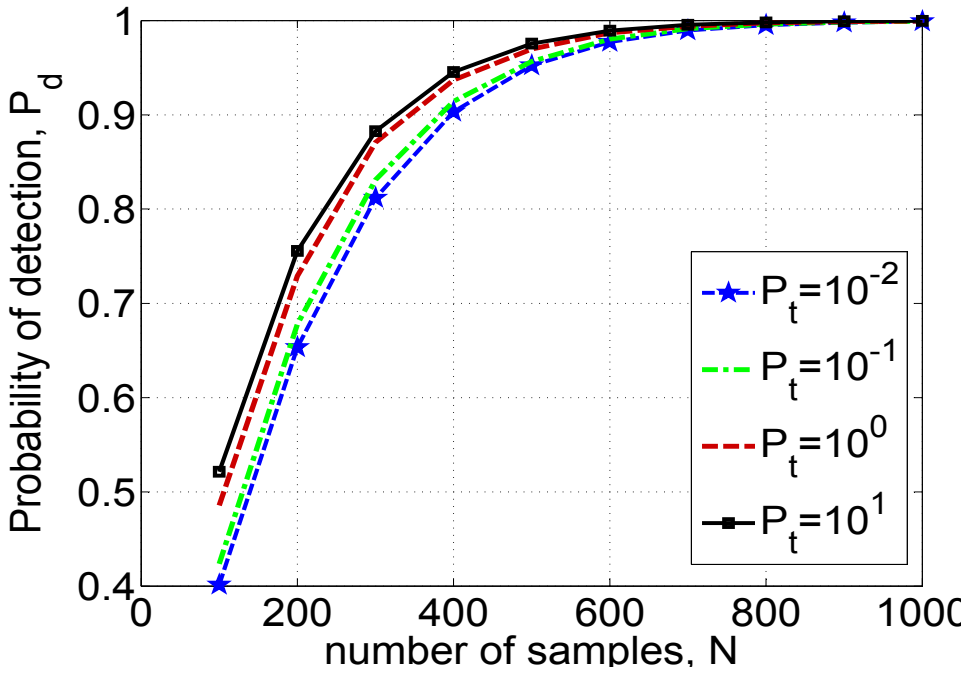

Figure 3.3: Probability of detection (P_d) for $P_{fa} = 0.1$, $M = 15$, $U = 0.2$ and optimum weight combining.

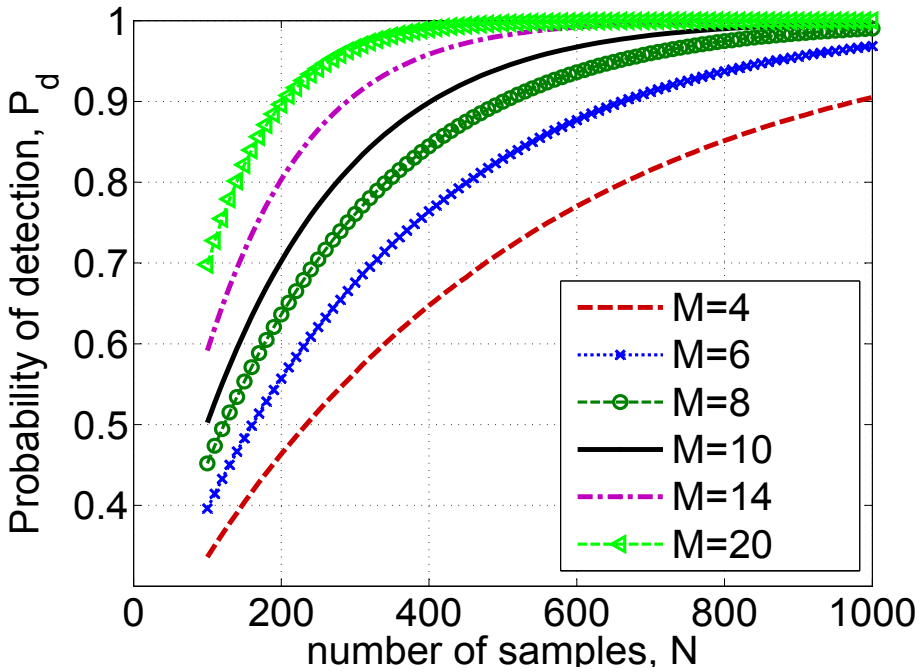

Figure 3.4: Probability of detection (P_d) for $P_{fa} = 0.1$, $P_t = 10$, $U = 0.1$ and optimum weight combining.

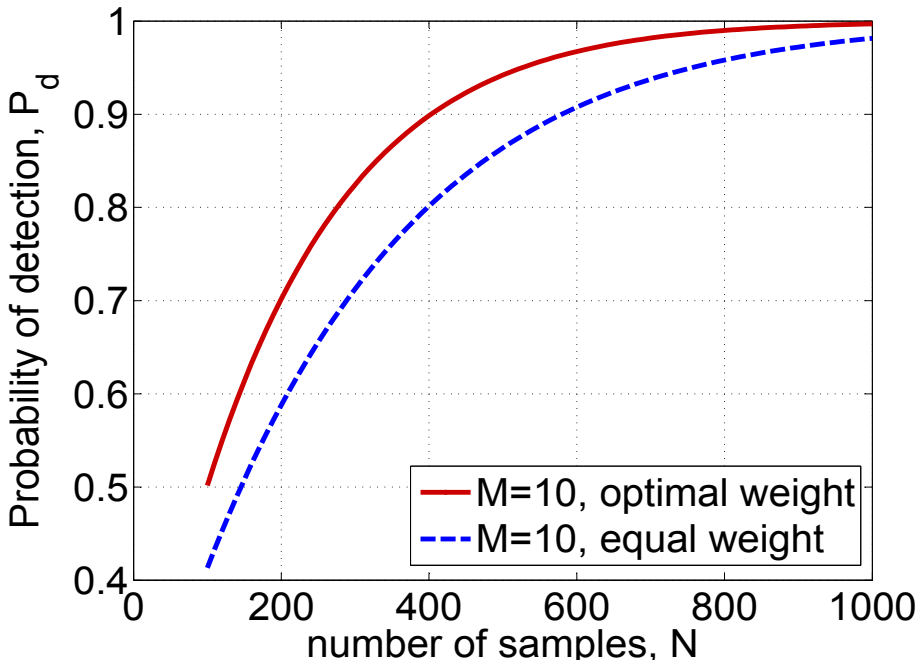

Figure 3.5: Probability of detection (P_d) for two different weighting schemes for $P_{fa} = 0.1$, $U = 0.1$ and $P_t = 10$.

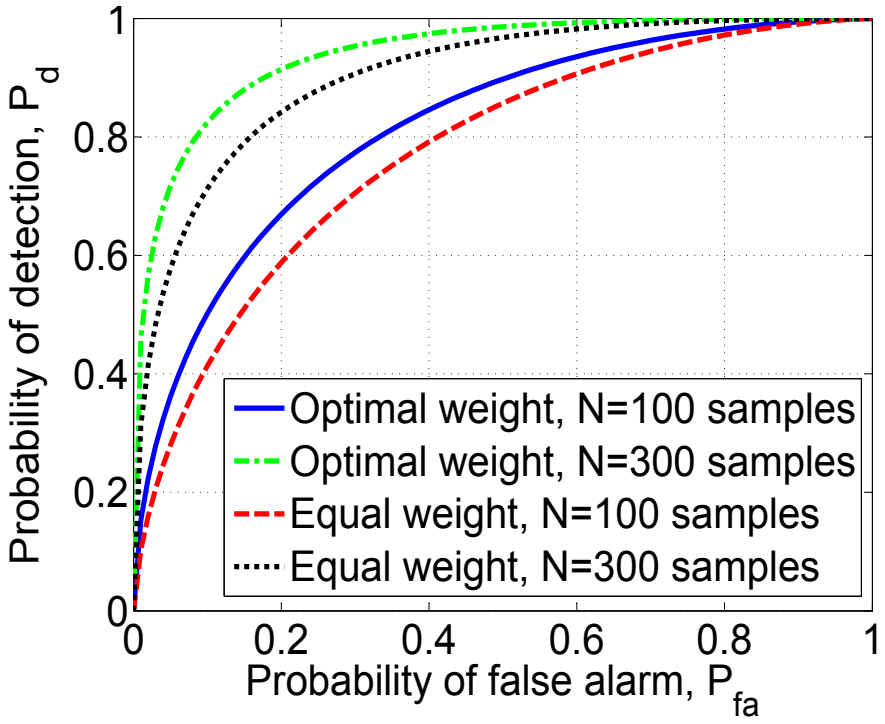

Figure 3.6: Receiver operating characteristic with $P_t = 10$, $U = 0.1$ and $M = 10$ for two different weighting schemes.

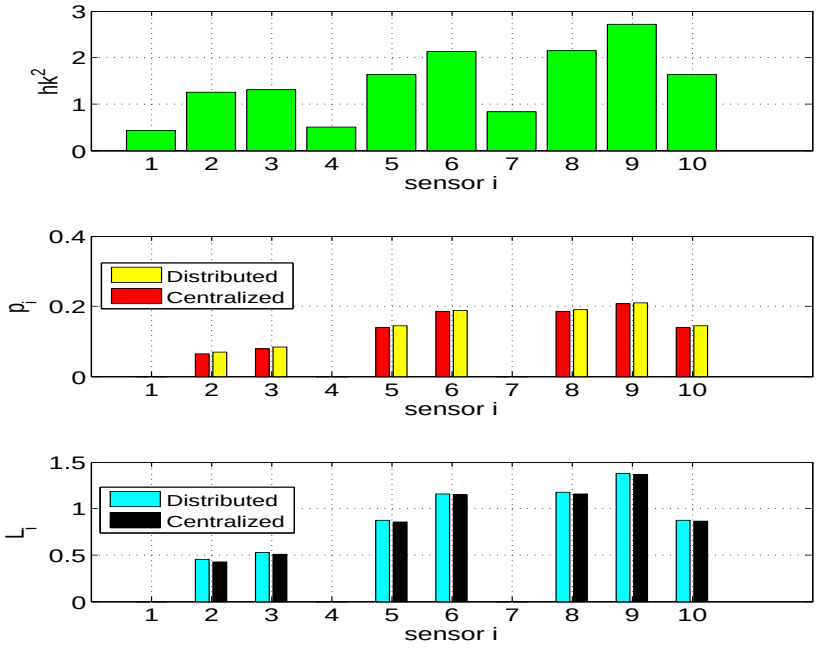

Figure 3.7: Centralized and decentralized sensor node transmit power and channel bit allocation for $P_{fa} = 0.1$, $P_t = 1$, $U = 3$, $\xi_a = -4$ dB, $N = 10$ and $s_i(n) = 0.2\ \forall i$.

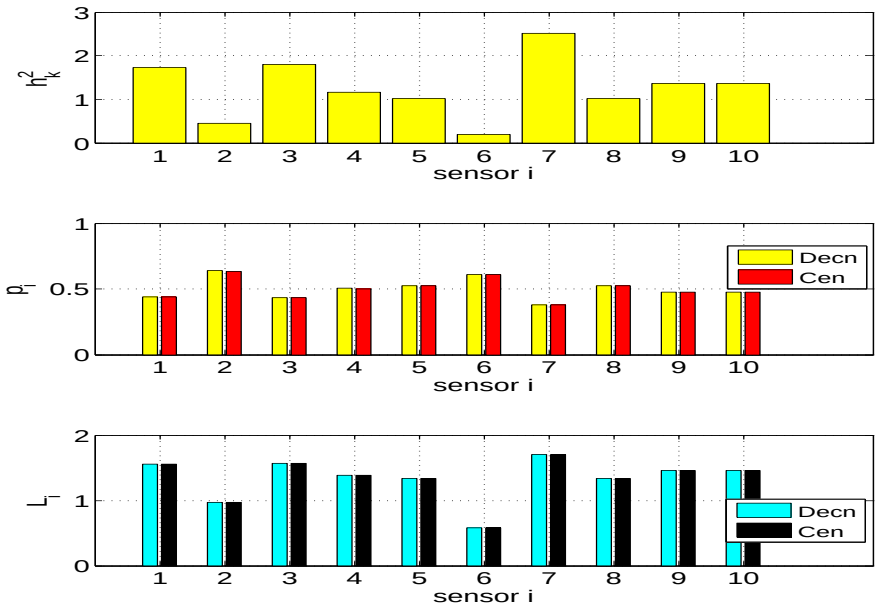

Figure 3.8: Centralized and decentralized sensor transmit power and channel bit allocation for $P_{fa} = 0.1$, $P_t = 5$, $U = 3$, $\xi_a = -1$ dB, $N = 50$ and $s_i(n) = 0.3\ \forall i$.

Fig. 3.6 shows the receiver operating characteristic (ROC) parametrized against the number of samples (N) for both optimal and equal weighting.

In Fig. 3.7, the middle plot shows the SN transmit power p_i for the i^{th} SN to the FC channel using two different approaches (i.e., distributed and centralized). The actual channel coefficients (randomly chosen) are in the upper plot in Fig. 3.7. Clearly, the performance of our proposed distributed method is very close to the centralized one. As expected, both centralized and decentralized methods allocate more power to the best channels. In this way, the nodes that have very bad channels (i.e., sensor nodes that require very high power to transmit) will be censored (i.e., will not transmit even a single bit).

In Fig. 3.8, we show that for a large number of samples (N) and equal SNs observation quality (more specifically for $s_i(n) = 0.3\ \forall i$) the optimum power allocation scheme tends to a uniform power allocation as expected (see the definition of $\mathbf{G}$ in Section 3.4). Clearly, when N is large, $\mathbf{G}$ will depend more on local ξ_i (which in this case are taken to be the same across the SNs) rather than $\sigma_{v_i}^2$ quantity. However, even in this case, still more quantization bits (i.e., larger information rate) are allocated to the best communication channels (for e.g., SN1, SN3, SN7).

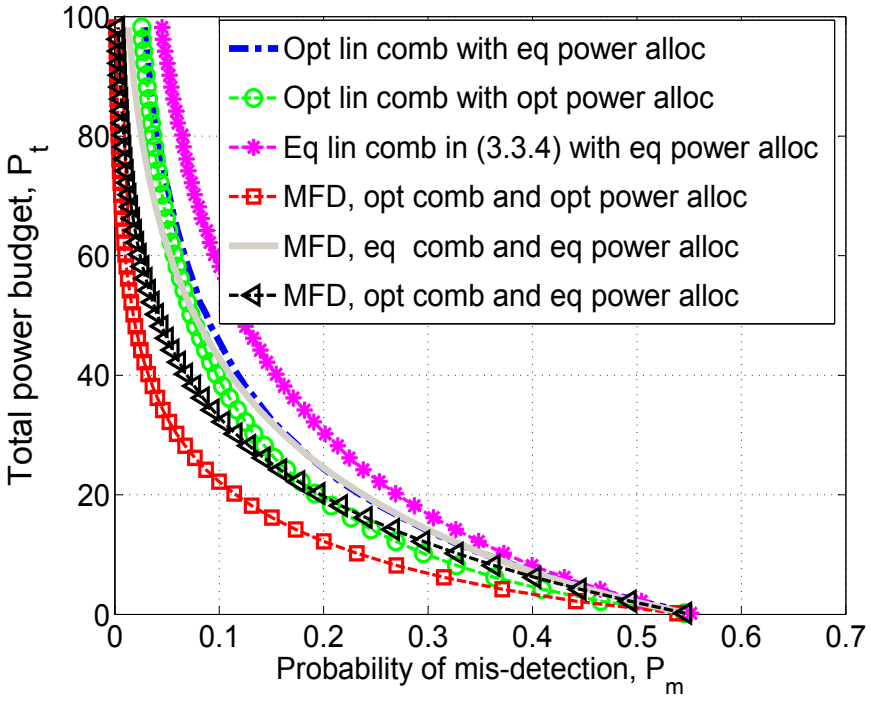

Figure 3.9: Total power budget (P_t) versus probability of mis-detection ($1 - P_d$), with $P_{fa} = 0.1$, $U = 3$, $\xi_a = -4$ dB, $N = 5$ and $M = 100$.

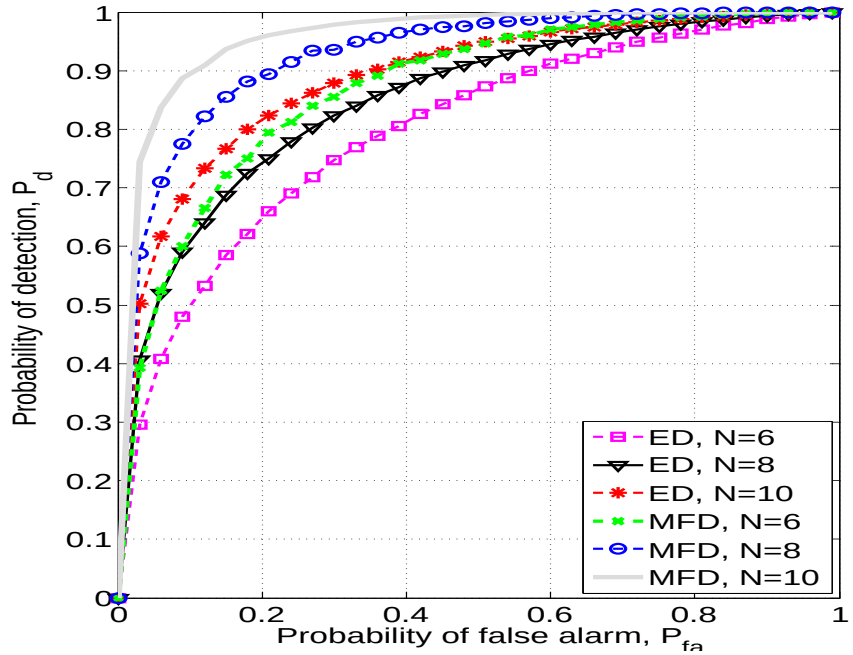

Figure 3.10: Probability of detection (P_d) versus probability of false alarm (P_{fa}), with $U = 3$, $\xi_a = -4$ dB, $P_t = 1$ and $M = 10$.

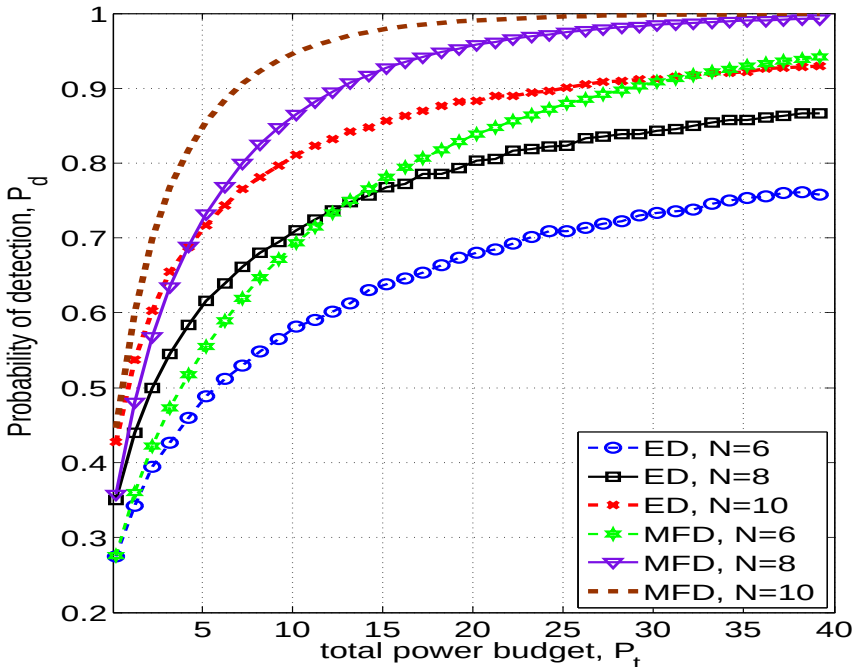

Figure 3.11: Probability of detection (P_d) versus total power budget (P_t), with $U = 3$, $\xi_a = -4$ dB, $P_{fa} = 0.1$ and $M = 20$.

Fig. 3.9 shows the total power budget (P_t) against the mis-detection (1-P_d) performance for 6 different schemes. The energy detector (ED) performance tends to converge to the matched filter detector for a low power budget (P_t).

Fig. 3.10 shows the receiver operating characteristic against the sample number (N). As expected, the matched filter detector outperforms the energy detector but it requires full knowledge of the useful signal.

And in Fig. 3.11, we examine the probability of detection (P_d) performance against the total power budget (P_t). As P_t increases, then P_d improves.

3.7 Chapter Summary and Conclusions

In this chapter, we have shown how to perform distributed detection, via SNs transmitting a quantized version of the received energy test statistic to the FC. In addition we have calculated the optimal linear combining coefficients at the FC and the optimal transmit power for each sensor in order to maximize P_d. Although we maximized the modified deflection coefficient (as an approximation to maximizing

P_d), the simulations have shown that this approach still allocates sensor transmit powers and quantization bits in a intuitively optimal way.

Then, we propose a novel distributed algorithm to calculate the optimal SN transmit power for each SN in order to maximize P_d. In this way, each SN can allocate its own transmit power by exchanging the information with its own neighbors. What makes this scheme very useful and attractive is that the only value that they should exchange among neighbors is their own transmit power at the current state. The algorithm is robust and easy implementable.

Chapter 4

Centralized Quantized Fusion Rules

IN THIS CHAPTER

Within this chapter, we address the problem of finding the optimal fusion rule that should be adopted by the FC for the centralized detection of an unknown deterministic spatially uncorrelated signal. The overview of the motivation behind this work is presented. The assumptions made and the problem formulation are similar to Chapter 3. The optimal fusion rule implementation requires $a-priori$ information that cannot usually be attained in practice. Motivated by this, majority of this chapter is dedicated to deriving sub-optimum but easy implementable fusion rules.

4.1 Introduction

4.1.1 Motivation

Distributed detection has been attracting significant interest in the context of WSNs [52] and [91]. This is due to the flexibility of WSNs, which can be seamlessly deployed over a wide geographic area for military monitoring and surveillance purpose [83]. However, WSNs suffer from constrained bandwidth and limited on-board power. This poses challenges in the design of distributed detection algorithms, especially

when the intruder's signature is unknown to the WSN. The main issue is to improve the detection by fusing the measurements provided by various SNs in a manner that efficiently utilizes the scarce bandwidth and overcomes the limitations of a fading wireless channel.

4.1.2 Related Work

There is a large literature reporting on the problem of decision over ideal parallel access channels (PACs) (e.g., [32, 61, 62] and references therein). Some optimum decision rules have been derived in the context of WSNs (e.g., [64], [65]) and in the context of spectrum sensing in cognitive radio networks (e.g., [32]). However, as the SNs are all battery operated (i.e., with limited energy available on-board) this assumption is unrealistic.

The problem of decentralized detection in bandwidth constrained sensor networks has been addressed in [92], where the authors investigated the design of sensor messages sent to the FC that minimize the error probability. The problem of detecting a known deterministic parameter is investigated in [93] under restricted channel capacity. The channel fading effect on distributed detection was tackled in [94]. In [85], the authors addressed both issues of limited bandwidth and channel imperfections. They optimized the transmission power, which consequently dictated the number of allocated bits, for the detection of a known signal. Decision fusion over Rayleigh fading channels is addressed in [29, 94]. Fusion of censored decisions is another approach to save power on limited bandwidth WSNs and is considered in a numerous research works (e.g., see [54, 95, 96] and references therein).

4.1.3 Chapter Contributions

In this chapter, we consider the problem of soft decision fusion in a bandwidth-constrained wireless sensor network (WSN). The WSN is tasked with the detection of an intruder transmitting an unknown signal over a fading channel. A binary hypothesis testing is performed using the soft decision of the sensor nodes (SNs). Using the likelihood ratio test, the optimal soft fusion rule at the fusion center (FC)

has been shown to be the weighted distance from the soft decision mean under the null hypothesis.

But as the optimal rule requires $a-priori$ knowledge that is difficult to attain in practice, suboptimal fusion rules are proposed that are realizable in practice. We show how the effect of quantizing the test statistic can be mitigated by increasing the number of SN samples size, i.e., bandwidth can be traded off against increased latency. Similarly, a simpler fusion rule is proposed based on the linear rule derived in Chapter 3. Then, the previous algorithms are revisited under noisy, flat fading channels with limited bandwidth. Finally, the SN's transmitted powers are optimized to achieve the best probability of detection.

4.1.4 Chapter Outline

This chapter is organized as follows. Section 4.2 presents the system model and the WSN communication architecture. Soft decision fusion rules are proposed in Section 4.3. The quantization effect is discussed in Section 4.4 and the optimal power allocation is derived in Section 4.5. Simulation results are given in Section 4.6 and conclusions are presented in Section 4.7.

4.2 Problem Formulation

In this section, we formulate the problem by first introducing and modeling the target as well as the WSN architecture adopted in this chapter. Then, the *centralized* detection set up is described.

4.2.1 System Model

Here we describe the target sensing, communication channel, and the WSN architecture.

Target Sensing

Identical to Chapter 3, in this chapter we consider a WSN with M sensor nodes reporting to a FC tasked with the detection of any intruders. The intruder leaves a

signature signal that is unknown to the WSN but it is assumed to be deterministic. The assumptions made regarding the target sensing are also identical to those stated in Chapter 3.

Communication Channel

Identical to Chapter 3, the communication between the local SNs and the FC are modeled as error-free (the SNs exchange quantized information matched to the channel capacity of each link) orthogonal flat fading channels and additive white Gaussian noise (AWGN) with a known variance ζ_i. Also, the assumptions considered regarding the communication channels are identical to those state in Chapter 3.

WSN Architecture

In this chapter we will use the same WSN architectures as in Chapter 3 shown in Fig. 3.1. As stated before, this is called a *centralized* architecture where there is a FC that communicates with spatially distributed SNs. In this chapter, different from Chapter 3, we do not program the SNs to communicate with each other (i.e., there are only SNs to FC communications).

4.3 Soft Decision Fusion Rules

In this section, the optimal soft decision fusion rule is investigated assuming infinite bandwidth for each WSN, i.e., no quantization is required. However, it turns out that the optimal rule requires prior information about the signal's energy, which cannot be known in practice. Hence, suboptimal rules are proposed as an implementable alternative.

4.3.1 Optimal Fusion Rule

For optimal detection, the SNs should send their measurements to the FC, where the ultimate detection decision about the intruder's presence will be made. However, this approach is not always feasible in the context of WSNs due to the limited bandwidth available. Thus, the WSN adopts a distributed detection algorithm in

which the SNs send their quantized soft decisions (i.e., the quantized local test statistics) to the FC, which combines them to arrive at the global decision. Since the intruder's signal is unknown at the SNs, the optimal detector in this case would be the energy detector, which is implemented at the i^{th} SN as follows:

$$T_i = \sum_{n=1}^{N} \left(y_i\left(n\right)\right)^2. \tag{4.3.1}$$

Given the local soft test statistic defined in (4.3.1), the optimal fusion rule follows from the likelihood ratio test (LRT):

$$\mathrm{LRT}\left(\boldsymbol{T}\right) = \frac{p\left\{T_1, T_2, ..., T_M|\mathcal{H}_1\right\}}{p\left\{T_1, T_2, ..., T_M|\mathcal{H}_0\right\}} \geq \gamma \tag{4.3.2}$$

where $p\left\{T_1, T_2, ..., T_M|\mathcal{H}_j\right\}$ is the joint probability distribution of local soft decisions under the j^{th} hypothesis. However, T_i has a χ^2 distribution under $\mathcal{H}_0$ and a non-central χ^2 under $\mathcal{H}_1$, which means evaluation of the LRT in (4.3.2) is complicated. Consequently, we invoke the central limit theorem to simplify the distribution of T_i when N is sufficiently large. So the distribution of any T_i can be adequately approximated by a Gaussian distribution with mean and variance given in (3.2.4) and (3.2.5). Since the noise at different SNs is independent, it can easily be shown (similar to the Proof given in Appendix A) that the log-likelihood ratio test (LLRT) takes the form

$$T_f = \sum_{i=1}^{M} \left(\frac{\left(T_i - N\sigma_i^2\right)^2}{2N\sigma_i^4} - \frac{\left(T_i - N\sigma_i^2\left(1+\xi_i\right)\right)^2}{2N\sigma_i^4\left(1+2\xi_i\right)} \right) \geq \gamma' \tag{4.3.3}$$

where $\gamma' = 2\ln\left(\prod_{i=1}^{M}\gamma\left(\frac{\sqrt{2N\sigma_i^4}}{\sqrt{2N\sigma_i^4(1+2\xi_i)}}\right)\right)$. The LLRT can be further simplified by completing the square in (4.3.3) to yield

$$T_f = \sum_{i=1}^{M} a_i \left(T_i - b_i\right)^2 \tag{4.3.4}$$

$$a_i = \frac{\xi_i}{N\sigma_i^4\left(1+2\xi_i\right)} \tag{4.3.5}$$

$$b_i = \frac{N\sigma_i^2}{2}. \tag{4.3.6}$$

The fusion rule in (4.3.4) has an interesting interpretation. It is, in fact, the *weighted distance* in the M-dimensional space between the local soft test statistic and half of

its mean under the null hypothesis (see (3.2.4) and (3.2.5)). It is also clear that SNs with lower noise get more weight in the fusion process. Another interesting note here is that at high SNR (ξ_i) the weight a_i depends only on the noise power at the SN and not on the measured signal energy.

4.3.2 Suboptimal Fusion Rules

Now, the performance evaluation and threshold computation of the optimal fusion rule in (4.3.4) are mathematically intractable, since the probabilities of detection (P_d) and the false alarm (P_{fa}) does not posses closed-form solutions. Hence, one has to use Monte Carlo simulations for evaluation. Furthermore, the computational complexity of (4.3.4) increases significantly as the number of SNs gets larger. To make the matter worst, the optimal fusion rule in (4.3.4) requires the exact knowledge of the SNR (ξ_i), which is difficult to be obtained in practice. However, its structure can be used to formulate low complexity suboptimal rules. So now we propose three suboptimal rules: weighted fusion, equal fusion and optimum linear fusion.

Weighted and Equal Fusion Rules

The weighted fusion rule takes the same structure as (4.3.4). However (for large ξ_i) a_i in (4.3.5) is replaced by $a_i^w = 1/2N\sigma_i^4$ and we let $b_i^w = b_i$. This rule approaches the optimal one when the SNR is large, as discussed earlier.

As for the equal fusion rule, equal weight is given for all the SNs, i.e., $a_i^e = 1$ for all $i = 1, 2, \cdots, M$. Also, $b_i^e = b_i$.

Optimum Linear Fusion Rule

The main motivation behind the linear combining rule consideration is that the probability of detection and the probability of false alarm metrics are obtained in closed-form. This gives insight into the design of the system's parameters, whereas for the LRT-based detector (4.3.4), analytically analyzing the detection performance

is not tractable. Now we examine the (sub-optimal) linear fusion rule:

$$T_f^l = \sum_{i=1}^{M} \alpha_i T_i \tag{4.3.7}$$

and the optimal weights to maximize the probability of detection are

$$\alpha_i = \frac{\xi_i}{N\sigma_i^2\left(1+2\xi_i\right)}. \tag{4.3.8}$$

The derivation and a detailed discussion can be found in Chapter 3. However, the above optimum linear combining fusion rule may not be implementable in practice or may have limited application as it requires $a-priori$ knowledge of ξ_i. In such situations, derivation of sub-optimum fusion rules are highly motivated.

4.4 Quantized Soft Decision Fusion Rule

The previous fusion rules assume the availability of an infinite bandwidth to send the exact T_i to the FC. Now (due to limited bandwidth and transmit power), we assume that the local soft test statistic T_i is quantized with L_i bits and transmitted to the FC with power p_i over a wireless channel (similar to Chapter 3). We will assume that the maximum channel capacity is utilized by the SNs. So our objective is to find the best soft fusion rule first, and then optimize the allocated power to maximize the detection probability. As in Chapter 3, we let the quantized test statistic ($\hat{T}_i$) at the i^{th} sensor be modeled (with L_i bits) as

$$\hat{T}_i = T_i + v_i \tag{4.4.1}$$

where v_i[1] is the quantization noise with uniform distribution in the interval $[-B, B]$ and variance

$$\sigma_{v_i}^2 = \frac{B^2}{3\times 2^{2L_i}}. \tag{4.4.2}$$

However, the distribution of $\hat{T}_i$ can be approximated [88] by a Gaussian distribution with mean and variance:

$$\begin{aligned} \mathbb{E}\left\{\hat{T}_i|\mathcal{H}_0\right\} &= N\sigma_i^2, & \mathrm{Var}\left\{\hat{T}_i|\mathcal{H}_1\right\} &= 2N\sigma_i^4\left(1+2\xi_i\right)+\sigma_{v_i}^2 \\ \mathbb{E}\left\{\hat{T}_i|\mathcal{H}_1\right\} &= N\sigma_i^2\left(1+\xi_i\right), & \mathrm{Var}\left\{\hat{T}_i|\mathcal{H}_0\right\} &= 2N\sigma_i^4+\sigma_{v_i}^2. \end{aligned} \tag{4.4.3}$$

[1] v_i is the quantization noise independent of $w_i(n)$ (in (3.2.1) and (3.2.2)) for all n and i.

4.4.1 Quantized Optimal/Suboptimal Fusion Rules

As stated before, the distribution of $\hat{T}_i$'s can be approximated by a Gaussian distribution with mean and variance given in (4.4.3). Then, in a similar manner to Section 4.3, the log-likelihood ratio test with quantization can be shown (similar to the Proof given in Appendix A) to be

$$T_f^q = \sum_{i=1}^{M} \left(\frac{\left(\hat{T}_i - N\sigma_i^2\right)^2}{2N\sigma_i^4 + \sigma_{v_i}^2} - \frac{\left(\hat{T}_i - N\sigma_i^2\left(1+\xi_i\right)\right)^2}{2N\sigma_i^4\left(1+2\xi_i\right) + \sigma_{v_i}^2} \right) \geq \gamma'' \tag{4.4.4}$$

where $\gamma'' = 2\ln\left(\prod_{i=1}^{M} \gamma\left(\frac{\sqrt{2N\sigma_i^4+\sigma_{v_i}^2}}{\sqrt{2N\sigma_i^4(1+2\xi_i)+\sigma_{v_i}^2}}\right)\right)$. As before, (4.4.4) can be now written in the following form

$$T_f^q = \sum_{i=1}^{M} a_i^q \left(\hat{T}_i - b_i^q\right)^2 \tag{4.4.5}$$

$$a_i^q = \frac{\xi_i}{N\sigma_i^4\left(1+2\xi_i+\frac{\sigma_{v_i}^2}{2N\sigma_i^4}\right)\left(1+\frac{\sigma_{v_i}^2}{2N\sigma_i^4}\right)} \tag{4.4.6}$$

$$b_i^q = \frac{N\sigma_i^2}{2} - \frac{\sigma_{v_i}^2}{4\sigma_i^2}. \tag{4.4.7}$$

Note that $T_f^q \to T_f$ as $\sigma_{v_i}^2 \to 0$ for all i. Consequently, $a_i^q \to a_i$ and $b_i^q \to b_i$ under the previous condition as well. More interestingly however, is that $T_f^q \to T_f$ as $N \to \infty$, regardless of $\sigma_{v_i}^2$. This implies that bandwidth can be saved but at the expense of increasing both the number of collected measurements and also the detection delay.

As for the suboptimal (quantized) fusion rule, it can be easily shown that

$$a_i^{wq} = \frac{1}{N\sigma_i^4\left(1+\frac{\sigma_{v_i}^2}{2N\sigma_i^4}\right)^2} \tag{4.4.8}$$

$a^{eq} = 1$ and $b^{eq} = b^{wq} = b_i^q$.

4.4.2 Quantized Optimal Linear Fusion Rule

The quantized version of the linear fusion weights in (4.3.8) can be shown to be [35]

$$\alpha_i^q = \frac{\xi_i}{2\sigma_i^2\left[1+2\xi_i+\frac{\sigma_{v_i}^2}{N\sigma_i^2}\right]}. \tag{4.4.9}$$

If the SNR is large, i.e., when either $\sigma_{v_i}^2 \to 0$ or $N \to \infty$ then it follows that $\alpha_i^q \to \alpha_i$.

4.5 Optimum Sensor Transmit Power Allocation

The performance of the proposed quantized fusion rules approach the performance of their unquantized counterparts if the number of (test statistic) bits is sufficiently large. However, this entails a large transmission power as predicted by (3.3.1). So, we desire to strike a trade-off between the fusion rule's performance and the transmit power. To this end, we first need to adopt an optimization criterion. A natural one is the probability of detection, which depends on the distribution of the fusion rule. So letting $\mho_i = \left(\hat{T}_i - b_i^q\right)^2$, then the optimum fusion rule (4.4.5) can be written as

$$T_f^q = \sum_{i=1}^{M} a_i^q \mho_i. \tag{4.5.1}$$

The mean and variance of $\mho_i$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ are now given in (4.5.2) and (4.5.3) respectively:

$$\begin{aligned}
\mathbb{E}\left\{\mho_i|\mathcal{H}_0\right\} &= 2N\sigma_i^4 + N^2\sigma_i^4 + \sigma_{v_i}^2 - 2b_i^q N\sigma_i^2 + \left(b_i^q\right)^2 \\
\mathbb{E}\left\{\mho_i|\mathcal{H}_1\right\} &= \mathbb{E}\left\{\hat{T}_i|\mathcal{H}_1\right\}^2 + \mathrm{Var}\left\{\hat{T}_i|\mathcal{H}_1\right\} - 2b_i^q\left(N\sigma_i^2 + N\sigma_i^2\xi_i\right) + \left(b_i^q\right)^2
\end{aligned} \tag{4.5.2}$$

$$\begin{aligned}
\mathrm{Var}\left\{\mho_i|\mathcal{H}_0\right\} &= \mathrm{Var}\left\{\hat{T}_i|\mathcal{H}_0\right\}\left[4N^2\sigma_i^4 + 2\mathrm{Var}\left\{\hat{T}_i|\mathcal{H}_0\right\} + 4\left(b_i^q\right)^2 - 8Nb_i^q\sigma_i^2\right] \\
\mathrm{Var}\left\{\mho_i|\mathcal{H}_1\right\} &= 4\mathbb{E}\left\{\hat{T}_i|\mathcal{H}_1\right\}^2 \mathrm{Var}\left\{\hat{T}_i|\mathcal{H}_1\right\} + 2\mathrm{Var}\left\{\hat{T}_i|\mathcal{H}_1\right\}^2 \\
&\quad + 4\left(b_i^q\right)^2 \mathrm{Var}\left\{\hat{T}_i|\mathcal{H}_1\right\} - 8b_i^q\mathbb{E}\left\{\hat{T}_i|\mathcal{H}_1\right\}\mathrm{Var}\left\{\hat{T}_i|\mathcal{H}_1\right\}.
\end{aligned} \tag{4.5.3}$$

Using the central limit theorem, T_f^q can be approximated by a Gaussian distribution

$$T_f^q \sim \begin{cases} \mathcal{N}\left(\mathbb{E}\left\{T_f^q|\mathcal{H}_0\right\}, \mathrm{Var}\left\{T_f^q|\mathcal{H}_0\right\}\right) \text{ under } \mathcal{H}_0 \\ \mathcal{N}\left(\mathbb{E}\left\{T_f^q|\mathcal{H}_1\right\}, \mathrm{Var}\left\{T_f^q|\mathcal{H}_1\right\}\right) \text{ under } \mathcal{H}_1 \end{cases} \tag{4.5.4}$$

where

$$\begin{aligned}
\mathbb{E}\left\{T_f^q|\mathcal{H}_0\right\} &= \sum_{i=1}^{M} a_i^q \mathbb{E}\left\{\mho_i|\mathcal{H}_0\right\} \\
\mathbb{E}\left\{T_f^q|\mathcal{H}_1\right\} &= \sum_{i=1}^{M} a_i^q \mathbb{E}\left\{\mho_i|\mathcal{H}_1\right\} \\
\mathrm{Var}\left\{T_f^q|\mathcal{H}_0\right\} &= \sum_{i=1}^{M} \left(a_i^q\right)^2 \mathrm{Var}\left\{\mho_i|\mathcal{H}_0\right\} \\
\mathrm{Var}\left\{T_f^q|\mathcal{H}_1\right\} &= \sum_{i=1}^{M} \left(a_i^q\right)^2 \mathrm{Var}\left\{\mho_i|\mathcal{H}_1\right\}.
\end{aligned} \tag{4.5.5}$$

It can be readily shown that the detection probability as a function of the false alarm probability has the form

$$P_d = Q\left(\frac{Q^{-1}\left(P_{fa}\right)\sqrt{\mathrm{Var}\left\{T_f^q|\mathcal{H}_0\right\}} - \Psi}{\sqrt{\mathrm{Var}\left\{T_f^q|\mathcal{H}_1\right\}}}\right) \tag{4.5.6}$$

where $Q(\cdot)$ is the Q-function and $\Psi = \mathbb{E}\left\{T_f^q|\mathcal{H}_1\right\} - \mathbb{E}\left\{T_f^q|\mathcal{H}_0\right\}$. The probability of detection implicitly depends on the transmission power through the relationships (4.5.2), (4.5.3) and (4.5.5). Based on this, we can optimize the transmission powers (p_i) to maximize P_d under the constraint of a maximum aggregate transmit power budget (P_t):

$$\begin{aligned} \boldsymbol{p}_{opt} = \ & \arg \ \max_{\boldsymbol{p}} P_d\left(\boldsymbol{p}\right) \\ & \text{subject to} \sum_{i=1}^{M} p_i \leq P_t \text{ for } \ p_i \geq 0, \ i = 1, \ldots, M \end{aligned} \tag{4.5.7}$$

where $\boldsymbol{p} = [p_1, p_2, \ldots, p_M]$. Now (4.5.7) is difficult to solve and there is no closed form solution. Hence, we propose a numerical solution by adopting the spatial branch-and-bound strategy [97] using the YALMIP optimization tools [98].

In the first step of the algorithm, we start by applying a standard nonlinear solver to obtain a locally optimal solution and then set it as an upper bound on the achievable objective. Secondly, in each node, a convex relaxation of the model is derived, and the resulting convex optimization problem is solved. We then assign this as a lower bound. Bound tightening using [98] is applied iteratively to detect and eliminate redundant constraints and variables, and tighten the bounds where possible. The algorithm outline is summarized in **Algorithm 4.5.1**.

The aim of the algorithm is to obtain the global minimum of the function $\beta\left(\boldsymbol{p}\right) = \frac{Q^{-1}\left(P_{fa}\right)\sqrt{\mathrm{Var}\left\{T_f^q|H_0\right\}} - \Psi}{\sqrt{\mathrm{Var}\left\{T_f^q|H_1\right\}}}$ over the solution space $\wp_{start}$ where $\boldsymbol{p} \in \wp_{start}$. For any $\wp \subseteq \wp_{start}$ we define F_{lb} (the lower bound) and F_{ub} (the upper bound) as functions that satisfy: $F_{lb}\left(\wp\right) \leq F_{min}\left(\wp\right) \leq F_{ub}\left(\wp\right)$. Then, the global optimum solution $\beta^* = F_{min}\left(\wp_{start}\right) = \inf_{\boldsymbol{p}\in\wp_{start}} \beta\left(\boldsymbol{p}\right)$.

We now define ϵ to be a small positive constant and $\boldsymbol{p}_{init}$ is the random initialization of the vector $\boldsymbol{p}$. We assume that the fusion center (FC) has full knowledge of the channel gains (h_i) quantity from sensors to FC. In the case where the conditions affecting the network do not change fast, the above assumption is realistic.

Algorithm 4.5.1: Optimum sensor node transmit power allocation

STEP1: Decide the upper bound and the lower bound of the global optimum solution β^* :

- set the upper bound: $U_o = F_{ub}(\wp_{start})$

F_{ub} is implemented using ***fmincon*** function in the optimization toolbox of Matlab by inputing a feasible solution $\boldsymbol{p}_{init}$ at the starting point.

- set the lower bound: $L_o = F_{lb}(\wp_{start})$

F_{lb} is implemented by deriving a convex relaxation of the problem by using Yalmip [98] and then using the ***linprog*** function in the optimization toolbox.

- if U_o-$L_o \leq \epsilon$ stop, the global optimum solution is within the acceptable range. Otherwise go to STEP2;

STEP2: Split $\wp_{start}$ into two nodes: $\wp_{start} = \wp_1 \cup \wp_2$;

STEP3: Evaluate $F_{ub}(\wp_i)$ and $F_{lb}(\wp_i)$ for $i = 1, 2$;

STEP4: Update the bounds:

- $U_1 = \min\{F_{ub}(\wp_1), F_{ub}(\wp_2)\}$;
- $L_1 = \min\{F_{lb}(\wp_1), F_{lb}(\wp_2)\}$;
- if U_1-$L_1 \leq \epsilon$ stop, the global optimum solution is within the acceptable range. Otherwise go to STEP5;

STEP5: Perform bound propagation using Yalmip and update the lower bound

- if U_1-$L_1 \leq \epsilon$ stop, the global optimum solution is within the acceptable range. Otherwise go to STEP6;

STEP6: Estimate $\wp^* = \arg\min\{F_{lb}(\wp_1), F_{lb}(\wp_2)\}$

- split $\wp^*$ into two nodes: $\wp^* = \wp_1 \cup \wp_2$ and go to STEP3;

4.6 Simulation Results

We simulate a WSN of M SNs detecting an intruder with $s_i(n) = A$, where $A = 0.1$. The communication noise variances are arbitrarily set to $\zeta_i = 0.1$ for all $i = 1, 2, \cdots, M$ (for simplicity). The measurement noise variances are generated randomly and used throughout all the simulations. The average measurement SNR for the network is defined as $\xi_a = 10 \log_{10} \left(\frac{1}{M} \sum_{i=1}^{M} \xi_i \right)$. In all simulations we assume perfect knowledge of ξ_i.

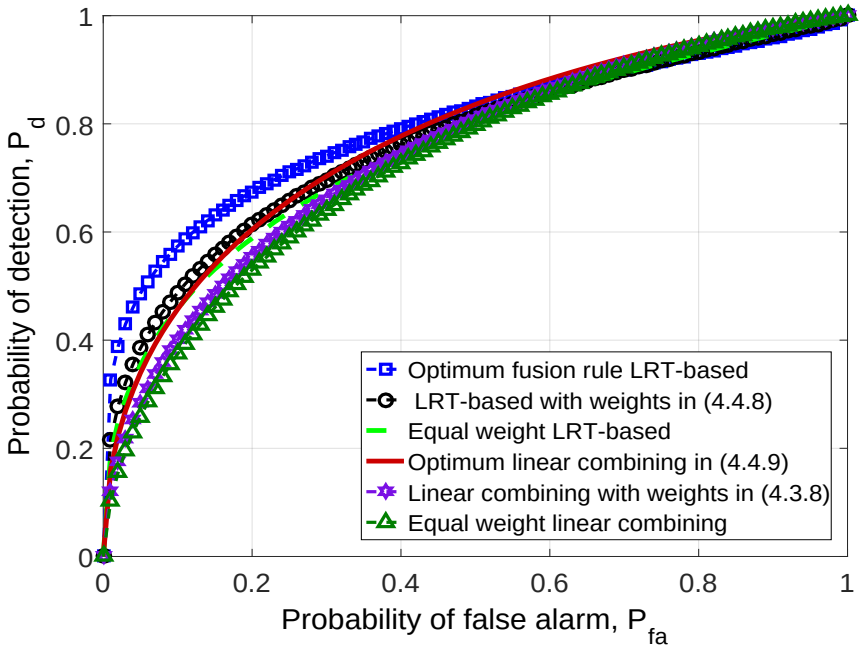

Figure 4.1: Receiver operating characteristics of six different fusion rules for $N = 10$, $M = 10$, $\xi_a = -8.5$ dB and $B = 0.5$.

Fig. 4.1 shows the receiver operating characteristic (ROC) curve for six different fusion rules. It is clear that the optimal fusion rule attains the best performance for ($\xi_a = -8.5$ dB) whereas the worst performance is that of the equal weight linear combining rule. However, all the rules converge when the parameter P_{fa} increases.

In Fig. 4.2 the effect of the number of measurement samples (N) on P_d is shown at a fixed P_{fa}. Obviously, as N increases P_d improves for all algorithms. Interestingly, the optimal linear fusion rule outperforms the suboptimal LRT-based one. This is explained by the structure of (4.4.8) where for large (but finite) N the effect of $\sigma^2_{v_i}$ (quantization noise variance) is still noticeable.

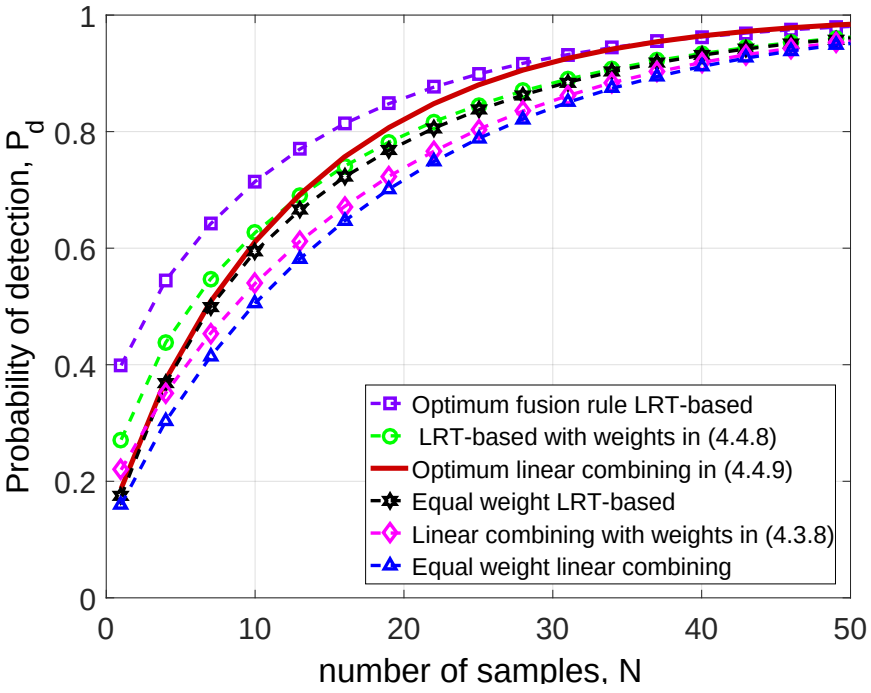

Figure 4.2: Probability of detection (P_d) versus the number of samples (N) with $M = 20$, $P_{fa} = 0.1$, $B = 0.5$ and $\xi_a = -8.5$ dB.

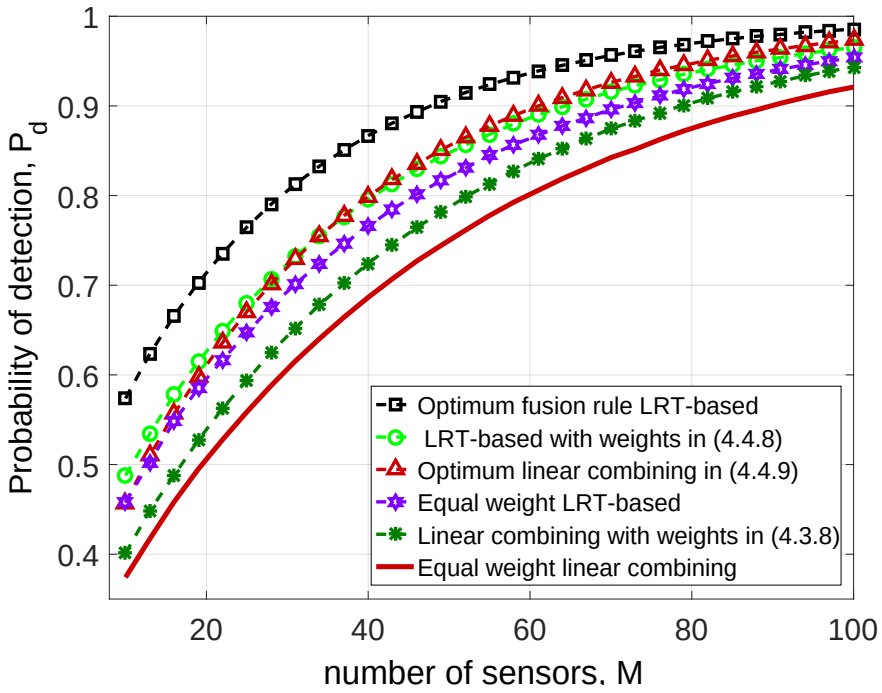

Figure 4.3: Probability of detection (P_d) versus number of sensors (M) for $N = 10$, $P_{fa} = 0.1$, $\xi_a = -8.5$ dB and $B = 0.5$.

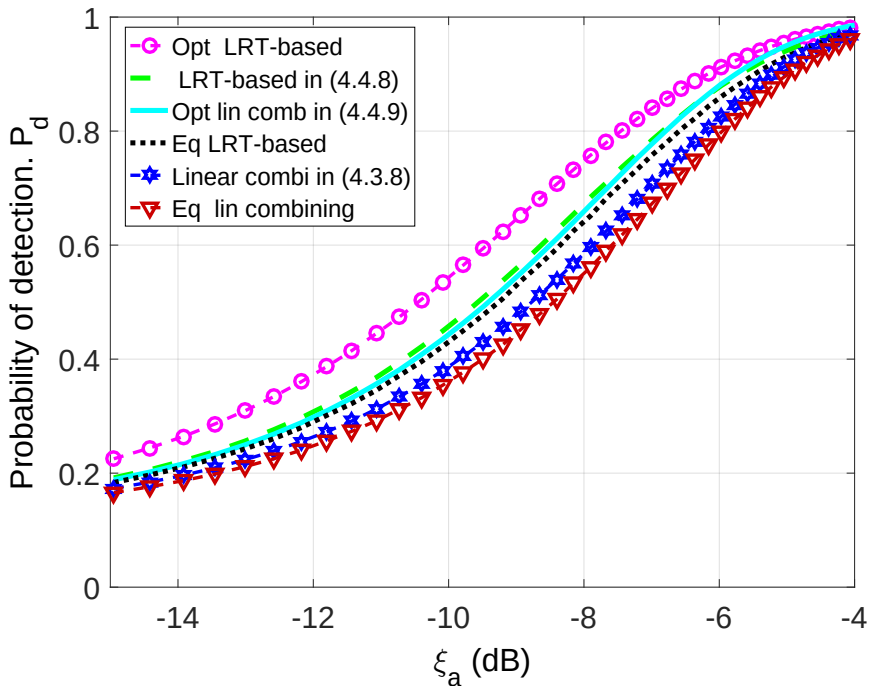

Figure 4.4: Probability of detection (P_d) versus the signal to noise ratio (ξ_a) for $M = 20$, $N = 10$, $P_{fa} = 0.1$ and $B = 0.5$.

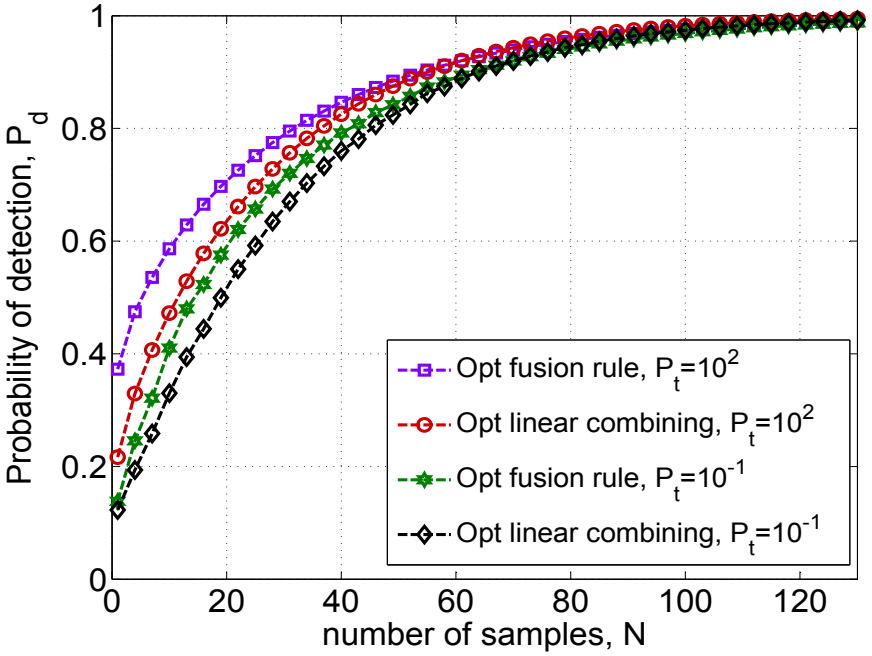

Figure 4.5: Probability of detection (P_d) versus the number of samples (N) for $M = 10$ sensors, $P_{fa} = 0.1$, $\xi_a = -8.5$ dB and $B = 1$.

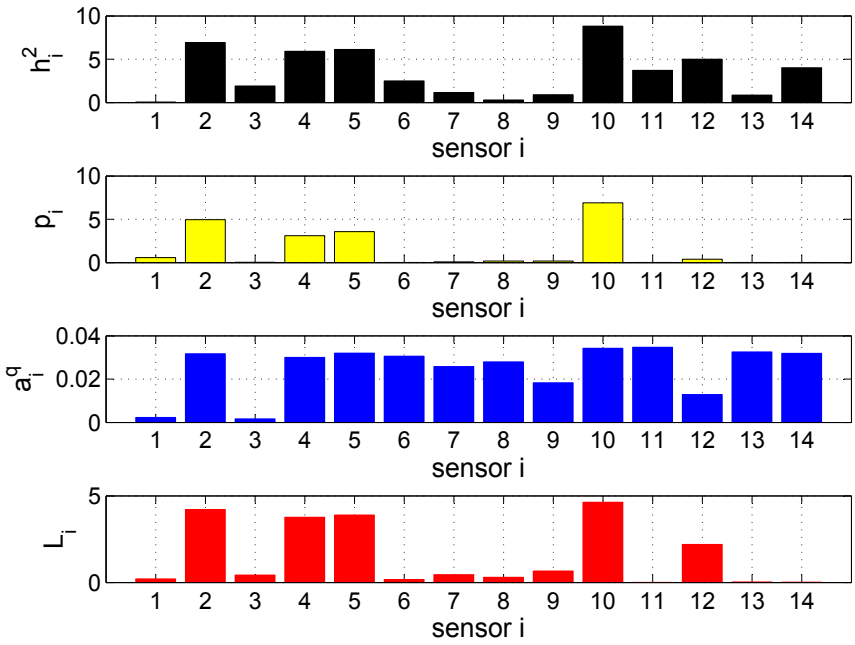

Figure 4.6: Optimum sensor transmit power and channel quantization bits allocation for $N = 10$, $P_{fa} = 0.1$, $\xi_a = -8.5$ dB and $P_t = 20$.

A similar trend is noticed in Fig. 4.3, in which P_d is plotted against the number of SNs, (M), for a fixed N. The P_d performance of both LRT-based and linear combining schemes as a function of the average SNR (ξ_a) is shown in Fig. 4.4.

Fig. 4.5 on the other hand, exhibits the effect of the transmission power p_i on P_d. Increasing p_i leads to a larger number of allocated bits, through (3.3.1), and consequently less quantization variance, which ultimately improves the detection performance. Interestingly, the dependence of P_d on p_i is alleviated when N is increased, since the effect of the quantization noise is mitigated as predicted by (4.4.6) and (4.4.9).

In Fig. 4.6, we report the optimized sensor transmit power and the corresponding number of bits allocated to quantize T_i by applying the branch and bound algorithm [97]. Clearly we allocate more power and bits to the best channels. However, note that the power and bit allocation are also affected by the weights a_i^q in (4.4.6) which are a function of the signal to noise ratio ξ_i. For instance, consider SN 12 which has a relatively good channel gain, but the corresponding local ξ_i is bad. Hence, it will allocate a relatively small amount of the transmit power. Those SNs with

bad channels are allocated *zero* bits, i.e., they will be censored or prevented from transmission.

4.7 Chapter Summary and Conclusions

In this chapter we have derived and shown that the optimal fusion (see (4.3.4)) for energy-based soft decisions is actually the weighted distance of the decisions from their mean under the null hypothesis. As this optimal fusion rule is not mathematically tractable and requires $a-priori$ knowledge that might be difficult to be estimated in practice, we have proposed some realizable simple and efficient sub-optimal fusion rules that are derived and inspired from the optimal one. These sub-optimum fusion rules intuitively are shown to give more weight in the actual fusion to the SN decisions with better local sensing quality.

We have also shown that the effect of test statistics quantization on the FC detection performance can be mitigated by increasing the number of sample measurements (N), or equivalently incurring more delay in the system. Finally, the SN's transmission power has been optimally allocated. Intuitively, more power is given to SNs having better channel gains and consequently increased number of quantization bits.

Chapter 5

Distributed Two-Step Quantized Fusion Rules

IN THIS CHAPTER

Within this chapter, we consider the problem of distributed soft decision fusion in a bandwidth-constrained spatially uncorrelated wireless sensor network (WSN). Existing distributed consensus-based fusion rule algorithms only ensure equal combining of local data. In the case of bandwidth-constrained WSNs, we show that their performance is poor and does not converge across the sensor nodes (SNs). Motivated by this, we propose a quantized two-step distributed detection algorithm that approaches the performance of the unquantized centralized (with a FC) detector and its power consumption is shown to be 50% less than the existing (unquantized) conventional algorithm.

5.1 Introduction

5.1.1 Motivation

Wireless sensor networks (WSNs), consisting of a large number of cheap SNs (with limited capabilities), are deployed over a geographical area for a wide range of applications such as personal health monitoring, traffic regulating, smart building infrastructure and so on. Particularly, reaching a consensus on a certain global decision

among these multi-sensors network is of great interest. Proper interaction among the SNs may help to improve their local reliability, reduce vulnerability and congestion events, and make a better usage of the limited radio resource capabilities. However, there are a number of different strategies as to how the test statistics from each SN will be used in order to arrive at a final decision. We will first give a brief review before introducing our proposed approach.

In the previous chapters (i.e., Chapter 3 and Chapter 4), we have considered the *centralized solution* where the local SNs communicate their noisy test statistics (inter-sensor collaboration is not considered) to a fusion center (FC) for a final decision [28]-[37]. In Chapter 3, we investigated the effect of $inter-sensor\ collaboration$ [99] in the context of SN transmit power allocation scheme. There are some recent publications [39]-[40] that consider the effect of $inter-sensor\ collaboration$ in the context of estimation. Here, in the first stage, the local SNs collaborate through error-free, low cost transmission links (defined by the symmetric adjacency matrix). After the first stage, the SNs (which in general can be a subset of all SNs) report to a FC where the final decision is made. Reference [39] proposes an "$efficient$" collaboration strategy in a distributed fashion (as opposed to [41] where this optimal interaction strategy is computed at a FC) by means of using only local SNs observations. While the authors in [39] claim to reduce the FC control overhead, [40] derives the optimum power allocation scheme such that the estimation quality back at the FC is further improved.

These two *hybrid approaches* [36, 99] (a SN interaction stage followed by reporting to a FC), like the first approach (no interaction stage and every SN communicate directly to a FC), rely greatly on the integrity of the FC. Clearly, the limitation of the centralized approach is both the requirement of the FC to process a large amount of information (i.e., possible bottleneck) and the possible total failure of the FC. Furthermore, collecting information at the FC lacks scalability, and may drain the energy and communication resources [42]. Hence, decentralized solutions are very attractive as both the computational load splits across the network and the final decision can be taken at any arbitrary SN. Compared to the centralized approach, the system is more reliable and offers a greater robustness against FC failure.

5.1.2 Related Work

While the related work on *centralized* and *hybrid* approach was reviewed in Chapter 3 and Chapter 4 in a great deal of detail, some key related research has been restated in Section 5.1.1 in order to motivate and make clear the purpose and the contributions of this chapter.

Within this section, we review the literature of the *fully distributed strategy* (i.e., without a FC) [23–26, 43–48], where the SNs exchange local information iteratively among their neighbors and are capable of reaching a global optimum decision. The authors of [43] and [44] adopts the diffusion-based protocol and propose a new diffusion LMS algorithm while [26] develop a fully distributed consensus-based LMS algorithm that outperforms the existing (relying on information diffusion) alternatives. The authors of [45] design a bio-inspired algorithm that can achieve globally optimal distributed decisions while in [46] they investigate the consensus problem in the presence of propagation delays. References [18, 46–48, 53, 54] employ the iterative distributed consensus algorithm [19] for distributed inference.

But these approaches consider ideal exchange of information among all the SNs, and as the SNs are battery operated (i.e., with limited energy available on-board) this assumption is unrealistic. Furthermore, practical WSN scenarios suffer from channel impairments such as fading and attenuation. Recently, to address the problem of consensus algorithms with quantized communications, a number of different approaches have been proposed. The authors in [20] propose a probabilistic quantization scheme that is shown to reach a consensus (almost surely) to a random variable whose expected value is equal to the desired average. Unfortunately, it is shown that this scheme performs poorly at low bit rate. Another approach to mitigate the quantization error in the consensus algorithm is to use an iteration dependent step size as in [21] and [52]. Adapting the weight link sequence in order to guarantee convergence is shown to decrease the convergence rate and so introduces a delay to the detection algorithm. Even employing such decaying link weights satisfying a persistence condition (i.e., their sum over time diverges, while their square sum is finite) cannot guarantee the convergence to the target average [21]. Recently [22] introduced a progressive quantization scheme that is shown to achieve the true av-

erage solution even at a low communication rate. However, this scheme has a high computational complexity and relies on a doubly stochastic weight matrix.

Now, most of the existing works on quantized consensus assume that the communication topology is symmetric (not the case here). Furthermore, all the above-mentioned algorithms either maintain the average value in the network but cannot reach a consensus effectively, or converge to a random variable that is not always the target average value.

So, the purpose of this chapter is to develop a fully distributed detection framework [23, 24] for realistic WSN scenarios. The communication links among SNs are modeled as channels with path loss, flat fading and additive white Gaussian noise (AWGN). The assumption of flat fading (see for e.g., [52]) is reasonable and valid in many WSN applications operating at both short distances and low bit rate (hence large symbol interval) due to resource limitations. Furthermore, the fact that they are (densely) spatially deployed across an open field result in a small delay spread. We will show that this new distributed framework can approach the performance of a centralized optimum detector (i.e., with a FC).

5.1.3 Chapter Contributions

So, the main contributions of this chapter are as follows:

(i) First, the (unquantized) consensus algorithm [19] is modified in such a way that the SNRs of the local SNs are taken into account in order to further improve the global detection performance. We re-state the necessary conditions for convergence to the (unquantized) optimum linear combining solution [35]. Based on this, we provide a distributed consensus-based detection framework with (weight combining) quantized test statistic exchange (SNs implement a low complexity uniform quantizer and the number of quantization bits is constrained to match the channel capacity of each link). Using the probability of detection and the probability of false alarm as metrics, we show that this approach: (a) does not converge to a global decision across the network, and (b) does not approach the optimum quantized centralized detector (i.e., with a FC) performance [35].

(ii) Second, motivated by the above, we propose a novel two-step quantized

distributed weighted fusion algorithm that now: (a) converges to a global decision across the network, (b) approaches the optimum centralized detector performance, and (c) achieves the global decision in a finite number of iterations. The main idea of this proposed two-step distributed (quantized) fusion algorithm is to arrive at an optimum global decision at every SN by taking advantage of the spatially distributed information across the WSN while combating flat fading.

5.1.4 Chapter Outline

Now, a summary of this chapter is as follows. In Section 5.2 we formulate the detection problem and recall some basic definitions from graph theory that we will be using. Section 5.3 describes two different approaches (i.e., the centralized approach (with a FC) and the fully distributed approach (without a FC)). In Section 5.4 we describe a consensus-based distributed detection framework and analyze the detection performance by proving that the quantized distributed detector performance does not converge across the SNs. Motivated by this, we then propose a two-step quantized weighted fusion algorithm with performance comparable to the centralized (unquantized) optimum detector. Finally, Section 5.5 presents simulation results that confirm our analytical findings and in Section 5.6 we give conclusions.

5.2 Problem Formulation

In this chapter, we consider two different schemes: a) the centralized approach (see Fig. 5.1), where each SN sends its test statistic (quantized to L_i bits) to the FC (see section 5.3.1) where the FC combines them and makes the final decision; and b) is the decentralized approach (see Fig. 5.2 and section 5.3.2), where SN i shares iteratively its current test statistic (quantized to q_i bits) across the set (Δ_i) of its neighbors (see Δ_i definition in section 5.2.2). Next, we explain in more detail the local sensing model and some graph theory definitions.

5.2.1 System Model

Next, we describe the target sensing, communication channel, and the WSN architecture.

Target Sensing

Similarly to Chapter 3 and Chapter 4, in this chapter we consider a WSN with M SNs that are tasked with the detection of any intruders. Again, we assume that the intruder leaves a signature signal that is unknown to the WSN but it is assumed to be deterministic. The other assumptions made regarding the target sensing are also identical to those stated in Chapter 3 and Chapter 4.

Communication Channel

Identical to Chapter 3, the communication links among SNs are modeled as channels with path loss, flat fading and additive white Gaussian noise (AWGN). The assumption of flat fading (see for e.g., [52]) is reasonable and valid in many WSN applications operating at both short distances and low bit rate (hence large symbol interval) due to resource limitations.

WSN Architecture

In this chapter (different from Chapter 3 and Chapter 4), we consider the distributed SNs detection architecture where there is no any FC. The SNs collaborate with their neighbors (through single-hop) iteratively based on the communication topology (no "overhearing" SNs assumed) that we describe next in the Section 5.2.2. This architecture is called the *distributed* WSN architecture and it is illustrated in Fig. 5.2. Each of the local spatially distributed SN is tasked with the detection problem.

5.2.2 Sensor Nodes Interaction Model

The interaction among SNs is according to the communication topology which is given by an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{1, 2, \ldots, M\}$ represents the set of M SNs and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the set of edges $\{i, j\}$. The graph properties can be represented by an *adjacency matrix* $\mathbf{E} \in \mathbb{R}^{M \times M}$ whose entries are defined as

$$e_{ij} = e_{ji} = \begin{cases} 1, & \text{if } j \in \Delta_i \\ 0, & \text{otherwise.} \end{cases} \tag{5.2.1}$$

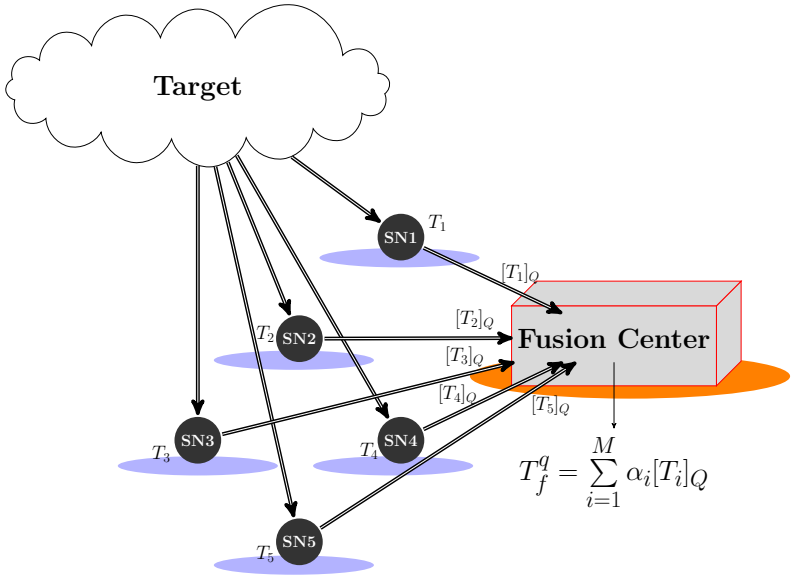

Figure 5.1: Schematic communication architecture between peripheral SNs and the fusion center (FC). Each SN generates a test statistic (T_i) by observing the target and can communicate (using $[T_i]_Q$) with the FC only over an energy-constrained/bandwidth-constrained link.

We denote the i^{th} SN neighbor set as Δ_i and $|\Delta_i|$ is the number of neighbors. The definition of the graph *Laplacian* matrix ($\mathbf{L} \in \mathbb{R}^{M\times M}$) is $\mathbf{L} = \mathbf{D} - \mathbf{E}$ with $\mathbf{D} = \text{diag}(|\Delta_1|, \ldots, |\Delta_M|)$. Next, we discuss the centralized and distributed detection approaches and provide an optimum distributed (i.e., without a FC) weight combining fusion rule framework.

5.3 Centralized vs. Distributed

The first scheme[1] (see Fig. 5.1) is a WSN consisting of M spatially distributed SNs that report to a FC. Upon receiving the contributions from each individual local SN, the FC linearly combines them and then declares a global decision. We refer to this approach as a *centralized scheme*. In the other approach (see Fig. 5.2) the SNs collaborate among each other iteratively to come up to a global decision

[1]Now, $[T_i]_Q$ is the i^{th} SN quantized test statistic (see (5.3.2)), $\{\alpha_i\}_{i=1}^{M}$ are the optimum weights (see (5.3.9)) and the superscript "q" refers to "quantized".

in a fully distributed fashion (i.e., without a FC). In this case, each SN i is able to perform a (global) decision. We refer to this approach as a *decentralized scheme*. Note that the results derived in this section will serve as the basis for developing the new optimum two-step quantized (weighted) fusion rule algorithm in section 5.4.

5.3.1 Centralized Approach

In order to better understand the fully distributed algorithm that we propose later, in this chapter we first describe two different centralized approaches: *quantized* and *unquantized*.

Quantized Centralized Approach [35]-[36]

Here, quantized linear[2] soft decision combining at the FC is proposed, where each individual SN has to quantize its observed test statistic (T_i) (prior to transmission to a FC) to L_i bits. So, to satisfy the capacity constraint on each SN to FC channel, we require:

$$L_i \leq \frac{1}{2}\log_2\left(1+\frac{p_i h_i^2}{\zeta_i}\right) \text{ bits/sample} \tag{5.3.1}$$

where p_i denotes the transmit power of SN i, h_i is the flat fading coefficient between SN i and the FC, and ζ_i is the variance of the AWGN at the FC. The quantized test statistic ($[T_i]_Q$) at the i^{th} SN can be modeled as

$$[T_i]_Q = T_i + v_i \tag{5.3.2}$$

where v_i is the quantization noise independent of $w_i\,(n)$ in (3.2.1) and (3.2.2). Assuming uniform quantization with $T_i \in [0, 2U]$, then

$$\sigma_{v_i}^2 = \frac{U^2}{3\times 2^{2L_i}}. \tag{5.3.3}$$

Linearly combining $\left\{[T_i]_Q\right\}_{i=1}^{M}$ at the FC gives[1]

$$T_f^q = \sum_{i=1}^{M}\alpha_i[T_i]_Q. \tag{5.3.4}$$

[2]The main motivation behind the linear combining rule consideration is that the probability of detection and the probability of false alarm metrics are obtained in a closed-form. This gives insight into the design of the system's parameters, whereas for the LRT-based detector, analytically analyzing the detection performance is not tractable.

For large M, T_f^q will be approximately Gaussian and we can show (5.3.5) and (5.3.8).

$$\mathbb{E}\left\{T_f^q|\mathcal{H}_0\right\} = \sum_{i=1}^{M}\alpha_i N\sigma_i^2 \tag{5.3.5}$$

$$\mathbb{E}\left\{T_f^q|\mathcal{H}_1\right\} = \sum_{i=1}^{M}\alpha_i\Big(N\sigma_i^2\left(1+\xi_i\right)\Big) \tag{5.3.6}$$

$$\mathrm{Var}\left\{T_f^q|\mathcal{H}_0\right\} = \sum_{i=1}^{M}\alpha_i^2\Big(2N\sigma_i^4+\sigma_{v_i}^2\Big) \tag{5.3.7}$$

$$\mathrm{Var}\left\{T_f^q|\mathcal{H}_1\right\} = \sum_{i=1}^{M}\alpha_i^2\Big(2N\sigma_i^4\left(1+2\xi_i\right)+\sigma_{v_i}^2\Big). \tag{5.3.8}$$

Now, the optimum weights $\{\alpha_i\}_{i=1}^M$ are given as [35]:

$$\boldsymbol{\alpha} = \left[\frac{N\sigma_1^2\xi_1}{2N\sigma_1^4(1+2\xi_1)+\sigma_{v_1}^2}, \frac{N\sigma_2^2\xi_2}{2N\sigma_2^4(1+2\xi_2)+\sigma_{v_2}^2}, \ldots, \frac{N\sigma_M^2\xi_M}{2N\sigma_M^4(1+2\xi_M)+\sigma_{v_M}^2}\right]. \tag{5.3.9}$$

So (5.3.9) establishes a relationship between the optimum weighting vector ($\boldsymbol{\alpha}$) and the SN transmit power (p_i) through the $\sigma_{v_i}^2$ quantity (see definition (5.3.1) and (5.3.3)). The FC then makes the following decisions:

$$\left.\begin{array}{l}\text{if } T_f^q < \Lambda_f, \text{ decide } \mathcal{H}_0\\ \text{if } T_f^q \geq \Lambda_f, \text{ decide } \mathcal{H}_1\end{array}\right\} \tag{5.3.10}$$

where Λ_f is the FC detection threshold. The probability of detection (P_d) for a fixed probability of false alarm (P_{fa}) is given as [78]:

$$P_d = Q\left(\frac{Q^{-1}\left(P_{fa}\right)\sqrt{\mathrm{Var}\left\{T_f^q|\mathcal{H}_0\right\}}-\mathbb{E}\left\{T_f^q|\mathcal{H}_1\right\}+\mathbb{E}\left\{T_f^q|\mathcal{H}_0\right\}}{\sqrt{\mathrm{Var}\left\{T_f^q|\mathcal{H}_1\right\}}}\right) \tag{5.3.11}$$

with appropriate quantities given in (5.3.5)-(5.3.8) (see [35]) and where $Q(.)$ is the Q-function.

Unquantized Centralized Approach

Given the local test statistic T_i (see (3.2.3)) at the i^{th} SN, the optimum (unquantized) linear fusion rule[3] has the structure [35]:

$$T_f^{uq} = \sum_{i=1}^{M}\alpha_i T_i \tag{5.3.12}$$

[3]This is a special case assuming that the FC receives all the local test statistics $\{T_i\}_{i=1}^M$ without errors and in practice it is a strong assumption.

where the superscript "*uq*" refers to "*unquantized*" and $\{\alpha_i\}_{i=1}^{M}$ are the optimum weights given in (5.3.9) but now with $\{\sigma_{v_i}^2\}_{i=1}^{M} = 0$. The probability of detection (P_d) for a fixed probability of false alarm (P_{fa}) is given again as in (5.3.11) (replacing T_f^q by T_f^{uq}) by substituting the appropriate quantities given in (5.3.5)-(5.3.8) with $\{\sigma_{v_i}^2\}_{i=1}^{M} = 0$. This gives an upper bound on the receiver operating characteristic performance and we will refer later to this in the simulation results.

Now the limitation of the centralized approach is both the requirement of the FC to process a large amount of data (i.e., possible bottleneck) and the possible failure of the FC. Hence, distributed solutions are very attractive as the computational load splits across the network. The final decision can be taken at any arbitrary SN. As a result, the system is more robust against FC failure than in a centralized system.

5.3.2 Distributed Approach

Now we are after the fully distributed approach (see Fig. 5.2) and we propose a distributed quantized linear fusion rule. Even though there are different distributed algorithms in the literature (i.e., average consensus, diffusion, gossip-type algorithms, etc), we will use the consensus algorithm [19] as a basic tool to develop the distributed quantized linear fusion rule.

Unquantized Distributed Equal Combining

Now consider the conventional consensus-based [19] distributed equal combining scheme that fuses the contributions received among SNs (i.e., it does not accommodate properly the *more informative* and the *less informative* neighbors). At iteration $k+1$, each SN i updates its test statistic ($T_i^{eq}[k+1]$) as follows [19]:

$$T_i^{eq}[k+1] = T_i^{eq}[k] - \epsilon \sum_{j=1}^{M} e_{ij} \left(T_i^{eq}[k] - T_j^{eq}[k] \right), \; k \geq 0, \text{for } i = 1, 2, \cdots, M \quad (5.3.13)$$

where the superscript "*eq*" refers to "*equal combining*", $0 < \epsilon < 1/\Delta_{\max}$ with $\Delta_{\max} = \max(|\Delta_1|, \ldots, |\Delta_M|)$, e_{ij} is defined in (5.2.1) and $T_i^{eq}[0] = T_i$ in (3.2.3). The time evolution of (5.3.13) can be written as

$$\mathbf{T}^{eq}[k] = \mathbf{W}^k \mathbf{T}^{eq}[0], \; k \geq 1 \quad (5.3.14)$$

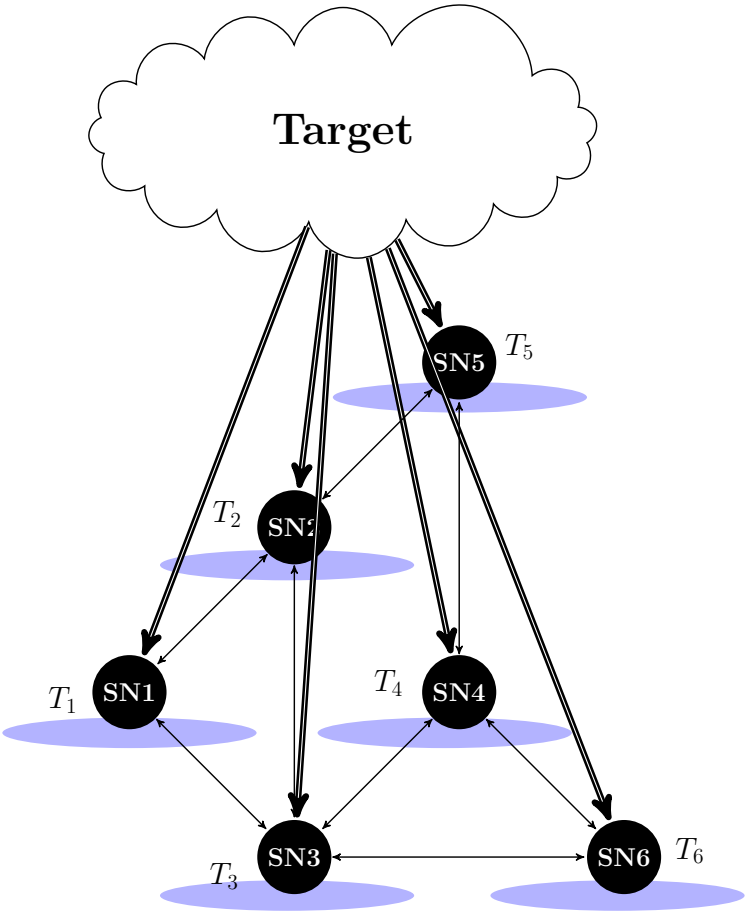

Figure 5.2: Schematic for a distributed communication architecture among peripheral SNs. Each SN generates a test statistic (T_i) by observing the target (thick lines). The SNs have partial connectivity (thin lines) among themselves (i.e., not a complete graph), but only over an energy-constrained/bandwidth-constrained network.

where $\mathbf{W} = \mathbf{I} - \epsilon\mathbf{L}$ and $\mathbf{T}^{eq}[k] = [T_1^{eq}[k], T_2^{eq}[k], \ldots, T_M^{eq}[k]]^T$. The decision can be taken locally at the i^{th} SN at the k^{th} iteration as follows:

$$\left.\begin{array}{l} \text{if } T_i^{eq}[k] < \Lambda_i[k], \text{ decide } \mathcal{H}_0 \\ \text{if } T_i^{eq}[k] \geq \Lambda_i[k], \text{ decide } \mathcal{H}_1 \end{array}\right\} \tag{5.3.15}$$

where $\Lambda_i[k]$ is the threshold for the i^{th} SN at the k^{th} iteration. We can write:

$$\mathbb{E}\left\{T_i^{eq}[k]|\mathcal{H}_p\right\}_{p=\{0,1\}} = (\mathbf{W}^k \mathbb{E}\left\{\mathbf{T}^{eq}[0]|\mathcal{H}_p\right\})_i \tag{5.3.16}$$

$$\text{Var}\left\{T_i^{eq}[k]|\mathcal{H}_p\right\}_{p=\{0,1\}} = (\text{Cov}\left\{\mathbf{T}^{eq}[k]|\mathcal{H}_p\right\})_{ii} = (\mathbf{W}^k \text{Cov}(\mathbf{T}^{\text{eq}}[0]|\mathcal{H}_{\text{p}})\mathbf{W}^k)_{ii} \tag{5.3.17}$$

where[4] $(\mathbf{a})_i$ denotes the i^{th} element of vector $\mathbf{a}$ and $(\mathbf{A})_{ij}$ denotes the (i,j) element of matrix $\mathbf{A}$.

$$P_{fa}^{i}[k] = \Pr\left(T_i^{eq}[k] \geq \Lambda_i[k]|\mathcal{H}_0\right) = Q\left(\frac{\Lambda_i[k] - \mathbb{E}\left\{T_i^{eq}[k]|\mathcal{H}_0\right\}}{\sqrt{\mathrm{Var}\left\{T_i^{eq}[k]|\mathcal{H}_0\right\}}}\right) \tag{5.3.18}$$

$$P_{d}^{i}[k] = \Pr\left(T_i^{eq}[k] \geq \Lambda_i[k]|\mathcal{H}_1\right) = Q\left(\frac{\Lambda_i[k] - \mathbb{E}\left\{T_i^{eq}[k]|\mathcal{H}_1\right\}}{\sqrt{\mathrm{Var}\left\{T_i^{eq}[k]|\mathcal{H}_1\right\}}}\right). \tag{5.3.19}$$

$$\tag{5.3.20}$$

For a fixed probability of false alarm (i.e., $P_{fa}^{i}[k] = P_{fa}, \forall i$ and $\forall k$), the detection probability for the i^{th} SN at the k^{th} iteration can be written as

$$P_{d}^{i}[k] = Q\left(\frac{Q^{-1}\left(P_{fa}\right)\sqrt{\mathrm{Var}\left\{T_i^{eq}[k]|\mathcal{H}_0\right\}} + \Psi}{\sqrt{\mathrm{Var}\left\{T_i^{eq}[k]|\mathcal{H}_1\right\}}}\right) \tag{5.3.21}$$

where $\Psi = \mathbb{E}\left\{T_i^{eq}[k]|\mathcal{H}_0\right\} - \mathbb{E}\left\{T_i^{eq}[k]|\mathcal{H}_1\right\}$. Now, (5.3.21) establishes a relationship between the probability of detection $(P_d^i[k])$ and the iteration number k at the i^{th} SN. It can be shown [19] that as k gets larger, the performance of the distributed detector (5.3.15) for a connected network[5] approaches that of the (unquantized) equal combining centralized detector (6.3.11) (i.e., $\lim_{k\to\infty} P_d^i[k] = P_d, \forall i$ with $\alpha_i = 1$ and $\sigma_{v_i}^2 = 0, \forall i$ in (5.3.12)). However, this distributed fusion rule realizable via (5.3.13) (and also its centralized counterpart) is not optimum.

What we require now is a distributed approach that will converge to the equivalent of the optimum weighted linear combining FC solution in (5.3.12).

Unquantized Distributed Weight Combining

In our previous work [35] we have optimized the weights (α_i) such that the probability of detection is maximized. As can be seen from (5.3.9), the optimum weights are a function of local sensing quality (σ_i^2), received signal strength (ξ_i) and the SN transmit power (p_i) through the quantization noise $(\sigma_{v_i}^2)$ (see (5.3.1) and (5.3.3)). So

[4] For a random vector $\boldsymbol{x}$, $\mathbb{E}\{\boldsymbol{x}\}$ denotes expectation and $\mathrm{Cov}\{\boldsymbol{x}\}=\mathbb{E}[(\boldsymbol{x}-\mathbb{E}\{\boldsymbol{x}\})(\boldsymbol{x}-\mathbb{E}\{\boldsymbol{x}\})^T]$ is the covariance matrix.

[5] A connected network is any network where there is a path (i.e., over one or more links) between every pair of SNs in the network.

now using these optimal weights we derive a weighted exchange of information version of (5.3.13). Because the i^{th} SN does not know its neighbors' weights $\{\alpha_j\}_{j\in\Delta_i}$, we propose to weight the contributions received from the $|\Delta_i|$ neighbors by $f(\alpha_i)$, where f is the function that we elaborate later on. More specifically, the i^{th} SN updates its test statistic as follows:

$$T_i^w[k+1] \;=\; T_i^w[k] - \epsilon f(\alpha_i)\sum_{j=1}^{M} e_{ij}\left(T_i^w[k] - T_j^w[k]\right),\;\; k \;\geq\; 0, \text{for } i \;=\; 1,2,...,M \tag{5.3.22}$$

where the superscript "w" refers to "*weighted*", α_i are the centralized weighting coefficients in (5.3.9) with $\sigma_{v_i}^2 = 0$, $f(\alpha_i) \geq 0$, ϵ is defined for (5.3.13) and $T_i^w[0] = T_i$ in (3.2.3). The time evolution of (5.3.22) can be written as

$$\mathbf{T}^w[k] = \mathbf{W}^k\mathbf{T}^w[0],\;\; k \geq 1 \tag{5.3.23}$$

with $\mathbf{W}$ defined as

$$\mathbf{W} = \mathbf{I} - \epsilon\mathbf{\Gamma}\mathbf{L} \tag{5.3.24}$$

and $\mathbf{\Gamma} = \text{diag}(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_M))$. We will now show that there exist a function f such that (5.3.23) (unquantized, distributed) converges to (5.3.12) (unquantized, centralized). First we prove two propositions.

Proposition 5.3.1 *Let* $\mathbf{W}$ *be a matrix defined in (5.3.24) with* $0 < \epsilon < 1/\Delta_{max}$. *Then* $\mathbf{W}$ *is a non-negative matrix (i.e.,* $\mathbf{W} \geq 0$*) if* $\mathbf{\Gamma} \leq 1$ *(i.e., a matrix in which all the elements are equal to or less than one).*

Proof: Note that from the definition of the Laplacian matrix ($\mathbf{L}$) defined in Section 6.3.2, (5.3.24) can be expressed as $\mathbf{W} = \mathbf{I} - \epsilon\mathbf{\Gamma}\mathbf{D} + \epsilon\mathbf{\Gamma}\mathbf{E}$. Now, by definition $\mathbf{\Gamma} \geq 0$, and so $\epsilon\mathbf{\Gamma}\mathbf{E}$ is also a non-negative matrix. The entries of the diagonal matrix $(\mathbf{I} - \epsilon\mathbf{\Gamma}\mathbf{D})$ have to be non-negative, $\forall i$ (i.e., $1 - \epsilon f(\alpha_i)\Delta_i \geq 0, \forall i$). This can be achieved with $1 - \frac{f(\alpha_i)\Delta_i}{\Delta_{max}} \geq 0$ and since $f(\alpha_i) \leq 1, \forall i$ (i.e., $\mathbf{\Gamma} \leq 1$) $\implies 1 - \frac{f(\alpha_i)\Delta_i}{\Delta_{max}} \geq 0$. Then $\mathbf{\Gamma} \leq 1 \implies \mathbf{W} \geq 0$. ■

Proposition 5.3.2 *Let* $\mathbf{W}$ *be a matrix defined in (5.3.24) with* $0 < \epsilon < 1/\Delta_{max}$,

$\mathbf{\Gamma} \leq 1$ *and assuming a connected graph* $\mathcal{G}$*, then*

$$\lim_{k\to\infty} \mathbf{W}^k \mathbf{T}^w[0] = \sum_{i=1}^{M} \frac{1}{f(\alpha_i)} \begin{bmatrix} \sum_{i=1}^{M} \frac{1}{f(\alpha_i)} T_i^w[0] \\ \sum_{i=1}^{M} \frac{1}{f(\alpha_i)} T_i^w[0] \\ \vdots \\ \sum_{i=1}^{M} \frac{1}{f(\alpha_i)} T_i^w[0] \end{bmatrix}_{M\times 1} . \tag{5.3.25}$$

Proof: The proof is given in Appendix B.1. ■

Now, the convergence of (5.3.25) (with $T_i^w[0] = T_i$) to (5.3.12) up to a positive scaling can be only achieved if $f(\alpha_i) = \frac{1}{\alpha_i}$. It is worth mentioning that the condition $(f(\alpha_i) \leq 1, \forall i)$ does not affect the optimality of the fusion rule defined in (5.3.12) for the structure considered in (5.3.11) and the condition can be satisfied by scaling the centralized weighting vector $(\boldsymbol{\alpha})$ by a positive constant c. Clearly, the distributed system (5.3.22) achieves the performance of the unquantized centralized approach in section 5.3.1.

We have now stated the necessary and sufficient conditions for the time evolution (5.3.22) to converge to the weighted centralized optimum linear fusion rule (5.3.12). The exchange of information between SNs is assumed error free and the bandwidth between two connected SNs is considered unlimited. In the next section, we relax these assumptions and provide a quantized distributed weighted linear fusion rule framework that operates over limited bandwidth fading channels.

5.4 Distributed Detection via Two-Step Quantized Distributed Weighted Fusion Rule over Fading Communication Links

Now, in section 5.4.1 we develop a consensus-based quantized distributed weighted linear fusion framework. Next, in Section 5.4.2, using the probability of detection and the probability of false alarm as metrics, we analyze performance and give a proof that the *quantized distributed weighted linear fusion rule* algorithm does not converge across the SNs. Finally, in Section 5.4.3, based on the framework

provided in Section 5.4.1, we propose a new two-step quantized distributed weighted fusion algorithm.

5.4.1 Quantized Distributed Weighted Fusion Rule

Here we propose a scheme, where each SN encodes the data (using a simple uniform quantizer with q_i bits) prior to information exchange with its neighbors. We also propose to establish a link between any two SNs i and j based on the (known) link SNR at node j, i.e.

$$\left.\begin{array}{l} \text{if } SNR_{ij} < \Upsilon,\ e_{ij} = e_{ji} = 0 \\ \text{if } SNR_{ij} \geq \Upsilon,\ e_{ij} = e_{ji} = 1. \end{array}\right\} \tag{5.4.1}$$

Now e_{ij} is defined in (5.2.1), Υ is a (link) SNR threshold parameter (see later) and SNR_{ij} is the received signal-to-noise ratio (at SN j) defined as:

$$SNR_{ij} = \frac{p_{ij}^t h_{ij}^2}{\zeta_i d_{ij}^{\gamma}}. \tag{5.4.2}$$

Here p_{ij}^t denotes the i^{th} to j^{th} SN transmit power, h_{ij} is the flat-fading coefficient[6] between the i^{th} and j^{th} SN, ζ_i is the variance of the AWGN at each receiving SN (assumed to be the same for simplicity), γ is the path loss coefficient and d_{ij} is the physical distance between SN i and j (assumed to be known).

The thresholding operation (5.4.1) defines the communication topology. There are different approaches taken in the literature in order to define the topology of the network. In [100] a simplified relaxed (centralized) solution was presented, where the energy minimization problem was formulated as a convex-concave fractional programming. Another approach was followed in [55], where a distributed algorithm to decide which subset of communication links provides the optimum power consumption and the best network lifetime (i.e., minimizing simultaneously both the total power consumption and the maximum power consumption per SN) was developed. While both ([100] and [55]) improve the total power consumption and/or the whole

[6]We assume that the channel coefficients are varying slowly enough to be considered constant over the time interval necessary for the network to converge within a prescribed accuracy. This assumption is reasonable as our proposed algorithm converges rapidly.

network lifetime, they also assume that the exchange of information among SNs is ideal. But here we propose to quantize with q_i bits at SN i before transmitting to SN j and to satisfy the capacity constraint between SNs i and j we require:

$$q_i \leq \frac{1}{2}\log_2\left(1+\Upsilon\right) \qquad \text{bits/sample} \tag{5.4.3}$$

where we let $q_i = q, \forall i$. Now, Υ establishes a relationship between the number of bits that each SN has to transmit to its neighbors and also the topology of the network that defines the connections between the SNs (see (5.4.1)-(5.4.3)). A large Υ means fewer communication links (see (5.4.1)) resulting in slower information diffusion across the network. However, this will be counterbalanced by an increase in the number of bits that each SN can transmit to its neighbors (see (5.4.3)). As a consequence, the quantization noise variance (5.4.5) becomes negligible. Alternatively, a small Υ establishes a more connected graph and dictates a faster information diffusion across the network. However, this allows less transmission bits per iteration resulting in an increase in the quantization noise variance. It is now clear that Υ establishes a relationship between transmission bits and the graph connectivity. With quantization, the time evolution of (5.3.22) (by taking $f(\alpha_i) = \frac{1}{\alpha_i}$) now becomes:

$$\begin{aligned}\bar{T}_i^w[k+1] &= \bar{T}_i^w[k] - \frac{\epsilon}{\alpha_i}\sum_{j=1}^{M} e_{ij}\left(\bar{T}_i^w[k] - [\bar{T}_j^w[k]]_Q\right) \\ &= \bar{T}_i^w[k] - \frac{\epsilon}{\alpha_i}\sum_{j=1}^{M} e_{ij}\left(\bar{T}_i^w[k] - \bar{T}_j^w[k] - b_j[k]\right), k \geq 0, \text{ for } i = 1, 2, \cdots, M\end{aligned} \tag{5.4.4}$$

with $\bar{T}_i^w[0] = T_i$ in (3.2.3). (Note that the bar "$-$" differentiates from (5.3.22) where no quantization is used). Now $[\bar{T}_j^w[k]]_Q = \bar{T}_j^w[k] + b_j[k]$ represents quantization and $b_j[k]$ is the quantization noise independent of $w_i(n)$ in (1) and (2), $j = 1, 2, \cdots M$, $\forall i$ and $\forall n$. Assuming $\bar{T}_j^w[k] \in [0, 2U]$ and uniform quantization then:

$$\text{Var}\left\{b_j[k]\right\} = \sigma_{b_j}^2 = \frac{U^2}{3 \times 2^{2q}} \tag{5.4.5}$$

and we assume $\mathbb{E}\left\{b_j[k]\right\} = 0$ since the quantization noise is bipolar (i.e., it may take positive or negative values). We also assume that the i^{th} SN is capable to store its own *soft information* at the k^{th} iteration and communicate a quantized version to its neighbors. In the next $(k+1)^{th}$ iteration, every SN can update

the test statistic (i.e., $\bar{T}_i^w[k+1]$)) by using its own *soft information* and the *quantized information* received from other neighbors (i.e., it does not have access to their *soft information*).

Now, the power consumed by the whole network at a single iteration can be given as:

$$P_{throughout} = \sum_{i=1}^{M}\sum_{j=1}^{M} e_{ij}p_{ij}^t. \tag{5.4.6}$$

It is clear that establishing fewer communication links through (5.4.1) reduces $P_{throughout}$ and simultaneously imposes a slower information diffusion across the WSN. The number of bits that each SN can transmit to its neighbors will increase (see (5.4.3)). As a consequence, the quantization noise becomes negligible (see (5.4.5)). Alternatively, a smaller Υ (smaller quantization bits) dictates a more connected WSN and an increase in $P_{throughout}$ value. This results in an increase of quantization noise level that will lead to poor detection performance. It is now clear that Υ also establishes a trade-off between the quantization noise effect and the WSN total power[7] consumption (P_T). In the simulation results section we will investigate the effect of the thresholding operation (5.4.1) on the P_T value as well as on the system detection performance. Therefore, the goal is to find an Υ_{opt} such that P_T and the detection performance are both improved. Next, we analyze the time evolution of (5.4.4) by using the probability of detection and the probability of false alarm as metrics.

5.4.2 Performance Analysis

Now we analyze the detection performance of the proposed distributed quantized (weighted) fusion rule (via the time evolution of (5.4.4)). Defining $\boldsymbol{\psi}[k] = [\psi_1[k], \psi_2[k], \ldots, \psi_M[k]]^T$ with $\psi_i[k] = \frac{1}{\alpha_i}\sum_{j=1}^{M} e_{ij}b_j[k]$ and so (5.4.4) can be written as:

$$\bar{\mathbf{T}}^w[k] = \mathbf{W}^k\bar{\mathbf{T}}^w[0] + \epsilon\sum_{z=1}^{k}\mathbf{W}^{z-1}\boldsymbol{\psi}[k-z],\ k \geq 1 \tag{5.4.7}$$

[7]The total power consumption is defined as $P_T = P_{throughout}K_T$, where K_T is the total number of iterations to run the time evolution (5.4.4) and (5.4.14) (i.e., $K_T = K_1 + K_2$) (see later section 5.4.3 for details).

where $\bar{\mathbf{T}}^w[k]$ is defined similarly to $\mathbf{T}^{eq}[k]$ in (5.3.14). The decision strategy for the i^{th} SN at the k^{th} iteration is again given in (5.3.15) (replacing $T_i^{eq}[k]$ by $\bar{T}_i^w[k]$), and the following also hold:

$$\mathbb{E}\left\{\bar{T}_i^w[k]|\mathcal{H}_p\right\}_{p=\{0,1\}} = \left(\mathbf{W}^k\mathbb{E}\left\{\bar{\mathbf{T}}^w[0]|\mathcal{H}_p\right\}\right)_i \tag{5.4.8}$$

$$\begin{aligned}\mathrm{Var}\left\{\bar{T}_i^w[k]|\mathcal{H}_p\right\}_{p=\{0,1\}} = &\left(\underbrace{\mathbf{W}^k\mathrm{Cov}\left\{\bar{\mathbf{T}}^{\mathrm{w}}[0]|\mathcal{H}_{\mathrm{p}}\right\}(\mathbf{W}^k)^T}_{\mathrm{(A)}}\right)_{ii} \\ &+\epsilon^2\left(\underbrace{\sum_{z=1}^{k}\mathbf{W}^{z-1}\mathrm{Cov}\left\{\boldsymbol{\psi}[k-z]\right\}(\mathbf{W}^{z-1})^T}_{\mathrm{(B)}}\right)_{ii}\end{aligned} \tag{5.4.9}$$

where $\mathrm{Cov}\{\boldsymbol{\psi}[k-z]\} = \frac{U^2}{3}\mathrm{diag}\left(\frac{|\Delta_1|}{2^{2q}}, \frac{|\Delta_2|}{2^{2q}}, \cdots, \frac{|\Delta_M|}{2^{2q}}\right)$. Now, the detection performance for the i^{th} SN at the k^{th} iteration can be evaluated using (5.3.21) (replacing $T_i^{eq}[k]$ by $\bar{T}_i^w[k]$) by substituting the expressions from (5.4.8) and (5.4.9). Note that as the dynamic system (5.4.7) evolves, the term (B) in (5.4.9) accumulates. Next we show how the detection performance for the i^{th} SN at the k^{th} iteration evolves by analyzing the variance term $\left(\mathrm{Var}\left\{\bar{T}_i^w[k]\right\}\right)$ in (5.4.9).

Proposition 5.4.1 *Assume that* $\lambda_{max}(\mathbf{\Gamma}) \leq \frac{1}{\epsilon\lambda_{max}(\mathbf{L})(M-1)}$, *where* $\lambda_{max}(\mathbf{\Gamma})$ *and* $\lambda_{max}(\mathbf{L})$ *are the maximum eigenvalues associated to* $\mathbf{\Gamma}$ *and* $\mathbf{L}$ *respectively. From (5.4.9), the "scaled total variance"* $\frac{1}{M-1}\sum_{i=1}^{M}\mathrm{Var}\left\{\bar{T}_i^w[k]\right\}$

$$\leq \quad \mathrm{Var}_{\mathrm{k}}^{\max}\left(\frac{1}{M-1} + \lambda_2^k(\mathbf{W})\right) + \epsilon^2\sigma_{max}^2\left(\frac{k}{M-1} + \frac{1-\lambda_2^k(\mathbf{W})}{1-\lambda_2(\mathbf{W})}\right) \tag{5.4.10}$$

where $\mathrm{Var}_{\mathrm{k}}^{\max} = \max\left(\mathrm{Var}\left\{\bar{T}_1^w[k]\right\}, \mathrm{Var}\left\{\bar{T}_2^w[k]\right\}, \cdots, \mathrm{Var}\left\{\bar{T}_M^w[k]\right\}\right)$, $\sigma_{max}^2 = \max\left(\mathrm{Var}\left\{\psi_1[k]\right\}, \mathrm{Var}\left\{\psi_2[k]\right\}, \cdots, \mathrm{Var}\left\{\psi_M[k]\right\}\right)$ *and* $\lambda_i(\mathbf{W})$, $i = 1, \cdots, M$ *are the eigenvalues of* $\mathbf{W}$ *satisfying* $\lambda_M \leq \lambda_{M-1} \leq \cdots < \lambda_1 = 1$.

Proof: The proof can be found in Appendix B.2. ■

As k becomes large, it is clear that the second term of (5.4.10) grows and the performance of the distributed algorithm using quantized distributed weighted linear fusion does not approach the performance of the centralized quantized detector [35] (i.e., $\lim_{k\to\infty} P_d^i[k] \neq P_d$ in (13) of [35], $\forall i$).

Now, it is also clear that k establishes a trade-off between the local SNs test statistic improvement and the quantization error degradation. There is a finite optimum $k = K_1$ to stop the SNs collaboration (see later), but after that the quantization error overcomes the improvement gained from this collaboration. So, using this framework (i.e., the consensus algorithm with quantization matched to the channel capacity) we will now propose a two-step approach (still using quantized test statistics shared among SNs) that will perform comparable to the optimum unquantized centralized detector in section 5.3.1 (i.e., when using a FC and no quantization). And what is more important, it converges across the network in a finite number of iterations.

5.4.3 Proposed Two-Step Quantized Distributed Weighted Fusion Rule Algorithm

(i) FIRST STEP: Run the quantized consensus algorithm in (5.4.7) to improve the local version of the test statistic at each SN. But then terminate the algorithm at $k = K_1$ (where the optimum value of K_1 is found later from simulation results and a sub-optimum solution to it is also proposed). We now have $\left\{\bar{T}_i^w[K_1]\right\}_{i=1}^M$ from (5.4.7) and we will use this to generate a binary indicator random variable $I_i[0]$ as follows

$$\left.\begin{array}{l} \text{if } \bar{T}_i^w[K_1] < \Lambda_1,\ I_i[0] = 0 \\ \text{if } \bar{T}_i^w[K_1] \geq \Lambda_1,\ I_i[0] = 1 \end{array}\right\} \tag{5.4.11}$$

where Λ_1 is a local (first step) detection threshold that is the same for all M SNs. We will now propose (for performance comparison purposes) two alternative *second step* decision rules:

1)

$$\left.\begin{array}{l} \text{if } \bar{T}_f^w[K_1] \neq M, \text{decide } \mathcal{H}_0 \\ \text{if } \bar{T}_f^w[K_1] = M, \text{decide } \mathcal{H}_1 \end{array}\right\} \tag{5.4.12}$$

2)

$$\left.\begin{array}{l} \text{if } \bar{T}_f^w[K_1] = 0, \text{decide } \mathcal{H}_0 \\ \text{if } \bar{T}_f^w[K_1] \neq 0, \text{decide } \mathcal{H}_1 \end{array}\right\} \tag{5.4.13}$$

where $\bar{T}_f^w[K_1] = \sum_{i=1}^{M} I_i[0]$ both in 1) and 2). But the problem is now how to evaluate $\bar{T}_f^w[K_1]$ in a distributed manner across SNs. This will be explained in the second step.

(ii) SECOND STEP:

1) *Second step defined in* (5.4.12): When the local individual SNs unanimously decide on the intruder presence, so also decides this (global) decision *second step* (i.e., intruder is present). Otherwise, it decides that the intruder is not present. Here we will use [56] to show how to effectively evaluate (5.4.12) by first sharing $\{I_i[0]\}_{i=1}^{M}$ and then iteratively updating across the SNs as follows:

$$I_i[k+1] = I_i[k] \bigwedge \left(\bigwedge_{j \in \Delta_i} I_j[k] \right), \ k = 0, 1, 2, \cdots, K_2 - 1, \ \text{for } i = 1, 2, \cdots, M \tag{5.4.14}$$

where K_2 is the diameter of network[8],"$\bigwedge$" denotes the logical "*and*" operation and Δ_i is defined for (5.2.1). Note that no quantization is needed and all $I_i[K_2]$ converge to either 1 or 0. So now we can easily show:

$$\left.\begin{array}{l} \text{If } I_i[K_2] = 0, \ \forall i \Rightarrow \ \bar{T}_f^w[K_1] \neq M, \ \text{decide } \mathcal{H}_0 \\ \text{If } I_i[K_2] = 1, \ \forall i \Rightarrow \ \bar{T}_f^w[K_1] = M, \ \text{decide } \ \mathcal{H}_1 \end{array}\right\} \tag{5.4.15}$$

and so $I_i[K_2]$ (at any arbitrary i^{th} SN) can be used to implement the decision rule (5.4.12).

2) *Alternative second step defined in* (5.4.13): Now, this alternative *second step* (global) decision fusion rule decides on the presence of the intruder if at least any arbitrary local SNs (at iteration $k = K_1$) has decided so. Again, $\bar{T}_f^w[K_1]$ can be evaluated in a distributer manner by first sharing $\{I_i[0]\}_{i=1}^{M}$ and then iteratively updating across the SNs using (5.4.14) (but now the "*and*" logical operation "$\bigwedge$" is replaced with the "*or*" logical operation "$\bigvee$"). Like before, all $I_i[K_2]$ converge to

[8]The geodesic distance between two nodes in a (connected) graph is the number of the edges (i.e., links) in the shortest path connecting these two nodes. The diameter of a graph is the maximum geodesic distance taken over all possible pairs of nodes in the graph.

either 1 or 0 and we can easily show:

$$\left.\begin{array}{l} \text{If } I_i[K_2]=0,\ \forall i \Rightarrow\ \bar{T}_f^w[K_1]=0,\ \text{decide } \mathcal{H}_0 \\ \text{If } I_i[K_2]=1,\ \forall i \Rightarrow\ \bar{T}_f^w[K_1]\neq 0,\ \ \text{decide } \mathcal{H}_1 \end{array}\right\} \tag{5.4.16}$$

and so $I_i[K_2]$ (at any arbitrary SN) can be used to implement the decision rule (5.4.13). Overall, the proposed two-step fully distributed algorithm requires ($K_T = K_1+K_2$) iterations in total. Now, the two-step algorithm (with *second step* decision rule (5.4.13) can be summarized in **Algorithm 5.4.1**.

Algorithm 5.4.1: Distributed Detection via Two-Step Consensus Algorithm

---

STEP 1: Choose Υ and evaluate $\bar{T}_i^w[0]=T_i$, $\forall i$ in (3.2.3);

STEP 2: Choose an approximation model ((5.5.17) or (5.5.18)) to estimate K_1 and compute $\bar{T}_i^w[k]$, $\forall i$ using (5.4.7) with $k=K_1$;

STEP 3: Generate the binary indicator random variable at each SN:

if $\bar{T}_i^w[K_1]<\Lambda_1,\ I_i[0]=0$

if $\bar{T}_i^w[K_1]\geq\Lambda_1,\ I_i[0]=1$.

STEP 4: Run (5.4.14) with $I_i[0]$ generated in step 3 for K_2 iterations to effectively perform the final test:

if $\bar{T}_f^w[K_1]=0$, decide $\mathcal{H}_0$

if $\bar{T}_f^w[K_1]\neq 0$, decide $\mathcal{H}_1$

where $\bar{T}_f^w[K_1]=\sum_{i=1}^{M} I_i[0]$.

Next, in the simulation results, we will show that the first step spatial collaboration among SNs is crucial for the system detection performance and also for the network total power consumption. We will also show via simulations that there is an optimum K_1 (for both decision fusion (5.4.12) and (5.4.13)) such that the system

detection performance is maximized. Then, we propose a sub-optimum but simple solution to find this optimum K_1.

5.5 Simulations Results

Here we will analyze the performance of our proposed two-step quantized (weighted) fusion rule algorithm for distributed detection deployment. First we have a WSN with M SNs with an arbitrary SN geometry, where the distances d_{ij} in (5.4.2) between SNs i and j are assumed to be known. The other parameters in (5.4.2) are $p_{ij}^t = 300$, $\gamma = 2$, $\zeta_i = 0.1, \forall i$ and h_{ij}^2 is an exponential random variable (r.v.) with mean $\mu_{h_{ij}^2} = 30$. Using the r.v. SNR_{ij} in (5.4.2) in (5.4.1), we then construct two example topologies for different values of Υ (see Fig. 5.5). These topologies will be used later for Fig. 5.15 and Fig. 5.16. To provide results of more general validity, we also report the average performance where the average is carried out over 500 channel realizations unless otherwise stated. We now generate the test statistics $\bar{T}_i^w[K_1]$ in (5.4.11), via (5.4.7) for $k = K_1$. As previously explained, any $I_i[K_2]$ in (5.4.15) or (5.4.16) can be used to decide either $\mathcal{H}_0$ or $\mathcal{H}_1$, and this will define the new global detection and false alarm probabilities (i.e., P_d^g and P_{fa}^g respectively). Here we use 10^5 Monte-Carlo simulations. Finally, $\xi_a = 10\log_{10}\left(\frac{1}{M}\sum_{i=1}^{M}\xi_i\right)$ = -9.5 dB unless otherwise stated, where $\xi_i = \sum_{n=1}^{N} s_i^2(n)/N\sigma_i^2$. We will also refer to "equal weight" combining in (5.3.12) (i.e., $\alpha_i = 1, \forall i$) and use this as a benchmark. Finally, we choose L_i with equality in (5.3.1). The detection performance of the proposed two-step algorithm is also compared with the *centralized* soft Likelihod Ratio Test (LRT) based fusion rule in [36].

5.5.1 Validity of Quantization Noise Assumption for Low Bit Rate

Before we investigate the performance of the proposed two-step detection algorithm, we evaluate via simulations the mismatch between the assumed uniform quantization and the actual quantization for low bit rate. In Fig. 5.3, we show the probability

distribution function (PDF) of the quantization error for $q = 2$ bits and $q = 3$ bits. The quantization error variance (σ_e^2) versus the number of quantization bits (q) is also plotted. In the case of $q = 2$ bits, the uniform (quantization error) PDF is

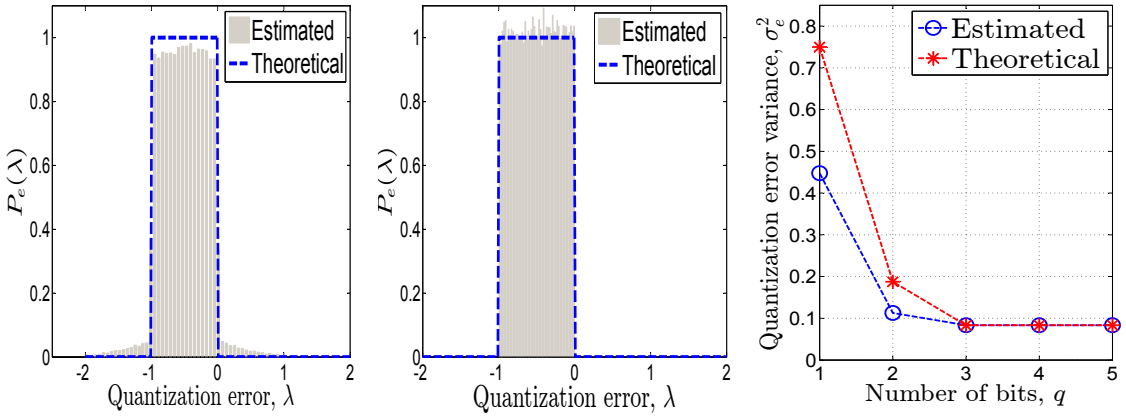

Figure 5.3: Quantization error mismatch: (left/middle) probability distribution function (PDF) $P_e(\lambda)$ for $q = 2$ bits/ $q = 3$ bits; (right) quantization error variance (σ_e^2) mismatch versus number of quantization bits.

an approximation. However, in the case of $q = 3$ bits, this approximation is quite accurate. As a result, we conclude that the assumption of a uniform (quantization error) PDF is a valid assumption (or at least for the simulation set-up considered in this paper).

5.5.2 Impact of Channel Estimation on the Network Density

Now, we investigate the channel estimation error effect on the network density (ρ) versus the SNR threshold (Υ). We model the channel estimation error as a Gaussian random variable (i.e., $\hat{h}_{ij} = h_{ij} + e_h$) where $e_h \sim \mathcal{N}(0, \sigma_{e_h}^2)$ and $\hat{h}_{ij}$ is the estimated flat fading channel coefficient.

In Fig. 5.4, we plot the network density[10] (ρ) versus the SNR threshold (Υ) for different values of the estimation error variance ($\sigma_{e_h}^2$). For small $\sigma_{e_h}^2$, the network density is shown to be robust against the channel estimation error. That is not the case for relatively large $\sigma_{e_h}^2$ where a performance mismatch is observed.

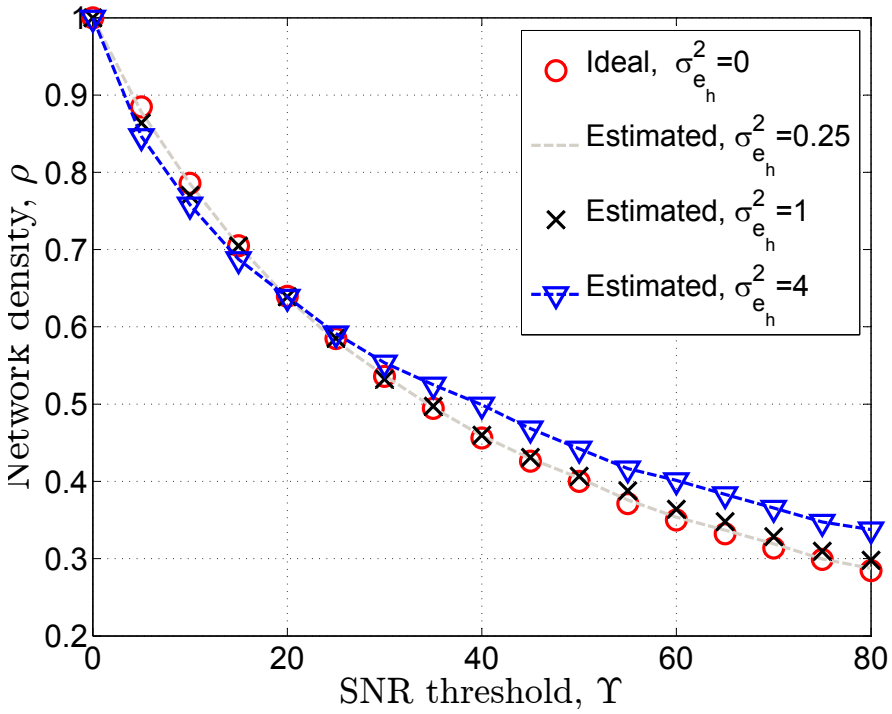

Figure 5.4: Averaged (over 10000 $\hat{h}^2_{ij}$ realizations) network density (ρ) versus Υ in (5.4.1), with $U = 3$, $N = 20$, and $M = 17$.

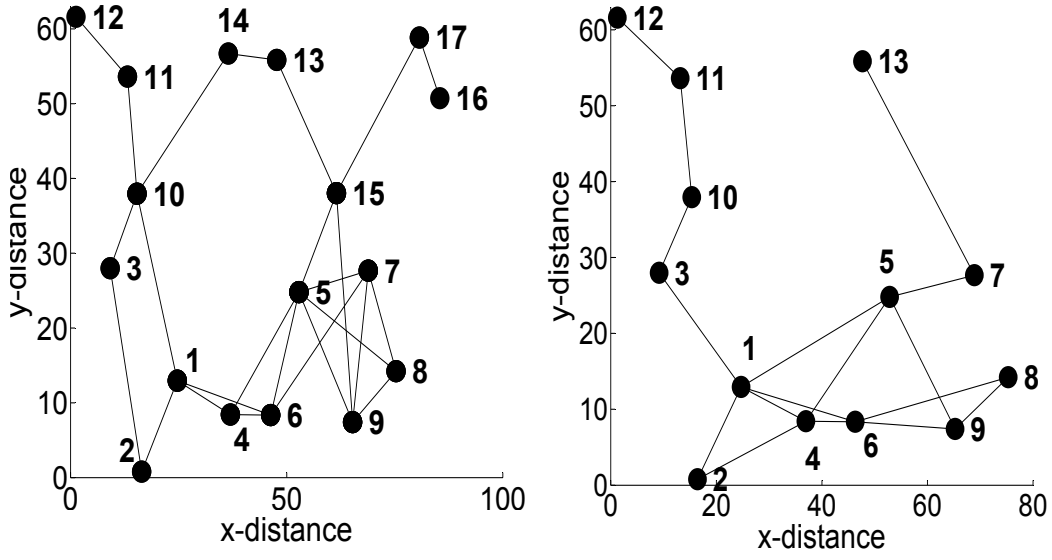

Figure 5.5: Two different communication topologies (generated via ((5.4.1) and (5.4.2)), with $\sigma^2_{e_h} = 0$ and the quantization bits following (5.4.3): (left) $M = 17$, $\Upsilon = 20$, $q = 2$ bits; (right) $M = 13$, $\Upsilon = 72$, $q = 3$ bits.

5.5.3 Impact of Thresholding Operation on the System Detection Performance and Total Power Consumption

In section 5.4, we have shown that the link SNR threshold (Υ) parameter establishes a relation between the number of bits that each SN has to transmit to its neighbors and the topology of the network that defines the connections among them (see definitions (5.4.1)-(5.4.3)). It is then very important to investigate the impact of the Υ parameter on the system (global) detection performance (P_d^g) and on the total power consumption (P_T).

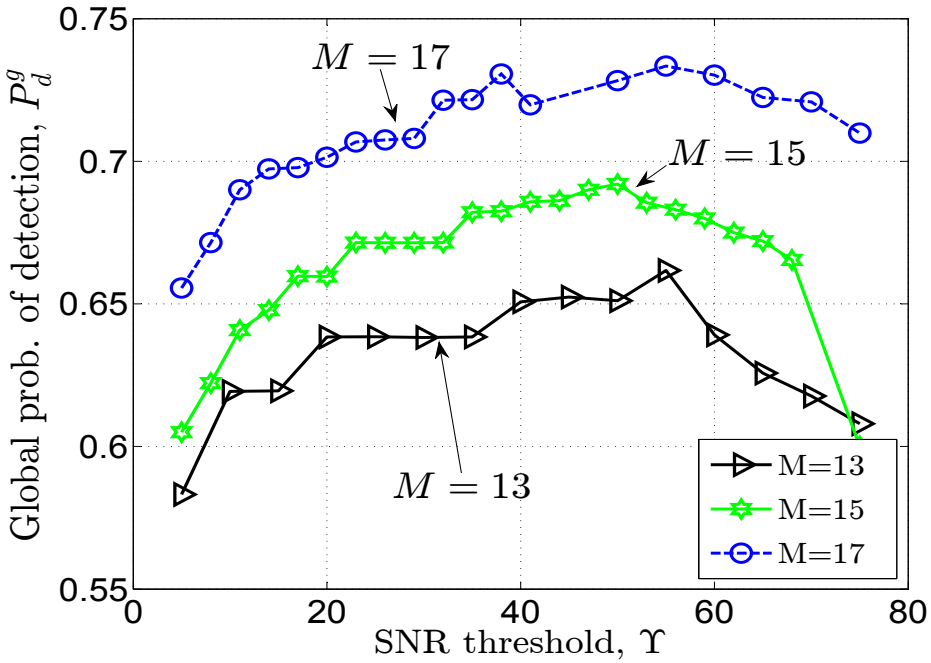

Figure 5.6: Averaged (over 500 h_{ij}^2 realizations) global probability of detection (P_d^g) (using two-step approach) versus Υ in (5.4.1), $\sigma_{e_h}^2 = 0$, with decision fusion in (5.4.15), $P_{fa}^g = 0.2$, $U = 2$, $N = 20$, $K_1 = 10$ and $\alpha_i = 1, \forall i$ in (5.4.4).

In Fig. 5.6 we plot the global probability of detection (P_d^g) versus Υ for different numbers of SNs (M) and for a fixed global probability of false alarm (P_{fa}^g) and K_1. We observe that there is an optimum Υ that maximizes P_d^g for any arbitrary M.

Now, to give a more general validity to the results, in Fig. 5.7 we show the conventional (unquantized) consensus-based algorithm (5.3.22) (with the decision rule (5.3.15) by substituting $T_i^{eq}[k]$ with $T_i^w[k]$) and the proposed two-step (quantized)

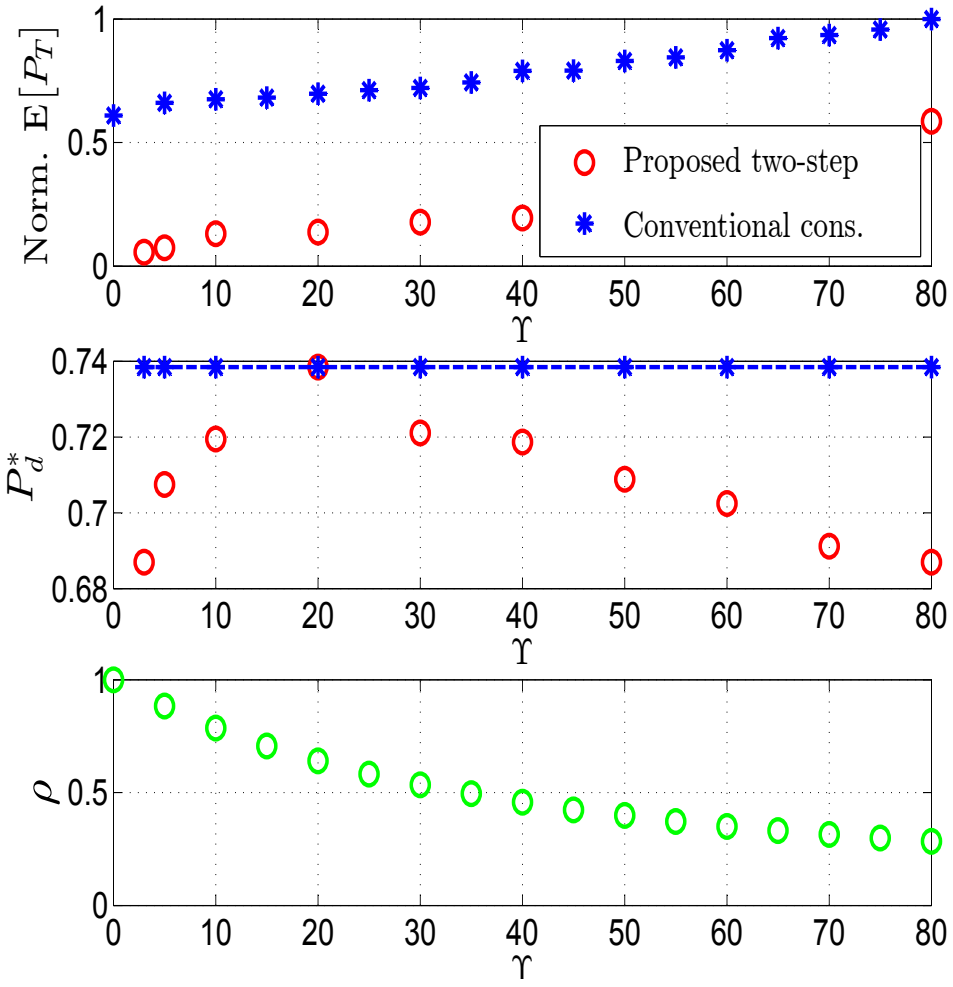

Figure 5.7: Normalized average power consumption ($\mathbb{E}[P_T]$), achievable[8] probability of detection (P_d^*) and the average communication link density (ρ) versus Υ in (5.4.1), with $\sigma_{e_h}^2 = 0$, decision fusion in (5.4.16), $P_{fa}^g = 0.1$, $U = 3$, $N = 20$, $M = 17$ and with α_i (scaled by M) in (5.3.9).

weighted fusion rule (summarized in **Algorithm 5.4.1**): (upper plot) the average total power consumption $\mathbb{E}[P_T]$ (refer for its definition to (5.4.6) and below) versus the link SNR threshold (Υ); (middle plot) the global achievable[9] probability of detection (P_d^*) versus link SNR threshold (Υ); (lower plot) the average network density[10] (ρ) versus the link SNR threshold (Υ). Even-though the comparison made

[9]The global achievable probability of detection (P_d^*) (for a fixed Υ) is defined as the best global probability of detection (P_d^g) with respect to K_1.

[10]The average network density ρ is defined as: $\rho = \mathbb{E}\left[\frac{\sum_{i=1}^{M}\sum_{j=1}^{M} e_{ij}}{M(M-1)}\right]$.

is not fair (i.e., for the proposed (quantized) two-step weighted fusion rule versus the (unquantized) conventional consensus-based fusion rule), clearly our proposed two-step fusion rule algorithm posses the following: a) it requires much less power budget for all Υ compared to the (unquantized) conventional consensus-based algorithm, and b) converges across the WSN much faster and in a finite number of iterations ($K_T = K_1 + K_2$), whereas for the conventional consensus-based, the convergence holds in limit. Finally, in the lower plot we verify (as expected) that a smaller/larger Υ dictates a more/less connected WSN respectively. In the case of the conventional consensus-based algorithm, the convergence criteria we use here is the relative absolute difference: $\frac{||\mathbf{T}^w[k+1]-\mathbf{T}^w[k]||}{||\mathbf{T}^w[k]||} \leq \kappa$, where $\kappa = 10^{-7}$. The averages are performed over 500 (h_{ij}^2) realizations.

5.5.4 Impact of the K_1 Parameter on the System Detection Performance

The first step *quantized collaboration* establishes a linear spatial collaboration among M SNs up to K_1 iterations for improving the overall detection performance. We have shown analytically (see proposition 3 and below) that the RHS of (5.4.10) diverges for $k = K_1$ (when K_1 is large) and the detection performance eventually declines. Next, we investigate (through simulations) the effect that (K_1) has on the global detection performance (P_d^g) and propose a sub-optimum (but simple) solution to evaluate K_1.

Optimal numerical solution to K_1

Now, in Fig. 5.8 we report the (averaged) receiver operating characteristic (ROC) against the first step number of iterations (K_1) for the proposed distributed two-step (weighted) algorithm with decision fusion in (5.4.15). As K_1 increases then P_d^g improves. In Fig. 5.9 we report the same for the proposed two-step (weighted) algorithm but now with the decision fusion in (5.4.16). As expected, the detection performance improves up to $K_1 = 150$ and after that it degrades. Then, in Fig. 5.10 we plot the (averaged) global detection performance (P_d^g) (for a fixed global prob-

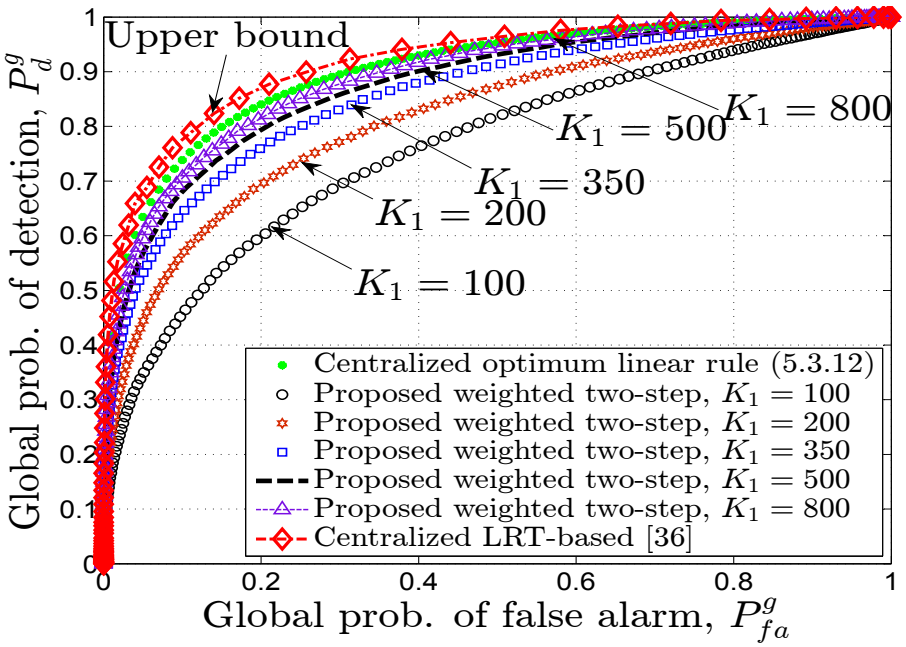

Figure 5.8: Averaged (over 500 h_{ij}^2 realizations) ROC for the proposed two-step weighted algorithm with decision fusion in (5.4.15), $U = 3$, $N = 20$, $M = 17$, $K_2 = 3$, $\Upsilon = 30$, $\sigma_{e_h}^2 = 0$ and with α_i (scaled by M) in (5.3.9).

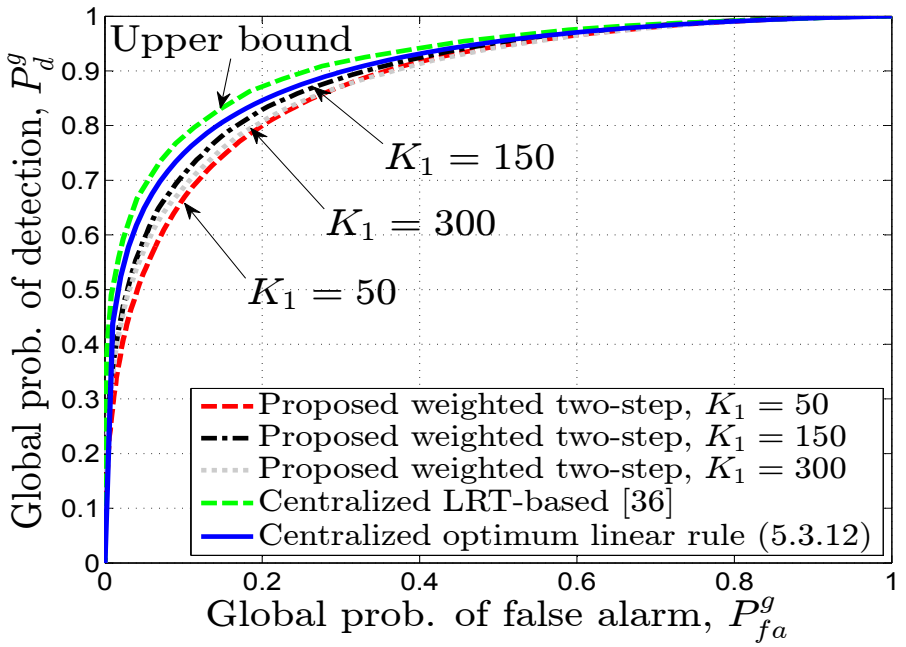

Figure 5.9: Averaged (over 500 h_{ij}^2 realizations) ROC against first step iterations number (K_1), with decision fusion in (5.4.16), $K_2 = 2$, $U = 3$, $N = 20$, $M = 17$, $\Upsilon = 10$, $\sigma_{e_h}^2 = 0$ and with α_i (scaled by M) in (5.3.9).

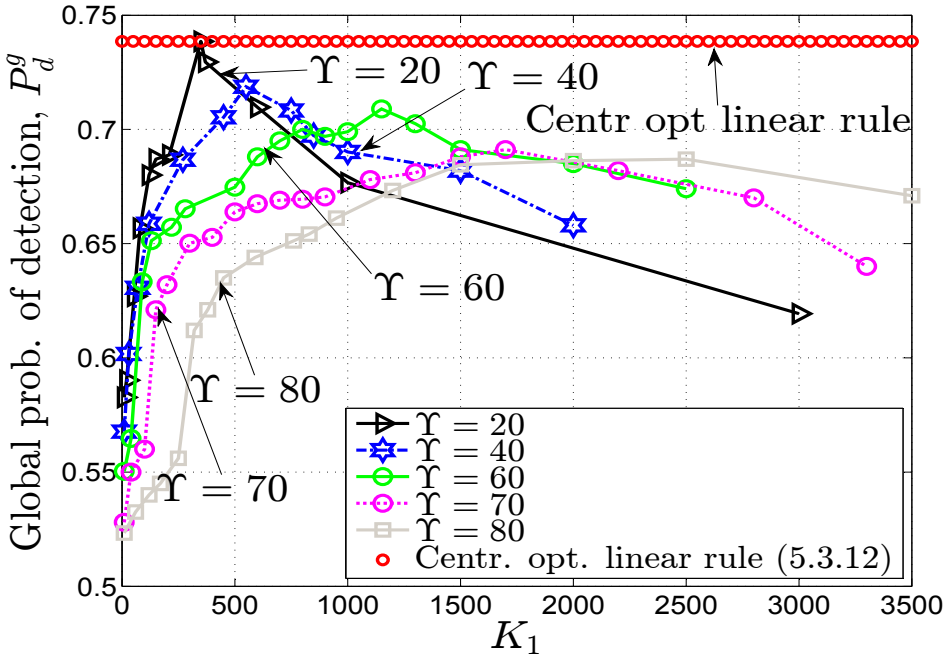

Figure 5.10: Averaged (over 500 h_{ij}^2 realizations) global probability of detection (P_d^g) versus first step iterations number (K_1), with decision fusion in (5.4.16), $P_{fa}^g = 0.1$, $U = 3$, $N = 20$, $M = 17$, $\sigma_{e_h}^2 = 0$ and with α_i (scaled by M) in (5.3.9).

ability of false alarm (P_{fa}^g)) versus first step number of iterations (K_1) for different link SNR thresholds (Υ). We observe that there exists an optimum K_1 to run the first step time evolution (5.4.4) such that P_d^g is maximized for any arbitrary Υ. We also note that the best performance is attained for $\Upsilon = 20$.

Now, selecting the pair ($\Upsilon = 20$, $K_1 = 320$) (i.e., the Υ and K_1 that attain the best performance in Fig. 5.10 with the decision fusion in (5.4.16)), in Fig. 5.11 we examine the P_d^g performance against ξ_a for the proposed distributed two-step (weighted) algorithm assuming: (left) ideal channel estimation; (right) non-ideal channel estimation. Interestingly, (for the ideal channel case) the proposed two-step (weighted) algorithm performance (with decision fusion in (5.4.16)) attains its centralized counterpart's upper bound performance for all ξ_a. So, it is now clear that the optimum values of parameters Υ and K_1 are independent of ξ_a (i.e., the local ξ_i). This independence is important as it shows that the algorithm is robust against the local ξ_i and allows evaluating these parameters once at the beginning. We also observe that the proposed two-step performance with decision fusion (5.4.16)

is the same (at low SNR) as that of decision fusion (5.4.15), but at high SNR it outperforms the latter. Now (for the non-ideal case), we can observe a slight detection performance degradation for the proposed two-step algorithm. Next, we propose (for the two-step algorithm with the second step decision rule (5.4.16)) a sub-optimum (but simple) solution to the optimum K_1. Note that the extension with the second step decision fusion rule (5.4.15) is straight forward.

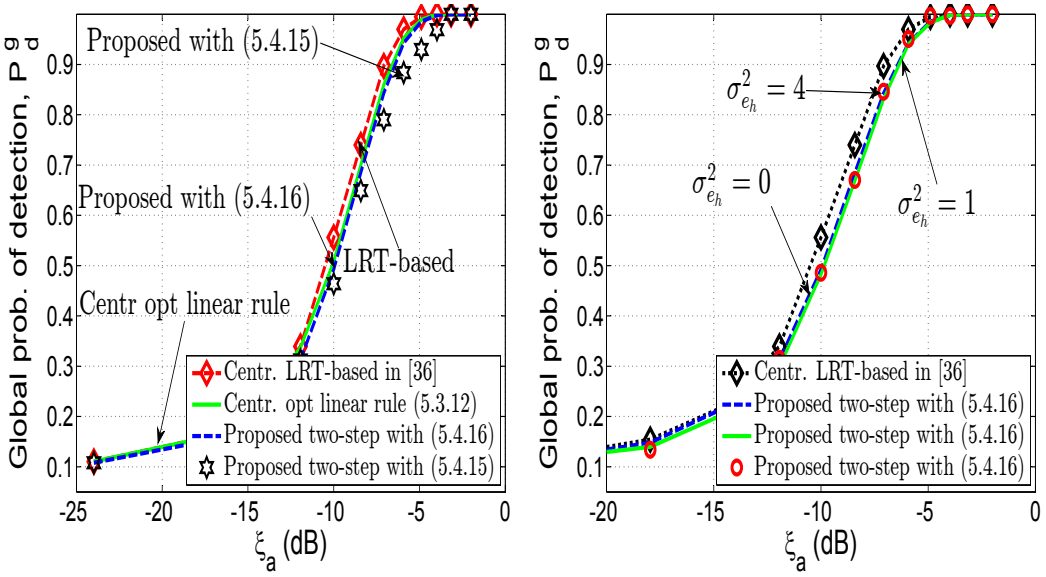

Figure 5.11: Averaged (over 500 h_{ij}^2 realizations) probability of detection (P_d^g) against the signal to noise ratio (ξ_a) with $P_{fa}^g = 0.1$, $U = 3$, $N = 20$, $M = 17$, $K_1 = 320$, $\Upsilon = 20$, $\xi_i = \xi, \forall i$ in (4) and with α_i (scaled by M) in (5.3.9): (left) ideal, $\sigma^2_{e_h} = 0$; (right) non-ideal, $\sigma^2_{e_h} \neq 0$.

Suboptimal Solution to K_1

Now, through simulation results shown in Fig. 5.10, we get an insight on how the optimum K_1 is related to the link SNR threshold (Υ). We also notice that an increase in Υ is translated into a corresponding increase in the optimum K_1 value (i.e., K_1 that corresponds to the maximum P_g^d). This result is not surprising and can be explained by the fact that a smaller Υ dictates a more connected graph (see (5.4.1)) and an increase in Υ dictates a sparse graph (hence more iterations are needed to diffuse the information across the SNs). Motivated by this fact, we now relate the first step iterations number (K_1) to the link SNR threshold parameter

(Υ) with two fitting models:

(i) *Exponential model* :

$$K_1 \approx g(\Upsilon) = \begin{cases} A\exp(b\Upsilon) & \text{type 1} \\ A\exp(b\Upsilon) + B\exp(c\Upsilon) & \text{type 2} \end{cases} \tag{5.5.17}$$

(ii) *Power model* :

$$K_1 \approx g(\Upsilon) = \begin{cases} A\Upsilon^b & \text{type 1} \\ A\Upsilon^b + \mathcal{C} & \text{type 2} \end{cases} \tag{5.5.18}$$

where A, B, $\mathcal{C}$, b and c are the coefficients given in Table 5.1 obtained using Matlab (Nonlinear Least Squares method and Trust-Region algorithm).

Table 5.1: Parameters for different fitting models

Model	Type	A	B	$\mathcal{C}$	b	c	RMSE
Exponential	Exp 1	173.6	x	x	0.03319	x	49.82
	Exp 2	188.1	1.561e-014	x	0.03166	0.4584	53.09
Power	Pow 1	0.5976	x	x	1.89	x	136.27
	Pow 2	0.0079	x	2.853	338.9	x	63.65

Now, in Fig. 5.12 we plot the first step number of iterations (K_1) versus the link SNR threshold (Υ) for two different fitting models (i.e., *exponential* and *power model*) and then compare these to the simulations. Clearly, the *exponential* of *type* 1 is the best candidate as it attains the minimum RMSE (see Table 5.1).

5.5.5 Detection Performance Comparison

We now compare the (averaged) global detection performance among/with: (a) the two-step (quantized) distributed weighted fusion rule algorithm with second step in (5.4.15) and (5.4.16), (b) the two-step (quantized) distributed equal combining fusion rule with second step in (5.4.15) and (5.4.16), (c) the optimum centralized (quantized) weighted fusion rule proposed in [35], and (d) the centralized (quantized) equal combining in [35].

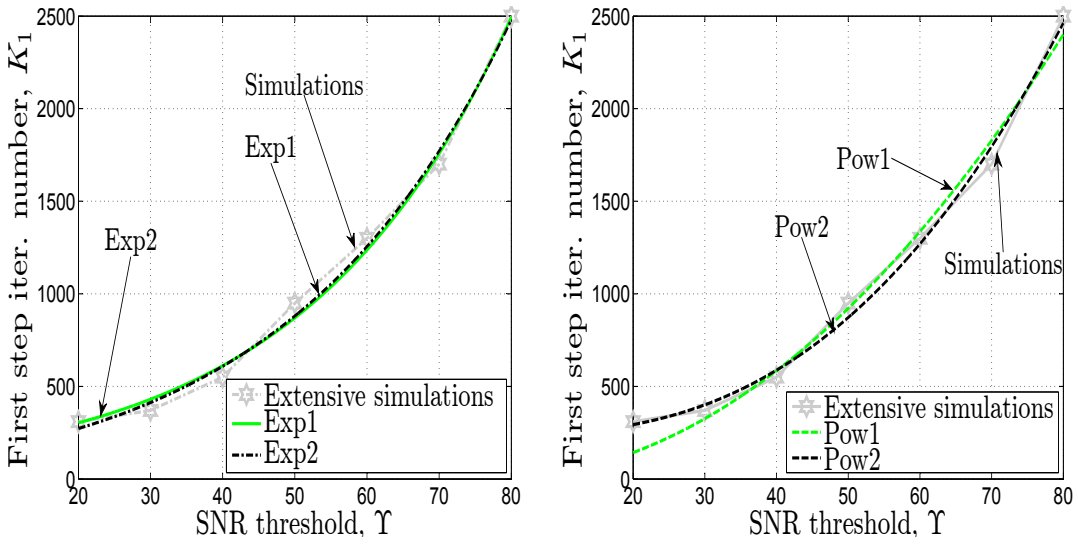

Figure 5.12: First step iterations number (K_1) versus Υ in (5.4.1), with $U = 3$, $N = 20$, $M = 17$ and with α_i (scaled by M) in (5.3.9): (left) exponential fitting model; (right) power fitting model.

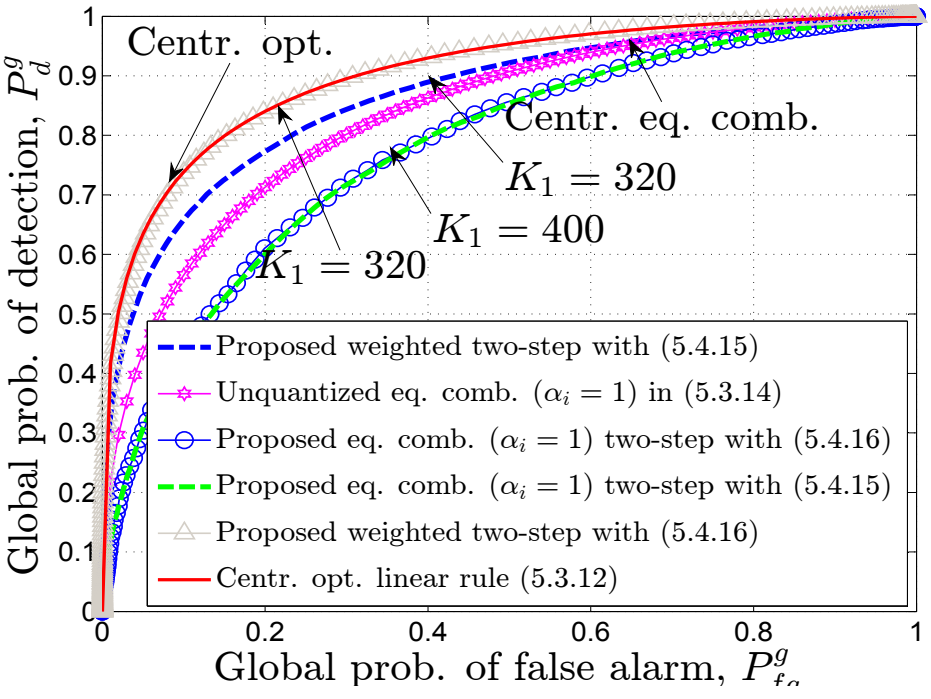

Figure 5.13: Averaged (over 500 h_{ij}^2 realizations) ROC for the proposed (quantized) two-step weighted fusion rule with $U = 3$, $N = 20$, $\Upsilon = 20$, $M = 17$ and with α_i (scaled by M) in (5.3.9).

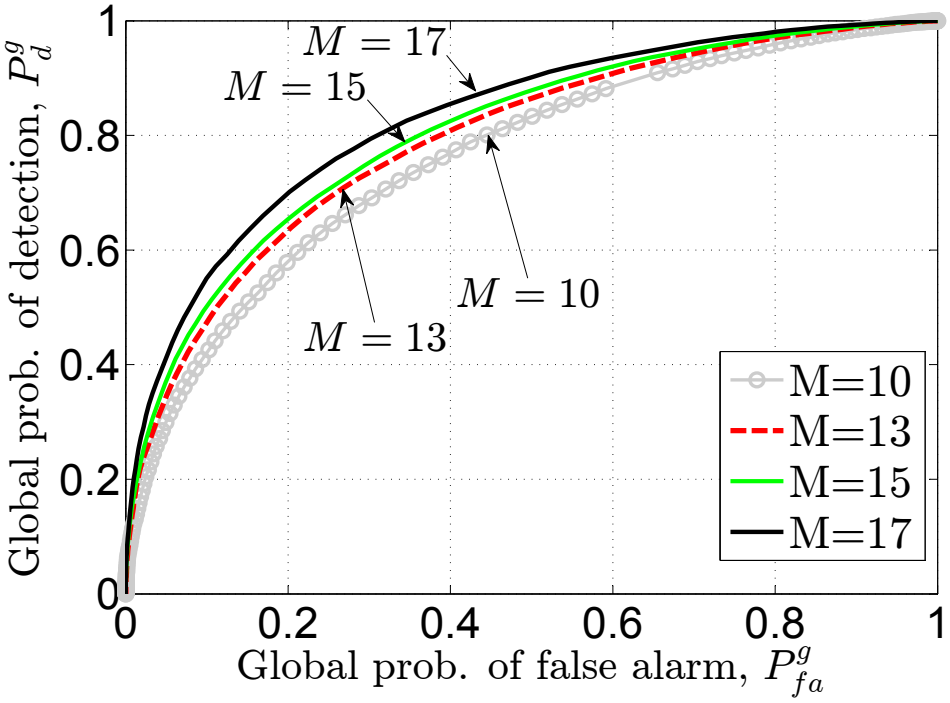

Figure 5.14: ROC for the proposed (quantized) two-step distributed scheme with $\Upsilon = 20$ in (5.4.1), $U = 2$, $N = 20$, $K_1 = 10$ and $\alpha_i = 1, \forall i$ in (5.4.4).

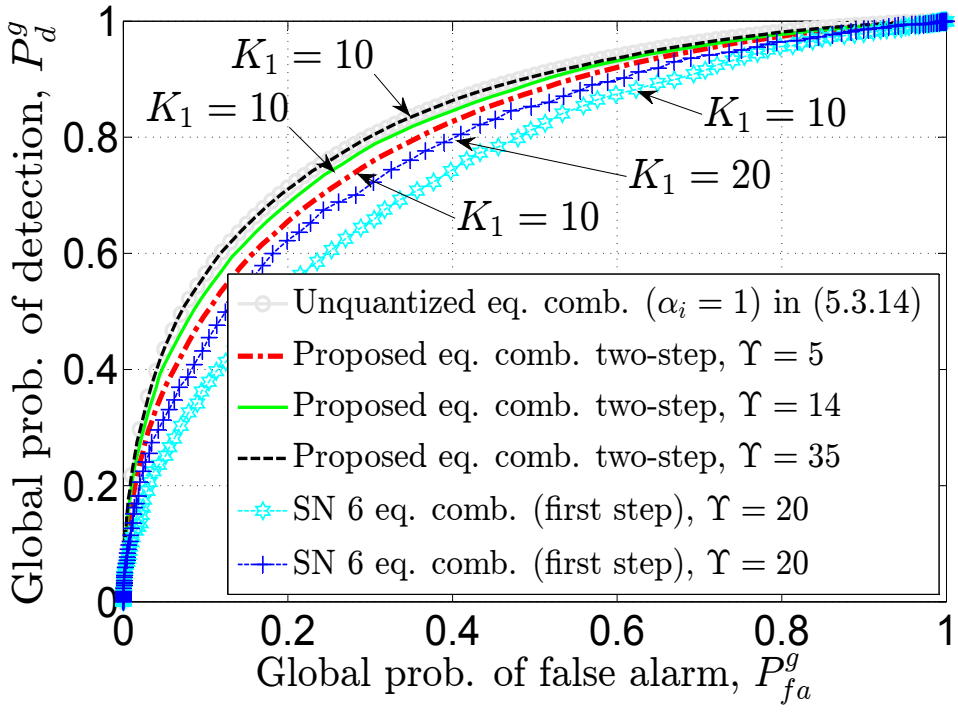

Figure 5.15: ROC with $U = 2$, $N = 20$, $M = 17$ and topology given in left of Fig. 5.5 and $\alpha_i = 1, \forall i$ in (5.4.4).

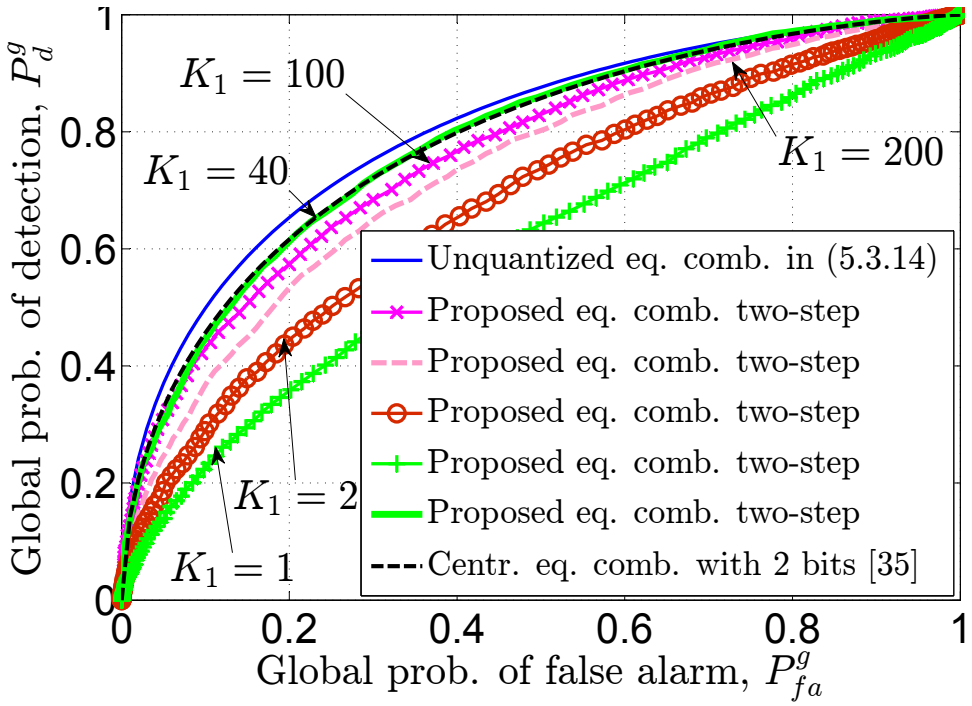

Figure 5.16: ROC with $U = 2$, $N = 20$, $M = 13$ and topology given in right of Fig. 5.5 and $\alpha_i = 1, \forall i$ in (5.4.4).

In Fig. 5.13 we report the ROC for the two different schemes (i.e., centralized and distributed two-step). As can be seen, the distributed two-step algorithm approaches the upper bound (i.e., the centralized unquantized scheme performance in (5.3.12)). Now, we examine in Fig. 5.14 the ROC parametrized against M for the distributed (equal combining) two-step algorithm, illustrating how P_d^g improves as M increases. The ROC performance[11] among different (equal combining) schemes is illustrated in Fig. 5.15 and Fig. 5.16. In Fig. 5.15 we show the advantage of our proposed distributed two-step (equal combining) scheme over only the first step part (at SN 6). Also, if Υ is carefully chosen the distributed two-step (equal combining) scheme performance approaches that of the (equal combining) centralized detector (i.e., with FC and no quantization) in (5.3.15). Fig. 5.16 shows the ROC for the proposed quantized (3 bits) distributed (equal combining) two-step algorithm

[11]SN 6 in Fig. 5.15 and SN 3 in Fig. 5.17 were chosen for comparison purposes as they possess the best performances among M SNs for each case.

against K_1 compared to the quantized (2 bits) centralized (equal combining) scheme in [35]. As expected (similar to the weighted two-step), there is an optimum K_1 that maximizes P_d^g and after that P_d^g decreases.

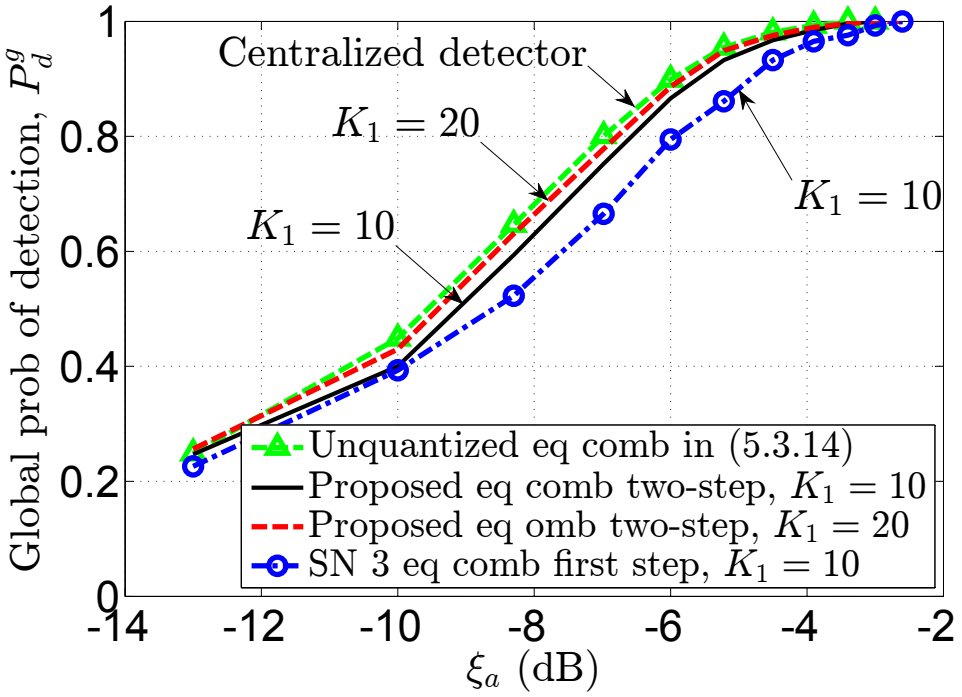

Figure 5.17: Probability of detection (P_d^g) versus the signal to noise ratio (ξ_a) for $M = 13$, $\Upsilon = 72$, $U = 2$, $N = 20$, $P_{fa}^g = 0.1$, $\xi_i = \xi, \forall i$ in (3.2.4) and $\alpha_i = 1, \forall i$ in (5.4.4). The topology used is given in right of Fig. 5.5.

Finally, Fig. 5.17 plots the P_d^g performance characterization against the average SNR (ξ_a) for 4 different (equal combining) schemes showing the performance improvement of our proposed distributed two-step algorithm.

5.6 Chapter Summary and Conclusions

In this chapter, we propose a fully distributed two-step consensus-based detection algorithm via SNs sharing with their neighbors a quantized version of the received energy test statistic. We relate the communication topology with the number of bits to be shared among SNs and through numerical results we show that there is an optimum topology (for a fixed first step number of iterations (K_1)) such that P_d^g (the

global probability of detection) is maximized. In addition, we show that there is an optimum K_1 to terminate the first step SN collaboration (for any arbitrary topology) and after that the P_d^g performance declines. When parameters K_1 and Υ (the link SNR threshold in (5.4.1)) are appropriately chosen, the detection performance of the proposed quantized distributed two-step algorithm approaches the unquantized centralized optimum combining scheme performance of (5.3.12). Overall, the algorithm requires a finite number of iterations $(K_1 + K_2)$. For example, targeting the optimum P_d^g (see Fig. 6.16 (middle plot) at $\Upsilon = 20$), our proposed two-step algorithm requires roughly 50% less power consumption (P_T) than the conventional consensus-based algorithm. Future work will investigate the analysis of the problem for time-varying SNs interaction topologies.

Chapter 6

Sensor Detection in the Presence of Falsified Observations

IN THIS CHAPTER

Within this chapter, we address the problem of centralized detection in the presence of β fraction falsifiable sensor nodes (SNs) (i.e., controlled by an attacker). The overview of the motivation behind this work is presented. The assumptions made and the problem formulation by describing the target sensing and the WSN architecture are stated. The core sections are mainly a) Section 6.2 that consider the detection problem under local soft-data falsification and analysis of the system performance; b) Section 6.3 that now consider the detection problem when the SNs send their one-bit test statistics to the FC instead of quantized soft decisions. This section also presents the derived expressions for the attacker parameters that makes the FC incapable of detecting, and the proposed novel and non-complex reliability-based strategy to possibly identify these compromised SNs. Simulation results illustrate our analytical findings performance gain of the proposed strategies.

6.1 Introduction

6.1.1 Motivation

Multiple low-cost sensor nodes (SNs) are often spatially deployed over a specific field to observe binary events. The SNs process the observed data and report back to a fusion center (FC) that optimally combines to reach a global decision. Being geographically dispersed to cover large areas, the SNs are constrained in both bandwidth and power. Moreover, SNs are usually unattended and this makes them vulnerable to different types of attacks. The overall detection performance strongly depends on the reliability of these SNs in the network. While fusing the data received by the spatially deployed SNs allows the FC to make a reliable decision, it is possible that one or more SNs (compromised by an attacker) deliberately falsify their local observations to degrade the overall FC detection performance. However, there are a number of different approaches as to how the test statistics received from each SN can be efficiently used in order to achieve a reliable FC decision. Before introducing our proposed strategies, we will first give a brief review of related work.

6.1.2 Related Work

The framework of distributed detection under $attack - free$ WSNs has been considered in previous chapters of this thesis and extensively studied in [30–32, 34–36, 52, 58–60], to name but just a few references. While [32, 52, 58–60] consider centralized detection by assuming WSNs with unlimited bandwidth/resources, the latter assumption was relaxed in [30, 31, 34–36] by considering centralized detection over bandwidth-constrained/energy-constrained WSNs. But these approaches are vulnerable to some security attacks as some of the SNs reporting to the FC may be compromised. As a result, the FC is not robust against such attacks and its detection performance may be degraded.

However, security issues in centralized detection using WSNs remain an open issue, see [9, 12, 66–69] and references therein. While there are many types of security threats, in this chapter we focus on a single type of attack, which is the test statistic falsification (TSF) attack part of the Byzantine attacks family originally proposed

by [8] and later widely used in the context of distributed detection (e.g., [9–11]).

Reference [11] characterizes the power of the attack analytically and a closed-form expression for the worst "detection error" is provided. Also, the minimum fraction of the compromised SNs that makes the FC incapable is derived. Reference [70] presents a technique to identify such compromised SNs and then to exclude them from contributing to the FC fusion process. In [71], a probabilistic TSF attack is proposed and the theoretical performance evaluation (in terms of destructiveness and stealthiness) is obtained. The authors of [72], in the context of smart grids, propose heuristic centralized algorithms to derive various strategies (attacker versus defender (i.e., FC) dynamics). Then, a distributed algorithm is proposed that guarantees convergence to the centralized solution taken at the FC.

Detection in the presence of binary falsification[1] (Byzantine) attacks is considered in [73]. Here, a reputation-based scheme is proposed for identifying the compromised SNs by accumulating the deviations between each SN and the FC decision over a time window duration. The authors in [74] also consider binary Byzantine attacks, in the context of target localization, where the SNs transmit their binary decisions to the FC. These authors also propose two techniques to mitigate the negative input of the compromised SNs on the FC decision. However, identifying and then excluding the contributions of the compromised SNs from the FC decision process may not be the best strategy. Furthermore, performing detection by means of one-bit SNs report combining at the FC is also not optimum. Recently, the authors in [75, 76] both consider a decentralized network in the presence of compromised SNs while in this paper we consider a centralized scheme. The authors in [75] propose a synchronous distributed weighted average consensus algorithm that is claimed to be robust to Byzantine attacks while reference [76] considers the detection and mitigation of data injection attacks in a randomized average consensus.

Now, the publication closest to the work presented in Section 6.2 is [9], where an $under-attack$ WSN framework over unlimited bandwidth is considered (i.e., infinite channel capacity) and the detection performance is investigated. But as the SNs

[1]The compromised SNs falsify their hard decisions instead of their actual test statistics prior to transmission to the FC.

are battery operated devices (i.e., limited power) and the bandwidth is finite, the assumption of infinite capacity is unrealistic. Furthermore, practical WSN scenarios suffer from fading and attenuation. The authors of [9] also do not propose any technique to mitigate the degradation caused by these compromised SNs. So, the work in Section 6.2 investigates the detection performance of the $under-attack$ energy-constrained/bandwidth-constrained WSNs. The compromised SNs (controlled by the attacker), are assumed to know the true hypothesis[2](e.g., [9, 11]) and they use this $a-priori$ knowledge to construct the most effective strategy to make the FC's decision unreliable. For the FC, we assume that it is not compromised and receives the test statistic from both types of SNs (i.e., compromised and honest). The transmission (SNs to FC) links are modeled as flat fading, additive white Gaussian noise (AWGN) channels. The assumption of flat fading is reasonable as most of the WSNs operate at both short distances and low bit-rate due to resource limitations.

The work in Section 6.2 investigates again the detection performance of an $under-attack$ WSN. However, to reduce the transmission and processing burden of the SNs, each SN generates the 1-bit local test statistic by performing energy detection [88] and reports this test statistic to the FC. As in [73], we relax the assumption of perfect knowledge of the true hypothesis [11] and we assume that the compromised SNs (controlled by the attacker) do not know the true state of the target. For the FC, we assume that it is not compromised and receives the test statistic from both types of SNs (i.e., compromised and honest). The transmission (SNs to FC) links are assumed error free (see eg., [11], [73]).

6.1.3 Chapter Contributions

While previous publications (as outlined above) have also examined sensor networks in the presence of falsified SNs, this chapter deals with more realistic scenarios that include limited bandwidth fading channels, quantization of test statistics, etc. So our main contributions are developed within Section 6.2 and Section 6.3 and are briefly stated in here for each section for clarity purposes.

[2]This leads to a conservative assessment but allows analytical tractability of the security risk.

Chapter Contributions- Section 6.2

The main contributions of Section 6.2 can be summarized as:

(i) We develop an efficient FC linear weight combining framework for an *under−attack* WSN that operates over limited bandwidth fading channels. The probability of detection (P_d) and the probability of false alarm (P_{fa}) based on this framework are derived in a closed-form. To maximize P_d for a fixed P_{fa} and to further reduce the optimisation complexity, we adopt the modified deflection coefficient (MDC) [32] as an alternative function to be optimized and provide an optimisation problem to be solved from both the FC's and the attacker's perspective. Based on this optimisation problem (from the FC's perspective), we derive analytically the optimal weight combining, the optimal SN to FC transmit power and the number of quantization bits for each SN. Unfortunately, these expressions require *a−priori* knowledge about the attacker parameters which cannot be attained in practice. Then (from the attacker's perspective), we derive analytically (for a fixed number of compromised SNs) the optimum attacker strategy which also depends upon the FC weight combining and the SNs transmit power.

(ii) So, motivated by the above, we next analyze the problem under different attacking and defending scenarios and characterize analytically the performance of sub-optimum strategies (from both the FC's and the attacker's perspective) that do not require knowledge of the FC mechanism and the attacker parameters. Also, based on the willingness of collaboration among the SNs (from the attacker's perspective), we distinguish between two setups: a) all the SNs (compromised and honest) share their data with their neighbors, and b) just the compromised SNs are willing to collaborate among themselves to improve their attack strength.

(iii) Finally, we re-cast the problem as a minimax game between the FC and attacker and show that the NE (Nash Equilibrium) exists. Having defined the game, we use numerical simulations to find this NE point, thus identifying the optimum behavior of both the FC and the attacker in a game-theoretical sense.

Chapter Contributions- Section 6.3

Now, the main contributions of Section 6.3 are as follows:

(i) First, as before, we adopt the MDC as an alternative function to be optimized and derive analytically in a closed form the optimal weight combiner for each SN (note that the attacker model considered in this section is different to that considered in Section 6.2). We now show that these weights are a function of the local SNs probability of false alarm and probability of detection metrics as well as the SNs local test statistics flipping probability. Unfortunately, for the compromised SNs this *a priori* knowledge cannot be attained in practice (we propose a solution to this (see later (ii))). Then (from the attacker's perspective), we derive analytically (for a fixed number of compromised SNs) the optimum attacker local test statistics flipping probability and the minimum fraction of the compromised SNs that makes the FC incapable of detecting.

(ii) Next, based on this framework (i.e., FC linear weight combing strategy), we also propose a new non-complex and efficient reputation-based FC detection scheme to identify the compromised SNs [104]. Our approach [104] is different from the existing approaches [11], [73], [101] mainly in two important aspects: 1) We introduce a new reputation-based metric at the FC to identify the compromised SNs. First, we count the inconsistency between the FC's decision (where all the SNs contributions are considered) and the i^{th} local SN's decision over a time window. Similarly, next we count the inconsistency between the FC's decision (where the i^{th} SN contribution is not considered) and the i^{th} local SN's decision. Finally, the proposed reputation metric is evaluated as the difference between these two; 2) Then, based on this reputation metric, we propose a novel FC weight computation strategy that ensures the following: a) for the identified compromised SNs, their weights are likely to be decreased proportionally to this metric (where the existing schemes assign a zero-weight). b) In this way (based on this new reputation metric), the FC decides how much a SN should contribute to its final decision. We will show that this strategy outperforms the existing schemes where the identified compromised SNs are totally excluded toward the FC final decision contribution (i.e., a zero-weight is assigned).

6.1.4 Chapter Outline

Now, the summary of the chapter is as follows. In the first part (more specifically for Section 6.2), in Subsection 6.2.1 we describe the system model and provide a data transmission scheme. Subsection 6.2.4 describes the optimisation problem from both the FC's and the attacker's perspective. In Subsection 6.2.5 we present our proposed attacker and FC strategies and in Subsection 6.2.6 we re-cast the problem and analyze the equilibrium. Then, in Subsection 6.2.7 we present some simulation results.

In the second part (more specifically for Section 6.3), in Subsection 6.3.1 we describe the system model (SN sensing and local decision) and describe the compromised SNs attack model. Subsection 6.3.3 introduces the simplified linear weighted fusion rule and analyzes the optimization problem from both the FC's and the attacker's perspective. In Subsection 6.3.7 we present our proposed compromised SNs identification metric and weight combining computation strategy. Then, in Subsection 6.3.8 we present simulation results. Finally, in Section 6.4 we give conclusions and chapter summary.

6.2 Centralized Detection: Under Soft-Data Falsification and Energy-Bandwidth Limitation

6.2.1 System Model

In this section, we describe the target sensing, communication channel, and the WSN architecture.

Target Sensing

In this chapter, we consider an under-attack WSN with M SNs (where a fraction (β) of these SNs are compromised) reporting to a FC tasked with the detection of a binary event. The event leaves a signature signal that is unknown to the WSN but it is assumed to be deterministic. The other assumptions made regarding the target sensing are also identical to those stated in the previous Chapters (e.g., Chapter

3) and each of the local SN estimates the test statistic as in (3.2.3). While the honest SNs transmit the actual test statistics (i.e., the true energies) to the FC, the compromised SNs falsify them before transmitting to the FC (see later the compromised SNs attack model subsection for more details).

Communication Channel

Identical to previous chapters (e.g., Chapter 3), the communication between the local SNs and the FC are modeled as error-free (the SNs transmit a quantized information matched to the channel capacity of each link) orthogonal flat fading channels and additive white Gaussian noise (AWGN) with a known variance ζ_i. Also, the assumptions considered regarding the communication channels are identical to those stated in the previous chapters (e.g., Chapter 3).

WSN Architecture

In this chapter, we adopt a similar WSN architecture as in Chapter 3 (i.e., the *centralized* architecture) where there is a FC that communicates with spatially distributed SNs. In this chapter, different from Chapter 3, we consider an under-attack WSN where a fraction (β) of these spatially distributed SNs are compromised and do not act in the normal "honest" way (see Fig. 6.1). The honest SNs are represented with a black color and the compromised SNs (i.e., the ones controlled by the attacker) with a red color. The attacker's aim is to successfully manipulate the FC global decision making process while the FC would like to detect reliably (i.e., with very high probability). Each SN collects N samples of the observed signal and performs energy estimation (see (3.2.3)). Next we introduce the attacker model.

6.2.2 Compromised SNs Attack Model

In this work, the same attack model used in [9] is considered. The attacker (which has under its control a fraction (β) of the SNs) is assumed to know the true hypothesis[2] in (6.2.1) (e.g., [9, 11]). The remaining SNs are honest and completely unaware of the presence of falsified SNs. The i^{th} compromised SN falsifies its test

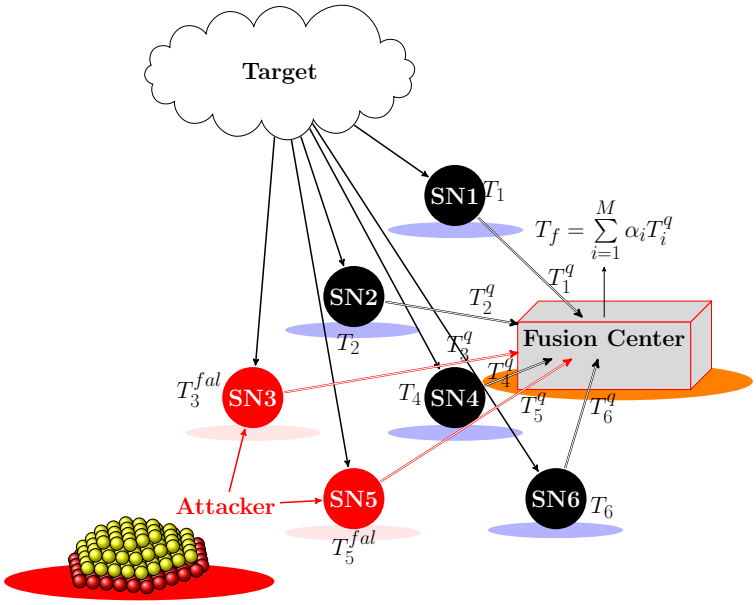

Figure 6.1: Under attack schematic communication architecture between peripheral SNs and the fusion center (FC). Each SN generates a test statistic (T_i) by observing the target and can communicate with the FC only over an energy-constrained/bandwidth-constrained link. While the honest SNs (represented by black color) test statistics remain unchanged, the compromised SNs (represented by red color) falsify their test statistics to T_j^{fal} with $j = \{3, 5\}$ (where j is the compromised SN index) before transmitting to the FC.

statistic (T_i) before transmitting to the FC as follows:

$$T_i^{fal} = \begin{cases} T_i + C_i, & \text{under } \mathcal{H}_0 \\ T_i - C_i, & \text{under } \mathcal{H}_1 \end{cases} \tag{6.2.1}$$

where $C_i > 0$ is the parameter under the attacker's control. As we show later, there is an optimum C_i such that the detection performance back at the FC will be degraded the most. So, the test statistic (assuming compromised SNs) at the i^{th} SN can be represented as

$$\hat{T}_i = \begin{cases} T_i^{fal}, & \text{with probability } \beta \\ T_i, & \text{with probability } (1-\beta) \end{cases} \tag{6.2.2}$$

where β is the fraction of the compromised SNs controlled by the attacker.

6.2.3 Data transmission

Now, because the SNs are battery operated devices (i.e., with limited on-board energy) then each SN i ($i = 1, 2, \cdots, M$) has to quantize its test statistic ($\hat{T}_i$) to L_i bits prior to transmission to the FC. We assume that the FC is able to collect data from all the SNs via bandwidth constrained communication channels and furthermore, it is not itself compromised. As in [35,36], we restrict the number of quantization bits at the i^{th} SN to satisfy the channel capacity constraint:

$$L_i \leq \frac{1}{2}\log_2\left(1+\frac{p_i h_i^2}{\zeta_i}\right) \text{ bits/sample} \tag{6.2.3}$$

where p_i denotes the transmit power of sensor i, h_i is the flat fading coefficient between SN i and the FC, and ζ_i is the variance of the AWGN at the FC. The quantized test statistic (T_i^q) at the i^{th} SN can be modeled (with L_i bits) as

$$T_i^q = \hat{T}_i + v_i \tag{6.2.4}$$

where v_i is quantization noise independent of $w_i\,(n)$ in (3.2.1) and (3.2.2). Assuming $T_i \in [0, 2U]$, then

$$\begin{cases} \hat{T}_i \in [C_i, 2U + C_i], & \text{under } \mathcal{H}_0 \text{ with probability } \beta \\ \hat{T}_i \in [-C_i, 2U - C_i], & \text{under } \mathcal{H}_1 \text{ with probability } \beta \\ \hat{T}_i \in [0, 2U], \text{ under } \{\mathcal{H}_p\}_{p=\{0,1\}} & \text{with probability } 1-\beta. \end{cases} \tag{6.2.5}$$

Now, assuming a uniform quantizer with L_i bits (i.e., with a total of 2^{L_i} quantization levels), the quantizer step-size is always $\epsilon = \frac{2U}{2^{L_i}}$ and now v_i (see (6.2.4)) can be modeled as a r.v. uniformly distributed[3] with $v_i \in [-\frac{\epsilon}{2}, \frac{\epsilon}{2}]$, where it is well-known that

$$\sigma_{v_i}^2 = \frac{U^2}{3 \times 2^{2L_i}}. \tag{6.2.6}$$

Note that the above analysis shows that the attacker (i.e., through the compromised SNs), does not introduce a larger quantization error noise (i.e., $\sigma_{v_i}^2$ in (6.2.6) remains

[3]This model that leads to (6.2.6) is only accurate for a relatively high number of bits (e.g., $L_i \geq 3$ in practice). For a smaller number of bits, the expression in (6.2.6) may not be very accurate but it is the only statistical measure available for such errors.

the same as in the case of $attack-free$ [35]). Now, linearly combining $\left\{T_i^q\right\}_{i=1}^{M}$ at the FC gives

$$T_f = \sum_{i=1}^{M} \alpha_i T_i^q \tag{6.2.7}$$

where the weights $\left\{\alpha_i\right\}_{i=1}^{M}$ will be optimized in Section 6.2.4. For large M, the probability of detection (P_d) and the probability of false alarm (P_{fa}) can be approximated and shown to be respectively [9]:

$$P_d = \Pr\left(T_f \geq \Lambda_f | \mathcal{H}_1\right) = \mathbf{1}^T \left(\mathbf{D} Q \left(\frac{\mathbf{\Lambda}_f - \bar{\boldsymbol{\mu}} | \mathcal{H}_1}{\sqrt{\sum_{i=1}^{M} \alpha_i^2 \left(\mathrm{Var}\left\{T_i | \mathcal{H}_1\right\} + \sigma_{v_i}^2 \right)}} \right) \right) \tag{6.2.8}$$

$$P_{fa} = \Pr\left(T_f \geq \Lambda_f | \mathcal{H}_0\right) = \mathbf{1}^T \left(\mathbf{D} Q \left(\frac{\mathbf{\Lambda}_f - \bar{\boldsymbol{\mu}} | \mathcal{H}_0}{\sqrt{\sum_{i=1}^{M} \alpha_i^2 \left(\mathrm{Var}\left\{T_i | \mathcal{H}_0\right\} + \sigma_{v_i}^2 \right)}} \right) \right) \tag{6.2.9}$$

with $\mathbf{\Lambda}_f = \Lambda_f [1, 1, \cdots, 1_{2^M}]^T$ (Λ_f is the FC detection threshold); $\mathbf{1}_{2^M}$ is a column vector of all ones; $\mathbf{D} = \mathrm{diag}\left([\boldsymbol{b}_1 \bigodot \boldsymbol{b}_2 \bigodot \cdots \bigodot \boldsymbol{b}_M]\right)$ ($\boldsymbol{b}_i$ is the i^{th} column vector of $\mathbf{B}$ (where $\mathbf{B} = \big(1-\beta\big)\mathbf{P} + \beta \mathbf{P}^c$) and $\bigodot$ represents element-wise multiplication); the matrix $\mathbf{P}$ is a binary matrix holding the 2^M possible combinations of M (compromised and honest) SNs on its rows with $(\mathbf{P})_{ij} = \{0, 1\}$ representing the compromised and honest SNs respectively (note that $(\mathbf{P})_{ij}$ represents the (i, j) element of $\mathbf{P}$); and $\mathbf{P}^c$ is the element-wise (i.e., bitwise) logical complement of $\mathbf{P}$. Now, $\{\bar{\boldsymbol{\mu}} | \mathcal{H}_p\}_{p=\{0,1\}} = \mathbf{P}\left\{\boldsymbol{\mu} | \mathcal{H}_p\right\}_{p=\{0,1\}} + \mathbf{P}^c \left\{\boldsymbol{\mu}^{fal} | \mathcal{H}_p\right\}_{p=\{0,1\}}$ with $\{\boldsymbol{\mu} | \mathcal{H}_p\} = [\alpha_1 \mathbb{E}\left\{T_1 | \mathcal{H}_p\right\}, \cdots, \alpha_M \mathbb{E}\left\{T_M | \mathcal{H}_p\right\}]^T$ and $\left\{\boldsymbol{\mu}^{fal} | \mathcal{H}_p\right\} = [\alpha_1 \mathbb{E}\left\{T_1^{fal} | \mathcal{H}_p\right\}, \alpha_2 \mathbb{E}\left\{T_2^{fal} | \mathcal{H}_p\right\}, \cdots, \alpha_M \mathbb{E}\left\{T_M^{fal} | \mathcal{H}_p\right\}]^T$ where $\mathbb{E}\left\{T_i | \mathcal{H}_p\right\}$ and $\mathbb{E}\left\{T_i^{fal} | \mathcal{H}_p\right\}$ are respectively:

$$\mathbb{E}\left\{T_i^{fal} | \mathcal{H}_0\right\} = N\sigma_i^2 + C_i, \mathrm{Var}\left\{T_i^{fal} | \mathcal{H}_0\right\} = 2N\sigma_i^4 \tag{6.2.10}$$

$$\mathbb{E}\left\{T_i^{fal} | \mathcal{H}_1\right\} = N\sigma_i^2 \left(1 + \xi_i\right) - C_i, \mathrm{Var}\left\{T_i^{fal} | \mathcal{H}_1\right\} = 2N\sigma_i^4 \left(1 + 2\xi_i\right). \tag{6.2.11}$$

Finally, $Q(.)$ represents the element-wise Q function operation. Next, we describe the optimisation problem under a power-constrained WSN.

6.2.4 FC and Attacker Performance Optimisation Under a Power-Constrained WSN

Now, if the attacker (which has under its control a fraction (β) of the M SNs) can successfully manipulate the FC global decision making process, the detection rate will be significantly low, the error rate in decision making will be high and the FC performance will be degraded. From the attacker's point of view, the more error it causes in the FC decision making, the more successful it is. The attacker has two available strategies: a) direct the compromised SNs to actually report their observation to the FC truthfully or b) direct the compromised SNs to falsify their observations prior to transmission to the FC. In the cases where the attacker decides to direct the compromised SNs to falsify their test statistics, what should be their optimum attacking parameter (C_i)? We will answer this question in Section 6.2.4.

From the FC's point of view, its data fusion mechanism should be robust and capable of defending against any attacking strategy adopted by any compromised SNs and directed by the attacker. The FC is aware that the attacker has an objective in conflict with its own (i.e., the FC tries to maximize the detection probability while the attacker tries to minimize it). However, the FC does not have any exact information about the attacking strategies. The only information available to the FC is: a) the quantized test statistics $\left\{T_i^q\right\}_{i=1}^{M}$ reported by M spatially distributed SNs, and b) the fraction[4] (β) of these test statistics that are falsified. But it cannot recognize where these SNs are and estimate their "falsification parameter", C_i. So, the fusion data mechanism (based on this limited $a-priori$ information) should be able to neutralize (or at least reduce) the impact of these compromised SNs.

So, in this Section, we would like to analyze the performance optimisation from the perspective of the FC and the attacker under a constraint of a maximum transmit power budget (P_t). Since the FC has under its control only the weight combiners ($\alpha_i, \forall i$) in (6.2.7) and the SN to FC transmit power ($p_i, \forall i$) in (6.2.3), its strategy is to maximize P_d with respect to the respective vectors containing these parameters (i.e., $\boldsymbol{\alpha}$ and $\boldsymbol{p}$). However, this is difficult and no closed-form solution can be obtained. Here, we introduce the MDC (which we will use later as an alternative function to

be optimized). The MDC provides a good measure of the detection performance since it characterizes the variance-normalized distance between the centers of two conditional PDFs. This is given as:

$$\tilde{d^2}\left(\boldsymbol{\alpha},\boldsymbol{p}\right)=\left(\frac{\mathbb{E}\left\{T_f|\mathcal{H}_1\right\}-\mathbb{E}\left\{T_f|\mathcal{H}_0\right\}}{\sqrt{\mathrm{Var}\left\{T_f|\mathcal{H}_1\right\}}}\right)^2=\frac{\left(\boldsymbol{b}^T\boldsymbol{\alpha}\right)^2}{\boldsymbol{\alpha}^T\mathbf{R}\boldsymbol{\alpha}} \tag{6.2.12}$$

with the appropriate quantities given in (6.2.17)-(6.2.19) and where

$$\mathbb{E}\left\{T_f|\mathcal{H}_0\right\}=\sum_{i=1}^{M}\alpha_i\left(N\sigma_i^2\right)+\sum_{i=1}^{M}\alpha_i\left(\beta C_i\right) \tag{6.2.13}$$

$$\mathbb{E}\left\{T_f|\mathcal{H}_1\right\}=\sum_{i=1}^{M}\alpha_i\left(N\sigma_i^2\left(1+\xi_i\right)\right)-\sum_{i=1}^{M}\alpha_i\left(\beta C_i\right) \tag{6.2.14}$$

$$\mathrm{Var}\left\{T_f|\mathcal{H}_0\right\}=\sum_{i=1}^{M}\alpha_i^2\left(2N\sigma_i^4+\beta(1-\beta)C_i^2+\sigma_{v_i}^2\right) \tag{6.2.15}$$

$$\mathrm{Var}\left\{T_f|\mathcal{H}_1\right\}=\sum_{i=1}^{M}\alpha_i^2\left(2N\sigma_i^4(1+2\xi_i)+\beta(1-\beta)C_i^2+\sigma_{v_i}^2\right) \tag{6.2.16}$$

$$\boldsymbol{b}=\left[N\sigma_1^2\xi_1-2\beta C_1,\ldots,N\sigma_M^2\xi_M-2\beta C_M\right]^T \tag{6.2.17}$$

$$\boldsymbol{\alpha}=\left[\alpha_1,\alpha_2,\ldots,\alpha_M\right]^T,\boldsymbol{p}=\left[p_1,p_2,\ldots,p_M\right]^T \tag{6.2.18}$$

$$\mathbf{R}=\mathrm{diag}\begin{bmatrix}2N\sigma_1^4(1+2\xi_1)+\beta(1-\beta)C_1^2+\sigma_{v_1}^2\\2N\sigma_2^4(1+2\xi_2)+\beta(1-\beta)C_2^2+\sigma_{v_2}^2\\\vdots\\2N\sigma_M^4(1+2\xi_M)+\beta(1-\beta)C_M^2+\sigma_{v_M}^2\end{bmatrix}. \tag{6.2.19}$$

FC Performance Optimisation

Now, the FC task (which knows that the WSN is *under−attack*) is to maximize the P_d (i.e., to detect with very high probability). We would like to make it clear that the FC knows[4] β (i.e., knows the average percentage of compromised SNs (e.g., [9,11])

[4]In practice, the fraction representing the (on average) compromised SNs can be learned by observing the data sent by the SNs to the FC over a time window. But such an approach is beyond the scope of this work.

but it cannot identify exactly who they are. Given the data fusion (6.2.7), the FC performs the following test:

$$\left.\begin{array}{l} \text{if } T_f < \Lambda_f, \text{ decide } \mathcal{H}_0 \\ \text{if } T_f \geq \Lambda_f, \text{ decide } \mathcal{H}_1 \end{array}\right\} \tag{6.2.20}$$

where Λ_f is the FC detection threshold. As we said earlier, the optimum weighting vector ($\boldsymbol{\alpha}^o$) and the optimum power allocation vector ($\boldsymbol{p}^o$) that maximize P_d under the constraint of a maximum transmit power budget (P_t) are desired. More specifically (adopting the MDC), we require:

$$\begin{aligned} (\boldsymbol{\alpha}^o, \boldsymbol{p}^o) &= \arg \max_{\boldsymbol{\alpha},\boldsymbol{p}} \left(\tilde{d}^2(\boldsymbol{\alpha}, \boldsymbol{p})\right) \\ \text{subject to} &\sum_{i=1}^{M} p_i \leq P_t, \ p_i \geq 0, \ i = 1, 2, \ldots, M. \end{aligned} \tag{6.2.21}$$

It is easily shown [35] that $\boldsymbol{\alpha}^o = \mathbf{R}^{-1}\boldsymbol{b}$ with

$$\alpha_i^o = \frac{(\sigma_i^2\xi_i - \frac{2\beta C_i}{N})}{2\sigma_i^4(1+2\xi_i) + \frac{\beta(1-\beta)C_i^2}{N} + \frac{\sigma_{v_i}^2}{N}}, \forall i = 1, 2, \cdots, M. \tag{6.2.22}$$

Note that the optimum weights $\left\{\alpha_i^o\right\}_{i=1}^M$ are a function of the SN transmit power (p_i) through the $\sigma_{v_i}^2$ terms (see (6.2.3) and (6.2.6)) and p_i is still to be optimized. We now substitute $\boldsymbol{\alpha}^o$ back into (6.2.12) and solve the following optimisation problem

$$\begin{aligned} \boldsymbol{p}^o &= \arg \max_{\boldsymbol{p}} \left(\tilde{d}^2(\boldsymbol{\alpha}^o, \boldsymbol{p})\right) \\ \text{subject to} &\sum_{i=1}^{M} p_i \leq P_t \text{ for } \ p_i \geq 0, \ i = 1, 2, \ldots, M. \end{aligned} \tag{6.2.23}$$

It can also be shown [35], that the above optimisation problem can be solved analytically by using the Lagrangian function and solving the appropriate K.K.T. conditions. The optimum SN to FC transmit power in this case (i.e., where the WSN is *under−attack*) can be shown to be

$$p_i^o = \left[\frac{U}{\sqrt{\lambda_0}}\sqrt{\frac{\zeta_i}{12h_i^2}}\left(\frac{\sigma_i^2\xi_i - \frac{2\beta C_i}{N}}{\sigma_i^4(1+2\xi_i) + \beta(1-\beta)\frac{C_i^2}{2N})}\right) - \frac{\frac{U^2\zeta_i}{h_i^2}}{6N\sigma_i^4(1+2\xi_i) + 3\beta(1-\beta)C_i^2} - \frac{\zeta_i}{h_i^2}\right]^+ \tag{6.2.24}$$

where $[y]^+$ equals 0 if $y < 0$, otherwise it equals y, and λ_0 is the Lagrangian multiplier that can be evaluated in a similar way as in [35] by imposing the equality constraint (i.e., $\sum_{i=1}^{M} p_i = P_t$) in (6.2.21). Now, (6.2.24) assumes that the FC knows the channel coefficients (h_i) for all SNs (honest and compromised). While the FC can obtain this information via a feedback from the honest SNs, the compromised SNs may transmit to the FC wrong information regarding the channel. Nevertheless, here we assume that the compromised SNs only falsify their test statistics as in (6.2.1) and report true channel[5] information to the FC. However, the channel information, for the compromised SNs, could be obtained by blind channel estimation techniques, etc., [102], [103]. Next, we analyze the performance optimisation from the attacker perspective.

Attacker Performance Optimisation

Now, the attacker would like to degrade as much as possible the FC detection performance. For a constant β (i.e., fraction of compromised SNs) the attacker plans the optimum C_i in (6.2.1) such that the FC becomes inefficient (i.e., useless). Adopting again the MDC (6.2.12), the optimisation problem can be expressed as:

$$C_i^o = \arg \min_{C_i} \left(\tilde{d}^2 \left(\alpha_i, p_i, C_i \right) \right). \tag{6.2.25}$$

Note that (6.2.12) reaches its minimum value (i.e., zero) when $\boldsymbol{b}^T \boldsymbol{\alpha} = \sum_{i=1}^{M} \alpha_i \Big(N\sigma_i^2 \xi_i - 2\beta C_i \Big) = 0$. Assuming that $C_i = C, \forall i$ (i.e., the same attack strength for all the compromised SNs) for simplicity, clearly the minimum of (6.2.12) can be achieved with

$$C^o = \sum_{i=1}^{M} \frac{\alpha_i N \sigma_i^2 \xi_i}{2\beta \sum_{i=1}^{M} \alpha_i}. \tag{6.2.26}$$

Now, this yields the maximum possible degradation that the attacker can cause to the FC. As can be seen, the optimum attacker strategy (C^o) is a function of

[5]The channel estimation error (for both the honest and compromised SNs) can be modeled as a Gaussian random variable (i.e., $\hat{h}_{ij} = h_{ij} + e_h$) where $e_h \sim \mathcal{N}(0, \sigma_{e_h}^2)$ and $\hat{h}_{ij}$ is the estimated flat fading channel coefficient.

the FC strategy (i.e., α_i in (6.2.7) which itself is a function of p_i through the $\sigma^2_{v_i}$ quantity (see (6.2.3), (6.2.6) and (6.2.22)). So, in order to adopt this strategy, the attacker needs to know α_i and p_i, $\forall i$. Since the FC is not compromised (i.e., still acts accordingly), these quantities cannot normally be obtained by the attacker.

As can be seen from the optimum FC weight protection strategy (6.2.22) and the attacker optimum strategy (6.2.26), there does not exist a dominant[6] approach. Clearly the FC weights (α_i in (6.2.7)) depend on the attacker parameter C_i and vice versa. Next, we discuss in more detail the attacker versus the FC strategies and provide performance analysis in cases where limited $a-priori$ knowledge about the attacker is available (i.e., without the need of exact knowledge of C_i).

6.2.5 Performance Analysis

In this Section, starting with the optimum attacker strategy (6.2.26) and depending on the collaboration willingness among SNs and the available $a-priori$ information that the attacker has about the FC combining strategy, we distinguish between two simulation setups in Section 6.2.5. Next, in Section 6.2.5 we distinguish again between two different simulation setups but now from the perspective of the FC mechanisms.

Sub-optimum Attacker's Strategies

Here, we assume that the attacker knows that the FC uses a linear combining strategy but it is not aware of the combining weights used in (6.2.7). We also assume that the FC does not act strategically and uses weight combining, without trying to optimize against the behavior of compromised SNs. We now distinguish between the two following setups, "HCSC" and "CSC".

1. **Honest and Compromised SNs Collaboration – HCSC**: Now, the optimum strategy (6.2.26) to be adopted by each compromised SN requires knowledge that cannot be obtained in practice as previously discussed. As

[6] A dominant FC (attacker) strategy is said to be strictly dominant if it is the best strategy for the FC (attacker), no matter how the attacker (FC) decides to act.

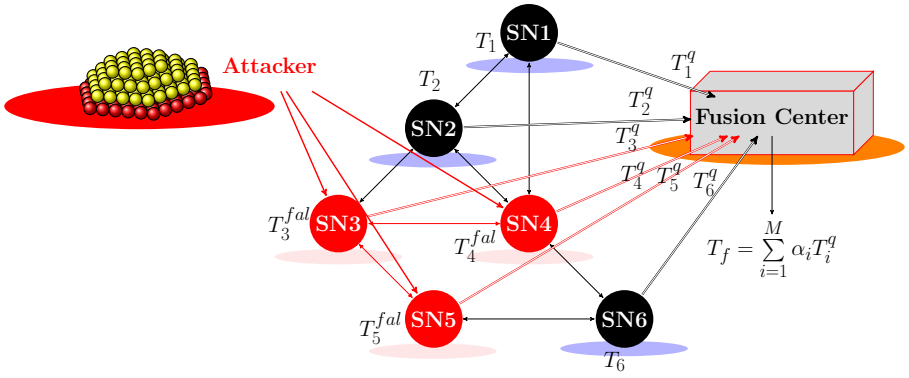

Figure 6.2: Under attack schematic communication architecture among peripheral SNs and the FC. Similarly to Fig. 6.1, each SN generates a test statistic (T_i) by observing the target (not shown here for clearance purposes)). While the honest SNs (black color) keep their test statistics unchanged, the compromised SNs (red color) directed by the attacker, will falsify their test statistics to T_j^{fal} with $j = \{3, 4, 5\}$ (where j is the compromised SN index). The SNs have partial connectivity among themselves (i.e., not a complete graph) (thin lines) and can communicate with the FC (thick lines) but only over an energy-constrained/bandwidth-constrained links.

a result, the attacker (not aware of α_i and p_i, $\forall i$) reasonably assumes equal combining at the FC (i.e., $\alpha_i = \frac{1}{M}, \forall i$) and directs the compromised SNs to attack with

$$C^{HCSC} = \frac{N}{M} \sum_{i=1}^{M} \frac{\sigma_i^2 \xi_i}{2\beta} \tag{6.2.27}$$

where the superscript "$HCSC$" refers to "Honest and Compromised SNs Collaborate". However, the compromised SNs still require knowledge of σ_i^2 and $\xi_i, \forall i$ (to evaluate $\sum_{i=1}^{M} \sigma_i^2 \xi_i$) in order to implement the attacking strategy (6.2.27). When all the M SNs (honest and compromised) form a connected network[7] and are willing to collaborate with each other (see Fig. 6.2), the quantity $\sum_{i=1}^{M} \sigma_i^2 \xi_i$ in (6.2.27) can be estimated using the average consensus algorithm [19]. Because of the communication topology for the M SNs (i.e., not fully connected), the average consensus algorithm ensures the availability

[7] A connected network is any network where there is a path (i.e., over one or more links) between every pair of SNs in the network.

of this term at each SN. The compromised SNs will still be camouflaged (i.e., unidentified) as they share with their neighbors just the true quantity $\sigma_i^2\xi_i$ and the SNs cannot identify if their neighbors are honest or compromised.

2. **Compromised SNs (only) Collaboration – CSC**: Now, in the cases where not all of the M SNs (compromised and honest) are willing to collaborate with each other, the quantity $\sum_{i=1}^{M}\sigma_i^2\xi_i$ in (6.2.26) cannot be obtained in practice. Note that the attacker has under its control just a fraction (β) ($\beta = \frac{F}{M} \leq 1$, where F is the number of falsified SNs) of M SNs (see Fig. 6.2) and the other remaining honest SNs ($M - F$) do not share their observations with their neighbors. In this situation, the F compromised SNs collaborate with each other in order to estimate in a distributed fashion the $\sum_{i\in J}\sigma_i^2\xi_i$ quantity, where J represents the compromised SNs set with cardinality F. Assuming that the F falsified SNs form a connected[7] network, the average consensus algorithm [19] (like before) ensures the availability of this term at each falsified SN. After this stage, the compromised SNs attack (i.e., falsify their test statistics (3.2.3) as in (6.2.1)) with $C_i = C^{CSC}, \forall i$ with

$$C^{CSC} = \frac{N(M-F)}{M}\sum_{i\in J}\frac{\sigma_i^2\xi_i}{2\beta} \tag{6.2.28}$$

where the superscript "CSC" refers to "$Compromised\ SNs\ (only)\ Collaborate$".

Sub-optimum FC's Strategies

Now, the optimum weights ($\alpha_i^o, \forall i$) in (6.2.22) are a function of the attacker parameter C_i which is difficult in practice (if not impossible) to obtain by the FC. In such a case, the FC adopts a sub-optimum but simple solution to minimize the degradation caused by the attacker. Assuming that the attacker does not act strategically (i.e., does not try to optimize against the FC approach) we now distinguish between the two following simulation setups, $WAFBB$ and the $OAFBB$.

1. **Weak Attack FC Based Belief – WAFBB**: Now, when the number of observed samples (N) is large and the FC believes that the attacker is directing the i^{th} compromised SN to attack with relatively small C_i, the FC

weight combining can be approximated with

$$\alpha_i^{WAFBB} = \frac{\sigma_i^2 \xi_i}{2\sigma_i^4(1+2\xi_i) + \frac{\sigma_{v_i}^2}{N}}, \forall i = 1, 2, \cdots, M \tag{6.2.29}$$

where the superscript "$WAFBB$" refers to "$Weak\ Attack\ FC\ Based\ Belief$" and the optimum SN to FC transmit power can be also approximated with

$$p_i^{WAFBB} = \left[\frac{U}{\sqrt{\lambda_0}} \sqrt{\frac{\zeta_i}{12 h_i^2}} \left(\frac{\sigma_i^2 \xi_i}{\sigma_i^4(1+2\xi_i)} \right) - \frac{\frac{U^2 \zeta_i}{h_i^2}}{6N\sigma_i^4(1+2\xi_i)} - \frac{\zeta_i}{h_i^2} \right]^+. \tag{6.2.30}$$

Now, (6.2.29) and (6.2.30) coincide with the optimum weights and with the optimal SN transmit power allocation scheme respectively derived for the case of $attack-free$ WSN in [35].

2. **Optimum Attack FC Based Belief – OAFBB**: Here, we consider the case when the FC believes that the attacker, with a fraction (β) of SNs under its control, attacks with the optimum parameter C^o (see (6.2.26)) (i.e., with $C_i = C^o$ in (6.2.1) but with $\alpha_i = \frac{1}{M}, \forall i$).

   First of all, note that the FC knows that the compromised SNs (i.e., the attacker) have an alternative objective (i.e., the attacker would like to minimize, while the FC would like to maximize, the MDC in (6.2.12)) (i.e., the FC can work out the optimisation problem from the attacker perspective and evaluate (6.2.26)). Secondly, the FC concludes that the attacker cannot adopt this strategy in practice (since this optimum strategy requires $\alpha_i, \forall i$ and this parameter is controlled by the FC itself). In such a situation, it is reasonable that the FC believes that the attacker guides the compromised SNs to attack with C^o (see (6.2.26) but with $\alpha_i = \frac{1}{M}, \forall i$). Now, the FC protection weights (α_i^{OAFBB}) can be shown to be (by substituting $C_i = \frac{N}{2\beta M} \sum_{i=1}^{M} \sigma_i^2 \xi_i$ in (6.2.22) and rearranging the terms):

$$\alpha_i^{OAFBB} = \frac{\sigma_i^2 \xi_i - \frac{1}{M} \sum_{i=1}^{M} \sigma_i^2 \xi_i}{2\sigma_i^4(1+2\xi_i) + N(1-\beta)\left(\frac{1}{2\sqrt{\beta M}} \sum_{i=1}^{M} \sigma_i^2 \xi_i \right)^2 + \frac{\sigma_{v_i}^2}{N}}. \tag{6.2.31}$$

   The SN to FC transmit power (p_i^{OAFBB}) can be obtained in a similar way (by substituting $C_i = \frac{N}{2\beta M} \sum_{i=1}^{M} \sigma_i^2 \xi_i$ into (6.2.24)). Lastly, the superscript "$OAFBB$" refers to "$Optimum\ Attack\ FC\ Based\ Belief$".

6.2.6 Equilibrium Analysis

In this section, we consider the case where both the attacker and the FC act strategically and formulate the problem as a minimax game between two players, i.e., the attacker and the FC. The attacker has under its control one parameter (i.e., $C_i \ \forall i \in J$, with J defined in Section 6.2.5, bottom of page 115) while the FC has control of the weight combining vector (i.e., $\boldsymbol{\alpha}$). As before, assuming $C = C_i$ (i.e., the same attack strength for each compromised SN) for simplicity, we first of all prove the existence of the Nash Equilibrium (NE)[8] by showing that there exists a unique saddle-point in the minimax game between the attacker and the FC. Then, we find the optimum solution numerically by maximizing the deflection coefficient with respect to the FC weight combining parameter and then by minimizing it with respect to the attacker parameter (i.e., w.r.t. C). Next, we present a theorem, by help of which in Section 6.2.6 (top of page 120) we prove the existence of NE.

Theorem 6.2.1 *(Nikaido, [105]). Let $\mathcal{K}(x, y)$ be a pay-off function defined on the product space of $\mathcal{X}$ by $\mathcal{Y}$, where $\mathcal{X}$ and $\mathcal{Y}$ are convex compact sets and continuous in each variable for any fixed value of the other. If $\mathcal{K}(x, y)$ is quasi-concave in x and quasi-convex in y, then:*

$$\max_{x \in \mathcal{X}} \min_{y \in \mathcal{Y}} \mathcal{K}(x, y) = \min_{x \in \mathcal{X}} \max_{y \in \mathcal{Y}} \mathcal{K}(x, y). \tag{6.2.32}$$

Next, we present the behavior of the MDC w.r.t. attacker strength C.

Modified Deflection Coefficient Behavior with Respect to C

In the next Lemma we prove the quasi-convexity behavior of the MDC w.r.t. C.

Lemma 6.2.2 *For a given $\boldsymbol{\alpha}$ and $\boldsymbol{p}$, $\tilde{d}^2$ in (6.2.12) is a quasi-convex function of C.*

Proof: The MDC can be written as:

$$\tilde{d}^2 = \frac{(x - 2\beta C b)^2}{y + dC^2} \tag{6.2.33}$$

[8] A Nash equilibrium, is a set of strategies, one for each player, such that no player has the incentive to unilaterally change its action. Players are in equilibrium if a change in strategies by any one of them would lead that player to earn less than if it remained with its current strategy.

where $x = \sum_{i=1}^{M} \alpha_i \left(N\sigma_i^2\xi_i\right)$, $b = \sum_{i=1}^{M} \alpha_i$, $d = \sum_{i=1}^{M} \alpha_i^2\Big(\beta(1-\beta)\Big)$, $y = \sum_{i=1}^{M} \alpha_i^2\Big(2N\sigma_i^4(1+2\xi_i) + \sigma_{v_i}^2\Big)$.

Now considering $\boldsymbol{\alpha}$ as a constant, differentiate $\tilde{d^2}$ w.r.t. C and by further simplification, we obtain:

$$\frac{\partial \tilde{d^2}}{\partial C} = \frac{\Big(2\beta bC - x\Big)\Big(4\beta by + 2xdC\Big)}{\Big(y + dC^2\Big)^2} = 0. \tag{6.2.34}$$

So solving the above yields two critical points:

$$C_1^* = \frac{x}{2\beta b}, \qquad C_2^* = -\frac{2\beta by}{xd}. \tag{6.2.35}$$

Now, for a feasible attacker strength (i.e., for $C > 0$), the critical point C_1^* is feasible if $x, b > 0$ or $x, b < 0$. So, we have the following:

$$\left.\begin{array}{l} \text{if } x, b > 0 \text{ and for } C > C_1^*,\ f'(C) > 0 \\ \text{if } x, b < 0 \text{ and for } C > C_1^*,\ f'(C) > 0 \\ \text{if } x, b > 0 \text{ and for } C < C_1^*,\ f'(C) < 0 \\ \text{if } x, b < 0 \text{ and for } C < C_1^*,\ f'(C) < 0 \end{array}\right\} \implies C_1^* \text{ is a global minimum.} \tag{6.2.36}$$

We also conclude that the other critical point C_2^* is not even a feasible point (i.e., $C_2^* < 0$) for $x, b > 0$ and $x, b < 0$. Hence, there is only one value of $C = C_1^*$ at which $\tilde{d^2} = 0$. As a result, C_1^* being the unique global minimum $\implies$ $\tilde{d^2}$ is a quasi-convex function of C.

This concludes the proof. ■

Modified Deflection Coefficient Behavior with Respect to $\boldsymbol{\alpha}$ and $\boldsymbol{p}$

Now, in Lemma 6.2.3, we show the behavior of $\tilde{d^2}$ in (6.2.12) from the perspective of the FC.

Lemma 6.2.3 *For a given C and $\boldsymbol{p}$, $\tilde{d^2}$ is a concave function of $\boldsymbol{\alpha}$*

Proof: Consider (6.2.12), then the Hessian of $\tilde{d^2}$ w.r.t. $\boldsymbol{\alpha}$ (i.e., $\mathbf{H}_{\tilde{d^2}}$) can be easily shown to be:

$$\mathbf{H}_{\tilde{d^2}} = 2\frac{\boldsymbol{b}\boldsymbol{b}^T}{\boldsymbol{\alpha}\mathbf{R}\boldsymbol{\alpha}} - 4\frac{\boldsymbol{b}^T\boldsymbol{\alpha}}{\left(\boldsymbol{\alpha}\mathbf{R}\boldsymbol{\alpha}\right)^2}\left(\boldsymbol{b}\boldsymbol{\alpha}^T\mathbf{R} + \mathbf{R}\boldsymbol{\alpha}\boldsymbol{b}^T\right) + 8\frac{\left(\boldsymbol{\alpha}^T\boldsymbol{b}\right)^2}{\left(\boldsymbol{\alpha}\mathbf{R}\boldsymbol{\alpha}\right)^3}\left(\mathbf{R}\boldsymbol{\alpha}\boldsymbol{\alpha}^T\mathbf{R}\right) - 2\frac{\left(\boldsymbol{\alpha}^T\boldsymbol{b}\right)^2}{\left(\boldsymbol{\alpha}\mathbf{R}\boldsymbol{\alpha}\right)^2}\left(\mathbf{R}\right). \quad (6.2.37)$$

Now, to prove that $\tilde{d^2}$ is a concave function of $\boldsymbol{\alpha}$, we need to show [90]: $\boldsymbol{\alpha}^T\mathbf{H}_{\tilde{d^2}}\boldsymbol{\alpha} \leq 0, \forall\boldsymbol{\alpha}$. This is given in Appendix C. From (C.1.2), $\boldsymbol{\alpha}^T\mathbf{H}_{\tilde{d^2}}\boldsymbol{\alpha} = 0, \forall\boldsymbol{\alpha} \implies \tilde{d^2}$ is a concave function of $\boldsymbol{\alpha}$ where the $\alpha_i^o, \forall i$ in (6.2.22) is the optimum solution.
This concludes the proof. ■

Similarly, treating C (i.e., the attacker strength) fixed and for a given $\boldsymbol{\alpha}$ (i.e., the weight combiner vector) it can be easily shown that $\tilde{d^2}$ is also a concave function of $\boldsymbol{p}$ and p_i^o in (6.2.24) is the optimum solution. The proof is straightforward and we omit it here due to lack of space.

Now, since any concave function is quasi-concave, then by Theorem 6.2.1, a unique saddle-point exists in the minimax game which is the NE. We numerically evaluate this NE in the simulation results section.

6.2.7 Simulation Results

Simulation Setup

In this Section, the performances of the proposed strategies are evaluated numerically and compared to the $attack-free$ scheme [35]. A WSN with a total of $M = 12$ SNs is considered (where a fraction of these SNs are compromised by the attacker with the same attacking strength (i.e., $C_i = C, \forall i$) for simplicity). We let $\sigma_i^2 = 0.1$, such that $\xi_a = 10\log_{10}\left(\frac{1}{M}\sum_{i=1}^{M}\xi_i\right) = -10.5$ dB with arbitrarily chosen $\boldsymbol{s}(n) = [s_1(n), s_2(n), \cdots, s_M(n)] = [0.022, 0.0011, 0.18, 0.02, 0.0143, 0.0011, 0.0024, 0.2, 0.06, 0.09, 0.0143, 0.15]$ unless otherwise stated. The corresponding SN to FC channel gains are assumed to be ideally estimated (i.e., $\sigma_{e_h}^2 = 0$) for simplicity and are shown in Fig. 6.3. In addition we let $\zeta_i = 0.1$, $\forall i$. Finally, we choose L_i with equality in (6.2.3).

SN to FC Optimal Transmit Power Allocation and FC Weight Combining Strategy

Now, we investigate the SN to FC transmit power for the optimum allocation scheme[9] and the FC optimal weight combining strategy derived in Section 6.2.4.

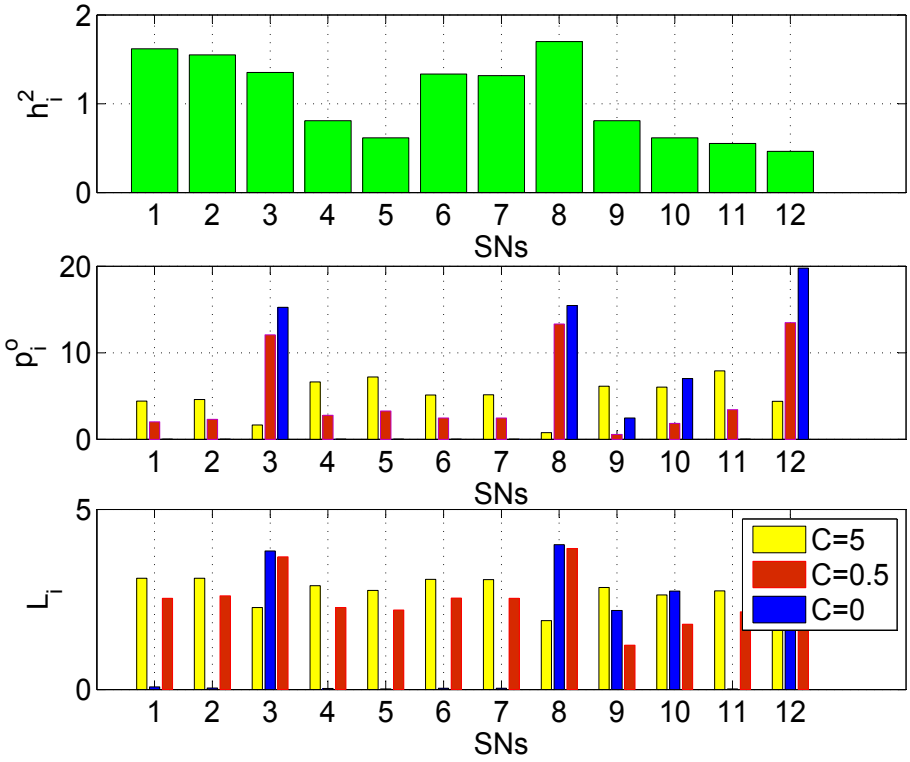

Figure 6.3: SN optimal transmit power (p_i^o) and channel bit allocation (L_i) with $P_t = 60$, $U = 3$, $\xi_a = -10.5$ dB, $N = 20$, $\beta = 0.1$ and $\sigma_{e_h}^2 = 0$.

Fig. 6.3 (the middle plot) shows the optimal SN transmit power p_i^o for the i^{th} SN to the FC channel versus the attacker strength C and the lower plot shows the corresponding quantization bits. The actual channel coefficients (randomly chosen) are in the upper plot. Clearly, for the case of $C = 0$ (i.e., the $attack - free$ scheme in [35]), more power is allocated to the SNs (i.e., SN3, SN8, SN9, SN10, and SN12) having both the best channels and high enough SNRs (ξ_i). Interestingly, those

[9]The optimum SN power allocation scheme requires knowledge of the attacker strength C_i (see (6.2.24)). This is a strong assumption in practice and the exact knowledge of C_i cannot be attained in general. Nevertheless, here we consider this situation for performance comparison purposes and to create an idea about how the SN to FC transmit power allocation is affected.

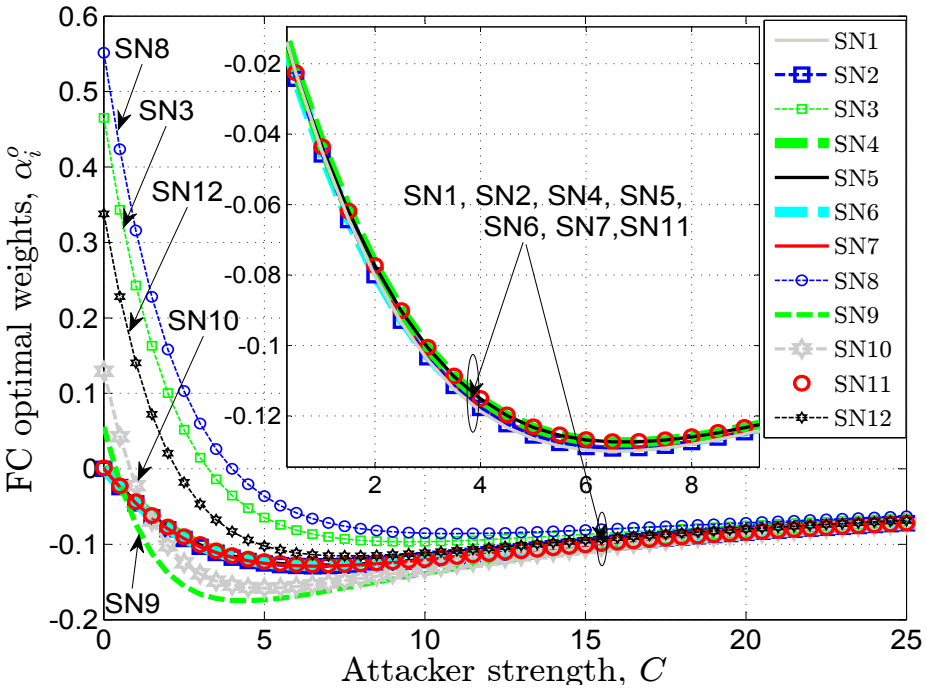

Figure 6.4: FC optimal weights (α_i^o) versus the attacker strength (C) with $U = 3$, $\xi_a = -10.5$ dB, $P_t = 60$, $M = 12$, $N = 20$, $\beta = 0.1$ and $\sigma^2_{e_h} = 0$.

remaining SNs having very low SNRs (i.e., having useless local information) but having good (or bad) corresponding channels, are censored (i.e., do not transmit even a single bit). In this way, the SNs that have very bad channels (i.e., SNs that require very high power to transmit) or the SNs that have low SNRs (i.e., SNs that do not contain useful information) will be censored (i.e., will not transmit even one bit). This is not the case when $C = 0.5$ or $C = 5$ (we give an explanation later)

In Fig. 6.4 we investigate the FC combining response (with weight in (6.2.22)) versus attacker strength C. Clearly, when $C = 0$, the weights for the SNs permitted to transmit to the FC (i.e., SN3, SN8, SN9, SN10, and SN12) are greater than 0. As expected, the weights for the other remaining SNs are set to 0 (as these SNs are censored). Now, when C starts to increase, the FC response is to decrease the weights for all the SNs up to around $C = 5$ and to allow all the SNs to transmit to the FC (see Fig. 6.3 (middle plot)). However, for around $C > 5$, the FC response is by first increasing the weights for the SNs having low SNRs and as C gets larger, the FC combining strategy tends towards equal combining.

Similar to Fig. 6.4, in Fig. 6.5 (for $C = 0.1$) and in Fig. 6.6 (for $C = 0.6$)

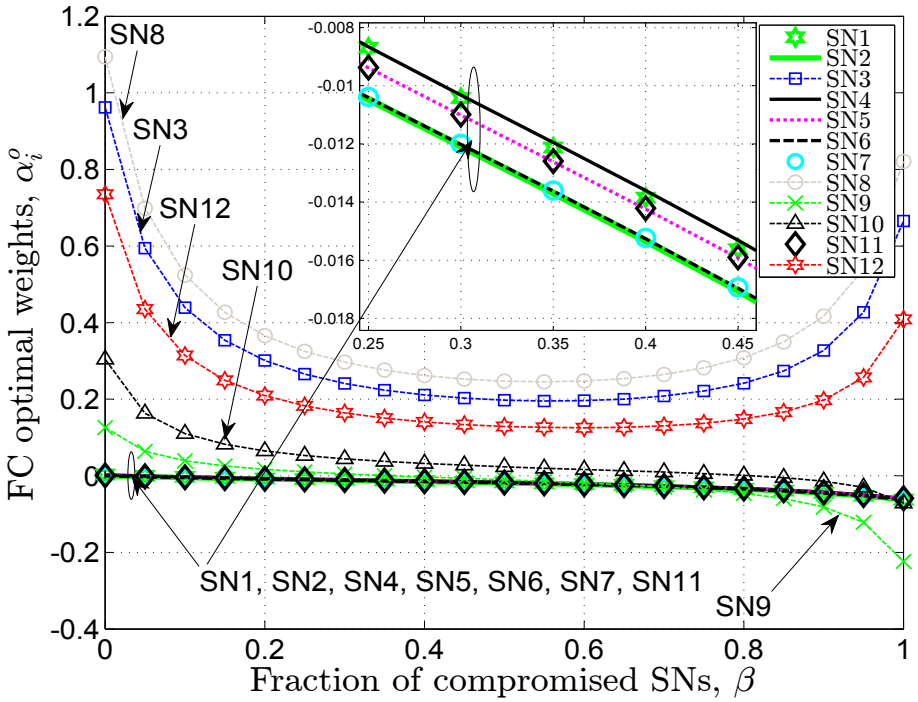

Figure 6.5: FC optimal weights (α_i^o) versus fraction of the compromised SNs (β) with $U = 3$, $P_t = 60$, $N = 20$, $C_i = 0.1, \forall i$ and $\sigma^2_{e_h} = 0$.

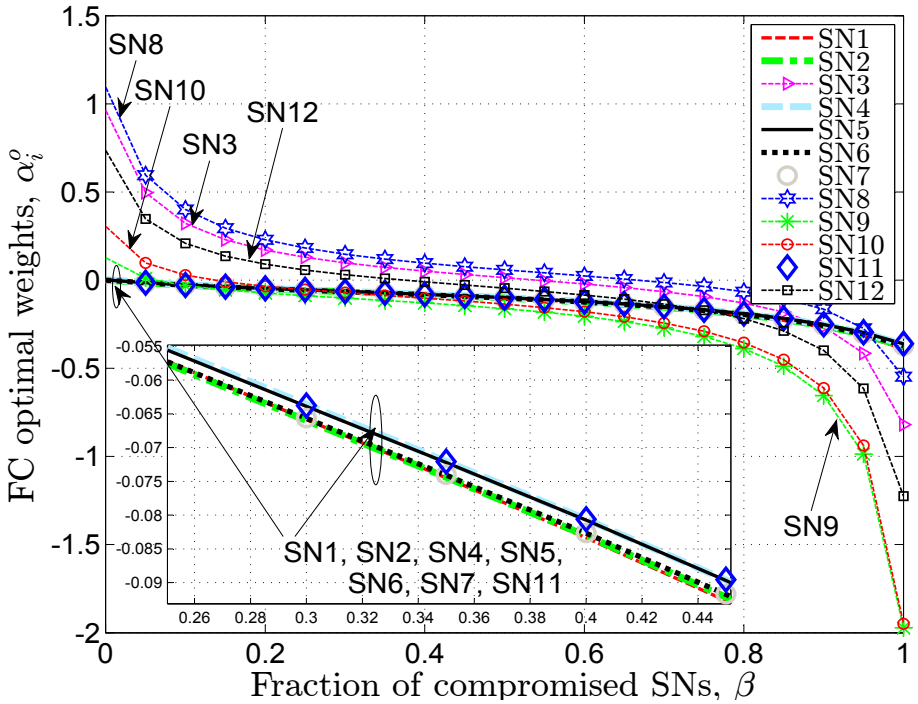

Figure 6.6: FC optimal weights (α_i^o) versus fraction of the compromised SNs (β) with $U = 3$, $P_t = 60$, $N = 20$, $C_i = 0.6, \forall i$ and $\sigma^2_{e_h} = 0$.

we plot the FC combining response (with weights in (6.2.22)) but now versus the fraction of compromised SNs (β). Interestingly, the optimal FC weight response for the *less informative* SNs (i.e., SN1, SN2, SN4, SN5, SN6, SN7, and SN11 classified by the power allocation scheme in the case of $attack-free$ (i.e., $C=0$)) remains almost constant with respect to β both in Fig. 6.5 and Fig. 6.6. However, that is not the case for the *more informative* SNs (i.e., SN3, SN8, SN9, SN10, and SN12). In Fig. 6.5, we observe that for the SNs 3, 8, and 12 (corresponding to the best SNRs) this relationship is convex while for the SNs 9 and 10 it is monotonically decreasing. Interestingly, in Fig. 6.6 (for a larger C) this relationship becomes monotonically decreasing for all the *more informative* SNs mentioned above.

The results provided in this Section cannot be attained in practice as the exact knowledge of C is required. However, they provide an insight as to how the FC power allocation and the weight combining strategy is influenced by both the attacker strength (C) and the compromised SNs fraction (β).

Detection Performance of the Proposed Strategies for Fixed β

Now, we investigate the detection performance of the proposed strategies described in Section 6.2.5 for a fixed β.

In Fig. 6.7, we show the receiver operating characteristic (ROC) parametrized on the attacker strength (C) for the proposed $WAFBB$ and $OAFBB$ strategies compared to the *attack free* (AF) case [35] (i.e., when there is no attack). We can observe that for $C=0.3$ (as expected), the $WAFBB$ strategy performs similar to the optimum strategy in (6.2.21) and better than $OAFBB$ (up to $C=0.6$) whereas after that, the $OAFBB$ strategy dramatically outperforms the latter. We also note that for relatively very large C, it is possible to totally blind the FC when the $WAFBB$ is used (i.e., to make it incapable of detecting) but only when the WSN operates at low probability of false alarm (P_{fa}).

Now, we would like to emphasize that the $WAFBB$ strategy has particular importance when the FC does not have any $a-priori$ knowledge about the β and C parameters. But the $OAFBB$ strategy requires just knowledge of the compromised SNs fraction[4] (β) which is possible to be obtained by the FC in practice.

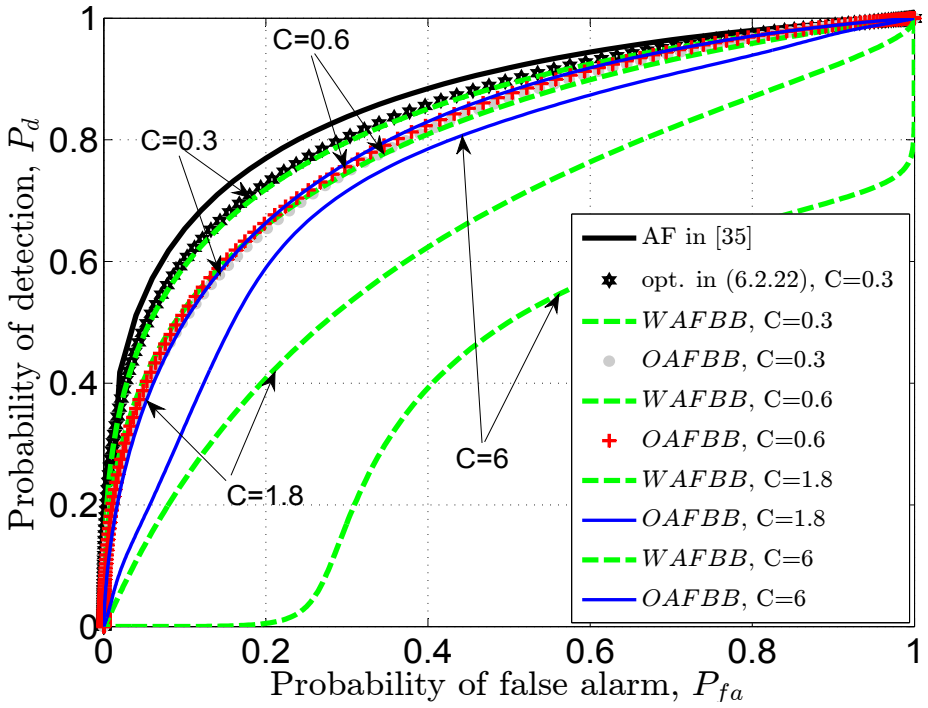

Figure 6.7: Probability of detection (P_d) versus probability of false alarm (P_{fa}), with $U = 3$, $P_t = 60$, $M = 12$, $N = 20$, $\beta = 0.1$ and $\sigma^2_{e_h} = 0$.

Detection Performance of the Proposed Strategies for Fixed C

Now, we investigate the detection performance of the proposed strategies described in Section 6.2.5 for a fixed C.

In Fig. 6.8, we show the ROC performance for the two different proposed strategies (parametrized on β) compared to the optimum strategy in (6.2.21) and AF in [35]. We can observe that for small β (more specifically $\beta = 0.1$), both the optimum and $OAFBB$ strategies outperform the $WAFBB$ strategy and their performances are worst than the AF performance. Interesting, when β increases (more specifically, $\beta = 0.5$ and $\beta = 1$), both the optimum and $OAFBB$ strategies outperform the AF detection performance for all the values of P_{fa} and their detection performances improve proportionally with β. However, this is not the case when $WAFBB$ is used (its performance degrades and when $\beta = 1$ it is sufficient to blind the FC even when the WSN operates at a relatively high P_{fa}).

In Fig. 6.9, we investigate the same situation as for Fig. 6.8 but now for $C = 0.6$. In this case (when $\beta = 0.1$), the optimum strategy slightly outperforms the

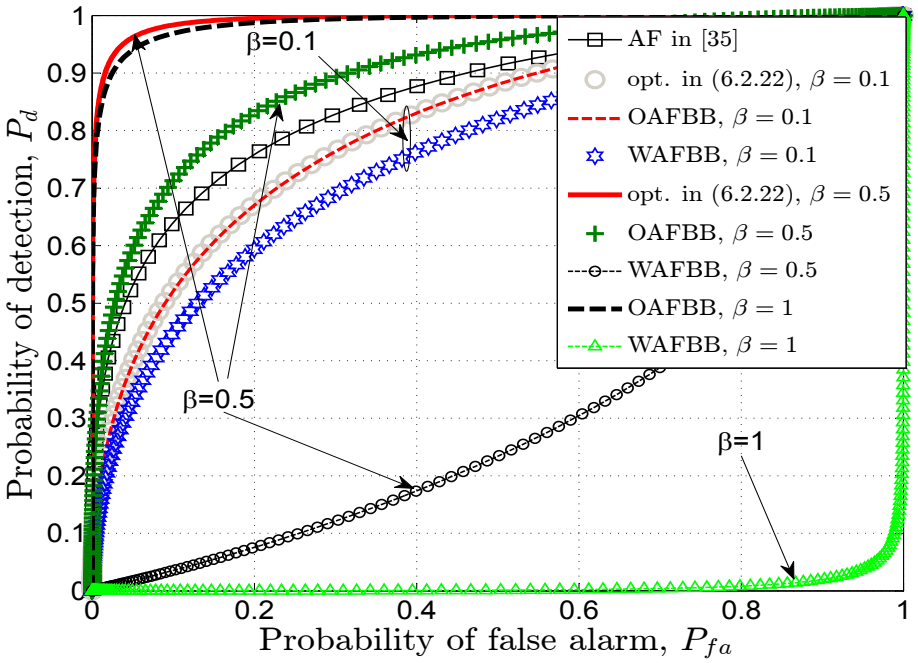

Figure 6.8: Probability of detection (P_d) versus probability of false alarm (P_{fa}) with $U = 3$, $P_t = 60$, $M = 12$, $N = 20$, $C_i = 0.9, \forall i$ and $\sigma^2_{e_h} = 0$.

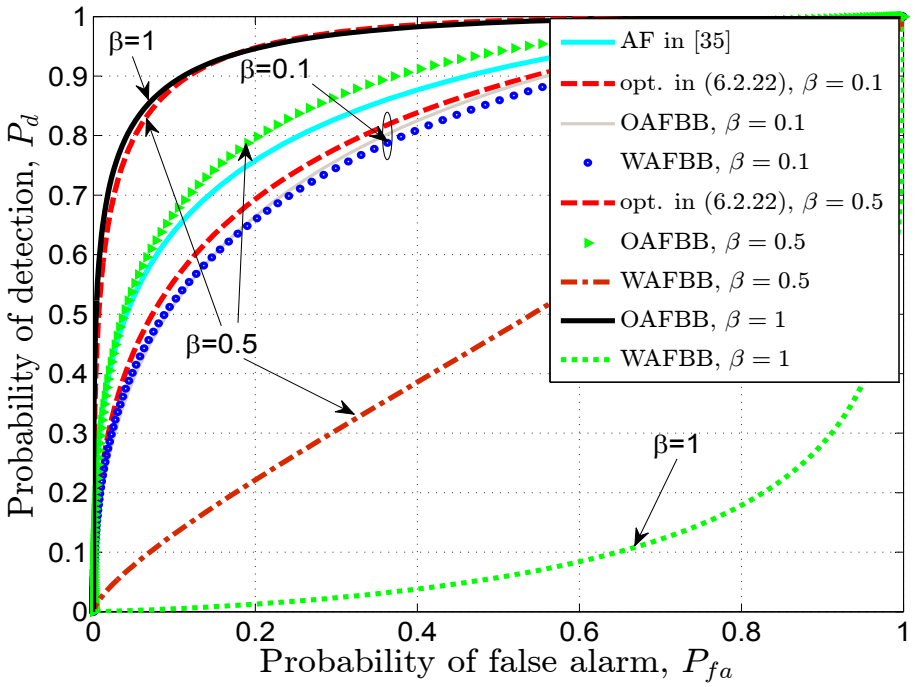

Figure 6.9: Probability of detection (P_d) versus probability of false alarm (P_{fa}) with $U = 3$, $P_t = 60$, $M = 12$, $N = 20$ and $C_i = 0.6, \forall i$, and $\sigma^2_{e_h} = 0$.

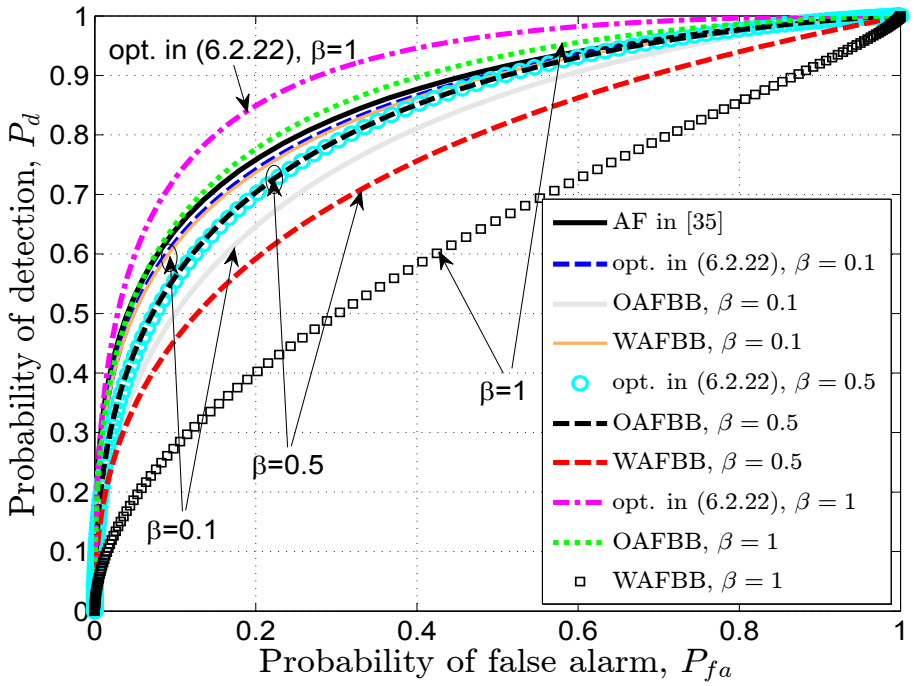

Figure 6.10: Probability of detection (P_d) versus probability of false alarm (P_{fa}) with $U = 3$, $P_t = 60$, $M = 12$, $N = 20$, $C_i = 0.2, \forall i$ and $\sigma^2_{e_h} = 0$.

$OAFBB$ and $WAFBB$ strategies. However, similar to Fig. 6.8, when more than 50% of the SNs are compromised, the $OAFBB$ strategy significantly outperforms the $WAFBB$ strategy. Furthermore, its detection performance improves proportionally as β increases.

In Fig. 6.10, we again show the ROC versus β but now for a lower C (more specifically for $C = 0.2$). As expected, the $WAFBB$ performs similar to the optimum strategy and outperforms the $OAFBB$ at low β and low C, as the $WAFBB$ is derived under these assumptions. Interestingly, when 50% of the SNs are compromised, both the optimum and $OAFBB$ strategies perform in a similar manner. Again, the $OAFBB$ strategy detection performance improves with β wheres for the $WAFBB$ strategy its performance degrades as β increases. It is now clear that (from the attacker perspective) there is an optimum number of compromised SNs (fraction β) that causes the maximum FC detection performance degradation when the optimum FC strategy in (6.2.21) is used.

Equilibrium Analysis of Minimax Game

In this section we analyze the equilibrium point of the minimax game and find the Nash Equilibrium (NE). The NE is the maximum probability of detection considering the FC's best linear weight combining strategy (joint optimization of $\boldsymbol{\alpha}, \boldsymbol{p}$) against attacker's strategy (i.e., C for a given fraction of compromised SNs β).

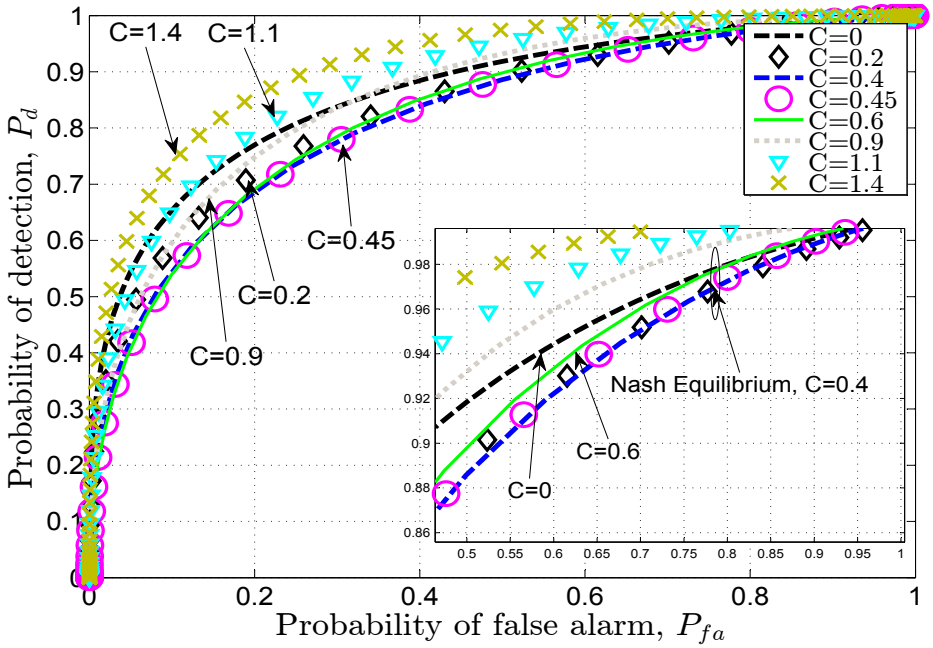

Figure 6.11: Probability of detection (P_d) versus probability of false alarm (P_{fa}), with $U = 3$, $\xi_a = -10.5$ dB, $P_t = 60$, $M = 12$, $N = 20$, $\beta = 0.2$, $\sigma^2_{e_h} = 0$ and with optimum weights in (6.2.22).

In Fig. 6.11 the ROC behavior against the attacker's strength and the FC's combining weights is shown. As expected, there does exist a NE and it is shown to occur for the pair $C = 0.4$ and $\boldsymbol{\alpha}^o$ (with α_i^o in (6.2.22)). Clearly, from the attacker perspective, this strategy causes the maximum detection performance degradation $\forall P_{fa}$ and deviating from this strategy will not benefit the attacker.

Now, in Fig. 6.12, the modified deflection coefficient against the attacker strength is shown for two examples (i.e., with optimum FC weights combining in (6.2.22) and non-optimum weight combining drawn from the uniform distribution (i.e., $\alpha_i \sim \mathcal{U}(0,1)$ in (6.2.7)). We can observe that the NE is shown to occur at $C = 1$ and deviating from this point (i.e., this strategy) the attacker will not benefit (i.e., it

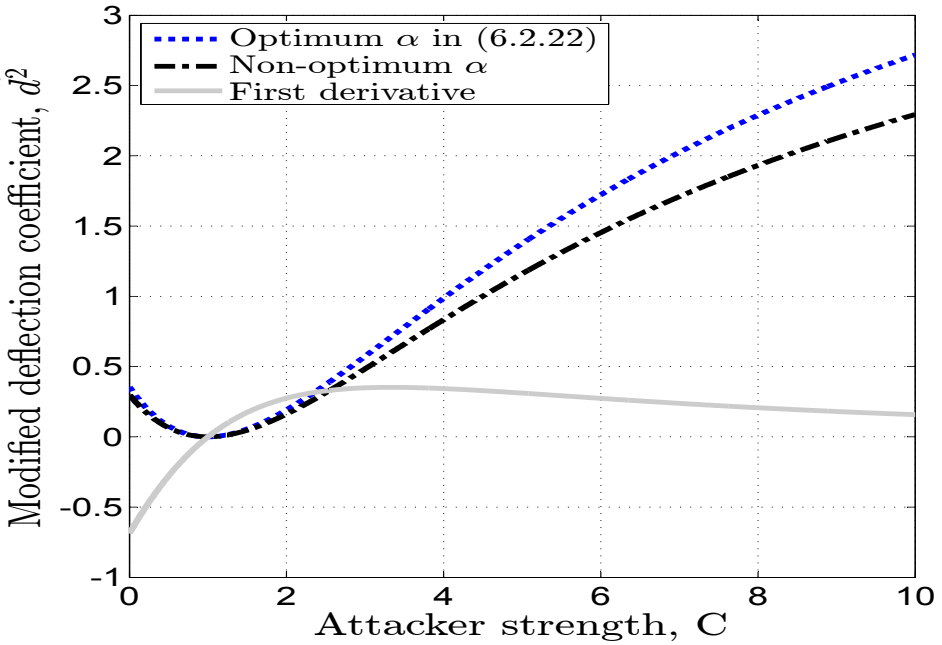

Figure 6.12: Modified deflection coefficient ($\tilde{d}^2$) versus the attacker strength (C) with $U = 3$, $\xi_a = -10$ dB, $s_i = 0.1, \forall i$, $P_t = 60$, $M = 12$, $N = 20$, $\beta = 0.1$ and $\sigma^2_{e_h} = 0$.

will not gain in terms of the FC's performance degradation). It is also clear that if the FC deviates from the optimum combining strategy (i.e., from the weights α_i^o in (6.2.22)), its detection performance will be worst or at least will not improve $\forall C$.

6.3 A Secure Sub-optimum Centralized Detection Scheme in Under-Attack WSNs

6.3.1 System Model

In this section, we describe the target sensing, communication channel, and the WSN architecture.

Target Sensing

In this section, we use the same system model used for Section 6.2. Identically, we consider an under-attack WSN with M SNs (where a fraction (β) of these SNs are compromised) reporting to a FC.

Communication Channel

Identical to the previous chapters (e.g., Chapter 3), the communication between the local SNs and the FC are modeled as error-free (the SNs transmit the 1-bit local decision) parallel access channels (PACs).

WSN Architecture

In this section, we adopt the identical WSN architecture as in Section 6.2 (i.e., the *centralized* under-attack WSN architecture) such that there is a FC that communicates with spatially distributed SNs. However, in this section we introduce a different attacking model and we refer the reader to the compromised SNs attack subsection within this section. Again, the honest SNs are represented with a black color and the compromised SNs (i.e., the ones controlled by the attacker) with a red color (see Fig. 6.13). Next, we explain in more detail the local decision.

Local Decision

Based on its local energy estimation (3.2.3), the i^{th} SN generates a binary indicator random variable I_i as follows:

$$\left.\begin{array}{rcl} \text{if } T_i < \Lambda, I_i = 0 & \Longrightarrow & \text{decide } \mathcal{H}_0 \\ \text{if } T_i \geq \Lambda, I_i = 1 & \Longrightarrow & \text{decide } \mathcal{H}_1 \end{array}\right\} \tag{6.3.1}$$

where Λ is a local detection threshold that is the same for all the M SNs. The i^{th} SN local probability of false alarm (p_{fa}^i) and the local probability of detection (p_d^i) can be expressed as:

$$p_{fa}^i = \Pr\left(T_i \geq \Lambda | \mathcal{H}_0\right) = Q\left(\frac{\Lambda - \mathbb{E}\left\{T_i | \mathcal{H}_0\right\}}{\sqrt{\text{Var}\left\{T_i | \mathcal{H}_0\right\}}}\right) \tag{6.3.2}$$

$$p_d^i = \Pr\left(T_i \geq \Lambda | \mathcal{H}_1\right) = Q\left(\frac{\Lambda - \mathbb{E}\left\{T_i | \mathcal{H}_1\right\}}{\sqrt{\text{Var}\left\{T_i | \mathcal{H}_1\right\}}}\right) \tag{6.3.3}$$

where $Q(.)$ is the Q-function. While the i^{th} honest SN transmit its actual one-bit test statistic (i.e., I_i in (6.3.1)) to the FC, the compromised SNs falsify them before transmitting to the FC. Next we introduce the attacker model.

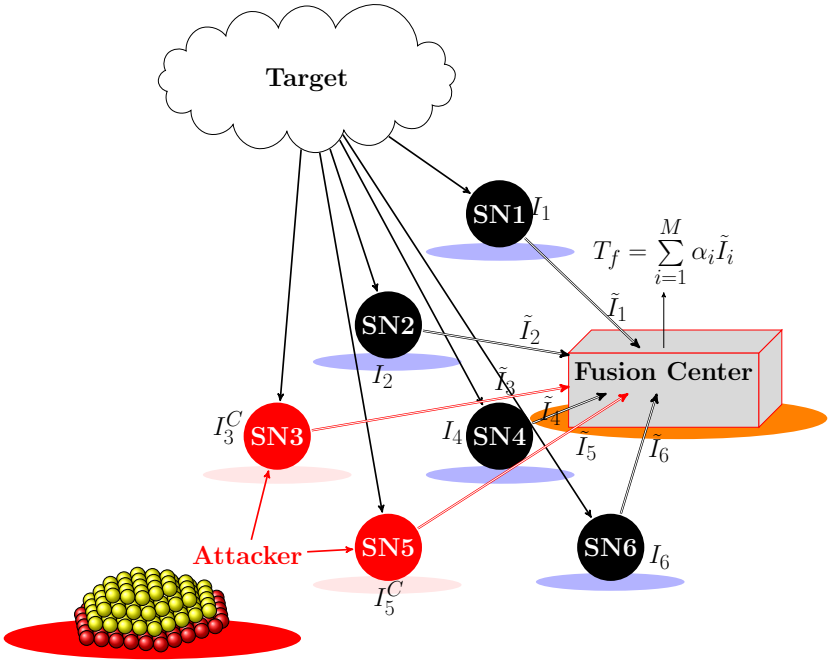

Figure 6.13: Under attack schematic communication architecture between peripheral SNs and the fusion center (FC). Each of the i^{th} honest/compromised SN represented with black/red color generates a local (binary) indicator variable (I_i/I_i^C) by observing the target and performing the test in (6.3.1) with local detection threshold Λ/Λ_C. While the i^{th} ($i = \{1, 2, 4, 6\}$) honest SN indicator (test statistic) remains unchanged (i.e., $\tilde{I}_i = I_i$), the j^{th} ($j = \{3, 5\}$) compromised SN falsify its indicator (test statistic) as in (6.3.7) before transmitting to the FC. Here i/j are the honest/compromised SN index.

6.3.2 Compromised SNs Attack

Different attack strategies could be adopted by the compromised SNs. In this work, the data falsification attack model widely used in [10, 11, 73] is considered. There is a β fraction of SNs controlled and compromised by the attacker. As before, (i.e., in the case of $attack - free$) each of the i^{th} compromised SNs perform the local test in (6.3.1) but now with a local detection threshold (Λ_C) controlled by the attacker and assumed to be the same for all the β fraction of compromised SNs. That is:

$$\left.\begin{array}{rcl} \text{if } T_i < \Lambda_C, I_i^C = 0 & \Longrightarrow & \text{decide } \mathcal{H}_0 \\ \text{if } T_i \geq \Lambda_C, I_i^C = 1 & \Longrightarrow & \text{decide} \mathcal{H}_1. \end{array}\right\} \tag{6.3.4}$$

Now, the probability of false alarm[10] ($p_{fa}^{i,C}$) and the probability of detection ($p_{d}^{i,C}$) at the i^{th} compromised SN are respectively given as:

$$p_{fa}^{i,C} = \Pr\left(T_i \geq \Lambda_C | \mathcal{H}_0\right) = Q\left(\frac{\Lambda_C - \mathbb{E}\left\{T_i | \mathcal{H}_0\right\}}{\sqrt{\mathrm{Var}\left\{T_i | \mathcal{H}_0\right\}}}\right) \tag{6.3.5}$$

$$p_{d}^{i,C} = \Pr\left(T_i \geq \Lambda_C | \mathcal{H}_1\right) = Q\left(\frac{\Lambda_C - \mathbb{E}\left\{T_i | \mathcal{H}_1\right\}}{\sqrt{\mathrm{Var}\left\{T_i | \mathcal{H}_1\right\}}}\right) \tag{6.3.6}$$

while for the honest SNs it remains as (6.3.2). After performing the test in (6.3.4), the compromised SNs further manipulate their binary indicator variables prior to FC transmission so as to yield the maximum possible FC degradation. Let P_C^{flip} be the probability that each compromised SN intentionally reports the opposite information to its actual local decision (i.e., flips the indicator random variable in (6.3.4) prior to FC transmission with probability P_C^{flip}). It is assumed that all the compromised SNs have the same probability of attack in a particular sensing period (see later Section 6.3.7 for details). The remaining (1-β) fraction SNs are honest and report to the FC accordingly. Now, the i^{th} local binary indicator test statistic for the compromised SN can be expressed as:

$$\tilde{I}_i = \begin{cases} 1 - I_i^C, & \text{with probability } P_C^{flip} \\ I_i^C, & \text{with probability } (1 - P_C^{flip}) \end{cases} \tag{6.3.7}$$

while for the honest SNs this relation is simply $\tilde{I}_i = I_i$. Next, we state a Lemma that will help us to derive (6.3.15)-(6.3.18) in the next page.

Lemma 6.3.1 *For the i^{th} compromised SN, the local probability of false alarm and probability of detection can be shown to be respectively:*

$$\tilde{p}_{fa}^{i} = P_C^{flip}\left(1 - p_{fa}^{i,C}\right) + \left(1 - P_C^{flip}\right) p_{fa}^{i,C} \tag{6.3.8}$$

$$\tilde{p}_{d}^{i} = P_C^{flip}\left(1 - p_{d}^{i,C}\right) + \left(1 - P_C^{flip}\right) p_{d}^{i,C}. \tag{6.3.9}$$

while for the honest SNs clearly we have $\tilde{p}_{fa}^{i} = p_{fa}^{i}$ and $\tilde{p}_{d}^{i} = p_{d}^{i}$.

Proof: The proof can be found in Appendix C.2. ■

Next, we introduce a simplified (optimum) linear fusion rule at the FC.

[10] Here the superscript i, C refers to the i^{th} compromised SN.

6.3.3 Simplified Fusion Rule-The Linear Approach

Now, the i^{th} SN transmits to the FC the one-bit local test statistic ($\tilde{I}_i$). The communication channels between SNs and the FC are assumed to be error-free in this paper. Upon receiving all the contributions (which are assumed to be independent, identically distributed (i.i.d.)) from all the SNs (i.e., compromised and honest), the FC linearly combines them:

$$T_f = \sum_{i=1}^{M} \alpha_i \tilde{I}_i \tag{6.3.10}$$

where $\{\alpha_i\}_{i=1}^{M}$ are the optimum weights that we will derive later in section 6.3.4. The FC then makes the final decisions:

$$\left.\begin{array}{l} \text{if } T_f < \Lambda_f, \text{ decide } \mathcal{H}_0 \\ \text{if } T_f \geq \Lambda_f, \text{ decide } \mathcal{H}_1 \end{array}\right\} \tag{6.3.11}$$

where Λ_f is the FC detection threshold. Let

$$P_d = \Pr\big(T_f \geq \Lambda_f | \mathcal{H}_1\big) \tag{6.3.12}$$

$$P_{fa} = \Pr\big(T_f \geq \Lambda_f | \mathcal{H}_0\big) \tag{6.3.13}$$

where P_d and P_{fa} are the system probability of detection and probability of false alarm respectively. For large M, T_f can be approximated by a Gaussian distribution and the P_d for a fixed P_{fa} is given as [78]:

$$P_d = Q\left(\frac{Q^{-1}\left(P_{fa}\right)\sqrt{\mathrm{Var}\left\{T_f|\mathcal{H}_0\right\}} - \mathbb{E}\left\{T_f|\mathcal{H}_1\right\} + \mathbb{E}\left\{T_f|\mathcal{H}_0\right\}}{\sqrt{\mathrm{Var}\left\{T_f|\mathcal{H}_1\right\}}}\right) \tag{6.3.14}$$

with appropriate quantities given in (6.3.15)-(6.3.18):

$$\mathbb{E}\left\{T_f|\mathcal{H}_1\right\} = (1-\beta)\sum_{i=1}^{M}\alpha_i p_d^i + \beta\left[P_C^{flip}\Big(\sum_{i=1}^{M}\alpha_i\big(1-p_d^{i,C}\big)\Big) + \big(1-P_C^{flip}\big)\Big(\sum_{i=1}^{M}\alpha_i p_d^{i,C}\Big)\right] \tag{6.3.15}$$

$$\mathbb{E}\left\{T_f|\mathcal{H}_0\right\} = (1-\beta)\sum_{i=1}^{M}\alpha_i p_{fa}^i + \beta\left[P_C^{flip}\Big(\sum_{i=1}^{M}\alpha_i\big(1-p_{fa}^{i,C}\big)\Big) + \big(1-P_C^{flip}\big)\Big(\sum_{i=1}^{M}\alpha_i p_{fa}^{i,C}\Big)\right]. \tag{6.3.16}$$

$$\begin{aligned}\mathrm{Var}\left\{T_f|\mathcal{H}_1\right\} &= (1-\beta)\sum_{i=1}^{M}\alpha_i^2 p_d^i\Big(1-p_d^i\Big) \\ &+\beta\Bigg[\Bigg(P_C^{flip}\Big(\sum_{i=1}^{M}\alpha_i^2\big(1-p_d^{i,C}\big)\Big)+\big(1-P_C^{flip}\big)\Big(\sum_{i=1}^{M}\alpha_i^2 p_d^{i,C}\Big)\Bigg) \\ &\Bigg(1-P_C^{flip}\Big(\sum_{i=1}^{M}\alpha_i^2\big(1-p_d^{i,C}\big)\Big)-\big(1-P_C^{flip}\big)\Big(\sum_{i=1}^{M}\alpha_i^2 p_d^{i,C}\Big)\Bigg)\Bigg]\end{aligned} \tag{6.3.17}$$

$$\begin{aligned}\mathrm{Var}\left\{T_f|\mathcal{H}_0\right\} &= (1-\beta)\sum_{i=1}^{M}\alpha_i^2 p_{fa}^i\Big(1-p_{fa}^i\Big) \\ &+\beta\Bigg[\Bigg(P_C^{flip}\Big(\sum_{i=1}^{M}\alpha_i^2\big(1-p_{fa}^{i,C}\big)\Big)+\big(1-P_C^{flip}\big)\Big(\sum_{i=1}^{M}\alpha_i^2 p_{fa}^{i,C}\Big)\Bigg) \\ &\Bigg(1-P_C^{flip}\Big(\sum_{i=1}^{M}\alpha_i^2\big(1-p_{fa}^{i,C}\big)\Big)-\big(1-P_C^{flip}\big)\Big(\sum_{i=1}^{M}\alpha_i^2 p_{fa}^{i,C}\Big)\Bigg)\Bigg].\end{aligned} \tag{6.3.18}$$

6.3.4 Weight Combining Optimisation

In this section, we would like to find the optimum weighting vector ($\boldsymbol{\alpha}_{opt}$) that maximize (6.3.14). However, maximizing (6.3.14)) w.r.t. $\boldsymbol{\alpha}$ is difficult and no closed form solution can be found. So we will approximate the optimal solution by adopting the MDC [32] (as in previous section) as an alternative function to be maximized:

$$\tilde{d}^2(\boldsymbol{\alpha}) = \left(\frac{\mathbb{E}\left\{T_f|H_1\right\}-\mathbb{E}\left\{T_f|H_0\right\}}{\sqrt{\mathrm{Var}\left\{T_f|H_1\right\}}}\right)^2 = \frac{\left(\boldsymbol{b}^T\boldsymbol{\alpha}\right)^2}{\boldsymbol{\alpha}^T\mathbf{R}\boldsymbol{\alpha}} \tag{6.3.19}$$

where

$$\boldsymbol{b} = \begin{bmatrix}(1-\beta)\big(p_d^1-p_{fa}^1\big)-\beta\big(p_d^{1,C}-p_{fa}^{1,C}\big)\big(2P_C^{fal}-1\big)\\(1-\beta)\big(p_d^2-p_{fa}^2\big)-\beta\big(p_d^{2,C}-p_{fa}^{2,C}\big)\big(2P_C^{fal}-1\big)\\\vdots\\(1-\beta)\big(p_d^M-p_{fa}^M\big)-\beta\big(p_d^{M,C}-p_{fa}^{M,C}\big)\big(2P_C^{fal}-1\big)\end{bmatrix}, \boldsymbol{\alpha} = \begin{bmatrix}\alpha_1\\\alpha_2\\\vdots\\\alpha_M\end{bmatrix} \tag{6.3.20}$$

$$\mathbf{R} = (1-\beta)\mathrm{diag}\begin{bmatrix} p_d^1(1-p_d^1)+\frac{\beta}{1-\beta}\Big(P_C^{flip}+p_d^{1,C}\big(1-2P_C^{flip}\big)\Big)\Big(1-P_C^{flip}+p_d^{1,C}\big(2P_C^{flip}-1\big)\Big) \\ p_d^2(1-p_d^2)+\frac{\beta}{1-\beta}\Big(P_C^{flip}+p_d^{2,C}\big(1-2P_C^{flip}\big)\Big)\Big(1-P_C^{flip}+p_d^{2,C}\big(2P_C^{flip}-1\big)\Big) \\ \vdots \\ p_d^M(1-p_d^M)+\frac{\beta}{1-\beta}\Big(P_C^{flip}+p_d^{M,C}\big(1-2P_C^{flip}\big)\Big)\Big(1-P_C^{flip}+p_d^{M,C}\big(2P_C^{flip}-1\big)\Big) \end{bmatrix}. \tag{6.3.21}$$

Now, our optimization problem is:

$$\boldsymbol{\alpha}_{opt} = \arg\max_{\boldsymbol{\alpha}}\Big(\tilde{d}^2(\boldsymbol{\alpha})\Big). \tag{6.3.22}$$

Further, via the transformation $\boldsymbol{\psi} = \mathbf{R}^{1/2}\boldsymbol{\alpha}$, the deflection coefficient (6.3.19) becomes:

$$\tilde{d}^2(\boldsymbol{\psi}) = \frac{\boldsymbol{\psi}^T\mathbf{D}\boldsymbol{\psi}}{||\boldsymbol{\psi}||^2},\ \mathbf{D} = \mathbf{R}^{-T/2}\boldsymbol{b}\boldsymbol{b}^T\mathbf{R}^{-1/2}. \tag{6.3.23}$$

So $\boldsymbol{\alpha}_{opt} = \mathbf{R}^{-1/2}\boldsymbol{\psi}_{opt} = k\mathbf{R}^{-1}\boldsymbol{b}$, where $\boldsymbol{\psi}_{opt} = k\mathbf{R}^{-1/2}\boldsymbol{b}$ is the normalized eigenvector corresponding to the maximum eigenvalue of $\mathbf{D}$. Now, the optimum weight combining in (6.3.10) can be easily shown to be (6.3.24).

$$\alpha_{opt}^i = \frac{(1-\beta)\big(p_d^i-p_{fa}^i\big)+\beta\big(p_{fa}^{i,C}-p_d^{i,C}\big)\big(2P_C^{fal}-1\big)}{(1-\beta)\big(p_d^i(1-p_d^i)\big)+\beta\Big(P_C^{flip}+p_d^{i,C}\big(1-2P_C^{flip}\big)\Big)\Big(1-P_C^{flip}+p_d^{i,C}\big(2P_C^{flip}-1\big)\Big)}. \tag{6.3.24}$$

Clearly, the optimum weights depend upon the local probability of false alarm and the probability of detection metrics as well as on the β (fraction of compromised SNs) and the probability of flipping the local decisions by the attacker. For the SNs that are honest (i.e., controlled by the FC) these local probabilities are known (since the FC can settle the local detection threshold itself). However, for the compromised SNs these local probabilities are not available at the FC (since the attacker takes control of the local detection threshold). To make the matter worst, the FC knows just the fraction of compromised SNs (i.e., β) but it cannot identify who they are. As a result, the FC cannot implement the optimum weight combining fusion rule (6.3.10) (i.e., with $\alpha^i = \alpha_{opt}^i$ in (6.3.24)).

Later, in section 6.3.7, we propose a simple but yet effective approach to possibly identify these compromised SNs and compute the optimum weights at the FC based on their assigned reliability. Next, we derive the optimum attacker flipping probability which makes the FC incapable of detecting.

6.3.5 Attacker Flipping Probability Optimisation

In this section, we derive the optimum flipping probability that the attacker needs to adopt to the compromised SNs in order to cause the maximum possible degradation to the FC (i.e., to possibly make the FC incapable of detecting). Again, we adopt the modified deflection coefficient as an alternative function to be optimized and assume that the FC does not act strategically against the attacker strategy.

Lemma 6.3.2 *The optimum flipping probability* $\left(P_{C,opt}^{flip}\right)$ *which minimizes the modified deflection coefficient is:*

$$P_{C,opt}^{flip} = \frac{\beta - 1}{2\beta}\left(\frac{\sum_{i=1}^{M}\alpha_i\left(p_d^i - p_{fa}^i\right)}{\sum_{i=1}^{M}\alpha_i\left(p_{fa}^{i,C} - p_d^{i,C}\right)}\right) + \frac{1}{2} \tag{6.3.25}$$

Proof: Since the modified deflection coefficient is always non-negative, then its minimum is always greater than or equal to zero. So, the condition to make the minimum of the modified deflection coefficient zero is:

$$\begin{aligned}\boldsymbol{b}^T\boldsymbol{\alpha} = \left(1-\beta\right)\sum_{i=1}^{M}\alpha_i\left(p_d^i - p_{fa}^i\right) + \beta P_C^{fal}\sum_{i=1}^{M}\alpha_i\left(p_{fa}^{i,C} - p_d^{i,C}\right) \\ + \beta\left(1 - P_C^{fal}\right)\sum_{i=1}^{M}\alpha_i\left(p_d^{i,C} - p_{fa}^{i,C}\right) = 0\end{aligned} \tag{6.3.26}$$

Further simplification of the above and re-arrangement of the terms yields:

$$\begin{aligned}\beta\Big(\sum_{i=1}^{M}\alpha_i\left(p_{fa}^{i,C} - p_d^{i,C}\right)\Big)\Big(2P_C^{fal} - 1\Big) &= \left(\beta - 1\right)\sum_{i=1}^{M}\alpha_i\left(p_d^i - p_{fa}^i\right) \\ \implies P_{C,opt}^{flip} &= \frac{\beta - 1}{2\beta}\left(\frac{\sum_{i=1}^{M}\alpha_i\left(p_d^i - p_{fa}^i\right)}{\sum_{i=1}^{M}\alpha_i\left(p_{fa}^{i,C} - p_d^{i,C}\right)}\right) + \frac{1}{2}.\end{aligned} \tag{6.3.27}$$

This concludes the proof. ■

The special case when the attacker does not change the local detection threshold in (6.3.4) (i.e., $p_d^i = p_d^{i,C}$ and $p_{fa}^i = p_{fa}^{i,C}$), the optimum probability of flipping the local decisions can be shown to be:

$$P_{C,opt}^{flip} = \begin{cases} \frac{1}{2} - \frac{\beta - 1}{2\beta} = \frac{1}{2\beta}, & \text{for } 0.5 \leq \beta \leq 1 \\ \text{not applicable}, & \text{for } \beta = 0 \\ \text{not defined}, & \text{otherwise.} \end{cases} \tag{6.3.28}$$

Interestingly, in this case the optimum probability of flipping the local SNs decision is inversely proportional to the fraction of the compromised SNs (β). As expected, when β increases, the optimum probability of flipping the local decision in order to make the modified deflection coefficient zero decreases and vice-versa. Furthermore, when the half of the network is compromised (i.e., $\beta = 0.5$), the attacker can make the modified deflection coefficient zero with $P_{C,opt}^{flip} = 1$ (i.e., the local SNs should always flip their local decisions). This is as expected because always flipping the local decisions of a 50% SNs manipulated network can totally make the FC incapable of detecting.

6.3.6 Minimum Fraction of Compromised SNs

Now, we are interesting in the minimum fraction of the compromised SNs that is needed to cause the maximum possible degradation to the FC. We state the result in the next Lemma.

Lemma 6.3.3 *The minimum fraction of the compromised SNs needed to make the FC incapable of detecting or to make the modified deflection coefficient zero is* $\beta_{min} \geq \frac{1}{2}$.

Proof: As we previously stated, the modified deflection coefficient is always non-negative and the minimum occurs at zero. From (6.3.26), the condition to make the

modified deflection coefficient zero is:

$$\begin{aligned}\boldsymbol{b}^T\boldsymbol{\alpha} = (1-\beta)\sum_{i=1}^{M}\alpha_i\big(p_d^i - p_{fa}^i\big) + \beta P_C^{fal}\sum_{i=1}^{M}\alpha_i\big(p_{fa}^{i,C} - p_d^{i,C}\big) \\ +\beta\big(1-P_C^{fal}\big)\sum_{i=1}^{M}\alpha_i\big(p_d^{i,C} - p_{fa}^{i,C}\big) = 0.\end{aligned} \tag{6.3.29}$$

After simplifying the above equation, the condition on β needed to make the FC incapable of detecting becomes:

$$\beta = \left(1 - \underbrace{\left(\frac{\left(\sum_{i=1}^{M}\alpha_i\big(p_d^{i,C} - p_{fa}^{i,C}\big)\right)\left(1-2P_C^{fal}\right)}{\sum_{i=1}^{M}\alpha_i\big(p_d^i - p_{fa}^i\big)}\right)}_{\text{(A)}}\right)^{-1}. \tag{6.3.30}$$

Now, the minimum of β (β_{min}) can be achieved when term (A) of (6.3.30) is minimum. We also know that for any real scalar a and b the following holds:

$$\min\big(\frac{a}{b}\big) \geq \frac{\min\big(a\big)}{\max\big(b\big)} \tag{6.3.31}$$

Using (6.3.30) and (6.3.31), we now derive a lower bound on the minimum β. Clearly, we require that both the numerator and the denominator of the term (A) takes the minimum and the maximum values respectively. Now, the minimum of the numerator (i.e., $\min\Big(\big(\sum_{i=1}^{M}\alpha_i\big(p_d^{i,C} - p_{fa}^{i,C}\big)\big)\big(1-2P_C^{fal}\big)\Big)$) can be achieved if both $p_d^{i,C} = P_C^{fal} = 0$ and $p_{fa}^{i,C} = 1$ or alternatively when both $p_d^{i,C} = P_C^{fal} = 1$ and $p_{fa}^{i,C} = 0$. Similarly, the maximum of the denominator of term (A) (i.e., $\max\Big(\sum_{i=1}^{M}\alpha_i\big(p_d^i - p_{fa}^i\big)\Big)$) can be achieved when both $p_d^i = 1$ and $p_{fa}^i = 0$. Finally, using the above analysis we can easily show that:

$$\beta_{min} \geq \left(1 - \frac{-M}{M}\right)^{-1} = \frac{1}{2}. \tag{6.3.32}$$

This concludes the proof. ■

In the special case when the attacker does not change the local detection threshold in (6.3.4) (i.e., $p_d^i = p_d^{i,C}$ and $p_{fa}^i = p_{fa}^{i,C}$), the minimum fraction of compromised SNs required to make the modified deflection coefficient zero (i.e., make the FC incapable of detecting) can be shown to be: $\beta_{min} = \frac{1}{2}$ and this can be achieved with $P_C^{fal} = 1$ (see (6.3.28)).

6.3.7 Compromised SNs Identification and Weight Combining Computation

In this section, we propose a scheme to identify the compromised SNs and compute the weight combining in (6.3.10) based on each SN assigned reliability. As in [73], [101], we divide the local sensing process into time windows consisting of K sensing periods[11].

Compromised SNs Identification

At the fusion center, the received observations corresponding to the i^{th} SNs can be expressed as $\tilde{\boldsymbol{I}}_i = [\tilde{I}_i(1), \tilde{I}_i(2), \cdots, \tilde{I}_i(K)]$, $\forall i = 1, 2, \cdots, M$. At the l^{th} sensing period, upon receiving the contributions from all the SNs (i.e., compromised and honest) the FC linearly combines them to yield:

$$T_f(l) = \sum_{j=1}^{M} \alpha_j^{AF} \tilde{I}_j(l), \quad l = 1, 2, \cdots, K \tag{6.3.33}$$

$$T_f^i(l) = \sum_{j=1, i\neq j}^{M} \alpha_j^{AF} \tilde{I}_j(l), \; l = 1, 2, \cdots, K, \; i = 1, 2, \cdots, M \tag{6.3.34}$$

where $T_f^i(l)$ is the final test statistic at the l^{th} sensing period without the contribution of the i^{th} SN, $\{\alpha_j^{AF}\}_{j=1}^{M}$ are the optimum weights under attack-free scenario and can be easily derived from (6.3.24) by substituting ($\beta = 0$, $P_C^{fal} = 0$, $p_{fa}^{i,C} = p_{fa}^i$ and $p_d^{i,C} = p_d^i$, $\forall i$). These can be shown to be:

$$\alpha_j^{AF} = \frac{p_d^j - p_{fa}^j}{p_d^j(1 - p_d^j)}. \tag{6.3.35}$$

Based on the test statistics (6.3.33), the FC then generates at the l^{th} sensing period two different indicator random variables as follows:

$$I_f(l) = \begin{cases} 0 \text{ if } T_f(l) < \Lambda_f \\ 1 \text{ if } T_f(l) \geq \Lambda_f \end{cases} \qquad I_f^i(l) = \begin{cases} 0 \text{ if } T_f^i(l) < \Lambda_f \\ 1 \text{ if } T_f^i(l) \geq \Lambda_f. \end{cases} \tag{6.3.36}$$

[11] Each SN samples N times (see (3.2.3)) in each sensing interval to then perform the energy detection as in (6.3.1).

Now that the FC has evaluated these two indicator random variables (i.e., $I_f(l)$ and $I_f^i(l)$), it then compares them to each of the i^{th} SN local indicator variable $\tilde{I}_i(l)$ to yield:

$$d_i(l) = \begin{cases} 1 \text{ if } I_f(l) \neq \tilde{I}_i(l) \\ 0 \qquad \text{otherwise} \end{cases} \qquad \hat{d}_i(l) = \begin{cases} 1 \text{ if } I_f^i(l) \neq \tilde{I}_i(l) \\ 0 \qquad \text{otherwise} \end{cases} \tag{6.3.37}$$

where $d_i(l)$ represents the inconsistency between the FC decision (where all the SNs contribution is counted) and the i^{th} SN local decision. Similarly, $\hat{d}_i(l)$ represents the same but now the i^{th} SN is not considered at the FC decision. Note that all of the above steps are performed during the same time window K. After observing the reports up to K sensing periods, the FC evaluates a reliability metric for the i^{th} SN as follows:

$$r_i \quad = \quad \frac{1}{K}\left|\sum_{l=1}^{K}\big(d_i(l) - \hat{d}_i(l)\big)\right|, \qquad i \quad = \quad 1, 2, \cdots, M. \tag{6.3.38}$$

It is worth mentioning that r_i's for the compromised SNs are expected to be larger than those for the honest ones (see simulations results section later). Finally, the FC performs the reliability test:

$$\left.\begin{array}{ll} \text{if } r_i < \delta, & \text{decide reliable} \\ \text{if } r_i \geq \delta, & \text{decide not reliable} \end{array}\right\} \tag{6.3.39}$$

where δ is the reliability detection threshold. Now, the probability that a compromised SNs has been *truly* detected and the probability that a honest SNs has been $falsely$ detected at the i^{th} SN are respectively:

$$P_d^{i,true} = \Pr\big(r_i \geq \delta | Compromised\big) \tag{6.3.40}$$

$$P_d^{i,false} = \Pr\big(r_i \geq \delta | Honest\big) \tag{6.3.41}$$

where the superscript "$i, true$" and "$i, false$" represents the $true$ and $false$ detection at the i^{th} SN respectively. Obviously, the compromised SNs detection performance depends on the choice of the reliability detection threshold (δ). If we choose a large δ, $P_d^{i,false}$ is expected to be low. However, this will also make $P_d^{i,true}$ be small. On the other hand, choosing a smaller δ is expected to increase the $P_d^{i,true}$ value but also an increase on $P_d^{i,false}$ value will be noticed. Clearly, the reliability detection

threshold imposes a trade-off between these two metrics. Note that in practice we wish to keep $P_d^{i,false}$ close to zero and $P_d^{i,true}$ close to one. Based on this reliability test (i.e., the test in (6.3.39)), next we will evaluate the weight combining in (6.3.10) such that the probability of detection in (6.3.14) is further improved.

Proposed Weight Combining Computation

In this section, we propose a weight combining computation based on the reliability test (6.3.39). Existing schemes use reputation-based metrics to possibly identify the compromised SNs and then totally exclude them from contributing to the FC process and decision. However, identifying and then excluding them from detection process is not the optimum solution. For instance, we might end up removing from contributing towards the global decision compromised SNs that hold useful information in general (for example those SNs with high local SNRs). Different from the existing approaches, here we propose to update the weight combining (i.e., (6.3.35)) of each SN based on the *correctness* of information reported to the FC. That is:

$$\alpha_i^{AF} = \begin{cases} \alpha_i^{AF} & \text{if } r_i < \delta \\ \alpha_i^{AF} - \mu r_i & \text{if } r_i \geq \delta \end{cases} \tag{6.3.42}$$

where $\mu \in [0, \infty]$ is the weight penalty that is the same for all the M SNs. For those SNs that are identified as being compromised by the attacker, the FC is likely to decrease their weights. For example, those SNs that are identified as influential and unreliable (i.e., where r_i turn out to be relatively large) the FC decreases the current weights most. However, for those SNs that are identified as compromised but not so influential to the FC decision process (i.e., r_i is relatively small) the FC decreases the weights proportional to r_i. With regard to the SNs identified as honest, the FC keeps their weights unchanged. In this way, the FC decides through the weight combiner how much a local report should contribute to the FC final decision. This is a reasonable approach as if the report from a SN tends to be incorrect, it should be counted less in the final decision.

Next, in the simulation results, we will show that the reliability detection threshold (δ) and the weight penalty (μ) are crucial for the system detection performance.

We will also show via simulations that there is an optimum δ and μ such that the system detection performance is maximized.

6.3.8 Simulation Results

Simulation Setup

Here we will evaluate numerically the performance of our proposed strategy and compare to the $attack-free$ scheme [35] and the strategy in [73]. A WSN with a total of $M = 40$ SNs is considered (where β fraction of these SNs are compromised by the attacker). We let all the $\sigma_i^2 = 0.1$, such that $\xi_a = 10\log_{10}\left(\frac{1}{M}\sum_{i=1}^{M}\xi_i\right) =$ -10.5 dB with arbitrary chosen $\boldsymbol{s}(n) = [s_1(n), s_2(n), \cdots, s_M(n)]$ =[0.1, 0.175, 0.065, 0.027, 0.024, 0.026, 0.06, 0.09, 0.153, 0.11, 0.22, 0.12, 0.1, 0.024, 0.019, 0.05, 0.12, 0.1, 0.023, 0.021, 0.1, 0.175, 0.18, 0.027, 0.024, 0.026, 0.06, 0.09, 0.1, 0.065, 0.1, 0.175, 0.027, 0.024, 0.18, 0.026, 0.2, 0.09, 0.1, 0.18]^T, where $\xi_i = \sum_{n=1}^{N} s_i^2(n)/N\sigma_i^2$. We will also refer to "equal weight" combining in (6.3.10) (i.e., $\alpha_i = 1, \forall i$) and use this as a benchmark. Finally, we use 10^5 Monte-Carlo simulations and choose a fixed (equal) local SNs threshold (Λ) in (6.3.1) and local SNs threshold (Λ_C) in (6.3.4) (i.e., more specifically, $\Lambda = \Lambda_C = 2.6$) such that $\bar{P}_d^{false} \leq 0.6$ (see Fig. 6.17-Fig. 6.19).

Impact of the Time Window Length K on the Malicious SN Detection Accuracy and on the System Detection Performance

In this section, we investigate the impact that the time window length (K) has on the compromised SNs identification accuracy of the proposed scheme. More precisely, we are interested in examining the two metrics, $P_d^{i,true}$ and $P_d^{i,false}$ (see (6.3.40)). Next, we are interested in the impact that this time window length (K) has on the system detection performance. More precisely, we will examine the two metrics P_d and P_{fa} (see (6.3.12)). Note that K affects these two metrics through the reliability metric r_i (see Fig. 6.14) in (6.3.38) which consequently affects the FC weight combining (6.3.42) that finally decides on the FC final test statistic (T_f) (see (6.3.10)).

In Fig. 6.14 we show the reliability metric (r_i) against the FC detection threshold

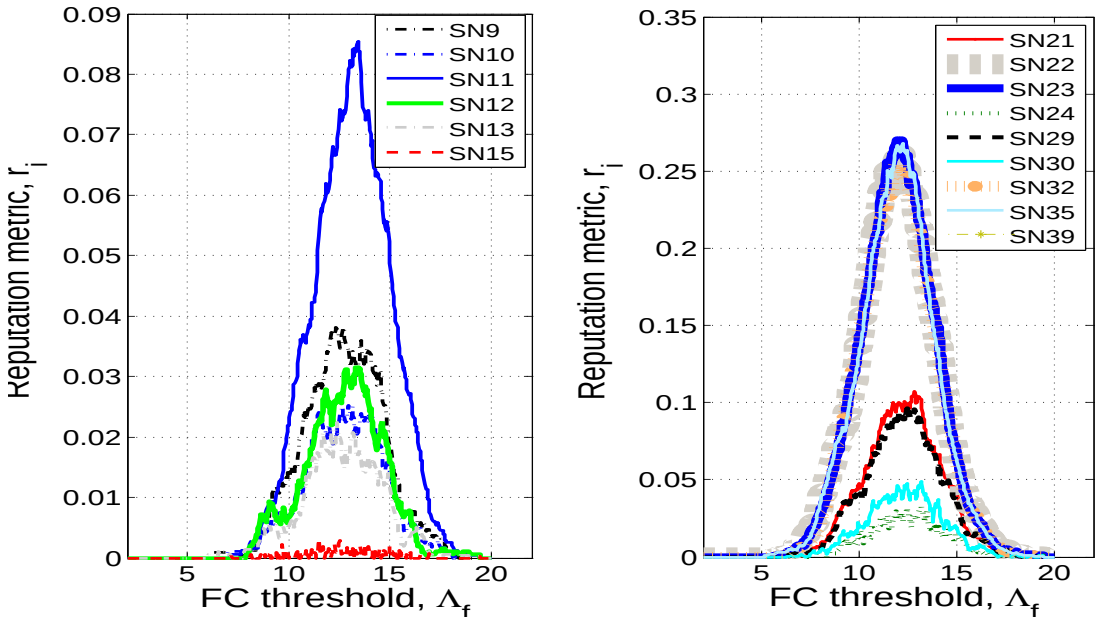

Figure 6.14: The reliability metric (r_i) versus the FC detection threshold (Λ_f) against the SNs with $M = 40$, $N = 20$, $\beta = 0.5$, $P_C^{flip} = 1$ and $K = 150$.

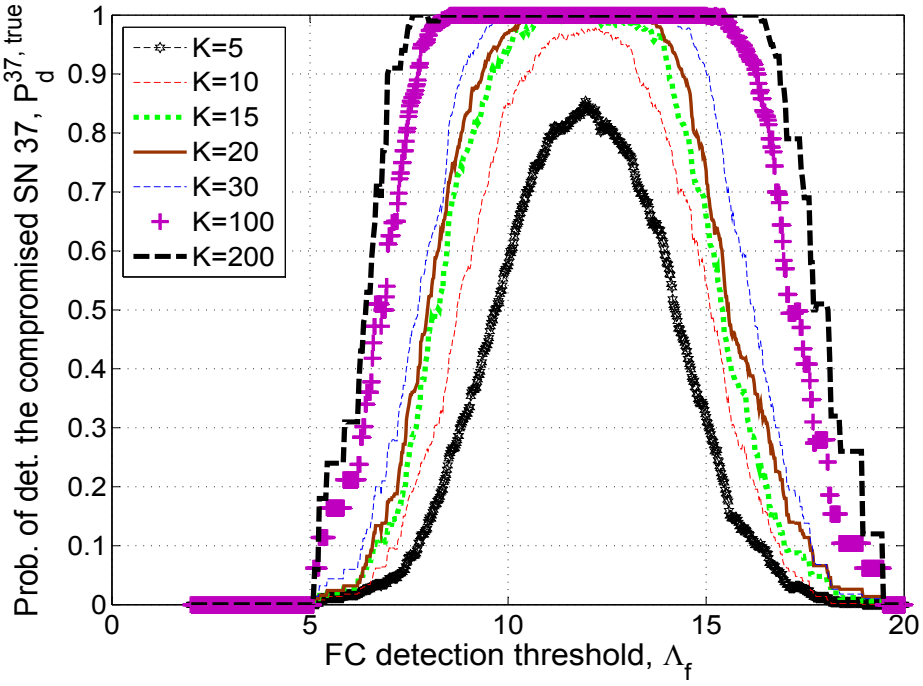

Figure 6.15: Probability that the (compromised) SN 37 has been truly detected ($P_d^{37,true}$) versus the FC detection threshold (Λ_f) with $M = 40$, $N = 20$, $\beta = 0.5$, $P_C^{flip} = 1$ and $\delta = 0.009$.

(Λ_f) for the compromised and the honest SNs. As expected, for the compromised but *influential* SNs (i.e., SNs with the high local SNRs), the corresponding reliability metrics will be higher. In contrary, the compromised or honest SNs but less *influential*, the corresponding reliability metrics with be lower.

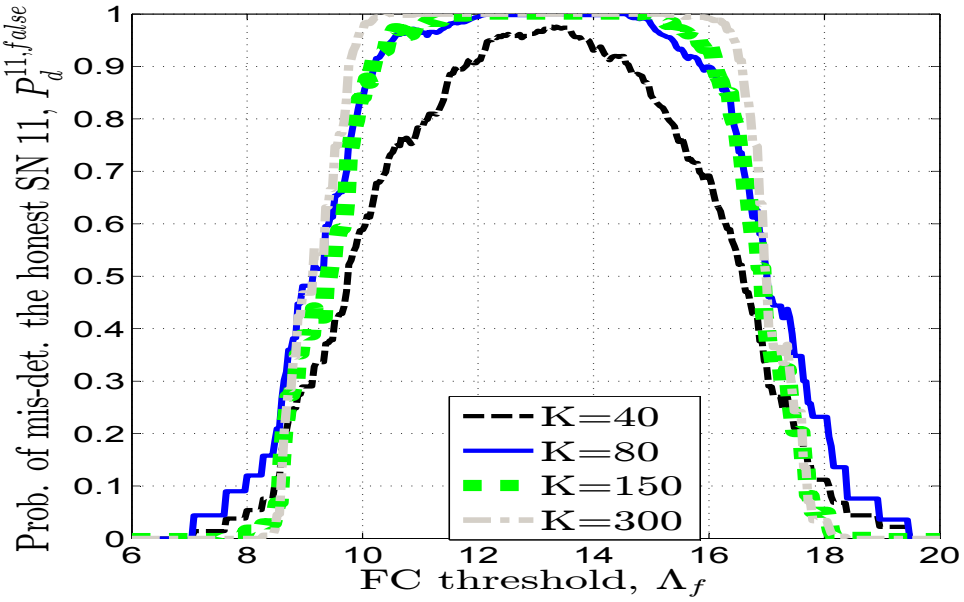

Figure 6.16: Probability that the (honest) SN 11 has been falsely detected ($P_d^{11,false}$) versus the FC detection threshold (Λ_f) with $M = 40$, $N = 20$, $\beta = 0.5$, $P_C^{flip} = 1$ and $\delta = 0.009$.

In Fig. 6.15 we plot the probability of compromised SN's detection[12] (i.e., *truly* detecting probability) ($P_d^{i,true}$) versus Λ_f for different time window length (K). Clearly, as K increases, the detection accuracy (of the (compromised) SN 37) $P_d^{37,true}$ improves.

In Fig. 6.16, we now plot the probability of honest SN's $mis-detection$12 (i.e., $falsely$ detecting probability) ($P_d^{i,false}$) (see (6.3.40)) versus (like before) Λ_f for different time window length (K). Similarly (as in Fig. 6.15), we observe that the $mis-detection$ performance (of the (honest) SN 11) $P_d^{11,false}$ increases with K. Now, from Fig. 6.15 and Fig. 6.16 we conclude that increasing the time window length K

[12]SN 37 (Fig. 6.15) and SN 11 (Fig. 6.16) were chosen for comparison purposes as they possess the best and the worst performances among F and $(M - F)$ SNs for each case respectively. Here F and $(M - F)$ represents the compromised and the honest SNs' cardinality.

not only improves the detection accuracy of the compromised SNs but at the same time increases (the undesired) $mis-detection$ probability of the honest SNs. This leads to a trade-off (while selecting the K parameter) between the compromised SNs detection accuracy and the honest SNs $mis-detection$ performance. Note that in practice we wish to keep $P_d^{i,true}$ high and $P_d^{i,false}$ low.

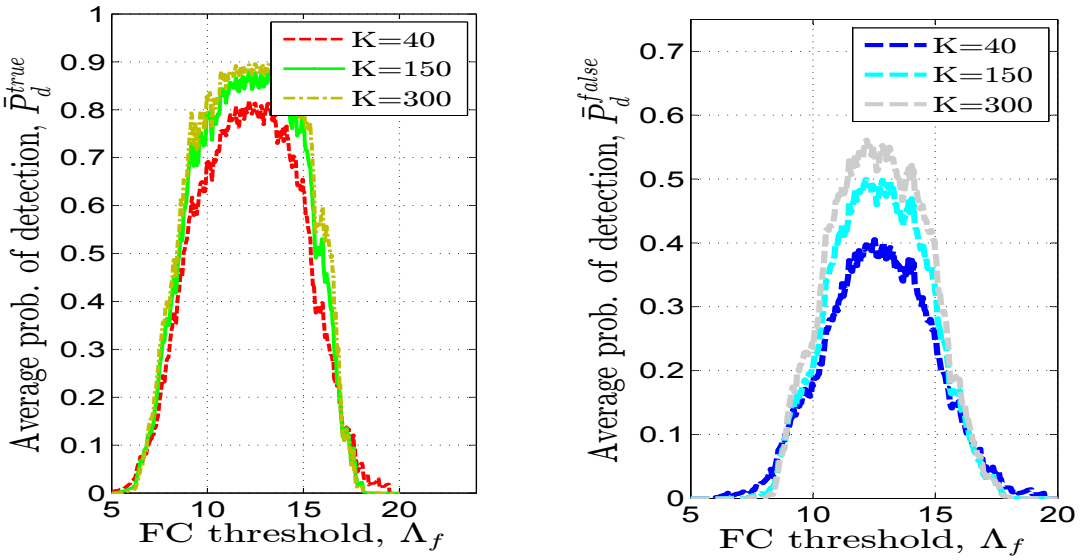

Figure 6.17: Average probabilities: (left) of compromised SNs detection; (right) of honest SNs mis-detection versus the FC detection threshold (Λ_f) with $M = 40$, $N = 20$, $\beta = 0.5$, $P_C^{flip} = 1$ and $\delta = 0.009$.

To give more generality to the results, in Fig. 6.17 we plot the average[13] performances (where the average is taken over the compromised/honest SNs cardinality). (left) We observe that while increasing K (more specifically from $K = 40$ to $K = 150$) we see an improvement in the average detection accuracy of compromised SNs. For larger K (e.g., $K = 300$) this improvement is negligible; (right) The same trend is observed for the average $mis-detection$ performance of the honest SNs.

In Fig. 6.18 we plot the $\bar{P}_d^{i,true}$ and $\bar{P}_d^{false}$ versus the time window length (K) for

[13]The average performances are defined respectively as: $\bar{P}_d^{true} = \frac{1}{F}\sum_{i\in J} P_d^{i,true}$ and $\bar{P}_d^{false} = \frac{1}{M-F}\sum_{i\in \hat{J}} P_d^{i,false}$, where J ($\hat{J}$) represents the compromised (honest) SNs set with cardinality F ($[M-F]$) respectively.

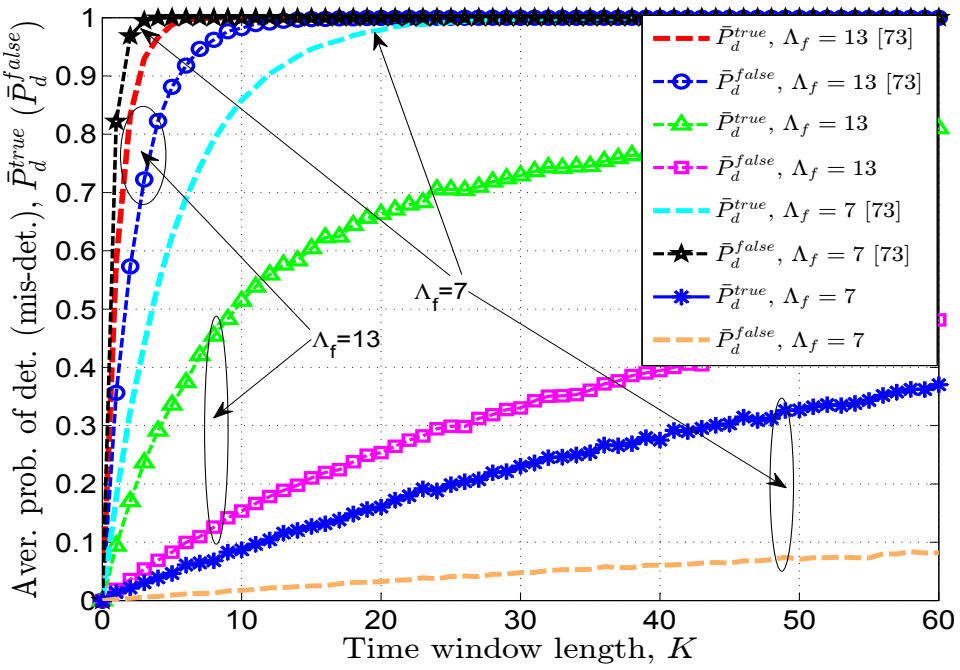

Figure 6.18: Average compromised SNs detection probability against honest SNs mis-detection probability versus the time window length (K) with $M = 40$, $N = 20$, $\beta = 0.5$, $P_C^{flip} = 1$ and $\delta = 0.009$.

a fixed FC detection threshold (Λ_f). We can observe that the average compromised SNs detection performance ($\bar{P}_d^{i,true}$) improves with the time window length (K) for both schemes (i.e., the proposed one in this paper and the scheme proposed in [73]). Similar behavior can be observed for the honest SNs $mis-detection$ probability. We also can observe that our proposed detection scheme outperforms the scheme proposed in [73] (or at least for the simulation setup considered in this paper), $\forall K$ in terms of $\bar{P}_d^{i,true} - \bar{P}_d^{false}$ quantity (e.g., for $\Lambda_f = 7$, $P_d^{i,true} - \bar{P}_d^{false} \leq 0, \forall K$ for the scheme proposed in [73]). We note that in practice we would like to have $P_d^{i,true}$ close to 1 and $\bar{P}_d^{false}$ close to 0 (i.e., $P_d^{i,true} - \bar{P}_d^{false}$ close to 1).

In Fig. 6.19 we plot the same (i.e., $P_d^{i,true}$ and $\bar{P}_d^{false}$ performances) but now against the fraction of compromised SNs (β). Clearly, the quantity $P_d^{i,true} - \bar{P}_d^{false}$ improves when the fraction of compromised SNs (β) decreases. This behavior is as expected resulting in a robust compromised SNs detection scheme.

Now, to give a more validity on the results, in Fig. 6.20 we show the difference between the system detection performance and the system false alarm probability

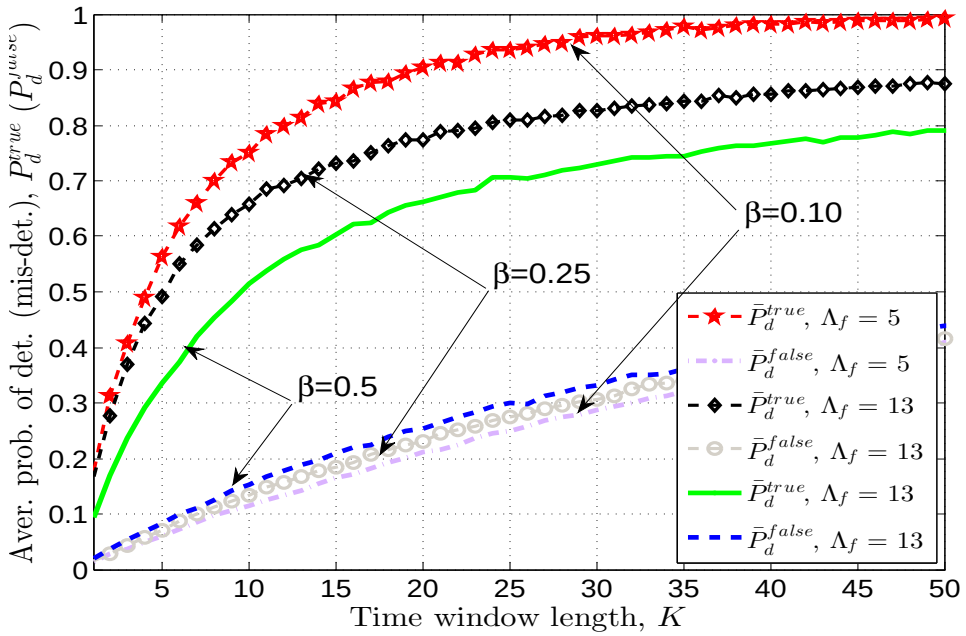

Figure 6.19: Average compromised SNs detection probability and honest SNs mis-detection probability versus the time window length (K) and against β with $M = 40$, $N = 20$, $P_C^{flip} = 1$ and $\delta = 0.009$.

($P_d - P_{fa}$) versus the time window length (K) against the FC detection threshold (Λ_f). Clearly, as K increases, the performance of $P_d - P_{fa}$ metric improves for all the presented cases. Also, we can observe that our proposed scheme outperforms the one proposed in [73]. For example, targeting a rate of 0.16, the proposed scheme requires roughly a time window of length 5 while the scheme in [73] requires a time window of length 11. Then, to better understand how these two important metrics (i.e., P_d and P_{fa}) evolve with K, in Fig. 6.21 we show both the system detection probability (P_d) and the system false alarm probability (P_{fa}) versus the time window length (K) against the FC detection threshold (Λ_f). As expected, the larger the time window length K is, the better detection performance. However, increasing K, results in an increase to the P_{fa} metric. Hence, while selecting K, ones have to consider the allowable system false alarm probability.

In Fig. 6.22 and in Fig. 6.23, we show the same (as in Fig. 6.20 and in Fig. 6.21 respectively) but now for (the attacker flipping probability) $P_C^{flip} = 0.2$ (see (6.3.7)). As expected, the $P_d - P_{fa}$ metric improves up to $K = 4$ whereas after that (i.e.,

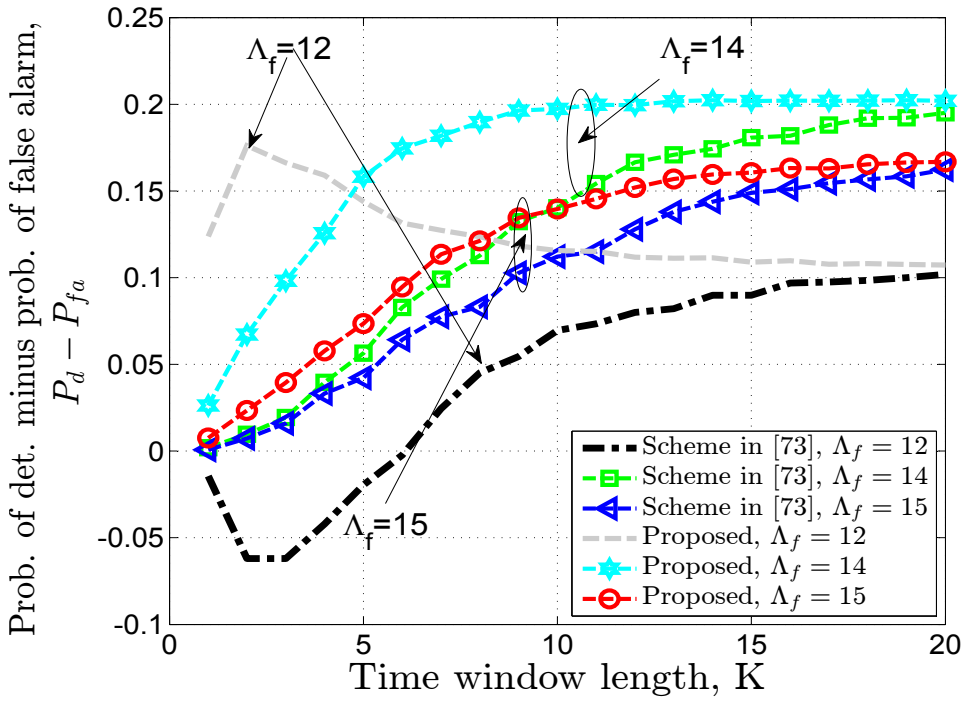

Figure 6.20: The $P_d - P_{fa}$ metric versus the time window length (K) against the FC detection threshold (Λ_f) with $M = 40$, $N = 20$, $\beta = 0.25$, $P_C^{flip} = 1$, $\delta = 0.95$ and $\mu = 0.5$.

for $K \geq 4$) a performance saturation gain is observed. We also note that the time window length (K^*) where this performance saturation gain is observed increases with the attacker flipping probability (P_C^{flip}) (see Fig. 6.20-Fig. 6.23). This is as expected, because increasing the (attacking) flipping probability in one hand would require a larger time window length (K) in the other hand for the FC in order to reduce as much as possible the attacker influence. However, increasing the value of K may introduce a delay to the FC detection algorithm. As a result, a careful choice on K value should be selected in practice. Nevertheless, clearly our proposed algorithm requires a short time window span to converge.

Impact of Reliability Detection Threshold and Weight Penalty Parameter on the System Detection Performance

As previously mentioned, the reliability detection threshold and the weight penalty (i.e., δ and μ) (see (6.3.42)) are the two important parameters that will seriously

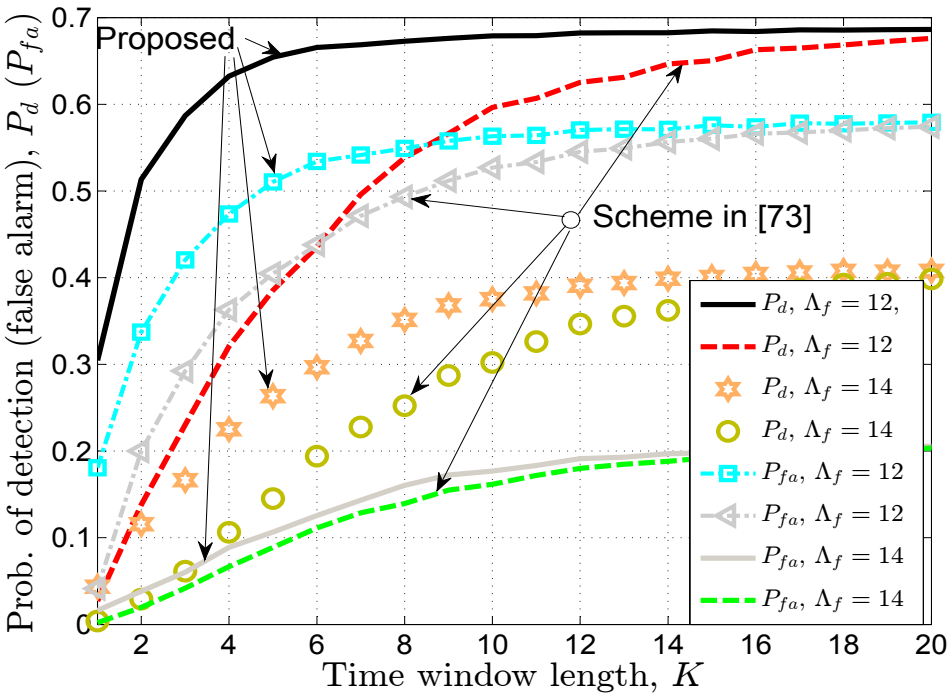

Figure 6.21: Probability of detection (false alarm) P_d (P_{fa}) versus the time window length (K) against the FC detection threshold (Λ_f) with $M = 40$, $N = 20$, $\beta = 0.25$, $P_C^{flip} = 1$, $\delta = 0.95$ and $\mu = 0.5$.

affect the system detection performance at the FC.

Then, in Fig. 6.24 we plot the ROC performance for different choices of the reliability detection threshold (δ) and for a fixed μ in (6.3.42). Obviously, there is an optimum value of δ such that P_d is maximized (for all the P_{fa} values). Also, the detection performance using the weights derived under the $attack - free$ scenario (i.e., $\alpha_i = \alpha_i^{AF}$, see (6.3.35)) in (6.3.10) is also plotted. This corresponds to the case when not any SNs identification scheme is used (i.e., $\mu_i = 0$ in (6.3.42)). Clearly, by appropriately choosing the reliability detection threshold (δ), the proposed identification scheme performance gain is significant compared to that when no identification scheme is used.

Now, in Fig. 6.25 we show the same but now for a fixed reliability detection threshold (δ) and by varying the weight penalty parameter (μ). Clearly, there does exist an optimum value of μ that maximizes the ROC performance. Furthermore, the performance improvement against μ is shown to be significant for $P_{fa} \geq 0.1$.

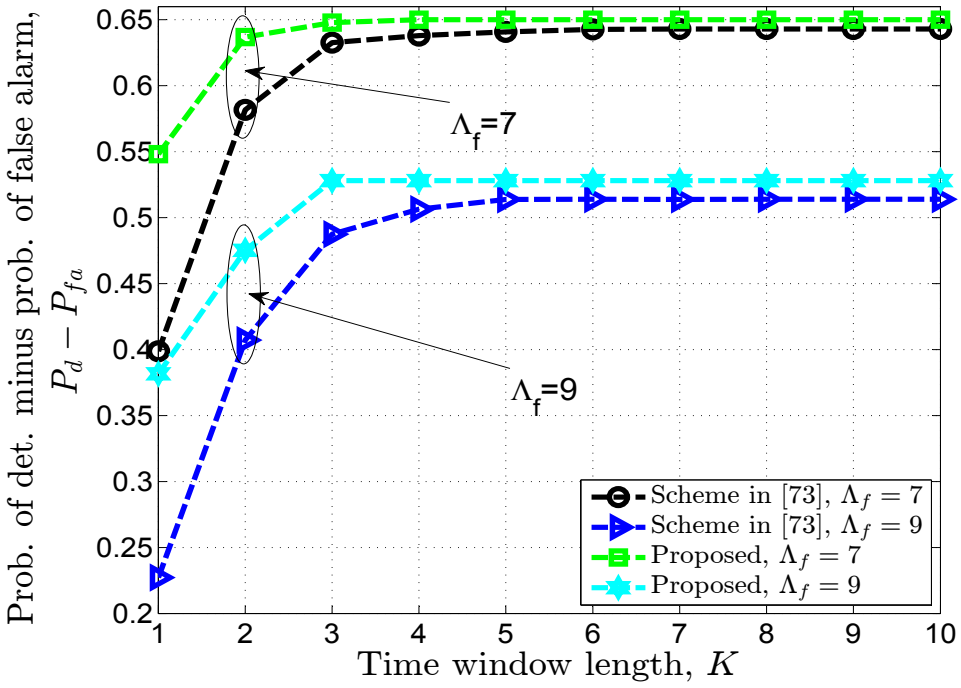

Figure 6.22: The $P_d - P_{fa}$ metric versus the time window length (K) against the FC detection threshold (Λ_f) with $M = 40$, $N = 20$, $\beta = 0.25$, $P_C^{flip} = 0.2$, $\delta = 0.95$ and $\mu = 10$.

Detection Performance Comparison

We now compare the system detection performance of the proposed strategy with the existing schemes.

In Fig. 6.26, selecting some optimum value for δ and μ (more precisely, $\delta = 0.009$ and varying μ), we now compare our proposed strategy with the existing ones such as equal combining scheme, the proposed scheme in [73] and the proposed scheme in [35] (i.e., with $\alpha_i = \alpha_i^{AF}$ in (6.3.10)) derived under attack free scenario. We can observe that the proposed approach performance improves up to $\mu = 10$ whereas after that a performance degradation is noticed. Also, we can observe that by further increasing the time window length K, it is possible to further improve the detection performance. However, a careful selection of K should be made in practice as increasing the value of K introduces a delay to the FC decision making process. Clearly, the proposed scheme attributes a significant detection performance improvement compared to the case where no identification scheme is applied and

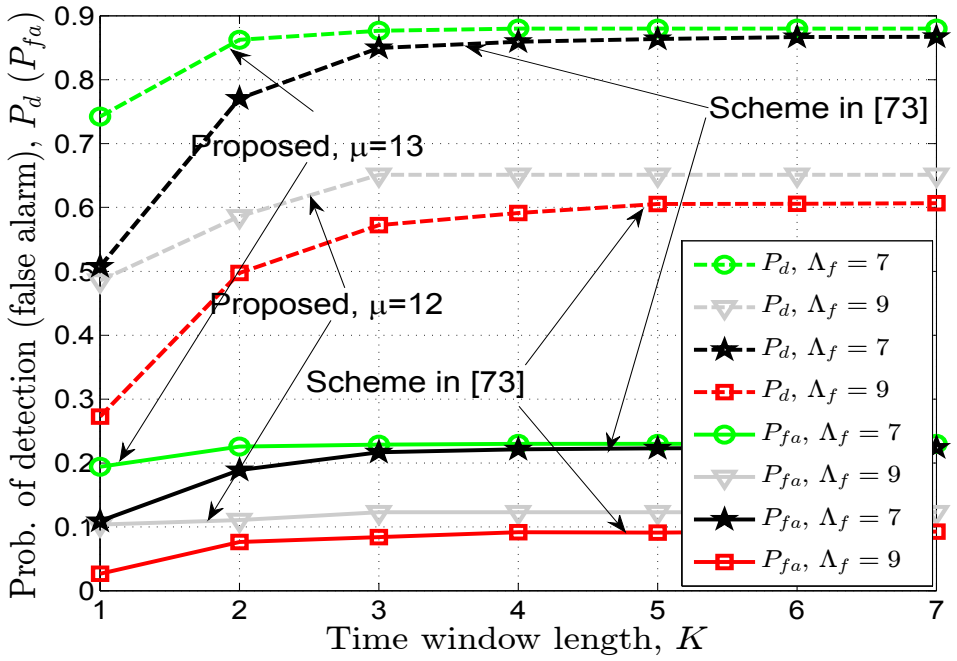

Figure 6.23: Probability of detection (false alarm) P_d (P_{fa}) versus the time window length (K) against the FC detection threshold (Λ_f) with $M = 40$, $N = 20$, $\beta = 0.25$, $P_C^{flip} = 0.2$, and $\delta = 0.95$.

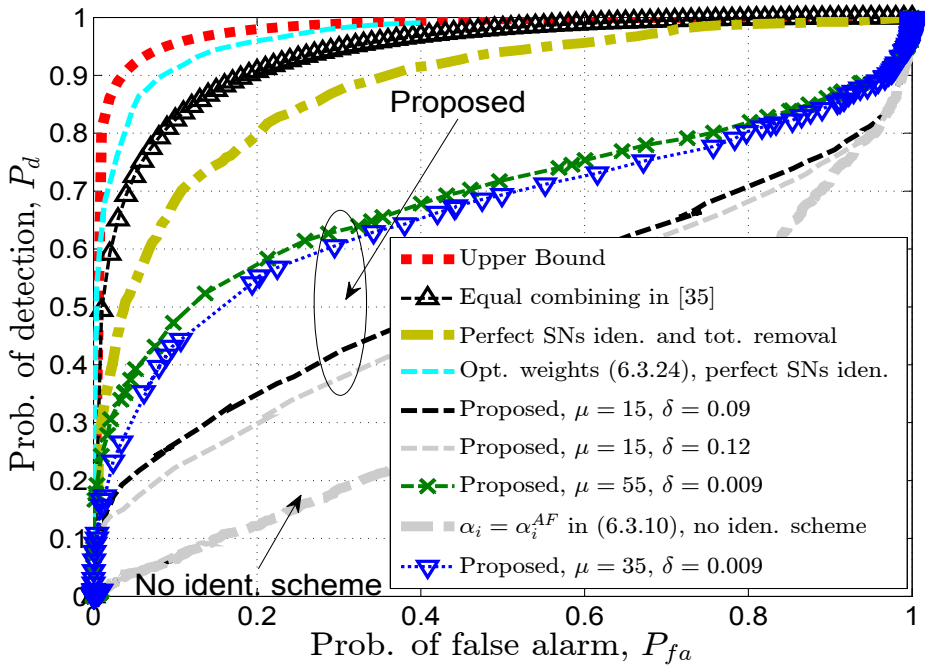

Figure 6.24: Probability of detection (P_d) versus probability of false alarm (P_{fa}) with $M = 40$, $N = 20$, $\beta = 0.5$, $P_C^{flip} = 1$ and $K = 5$.

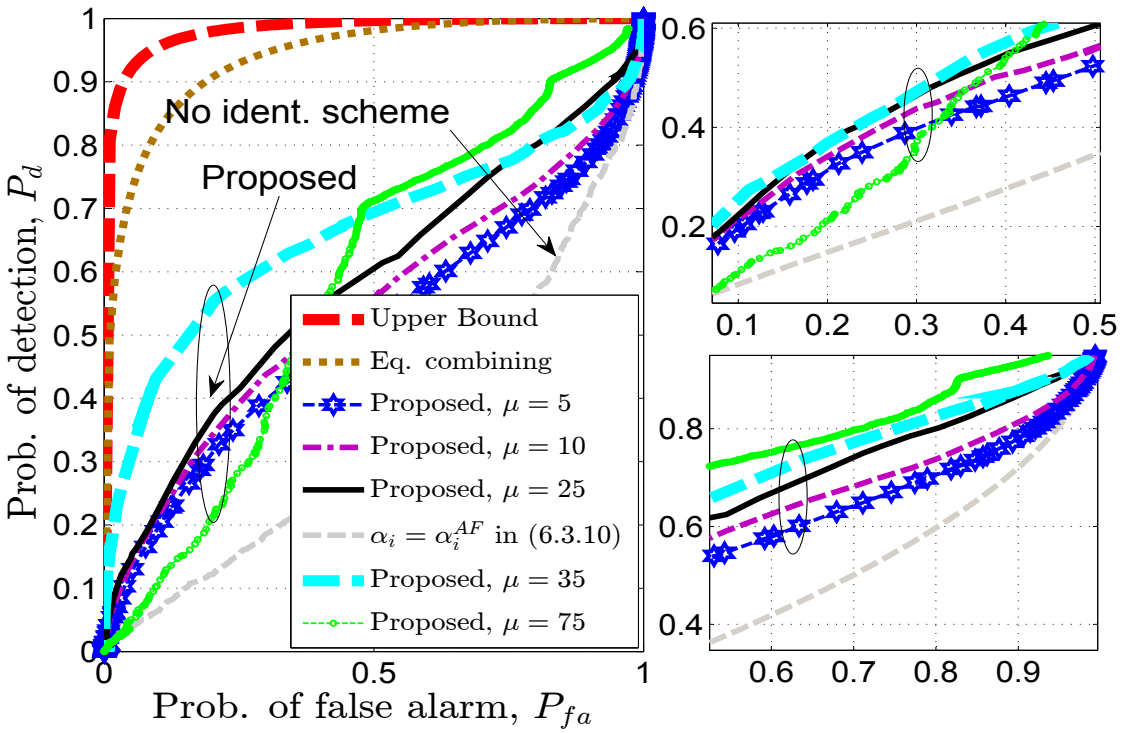

Figure 6.25: Probability of detection (P_d) versus probability of false alarm (P_{fa}) with $M = 40$, $N = 20$, $\beta = 0.5$, $P_C^{flip} = 1$, $K = 5$, and $\delta = 0.009$.

also outperforms the existing strategy [35] and [73] .

In Fig. 6.27, we report the ROC for the two different schemes (i.e., the one derived under attack free scenario and the proposed one in this paper) against the fraction of compromised SNs (β) and flipping probability (P_C^{flip}) parameters. As expected (refer to (6.3.28)), the worst detection performance is observed for the case when $\beta = 0.5$ and $P_C^{flip} = 1$ as this is the case where the attacker causes the maximum possible FC degradation. Clearly, for a fixed β (i.e., $\beta = 0.5$), the detection performance improves as the flipping probability decreases. A significant improvement is observed specially for high probability of false alarm (P_{fa}) values. Now, for low probability of false alarm (P_{fa}) and for e.g., choosing $\beta = 0.25$ and $P_C^{flip} = 0.2$, the proposed scheme significantly outperforms the case when no identification scheme is applied (i.e., $\alpha_i = \alpha_i^{AF}$ in (6.3.10)) while for high P_{fa} its performance approaches the effective upper bound (i.e., when optimum weights in (6.3.24) are used and perfect SNs identification is assumed). Similarly, for e.g., $\beta = 0.25$

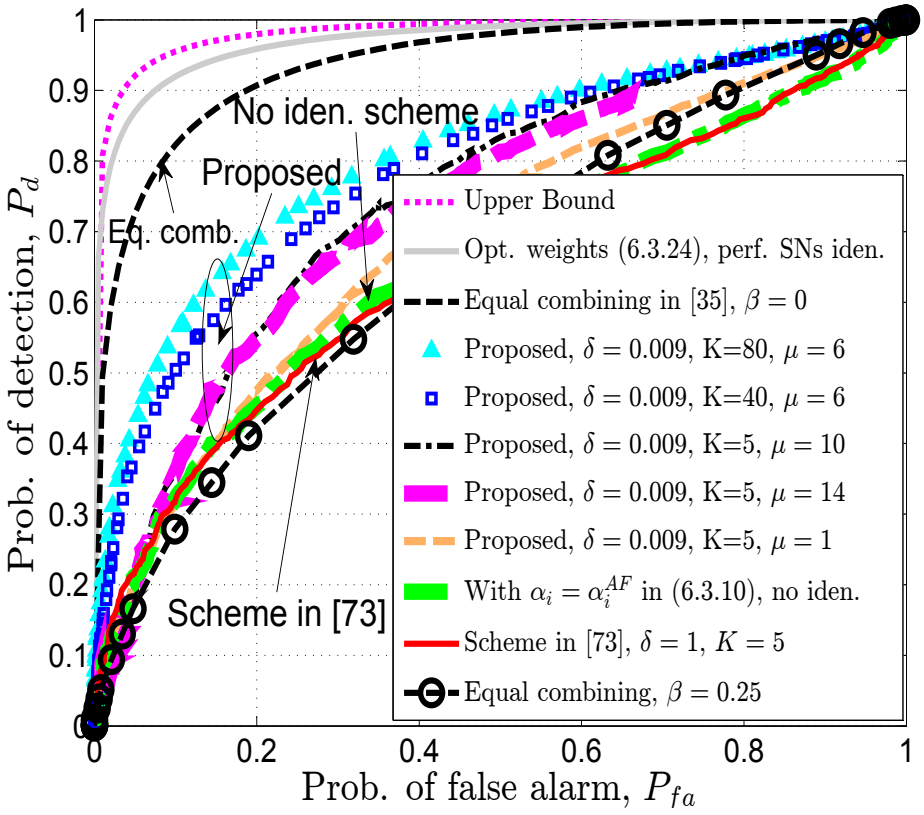

Figure 6.26: Probability of detection (P_d) versus probability of false alarm (P_{fa}) against δ and μ with $M = 40$, $N = 20$, $\beta = 0.25$, and $P_C^{flip} = 1$.

and $\beta = 0.5$ (for (fixed) $P_C^{flip} = 0.8$), the proposed approach possesses a remarkable detection performance gain compared to that of where no identification scheme is applied.

6.4 Chapter Summary and Conclusions

In this chapter, we have addressed the problem of distributed detection by an *under–attack* WSN that operates over limited bandwidth communication fading channels. In section 6.2, based on a simple linear weight combining rule at the FC and adopting the modified deflection coefficient (as an alternative function to be optimized), we give closed-form expressions for the optimal FC combining weights, the SN to FC transmit power allocation, and the test statistics quantization bits. The attacker

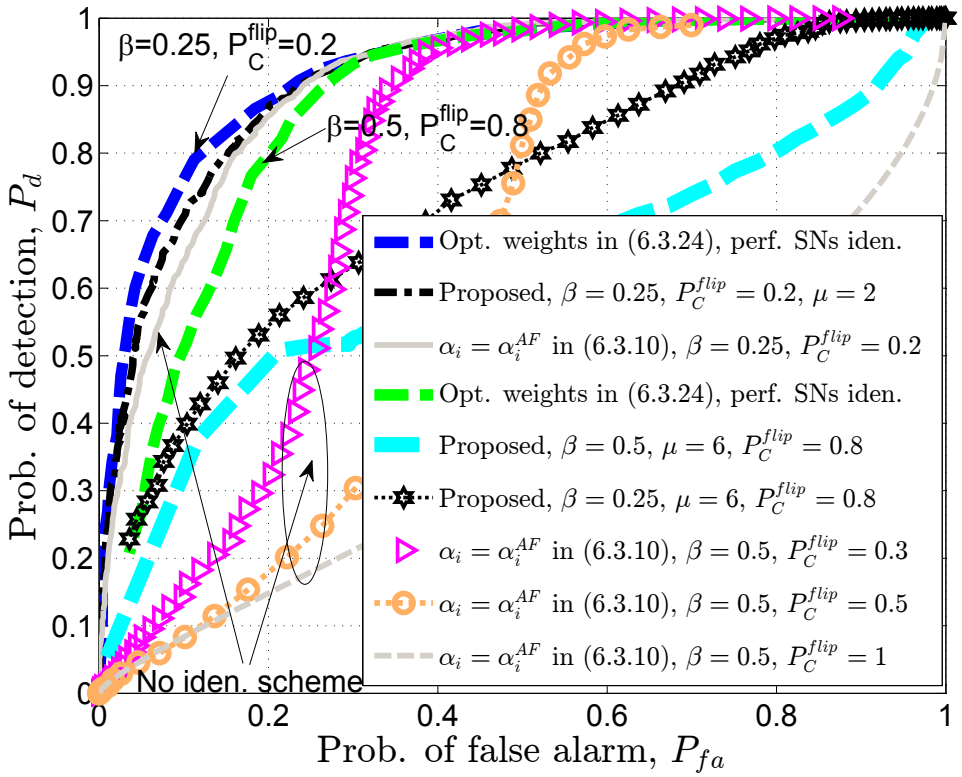

Figure 6.27: Probability of detection (P_d) versus probability of false alarm (P_{fa}) against P_C^{flip} and β with $M = 40$, $N = 20$, $K = 5$, and $\delta = 0.009$.

optimal strategy is also derived and shown to be dependent on the FC combining weights. Furthermore, sub-optimum FC strategies (based on weight combining and the SN transmit power) that do not require the exact knowledge of the attacker strength C are also derived and analyzed. We have also analyzed the equilibrium to the minimax problem and have proved that the Nash Equilibrium (NE) exists and found this optimal solution numerically in the simulation results. We compare our proposed FC strategies with the one derived under an $attack - free$ scenario and show significant detection performance improvement.

In section 6.3, we studied attackers that (unlike in section 6.3) do not know the true state of the target (i.e., they are less dangerous attackers). We have considered some of the key issues related to the under-attack WSNs. We have extended the results presented in our previous work [99] by considering a more realistic scenario where the perfect knowledge of the true hypothesis is not required by the

Attacker. Optimal strategies from the FC's and the Attacker's perspective have also been characterized and some bounds have been derived. We also proposed a novel reputation-based scheme to possibly identify the compromised SNs in the network and control their contributions toward FC's final decision. This new reputation metric is evaluated as the difference between the inconsistency (counted over a time window K) of the i^{th} local SN's decision and a) the FC's decision (where all the SNs contributions are considered [73]) and b) the FC's decision (where the i^{th} SN's contribution is not considered). The proposed approach decreases the weights of the compromised SNs proportionally to this new reputation metric whereas the existing schemes totally exclude the compromised SNs (i.e., a zero-weight is assigned) from the fusion process. Simulation results have shown that the proposed approach significantly outperforms, in terms of detection performance improvement, the existing FC rules and compromised SNs identification schemes.

While this work and the other related publications assume that during the SNs identification stage, the Attacker's parameters (i.e., β and P_C^{flip}) are fixed (i.e., not dynamic), there are interesting questions as to how the dynamic Attacker's parameters will affect the network and how well the existing schemes can isolate the compromised SNs in the network. In this case, the dynamic optimum FC rules and the dynamic Attacker strategies will be of particular useful interest and will be considered and investigated in our future work in order to cope with such dynamic scenarios. Future work will also consider a general (non-linear) optimal combining strategy (unlike in this chapter) at the FC.

Chapter 7

Overview, Conclusions, and Future Work

IN THIS CHAPTER

The work presented in this thesis is summarized. The most important conclusions are presented. Possible extension and future work directions are given in the context of resource allocations and fusion rules, the fully distributed detection approach, and network security.

7.1 Summary

In this thesis, we have considered the problem of detection and estimation in bandwidth-constrained/energy-constrained WSNs. Both, the centralized and the fully decentralized approaches have been considered and network security is also analyzed.

For the centralized approach, we propose a SN transmit power allocation algorithm, SN test statistic quantization bits, and derive various fusion rules. We first start by deriving the optimum fusion rule and then analyze sub-optimum fusion rules that are realizable and easily implemented in practical WSN deployment scenarios. These (sub-optimum) but simple fusion rules do not require $a-priori$ knowledge

about the target or any system's parameter estimation. Clearly, this significantly simplifies the distributed (SNs) detection algorithm and offers an advantage from the perspective of signal processing as the SNs are battery-operated devices. The effect of fading channels on detection performance is minimized by solving the resource allocation problem. There is an optimal SN transmit power and test statistic quantization bits that maximizes the fusion center (FC) detection probability. Furthermore, SNs that have high local SNRs and good channels, transmit more bits. In contrary, the SNs with low SNRs or bad channels are censored (i.e., put in sleeping mode) which further preserves the limited available SNs resources.

For the fully decentralized approach, we develop a fully distributed detection framework that operates over flat fading communication links. We propose a two-step consensus-based approach with weight combining quantized test statistics exchange. We relate the communication topology with the number of bits to be shared among SNs. It turns out that there is an optimum topology that maximizes the detection performance. Furthermore, there is an optimum first step number of iterations (K_1). Choosing carefully the K_1 and Υ parameters, it can be shown that the proposed algorithm converges to the global decision across the network, approaches the centralized detector performance, and requires a finite number of iterations to converge to a global decision. The proposed two-step algorithm requires about 50% less power consumption than the conventional consensus-based existing algorithms.

The problem of centralized detection in the presence of compromised SNs is also investigated. Attacker-based and FC-based parameter optimization are considered and some expressions have been derived. A reputation based scheme to identify the compromised SNs in the network and control their influence to the global FC decision is also proposed. Through simulation results, we have shown that the proposed approach offers a great deal of detection performance improvement and outperforms the existing schemes.

7.2 Conclusions

It has been shown that spatially distributed SNs across the field can offer a reliable operation for event detection applications. The system detection performance and the WSN's operating lifetime can be further improved by means of resource allocations, optimisation and signal processing algorithms. In practical WSN systems, it is important to keep the SNs signal processing complexity as simple as possible. Thus, part of the focus in this thesis was based on deriving and proposing simple but efficient signal processing algorithms.

Another important issue in WSN systems that was addressed in this thesis is the data fusion problem. We have started by deriving the optimal fusion rules (i.e., for $attack-free$ and $under-attack$ WSN scenarios) and have shown that these fusion rules are not implementable in practice and require complex local signal processing. Based on this, we then derive sub-optimum but simple fusion rules (requiring simple hardware) that offer reliable and good detection performance. While the local spatially distributed SNs allow the FC to make a reliable decision, it is possible that one or more SNs deliberately falsify their local observations. The overall detection performance strongly depends on the reliability of these SNs in the network. We have proposed new low-complexity fusion rules to deal with such scenarios that do not require the Attacker's parameters. These blind fusion rules are sub-optimum but are highly desirable from the perspective of complexity and practical deployment. A better but more complex approach is to possibly identify these compromised SNs and control their influence on the FC decision. This approach offers an improved detection performance but requires observing the SN's local reports for a period of time. A larger observation time period (K) may lead to a large detection delay that is critical for most of the event detection applications. Also, the performance of the proposed identification scheme depends strongly on parameters (μ, δ, and Λ_f) , which are the the weight penalty, the reliability detection threshold, and the FC detection threshold respectively. Hence, a careful choice of these parameters should be made in practice.

We have also addressed the fully distributed detection problem and proposed signal processing algorithms for such an approach. In practice, these fully distributed

solutions (i.e., without the FC) are very attractive from both the signal processing perspective as well as from the communication point of view. We have proposed fully distributed two-step quantized fusion rules for energy-constrained/ bandwidth-constrained WSNs and have shown that by carefully choosing the Υ and K_1 (SNR threshold and first step iterations number) parameters, it is possible to achieve the centralized detector performance.

7.3 Future Work

While we have tackled some of the most important issues and challenges in the WSNs, there are still many remaining questions and problems to be solved. We next discuss the future work for the resource allocation and fusion rules, the fully distributed detection approach, and network security.

7.3.1 Resource Allocations and Fusion Rules

While in this work we have considered a simplified but yet very useful sensing model that captures most of the practical issues in a WSN system, future work can consider a more complex sensing model by incorporating say, the target sensing distance into the model. Here, we have implicitly assumed that the target location is known and focused more on the post-sensing signal processing algorithms. The future work can consider the target location estimation error and incorporate this into the system model and fusion rules design.

The power and quantization bits allocation rely on channel state information that was assumed to have been perfectly estimated by the FC. Future work can extend the results provided in this thesis by considering the channel estimation error and investigate the effect on detection performance. Similarly, the Generalized Likelihood Ratio Test (GLRT) based fusion rules can be derived and so compare the results with the fusion rules derived here.

Fully Distributed Detection

In the case of a fully distributed detection approach, there are lot of questions that remain to be answered, such as investigating the current problem in the context of time-varying SNs interaction topologies and the the network security in the presence of compromised SNs.

Network Security

In the network security research domain, there remain a lot of issues and challenges to be considered in future work. While this work has captured and analyzed some very interesting issues, it will be both interesting and important to extend this work to the scenarios where both the FC and the Attacker act strategically. Also, other attacking and defending strategies should be considered and developed such as those where the Attackers collaborate to further degrade the detection performance. It is important to examine the analysis and consideration of the cases where the Attacker does not only flip the local SNs decisions but also controls the local SNs thresholds used to make these decisions. As mentioned above, the security issues in the context of fully distributed algorithms is another direction of future work research that requires long term investigation and research.

Bibliography

[1] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, "Smart objects as building blocks for the Internet of things," in *IEEE Internet Computing*, vol. 14, no. 1, pp. 44-51, Feb. 2010.

[2] B. Sadler, "Fundamentals of energy-constrained sensor network systems," in *IEEE Aerospace and Electronic Systems Magazine*, vol. 20, no. 8, pp. 17–35, Aug. 2005.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," in *IEEE Communication Magazine*, pp. 102–114, August 2002.

[4] G. J. Pottie and W. J. Kaiser, "Wireless integrated network sensors," in *Communications of the ACM*, vol. 43, no. 5, pp. 51-58, May 2000.

[5] B. Warneke, M. Last, B. Liebowitz, and K. S. J. Pister, "Smart dust: communicating with a cubic millimeter computer," *Computer*, vol. 34, no. 1, pp. 44–51, January 2001.

[6] The Libelium company, "Wireless Sensor Networks with Waspmote and Meshlium", *Available at:* http://www.libelium.com/v11-files/documentation/mesh_extreme/wsn-waspmote_and_meshlium_eng.pdf Accessed: 02 February 2014.

[7] M. Hempstead, M. J. Lyons, D. Brooks, and G-Y Wei, "Survey of Hardware Systems for Wireless Sensor Networks," *Journal of Low Power Electronics,* vol. 4, pp. 1–10, 2008.

[8] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," in *ACM Trans. Program. Lang. Syst.,* vol. 4, no. 3, pp. 382-401, Jul. 1982. [Online]. Available at: http://doi.acm.org/10.1145/357172.357176

[9] B. Kailkhura, S. Brahma, and P. K. Varshney, "On the performance analysis of data fusion schemes with Byzantines," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2014.

[10] V. S. S. Nadendla, Y. S. Han, and P. K. Varshney, " Distributed Inference With M-Ary Quantized Data in the Presence of Byzantine Attacks," in *IEEE Transactions on Signal Processing*, vol. 62, no. 10, pp. 2681-2695, May 2014.

[11] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of byzantine attacks," in *IEEE Trans. Signal Process.*, vol. 57, no. 1, pp. 16-29, Oct. 2009.

[12] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine Attack and Defense in Cognitive Radio Networks: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. PP, issue: 99, Apr. 2015.

[13] R. O. Saber, and R.M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," in *IEEE Trans. on Automatic Control*, vol. 49, no. 9, pp. 1520-1533, Sept. 2004.

[14] J. N. Tsitsiklis, "Problems in decision making and computation," Department of Electrical Engineering and Computer Science, MIT, Cambridge, MA, 1984. [Online]. Available at: www.mit.edu/~jnt/Papers/PhD-84-jnt.pdf

[15] J. Tsitsiklis and M. Athans, "Convergence and asymptotic agreement in distributed decision problems," in *IEEE Transactions on Automatic Control,* vol. 29, no. 1, pp. 42-50, Jan. 1984.

[16] W. Zhang, Z. Wang, Y. Guo, H. Liu, Y. Chen, and J. Mitola, "Distributed cooperative spectrum sensing based on weighted average consensus," in *Proc. GLOBECOM*, Houston, Texas, USA, 5-9 Dec. 2011.

[17] L. Xiao and S. Boyd, "Fast linear iteration for distributed averaging," in *Sys. Contr. Lett*, vol. 53, pp. 65-78, 2004.

[18] P. Braca, S. Marano, V. Matta, and P. Willett, "Asymptotic optimality of running consensus in testing binary hypotheses," in *IEEE Trans. Signal Process.,* vol. 58, no. 2, pp. 814-825, Feb. 2010.

[19] R. O. Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," in *Proc. of the IEEE*, 95(1), pp. 215-233, Jan. 2007.

[20] T. Aysal, M.Coates, and M. Rabbat, "Distributed Average Consensus with Dithering Quantization," in *IEEE Trans. Automatic Control*, vol. 56, no. 10, Oct. 2008.

[21] S. Kar and J. M. F. Moura, "Distributed consensus algorithms in sensor networks: quantized data and random link failures," in *IEEE Trans. Automatic Control*, vol. 58, no. 3, pp. 1383-1400, Mar. 2010.

[22] D. Thanou, E. Kokiopoulou, Y. Pu, and P. Frossard, "Distributed average consensus with quantization re-finement," in *IEEE Trans. Signal Process.,* vol. 61, no. 1, pp. 194-205, 2013.

[23] E. Nurellari, D. McLernon, and M. Ghogho "Distributed detection in practical wireless sensor networks via a two step consensus algorithm," in *Proc. Int. conf. on Intelligent Signal Process. (ISP)*, London, United Kingdom, 1-2 Dec. 2015.

[24] E. Nurellari, D. McLernon, and M. Ghogho, "Distributed Two-Step Quantized Fusion Rules via Consensus Algorithm for Distributed Detection in Wireless Sensor Networks," in *IEEE Transactions on Signal and Information Processing over Networks,* vol. 2, no. 3, pp. 321-335, Sept. 2016.

[25] I. D. Schizas, A. Ribeiro, and G. B. Giannakis, "Consensus in Ad Hoc WSNs With Noisy Links—Part I: Distributed Estimation of Deterministic Signal," in *IEEE Trans. on Signal Processing*, vol. 56, no. 1, pp. 350-364, 2008.

[26] I. D. Schizas, G. Mateos, and G. B. Giannakis, "Distributed LMS for consensus-based in-network adaptive processing," in *IEEE Trans. Signal Process.*, vol. 8, no. 6, pp. 2365-2381, Jun. 2009.

[27] J. Zhao, R. Govindan, and D. Estrin, "Computing aggregates for monitoring wireless sensor network," in *Proc. of the First IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 139-148, May 2003.

[28] J. N. Tsitsiklis, "Decentralized detection," in *Advances in Statistical Signal Processing: vol. 2 - Signal Detection,* H. V. Poor, and John B. Thomas, eds., JAI Press, Greenwich, CT, pp. 297-344, Nov. 1993.

[29] R. Niu, B. Chen, and P. K. Varshney, "Fusion of decisions transmitted over Rayleigh fading channels in wireless sensor networks," in *IEEE Trans. Signal Process.,* vol. 54, pp. 1018-1027, Mar. 2006.

[30] J. F. Chamberland and V. V. Veeravalli, "Asymptotic results for decentralized detection in power constrained wireless sensor networks," in *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 6, pp. 1007-1015, Aug. 2004.

[31] A. Ribeiro and G. B. Giannakis, "Bandwidth-constrained distributed estimation for wireless sensor networks, part I: Gaussian case," in *IEEE Trans. Signal Process.,* vol. 54, no. 3, pp. 1131-1143, 2006.

[32] Z. Quan, S.Cui, and A. H. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," in *IEEE J. Sel. Topics in Signal Processing*, vol. 2, no. 1, pp. 28-40, Feb. 2008.

[33] J. Li and G. Alregib, "Rate-constrained distributed estimation in wireless sensor networks," in *IEEE Trans. Signal Process.,* vol. 55, pp. 1634-1643, May 2007.

[34] X. Zhang, H. V. Poor, and M. Chiang, "Optimal power allocation for distributed detection over MIMO channels in wireless sensor networks," in *IEEE Trans. Signal Process.*, vol. 56, no. 9, pp. 4124-4140, Sep. 2008.

[35] E. Nurellari, D. McLernon, M. Ghogho, and S. Aldalahmeh, "Optimal quantization and power allocation for energy-based distributed sensor detection," in *Proc. 22nd European Signal Processing Conference (EUSIPCO)*, Lisbon, Portugal, pp. 141-145, 1-5 Sept. 2014.

[36] E. Nurellari, S. Aldalahmeh, M. Ghogho, and D. McLernon, "Quantized Fusion Rules for Energy-Based Distributed Detection in Wireless Sensor Networks," in *Proc. Sensor Signal Processing for Defence (SSPD)*, Edinburgh, Scotland, pp. 1-5, 8-9 Sept. 2014.

[37] J. J. Xiao and Z. Q. Luo, "Universal Decentralized Detection in a Bandwidth-Constrained Sensor Network," in *IEEE Trans. Signal Process.*, vol. 53, no. 8, pp. 2617-2624, Aug. 2005.

[38] E. Nurellari, D. McLernon, M. Ghogho and S. A. R. Zaidi, "Distributed Optimal Quantization and Power Allocation for Sensor Detection via Consensus," in *IEEE 81st Vehicular Technology Conference (VTC Spring)*, Glasgow, pp. 1-5, 2015.

[39] S. Kar and P. K. Varshney, "A decentralized framework for linear coherent estimation with spatial collaboration," in *Proc. ICASSP*, Florence, Italy, 4-9 May. 2014.

[40] M. Fanaei, M. C. Valenti, A. Jamalipour, and N. A. Schmid, "Optimal power allocation for distributed blue estimation with linear spatial collaboration," in *Proc. ICASSP*, Florence, Italy, 4-9 May 2014.

[41] S. Kar and P. K. Varshney, "Linear coherent estimation with spatial collaboration," in *IEEE Trans. Information Theory*, vol. 59, no. 6, pp. 3532-3553, 2013.

[42] D. Estrin, L. Girod, G. Pottie, and M. Srivastava, "Instrumenting the world with wireless sensor networks," in *Proc. ICASSP*, Salt Lake City, UT, vol. 4, pp. 2033-2036, May 2001.

[43] F. Cattivelli and A. H. Sayed, "Diffusion LMS strategies for distributed estimation," in *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1035-1048, Mar. 2010.

[44] F. Cattivelli and A. H. Sayed, "Distributed Detection Over Adaptive Networks Using Diffusion Adaptation," in *IEEE Trans. Signal Process.*, vol. 59, no. 5, pp. 1917-1932, May 2011.

[45] E. Kantoch, D. Grochala and M. Kajori, "Bio-inspired Topology of Wearable Sensor Fusion for Telemedical Application," in *International Conference on Artificial Intelligence and Soft Computing*, pp. 658-667, May 2017.

[46] S. Barbarossa and G. Scutari, "Distributed Decision Through Self-Synchronizing Sensor Networks in the Presence of Propagation Delays and Asymmetric Channels," in *IEEE Trans. Signal Process.,* vol. 56, no. 4, pp. 1667-1684, Apr. 2008.

[47] A. Bertrand and M. Moonen, "Distributed computation of the Fiedler vector with application to topology inference in ad hoc networks," in *Signal Process.*, vol. 93, no. 5, pp. 1106-1117, May 2013.

[48] A. Bertrand and M. Moonen, "Topology-aware distributed adaption of laplacian weights for in-network averaging," in *Proc. EUSIPCO*, Marrakech, Morocco, 9-13 Sep. 2013.

[49] A. Hassani, A. Bertrand, and M. Moonen, "LCMV beamforming with subspace projection for multi-speaker speech enhancement," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Marrakech, Morocco, pp. 91-95, 20-25 Mar. 2016.

[50] A. Bertrand and M. Moonen, "Distributed computation of the Fiedler vector with application to topology inference in ad hoc networks," in *Signal Processing*, vol. 93, no. 5, pp. 1106-1117, 2013.

[51] P. Di Lorenzo and S. Barbarossa,"Distributed Estimation and Control of Algebraic Connectivity over Random Graphs," in *IEEE Transactions on Signal Processing*, vol. 62, no. 21, pp. 5615-5628, Nov. 2014.

[52] S. Barbarossa, S. Sardellitti, and P. Di Lorenzo, "*Distributed Detection and Estimation in Wireless Sensor Networks*," In Rama Chellappa and Sergios Theodoridis eds., Academic Press Library in Signal Processing, vol. 2, Communications and Radar Signal Processing, pp. 329-408, 2014.

[53] S. Kar and J. M. F. Moura, "Topology for Distributed Inference on Graphs," in *IEEE Trans. Signal Process.,* vol. 56, no. 6, pp. 2609-2613, Jun. 2008.

[54] V. W. Cheng and T. Y. Wang, "Performance Analysis of Distributed Decision Fusion Using A Multilevel Censoring Scheme in Wireless Sensor Networks," in *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1610-1619, May 2012.

[55] C. Asensio-Marco and B. Beferull-Lozano, "Network topology optimization for accelerating consensus algorithms under power constraints," in *Proc. DCOSS*, 16-18 May 2012.

[56] S. Zheng, X. Yang, and C. Lou, "Distributed consensus algorithms for decision fusion based cooperative spectrum sensing in cognitive radio," *Communications and Information Technologies (ISCIT)*, Hangzhou, China, 12-14 Oct. 2011.

[57] R. Blum, S. Kassam, and H. Poor, "Distributed detection with multiple sensors: Part II-advanced topics," in *Proc. IEEE*, vol. 85, no. 1, pp. 64-79, Jan. 1997.

[58] P. K. Varshney, *Distributed Detection and Data Fusion*, 1st edn., Springer, NewYork, 1997.

[59] J. N. Tsitsiklis, "Decentralized detection," in *Advances in Signal Process.*, H. V. Poor and J. B. Thomas, Eds. New York: JAI, 1993, vol. 2, pp. 297-344.

[60] R. Blum, S. Kassam, and H. Poor, "Distributed detection with multiple sensors: Part II-advanced topics," in *Proc. IEEE*, vol. 85, no. 1, pp. 64-79, Jan. 1997.

[61] P. K. Varshney, "*Distributed Detection and Data Fusion*," 1st ed. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 1996.

[62] R. Viswanathan and P. K. Varshney, "Distributed detection with multiple sensors I. Fundamentals," in *Proceedings of the IEEE*, vol. 85, no. 1, pp. 54-63, Jan 1997.

[63] R. Niu and P. K. Varshney, "Decision fusion in a wireless sensor network with a random number of sensors," in *Proceedings. (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 4, pp. iv/861-iv/864, 2005.

[64] Z. Chair and P. K. Varshney, "Optimal data fusion in multiple sensor detection systems," in *IEEE Trans. on Aerospace and Electronics Systems*, vol. AES 22, no. 1, pp. 98-101, 1986.

[65] S. Thomopoulos, R. Viswanathan, and D. Bougoulias, "Optimal decision fusion multiple sensor systems," in *IEEE Trans. on Aerospace and Electronics Systems*, vol. AES 23, no. 5, pp. 644-653, Sep. 1987.

[66] Z. Qin, Q. Li and G. Hsieh, "Defending Against Cooperative Attacks in Cooperative Spectrum Sensing," in *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2680-2687, June 2013.

[67] T. Zhao and Y. Zhao, "A new cooperative detection technique with malicious user suppression," in *Proc. ICC*, Germany, 14-18 Jun. 2009.

[68] A. Vempaty, L. Tong, and P. Varshney,"Distributed Inference with Byzantine Data: State-of-the-Art Review on Data Falsification Attacks," in *Signal Processing Magazine, IEEE*, vol. 30, no. 5, pp. 65-75, 2013.

[69] Y. Cai, Y. Mo, K. Ota, C. Luo, M. Dong, and L. Yang, "Optimal data fusion of collaborative spectrum sensing under attack in cognitive radio networks," in *IEEE Network*, vol. 28, no. 1, pp. 17-23, Jan-Feb. 2014.

[70] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *Proc. ICC*, pp. 3406- 3410, Beijing, China, 19-23 May 2008.

[71] L. Zhang, Q. Wu, G. Ding, S. Feng, and J. Wang, "Performance analysis of probabilistic soft SSDF attack in cooperative spectrum sensing," in *EURASIP J. Adv. Signal Process.*, vol. 2014, no. 1, pp. 81, May 2014.

[72] S. Cui, Z. Han, S. Kar, T. T. Kim, H. Poor, and A. Tajer, "Coordinated data-injection attack and detection in smart grid," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106-115, Sept. 2012.

[73] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," in *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 774-786, Jan. 2011.

[74] A. Vempaty, O. Ozdemir, K. Agrawal, H. Chen, and P. Varshney, "Localization in wireless sensor networks: Byzantines and mitigation techniques," in *IEEE Trans. Signal Process.*, vol. 61, no. 6, pp. 1495-1508, Mar. 2013.

[75] B. Kailkhura, S. Brahma and P. K. Varshney, "Data Falsification Attacks on Consensus-Based Detection Systems," *in IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 1, pp. 145-158, Mar. 2017.

[76] R. Gentz, S. X. Wu, H. T. Wai, A. Scaglione, and A. Leshem, "Data Injection Attacks in Randomized Gossiping," *in IEEE Transactions on Signal and Information Processing over Networks*, vol. 2, no. 4, pp. 523-538, Dec. 2016.

[77] S. Aldalahmeh, M. Ghogho, D. McLernon, and E. Nurellari, "Optimal fusion rule for distributed detection in clustered wireless sensor networks", *EURASIP Journal on Advances in Signal Process.*, 2016:5, Jan. 2016.

[78] S. M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory* , Englewood Cliffs, NJ: Prentice-Hall PTR, 1993.

[79] C. Godsil and G. Royle, *Algebraic Graph Theory*, New York: Springer, 2001.

[80] M. Fiedler, "Algebraic connectivity of graphs", in *Czech. Math. J.,* vol. 23, no. 98, pp. 298-305, 1973.

[81] J. Nash, "Non-cooperative games", in *Annals of Mathematics*, vol. 54, no. 2, pp. 286-295, September 1951.

[82] N. D. Gaubitch, W. B. Kleijn, and R. Heusdens, "Auto-Localization in ad-hoc microphone arrays", in *International Conference on Acoustics, Speech, and Signal Processing, 2013. ICASSP 2013. IEEE International Conference on, May. 2013.*

[83] O. Songhwai, C. Phoebus, M. Michael, M. Srivastava, and S. Shankar, "Instrumenting Wireless Sensor Networks for Real-time Surveillance," in *Proceedings 2006 IEEE International Conference on Robotics and Automation (ICRA 2006), Orlando, FL, pp. 3128-3133,* May 2006.

[84] J. F. Chamberland and V. V. Veeravalli, "Wireless sensors in distributed detection applications," in *IEEE Signal Processing Magazine*, vol. 24, no. 3, pp. 16-25, May 2007.

[85] S. Barbarossa and S. Sardellitti, "Optimal bit and power allocation for rate-constrained decentralized detection and estimation," in *Proc. EUSIPCO 2013.*

[86] J. J. Xiao, S. Cui, Z. Q. Luo, and A. J. Goldsmith, "Power scheduling of universal decentralized estimation in sensor networks," in *IEEE Transactions on Signal Processing*, vol. 54, no.2, pp.413-422, Feb. 2006.

[87] H. R. Ahmadi and A. Vosoughi, "Optimal training and data power allocation in distributed detection with inhomogeneous sensors," in *IEEE Signal Processing Letters*, vol. 20, no.4, April 2013.

[88] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE* , vol. 55, pp. 523–531, Apr. 1967.

[89] R. Niu, P. K. Varshney, "Performance Analysis of Distributed Detection in a Random Sensor Field," in *IEEE Trans. Signal Process.,* vol. 56, no. 1, Jan. 2008.

[90] S.Boyd and L. Vandenberghe, *Convex Optimization,* Cambridge Univ. Press, 2003.

[91] J. F. Chamberland and V. V. Veeravalli, "Wireless sensors in distributed detection applications," in *IEEE Signal Processing Magazine*, vol.24, no.3, pp.16-25, May 2007.

[92] J. F. Chamberland and V. V. Veeravalli, "Decentralized detection in sensor networks," in *Signal Processing, IEEE Transactions on*, vol.51, no.2, pp.407,416, Feb 2003.

[93] J. J, Xiao and Z. Q. Luo, "Universal decentralized detection in a bandwidth-constrained sensor network," in *Signal Processing, IEEE Transactions on*, vol.53, no.8, pp.2617-2624, Aug 2005.

[94] B. Chen, L. Tong, and P. K. Varshney "Channel aware distributed detection in wireless sensor networks," *IEEE Signal Processing Mag*, vol.24, no.4, pp.16-26, July 2006.

[95] V. Saligrama, M. Alanyali and O. Savas, "Distributed Detection in Sensor Networks With Packet Losses and Finite Capacity Links," in *IEEE Transactions on Signal Processing*, vol. 54, no. 11, pp. 4118-4132, Nov. 2006.

[96] R.Jiang and B. Chen, "Fusion of censored decisions in wireless sensor networks," in *IEEE Transactions on Wireless Communications*, vol. 4, no. 6, pp. 2668-2673, Nov. 2005.

[97] E. L. Lawler and D. E. WoodSource, "Branch-And-Bound Methods: A Survey," *Operations Research*, vol. 14, pp. 699-719, no. 4 (Jul. - Aug., 1966).

[98] J. Lofber, "YALMIP : A toolbox for modeling and optimization in MATLAB," in *CACSD, IEEE International Symposium on*, vol.4, pp.284-289, Sept 2004.

[99] E. Nurellari, D. McLernon, M. Ghogho, and S. Aldalahmeh, "Distributed Binary Event Detection Under Data-Falsification and Energy-Bandwidth Limitation," in *IEEE Sensors Journal*, vol. 16, no. 16, pp. 6298- 6309, Aug. 15, 2016.

[100] S. Sardelliti, S. Barbarossa, and A. Swami, "Optimal Topology Control and Power Allocation for Minimum Energy Consumption in Consensus Networks," in *IEEE Trans. Signal Process.,* vol. 60, no. 1, Jan. 2012.

[101] H. Chen , X. Jin, and L. Xie, "Reputation-based Collaborative Spectrum Sensing Algorithm in Cognitive Radio Networks," in *proc. PIRMC*, pp. 582-587, Tokyo, Japan, 13-16 Sep. 2009.

[102] A. Taherpour, M. N. Kenari, and S. Gazor, "Multiple antenna spectrum sensing in cognitive radios," in *IEEE Trans. Wireless Commun.,* vol. 9, no. 2, pp. 814-823, Feb. 2010.

[103] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *Proc. IEEE International Performance Comput. Commun. Conf.,* pp. 208-215, Dec. 2009.

[104] E. Nurellari, D. McLernon, and M. Ghogho, "A Secure Optimum Distributed Detection Scheme in Under-Attack Wireless Sensor Networks," in *IEEE Transactions on Signal and Information Processing over Networks,* vol. , no. , pp. , May 2017.

[105] H. Nikaido and L. Vandenberghe, "On von neumann's minimax theorem," in *Pacific Journal of Mathematics*, vol. 4, no. 1, pp. 65-72, 1954.

[106] R. Horn and C. R. Johnson, "*Matrix Analysis*," Cambridge University Press, 1985.

[107] C.R. Johnson, *Positive definite matrices*, American Mathematical Monthly, vol. 77, issue 3, pp. 259-264, Mar. 1970.

[108] D. L. Kleinman and M. Athans, "The design of suboptimal linear time-varying systems," in *IEEE Trans. Automatic Control*, vol. AC-13, pp. 150-159, Apr. 1968.

[109] C.-Y. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges," in *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247-1256, Aug. 2003.

[110] S. Oh, P. Chen, M. Manzo and S. Sastry, "Instrumenting wireless sensor networks for real-time surveillance," in *Proceedings 2006 IEEE International Conference on Robotics and Automation*, pp. 3128-3133, Orlando, FL, 2006.

[111] M. Xie, J. Hu, S. Guo and A. Y. Zomaya, "Distributed Segment-Based Anomaly Detection With Kullback–Leibler Divergence in Wireless Sensor Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 101-110, Jan. 2017.

[112] R. Niu, P. K. Varshney, "Distributed detection and fusion in a large wireless sensor network of random size," in *EURASIP Journal on Wireless Communication and Networking,* vol. 2005(4), pp. 462-472, 2005.

[113] M. Guerriero, P. Willett and J. Glaz,, "Distributed Target Detection in Sensor Networks Using Scan Statistics," in *IEEE Transactions on Signal Processing,* vol. 57, no. 7, pp. 2629-2639, July 2009.

[114] M. Guerriero, L. Svensson and P. Willett, "Bayesian Data Fusion for Distributed Target Detection in Sensor Networks," in *IEEE Transactions on Signal Processing,* vol. 58, no. 6, pp. 3417-3421, June 2010.

[115] T. Rault, A. Bouabdallaha, Y. Challal and F. Marinb, "A survey of energy-efficient context recognition systems using wearable sensors for healthcare applications," *Pervasive and Mobile Computing*, vol. 37, pp. 23-44, Jun. 2017.

[116] A.A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," in *Computer Networks*, vol. 30(14), pp. 2826-2841, 2007.

[117] A. Thakkar and K. Kotecha, "Cluster Head Election for Energy and Delay Constraint Applications of Wireless Sensor Network," in *IEEE Sensors Journal*, vol. 14, no. 8, pp. 2658-2664, Aug. 2014.

[118] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," in *Ad Hoc Networks*, vol. 3(3), pp. 325-349, 2003.

[119] R. Rajagopalan and P. K. Varshney, "Data-aggregation techniques in sensor networks: A survey," in *IEEE Communications Surveys & Tutorials*, vol. 8, no. 4, pp. 48-63, Fourth Quarter 2006.

[120] M. H. Chaudhary and L. Vandendorpe, "Performance of Power-Constrained Estimation in Hierarchical Wireless Sensor Networks," in *IEEE Transactions on Signal Processing*, vol. 61, no. 3, pp. 724-739, Feb. 2013.

[121] W. A. Zhang, B. Chen and M. Z. Q. Chen, "Hierarchical Fusion Estimation for Clustered Asynchronous Sensor Networks," in *IEEE Transactions on Automatic Control*, vol. 61, no. 10, pp. 3064-3069, Oct. 2016.

[122] Q. Tian and E. J. Coyle, "Optimal Distributed Estimation in Clustered Sensor Networks," in *IEEE International Conference on Acoustics Speech and Signal Processing Proceedings*, pp. IV-IV, Toulouse, 2006.

[123] X. Sun and E. J. Coyle, "Quantization, channel compensation, and optimal energy allocation for estimation in sensor networks," in *ACM Transactions on Sensor Networks (TOSN)*, vol. 8(2), no. 15, pp. 15:1-15:25, Mar. 2012.

[124] G. Ferrari, M. Martalo and R. Pagliari, "Decentralized Detection in Clustered Sensor Networks," in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 47, no. 2, pp. 959-973, Apr. 2011.

[125] M. Martalo and G. Ferrari, "A simple information-theoretic analysis of clustered sensor networks with decentralized detection," in *IEEE Communications Letters*, vol. 14, no. 6, pp. 560-562, Jun. 2010.

[126] G. Ferrari, P. Medagliani, M. Martalo and A. Muzzini, "Zigbee sensor networks with data fusion," in *3rd International Symposium on Communications, Control and Signal Processing*, pp. 472-477, St Julians, 2008.

[127] Q. Tian and E. J. Coyle, "Optimal Distributed Detection in Clustered Wireless Sensor Networks," in *IEEE Transactions on Signal Processing*, vol. 55, no. 7, pp. 3892-3904, July 2007.

[128] D. Stoyan, *Stochastic Geometry and Its Applications*. Wiley, Chichester New York, 1995.

[129] R. Streit, *Poisson Point Processes Imaging, Tracking, and Sensing. Springer*, Springer, New York, 2010.

[130] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," in *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 7, pp. 1029-1046, Sept. 2009.

[131] J. G. Andrews, R. K. Ganti, M. Haenggi, N. Jindal and S. Weber, "A primer on spatial modeling and analysis in wireless networks," in *IEEE Communications Magazine*, vol. 48, no. 11, pp. 156-163, Nov. 2010.

[132] H. ElSawy, E. Hossain and M. Haenggi, "Stochastic Geometry for Modeling, Analysis, and Design of Multi-Tier and Cognitive Cellular Wireless Networks: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 996-1019, Third Quarter 2013.

[133] S. Aldalahmeh, M. Ghogho and A. Swami, "Distributed detection of an unknown target in clustered wireless sensor networks," in *IEEE 12th International Workshop on Signal Processing Advances in Wireless Communications*, pp. 126-130, San Francisco, CA, 2011.

Appendix A

Proofs in Chapter 3

A.1 Derivation of MFD-Optimum Fusion Rule Used in Section 3.6

In the case of MFD, the i^{th} sensor node evaluates

$$T_i = \sum_{n=1}^{N} x_i(n)\, s_i(n)\,,\ \ i = 1, 2, \ldots, M \tag{A.1.1}$$

Quantizing T_i wit L_i bits satisfying (3.3.1) with $\sigma_{v_i}^2$ in (3.3.3), then, it is not difficult to show that

$$\mathbb{E}\left\{\hat{T}_i|\mathcal{H}_0\right\} = \sum_{n=1}^{N} \mathbb{E}\left\{w_i(n)s_i(n)\right\} = 0, \tag{A.1.2}$$

$$\mathbb{E}\left\{\hat{T}_i|\mathcal{H}_1\right\} = \sum_{n=1}^{N} \mathbb{E}\left\{\left(s_i(n) + w_i(n)\right) s_i(n)\right\} = \sum_{n=1}^{N} s_i^2(n), \tag{A.1.3}$$

$$\mathrm{Var}\left\{\hat{T}_i|\mathcal{H}_0\right\} = \sum_{n=1}^{N} \mathrm{Var}\left\{w_i(n)s_i(n)\right\} + \sigma_{v_i}^2 = \sigma_i^2 \sum_{n=1}^{N} s_i^2(n) + \sigma_{v_i}^2 \tag{A.1.4}$$

$$\mathrm{Var}\left\{\hat{T}_i|\mathcal{H}_1\right\} = \sum_{n=1}^{N} \mathrm{Var}\left\{\left(s_i(n) + w_i(n)\right) s_i(n)\right\} + \sigma_{v_i}^2 = \sigma_i^2 \sum_{n=1}^{N} s_i^2(n) + \sigma_{v_i}^2. \tag{A.1.5}$$

The log-likelihood ratio test (LLRT)

$$LLRT\left(\hat{\boldsymbol{T}}\right) = \ln \frac{\mathrm{p}\left\{\hat{T}_1, \hat{T}_2, \cdots, \hat{T}_M|\mathcal{H}_1\right\}}{\mathrm{p}\left\{\hat{T}_1, \hat{T}_2, \cdots, \hat{T}_M|\mathcal{H}_0\right\}} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \gamma_{NP} \tag{A.1.6}$$

where γ_{NP} is the detection threshold, $p\left\{\hat{T}_1, \hat{T}_2, ..., \hat{T}_M|\mathcal{H}_j\right\}$ is the joint probability distribution of quantized local decisions under the j^{th} hypothesis. However, $\hat{T}_i$ has

a χ^2 distribution under $\mathcal{H}_0$ and a non-central χ^2 under $\mathcal{H}_1$, which means evaluation of the LRT in (A.1.6) is complicated. Hence, we evoke the central limit theorem to simplify the distribution of $\hat{T}_i$ when N is sufficiently large and $\sigma_{v_i}^2$ is relatively small. Since the noise at different SNs is independent, each quantized test statistic ($\hat{T}_i$) can be adequately modeled as independent and normally distributed. Then, the following holds:

$$\begin{aligned} LLRT\left(\hat{\boldsymbol{T}}\right) &= \ln \frac{\prod_{i=1}^{M} \mathrm{p}\left\{\hat{T}_i|H_1\right\}}{\prod_{i=1}^{M} \mathrm{p}\left\{\hat{T}_i|H_0\right\}} \\ &= \ln \frac{\prod_{i=1}^{M} \frac{1}{\sqrt{\mathrm{Var}\left\{\hat{T}_i|H_1\right\}}\sqrt{2\pi}} \exp -\frac{\left(\hat{T}_i - \mathrm{E}\left\{\hat{T}_i|H_1\right\}\right)^2}{2\mathrm{Var}\left\{\hat{T}_i|H_1\right\}}}{\prod_{i=1}^{M} \frac{1}{\sqrt{\mathrm{Var}\left\{\hat{T}_i|H_0\right\}}\sqrt{2\pi}} \exp -\frac{\left(\hat{T}_i - \mathrm{E}\left\{\hat{T}_i|H_0\right\}\right)^2}{2\mathrm{Var}\left\{\hat{T}_i|H_0\right\}}}. \end{aligned} \tag{A.1.7}$$

Substituting the quantities in (A.1.2)-(A.1.5) and further rearrangement, we get:

$$\begin{aligned} LLRT\left(\hat{\boldsymbol{T}}\right) &= \ln\left(\prod_{i=1}^{M} \frac{\sqrt{\mathrm{Var}\left\{\hat{T}_i|H_0\right\}}}{\sqrt{\mathrm{Var}\left\{\hat{T}_i|H_1\right\}}}\right) \\ &\quad -\frac{1}{2}\sum_{i=1}^{M}\left(\frac{\left(\hat{T}_i - \mathrm{E}\left\{\hat{T}_i|H_1\right\}\right)^2}{\mathrm{Var}\left\{\hat{T}_i|H_1\right\}} - \frac{\left(\hat{T}_i - \mathrm{E}\left\{\hat{T}_i|H_0\right\}\right)^2}{\mathrm{Var}\left\{\hat{T}_i|H_0\right\}}\right) \\ &= -\frac{1}{2}\sum_{i=1}^{M}\left(\frac{-2\hat{T}_i\sum_{n=1}^{N} s_i^2(n) + \left(\sum_{n=1}^{N} s_i^2(n)\right)^2}{\sigma_i^2\sum_{n=1}^{N} s_i^2(n) + \sigma_{v_i}^2}\right). \end{aligned} \tag{A.1.8}$$

By rearranging the terms and further simplification of (A.1.8), it can be shown that (A.1.6) can be expressed as

$$LLRT\left(\hat{\boldsymbol{T}}\right) = \sum_{i=1}^{M}\left(\frac{\hat{T}_i\sum_{n=1}^{N} s_i^2(n)}{\sigma_i^2\sum_{n=1}^{N} s_i^2(n) + \sigma_{v_i}^2}\right) \lessgtr \gamma'_{NP} \tag{A.1.9}$$

where γ'_{NP} is the detection threshold given as

$$\gamma'_{NP} = \ln\gamma_{NP} + \frac{1}{2}\sum_{i=1}^{M}\left(\frac{\left(\sum_{n=1}^{N} s_i^2(n)\right)^2}{\sigma_i^2\sum_{n=1}^{N} s_i^2(n) + \sigma_{v_i}^2}\right). \tag{A.1.10}$$

Now, let $\alpha_i^{MFD} = \left(\frac{\sum_{n=1}^{N} s_i^2(n)}{\sigma_i^2 \sum_{n=1}^{N} s_i^2(n) + \sigma_{v_i}^2} \right)$, then (A.1.9) can be expressed as

$$T_f \triangleq LLRT\left(\hat{\boldsymbol{T}}\right) = \sum_{i=1}^{M} \alpha_i^{MFD} \hat{T}_i \tag{A.1.11}$$

which is in the form of (3.3.4) but with $\alpha_i = \alpha_i^{MFD}$.

This concludes the proof. ■

Appendix B

Proofs in Chapter 5

B.1 Proof of Proposition 5.3.2

Let $\mathbf{W} \geq 0$ (i.e., a non-negative matrix in which all the elements are equal to or greater than zero) be defined as in (5.3.24) with $0 < \epsilon < 1/\Delta_{max}$ and $\mathbf{\Gamma} \leq 1$ (i.e., a matrix in which all the elements are equal to or less than one). Since we have assumed that the WSN forms a connected graph, then $\mathbf{W}$ is irreducible and also primitive (i.e., the maximum eigenvalue has multiplicity one). So by the Perron Frobenius theorem [106], $\mathbf{W}$ has unique left and right eigenvectors corresponding to the maximum eigenvalue[1] and also $\lim_{k\to\infty} \mathbf{W}^k = \boldsymbol{v}^r(\boldsymbol{v}^l)^T$, where $\boldsymbol{v}^l = \left[v_1^l, v_2^l, \cdots, v_M^l\right]^T$ is the left and $\boldsymbol{v}^r = [v_1^r, v_2^r, \cdots, v_M^r]^T$ is the right eigenvector corresponding to the maximum eigenvalue of $\mathbf{W}$. The problem is now finding these eigenvectors. Consider

$$\mathbf{W}\boldsymbol{v}^r = \boldsymbol{v}^r - \epsilon\mathbf{\Gamma}\mathbf{L}\boldsymbol{v}^r = \boldsymbol{v}^r. \tag{B.1.1}$$

Now, the above relation is equivalent to $\epsilon\mathbf{\Gamma}\mathbf{L}\boldsymbol{v}^r = \mathbf{0}$. It can be easily shown that if $\boldsymbol{v}^r$ is in the right null space of $\mathbf{L}$ (i.e., $\mathbf{L}\boldsymbol{v}^r = \mathbf{0}$), it is also true that $\boldsymbol{v}^r$ is in the right null space of $(\mathbf{\Gamma}\mathbf{L})$. Using this fact and the definition of $\mathbf{L}$ (i.e., symmetric real matrix with rows and columns summing to zero), we can easily show that $\boldsymbol{v}^r = c_r[1, 1, \ldots, 1]^T$ (where c_r is a positive constant (see later)). Similarly, we can

[1] For a connected graph the maximum eigenvalue of $\mathbf{W}$ is unity (i.e., the zero eigenvalue associated to $\mathbf{L}$ has multiplicity one).

find the left eigenvector $(\boldsymbol{v}^l)$ by using the following:

$$(\boldsymbol{v}^l)^T\mathbf{W} = (\boldsymbol{v}^l)^T - \epsilon(\boldsymbol{v}^l)^T\boldsymbol{\Gamma}\mathbf{L} = (\boldsymbol{v}^l)^T. \tag{B.1.2}$$

Again, the above relation can be equivalently expressed as $\epsilon(\boldsymbol{v}^l)^T\boldsymbol{\Gamma}\mathbf{L} = \mathbf{0}$. Using the same analogy (like in the case of right eigenvector) we can also show that $(\boldsymbol{v}^l)^T$ is in the left null space of $\boldsymbol{\Gamma}\mathbf{L}$ if $(\boldsymbol{v}^l)^T\boldsymbol{\Gamma} = c_l[1, 1, \ldots, 1]^T$ (i.e., if $v_i^l = \frac{c_l}{f(\alpha_i)}, \forall i$). Choosing $c_r = 1$ and $c_l = \frac{1}{\sum_{i=1}^{M}\frac{1}{f(\alpha_i)}}$ such that $(\boldsymbol{v}^r)^T\boldsymbol{v}^l = 1$, we can now easily show that:

$$\lim_{k\to\infty}\left(\mathbf{W}^k\mathbf{T}^w[0]\right)_i \quad = \quad \left(\boldsymbol{v}^r(\boldsymbol{v}^l)^T\mathbf{T}^w[0]\right)_i \quad = \quad \frac{\sum_{i=1}^{M}\frac{1}{f(\alpha_i)}T_i^w[0]}{\sum_{i=1}^{M}\frac{1}{f(\alpha_i)}}, \forall i. \tag{B.1.3}$$

This concludes the proof. ■

B.2 Proof of Proposition 5.4.1

Let $\mathbf{W}$ be defined as in (5.3.24) with $0 < \epsilon < 1/\Delta_{max}$, $\boldsymbol{\Gamma} \leq 1$ and $f(\alpha_i) = \frac{1}{\alpha_i}, \forall i$. We complete the main proof as follows: 1) prove that the $(\boldsymbol{\Gamma}\mathbf{L})$ has both real and positive eigenvalues, and then 2) prove that the $\mathbf{W}$ is a positive semi-definite matrix if $\lambda_{max}(\boldsymbol{\Gamma}) \leq \frac{1}{\epsilon\lambda_{max}(\mathbf{L})(M-1)}$, where $\lambda_{max}(\boldsymbol{\Gamma})$ and $\lambda_{max}(\mathbf{L})$ are the maximum eigenvalues associated to $\boldsymbol{\Gamma}$ and $\mathbf{L}$ respectively, and finally 3) derive the upper bound on the "scaled total variance" at each SN.

Sub−proof 1: Consider the matrix multiplication $\boldsymbol{\Gamma}\mathbf{L}$ (which gives a non-symmetric matrix) with $\boldsymbol{\Gamma}$ defined below (5.3.24) and $\mathbf{L}$ defined in section 6.3.2. Note that $\boldsymbol{\Gamma}$ and $\mathbf{L}$ are real diagonal and real symmetric matrices respectively by definition. It is not difficult to show that the eigenvalues of $\boldsymbol{\Gamma}\mathbf{L}$ are the same as the eigenvalues of $\mathbf{K} = \boldsymbol{\Gamma}^{-\frac{1}{2}}(\boldsymbol{\Gamma}\mathbf{L})\boldsymbol{\Gamma}^{\frac{1}{2}}$. Now, $\mathbf{K}$ can be simplified to $\left(\boldsymbol{\Gamma}^{\frac{1}{2}}\mathbf{L}\boldsymbol{\Gamma}^{\frac{1}{2}}\right)$ (a real symmetric positive semi-definite matrix) which implies that the eigenvalues of $\left(\boldsymbol{\Gamma}\mathbf{L}\right)$ are real and positive. This concludes the sub-proof 1. ■

Sub−proof 2: Now, to ensure that $\mathbf{W}$ is positive semi-definite we require $\boldsymbol{z}^T\mathbf{W}\boldsymbol{z} \geq 0$ for $\boldsymbol{z} \neq \mathbf{0}$. Decomposing $\mathbf{W}$ as:

$$2\mathbf{W} = \underbrace{\left(\mathbf{W} + \mathbf{W}^T\right)}_{\text{(symmetric)}} + \underbrace{\left(\mathbf{W} - \mathbf{W}^T\right)}_{\text{(skew-symmetric)}} \tag{B.2.1}$$

then, it can be shown that $\boldsymbol{z}^T\mathbf{W}\boldsymbol{z} \geq 0$ iff $\frac{\boldsymbol{z}^T(\mathbf{W}+\mathbf{W}^T)\boldsymbol{z}}{2} \geq 0$ (since $\frac{\boldsymbol{z}^T(\mathbf{W}-\mathbf{W}^T)\mathbf{z}}{2} = 0$). Now, $0 \leq \frac{\boldsymbol{z}^T(\mathbf{W}+\mathbf{W}^T)\boldsymbol{z}}{2} = \frac{\boldsymbol{z}^T\mathbf{W}\boldsymbol{z}}{2} + \frac{(\boldsymbol{z}^T\mathbf{W}\boldsymbol{z})^T}{2} = \boldsymbol{z}^T\mathbf{W}\boldsymbol{z} \implies \mathbf{W}$ is positive semi-definite iff $\left(\frac{\mathbf{W}+\mathbf{W}^T}{2}\right)$ is so. Now from [107], $\lambda_i\left(\mathbf{W}+\mathbf{W}^T\right) \geq 0, \forall i \implies \boldsymbol{z}^T\mathbf{W}\boldsymbol{z} \geq 0$ and from (5.3.24) we can easily show that: $\lambda_i(\mathbf{W}+\mathbf{W}^T) = 2 - \epsilon\lambda_i\left(\mathbf{\Gamma L} + (\mathbf{\Gamma L})^T\right)$. Now, it is clear that:

$$\lambda_i\left(\mathbf{\Gamma L} + (\mathbf{\Gamma L})^T\right) \leq \frac{2}{\epsilon} \implies \lambda_i\left(\mathbf{W}+\mathbf{W}^T\right) \geq 0$$
$$\implies \lambda_{max}\left(\mathbf{\Gamma L} + (\mathbf{\Gamma L})^T\right) \leq \frac{2}{\epsilon} \implies \lambda_i\left(\mathbf{W}+\mathbf{W}^T\right) \geq 0. \quad \text{(B.2.2)}$$

Using the result in sub-proof 1 and (B.2.2), then:

$$\lambda_{max}\left(\mathbf{\Gamma L} + (\mathbf{\Gamma L})^T\right) \leq 2\sum_{i=1}^{M}\lambda_i\left(\mathbf{\Gamma L}\right) \leq 2\left(M-1\right)\lambda_{max}\left(\mathbf{\Gamma L}\right)$$
$$\text{So, } \lambda_{max}\left(\mathbf{\Gamma L}\right) \leq \frac{1}{\epsilon\left(M-1\right)} \implies \lambda_i\left(\mathbf{W}+\mathbf{W}^T\right) \geq 0. \quad \text{(B.2.3)}$$

Because of the structure of $\mathbf{\Gamma}$ and $\mathbf{L}$, then from [106]:

$$\lambda_{max}\left(\mathbf{\Gamma L}\right) \leq \lambda_{max}\left(\mathbf{\Gamma}\right)\lambda_{max}\left(\mathbf{L}\right) \quad \text{(B.2.4)}$$

and from (B.2.3) and (B.2.4) we can show:

$$\lambda_{max}\left(\mathbf{\Gamma}\right) \leq \frac{1}{\epsilon\lambda_{max}\left(\mathbf{L}\right)\left(M-1\right)} \implies \lambda_i(\mathbf{W}+\mathbf{W}^T) \geq 0 \quad \text{(B.2.5)}$$

and so $\mathbf{W}$ is proved to be positive semi-definite.

Sub − proof 3: In [108], for any two $M \times M$ positive semi-definite matrices $\mathbf{G}$ and $\mathbf{H}$, it was shown that:

$$\lambda_M(\mathbf{G})\text{tr}(\mathbf{H}) \leq \text{tr}(\mathbf{GH}) \leq \lambda_1(\mathbf{G})\text{tr}(\mathbf{H}) \quad \text{(B.2.6)}$$

where $\lambda_i(\mathbf{G})$ is the i^{th} largest eigenvalue of $\mathbf{G}$. Using the condition on $\lambda_{max}\left(\mathbf{\Gamma}\right)$ in (B.2.5) and the bound in (B.2.6) we get:

$$\frac{1}{M-1}\sum_{i=1}^{M}\text{Var}\left\{\bar{T}_i^w[k]\right\} = \frac{1}{M-1}\text{tr}\left((\mathbf{W}^k\text{Cov}(\bar{\mathbf{T}}^{\text{w}}[\text{k}]|\mathcal{H}_{\text{p}})(\mathbf{W}^k)^T\right)$$
$$\leq \frac{1}{M-1}\left(\text{Var}_{\max}\text{tr}\left(\mathbf{W}^k(\mathbf{W}^k)^T\right) + \epsilon^2\sigma_{max}^2\text{tr}\left(\sum_{z=1}^{k}\mathbf{W}^{z-1}(\mathbf{W}^{z-1})^T\right)\right)$$
$$\leq \frac{1}{M-1}\left(\lambda_1(\mathbf{W})\text{Var}_{\max}\text{tr}\left(\mathbf{W}^k\right) + \epsilon^2\sigma_{max}^2\lambda_1(\mathbf{W})\text{tr}\left(\sum_{z=1}^{k}\mathbf{W}^{z-1}\right)\right) \quad \text{(B.2.7)}$$

where tr(.) denotes the trace operator, $\text{Var}_{\max} = \max(\text{Var}\left\{\bar{T}_i^w[k]\right\}, \cdots, \text{Var}\left\{\bar{T}_M^w[k]\right\})$ and $\sigma_{max}^2 = \max(\text{Var}\left\{\psi_1[k]\right\}, \cdots, \text{Var}\left\{\psi_M[k]\right\})$. Now we can show that:

$$\frac{1}{M-1}\left(\lambda_1(\mathbf{W})\text{Var}_{\max}\text{tr}\Big(\mathbf{W}^k\Big) + \epsilon^2\sigma_{max}^2\lambda_1(\mathbf{W})\text{tr}\Big(\sum_{z=1}^{k}\mathbf{W}^{z-1}\Big)\right) \leq \text{Var}_{\max}\left(\frac{1}{M-1} + \lambda_2^k(\mathbf{W})\right) + \epsilon^2\sigma_{max}^2\left(\frac{k}{M-1} + \frac{1-\lambda_2^k(\mathbf{W})}{1-\lambda_2(\mathbf{W})}\right) \tag{B.2.8}$$

where $\lambda_i(\mathbf{W}),$ for $i = 1, 2, \cdots, M$ are the eigenvalues of $\mathbf{W}$ satisfying $\lambda_M \leq \lambda_{M-1} \leq \cdots < \lambda_1 = 1$ and we have used $\text{tr}(\mathbf{W}) = \sum_{i=1}^{M}\lambda_i(\mathbf{W})$ and

$$\sum_{z=1}^{k}\lambda_i^z(\mathbf{W}) = \begin{cases} \dfrac{\lambda_i(\mathbf{W}) - \lambda_i^{k+1}(\mathbf{W})}{1-\lambda_i(\mathbf{W})}, & \text{for } i = 2, 3, \cdots, M \\ k, & \text{for } i = 1. \end{cases} \tag{B.2.9}$$

This concludes the proof. ■

Appendix C

Proofs in Chapter 6

C.1 Proof of $\boldsymbol{\alpha}^T \mathbf{H}_{\tilde{d}^2} \boldsymbol{\alpha} \leq 0, \forall \boldsymbol{\alpha}$ in (6.2.37)

Multiplying (6.2.37) from the left by $\boldsymbol{\alpha}^T$ and from the right by $\boldsymbol{\alpha}$, we get:

$$\boldsymbol{\alpha}^T \mathbf{H}_{\tilde{d}^2} \boldsymbol{\alpha} = 2\frac{\boldsymbol{\alpha}^T \boldsymbol{b}\boldsymbol{b}^T \boldsymbol{\alpha}}{\boldsymbol{\alpha}^T \mathbf{R} \boldsymbol{\alpha}} - 4\frac{\boldsymbol{\alpha}^T \boldsymbol{b}^T \boldsymbol{\alpha}}{\left(\boldsymbol{\alpha}^T \mathbf{R} \boldsymbol{\alpha}\right)^2}\Big(\boldsymbol{b}\boldsymbol{\alpha}^T \mathbf{R} + \mathbf{R}\boldsymbol{\alpha}\boldsymbol{b}^T\Big)\boldsymbol{\alpha} + 8\frac{\boldsymbol{\alpha}^T \left(\boldsymbol{\alpha}^T \boldsymbol{b}\right)^2}{\left(\boldsymbol{\alpha}^T \mathbf{R} \boldsymbol{\alpha}\right)^3}\Big(\mathbf{R}\boldsymbol{\alpha}\boldsymbol{\alpha}^T \mathbf{R}\Big)\boldsymbol{\alpha} - 2\frac{\left(\boldsymbol{\alpha}^T \boldsymbol{\alpha}^T \boldsymbol{b}\right)^2}{\left(\boldsymbol{\alpha}^T \mathbf{R} \boldsymbol{\alpha}\right)^2}\Big(\mathbf{R}\Big)\boldsymbol{\alpha}. \quad \text{(C.1.1)}$$

Rearranging the terms and by further simplification, we obtain:

$$\boldsymbol{\alpha}^T \mathbf{H}_{\tilde{d}^2} \boldsymbol{\alpha} = 2\frac{\boldsymbol{\alpha}^T \boldsymbol{b}\boldsymbol{b}^T \boldsymbol{\alpha}}{\boldsymbol{\alpha}^T \mathbf{R} \boldsymbol{\alpha}} - 8\frac{\boldsymbol{b}^T \boldsymbol{\alpha}\boldsymbol{\alpha}^T \boldsymbol{b}}{\boldsymbol{\alpha}^T \mathbf{R} \boldsymbol{\alpha}} + 8\frac{\boldsymbol{b}^T \boldsymbol{\alpha}\boldsymbol{\alpha}^T \boldsymbol{b}}{\boldsymbol{\alpha}^T \mathbf{R} \boldsymbol{\alpha}} - 2\frac{\boldsymbol{\alpha}^T \boldsymbol{b}\boldsymbol{b}^T \boldsymbol{\alpha}}{\boldsymbol{\alpha}^T \mathbf{R} \boldsymbol{\alpha}} = 0. \quad \text{(C.1.2)}$$

This concludes the proof. ■

C.2 Proof of Lemma 6.3.1

Clearly, for the i^{th} honest SN, the $\tilde{I}_i$ in (6.3.7) is a Bernoulli random variable characterized by the detection probability (p_d^i) in (6.3.3) if the target is present and false alarm probability (p_{fa}^i) in (6.3.2) if the target is absent.

Similarly, for the i^{th} compromised SN, the $\tilde{I}_i$ in (6.3.7) is a Bernoulli random variable characterized by the detection probability ($p_d^{i,C}$) in (6.3.6) if the target is present and false alarm probability ($p_{fa}^{i,C}$) in (6.3.5) if the target is absent.

The probability mass function (pmf) f of this distribution (for the i^{th} compromised SN), over possible outcomes $\left\{\tilde{I}_i = 1|\mathcal{H}_0\right\}$ and $\left\{\tilde{I}_i = 0|\mathcal{H}_0\right\}$, is given as

$$f\left(\tilde{I}_i|\mathcal{H}_0; p_{fa}^{i,C}\right) = \begin{cases} p_{fa}^{i,C}, & \text{if } \tilde{\mathrm{I}}_{\mathrm{i}} = 1|\mathcal{H}_0 \\ 1 - p_{fa}^{i,C}, & \text{if } \tilde{\mathrm{I}}_{\mathrm{i}} = 0|\mathcal{H}_0 \end{cases} \qquad \text{if } P_C^{flip} = 0 \tag{C.2.3}$$

Now, if the i^{th} compromised SN flips its local decision with probability $P_C^{flip} > 0$, then:

$$\text{for } \tilde{I}_i = 1|\mathcal{H}_0 \implies \begin{cases} \tilde{I}_i = 1|\mathcal{H}_0, & \text{with probability } \left(1 - P_C^{flip}\right) \\ \tilde{I}_i = 0|\mathcal{H}_0, & \text{with probability } P_C^{flip} \end{cases} \tag{C.2.4}$$

$$\text{for } \tilde{I}_i = 0|\mathcal{H}_0 \implies \begin{cases} \tilde{I}_i = 0|\mathcal{H}_0, & \text{with probability } \left(1 - P_C^{flip}\right) \\ \tilde{I}_i = 1|\mathcal{H}_0, & \text{with probability } P_C^{flip} \end{cases} \tag{C.2.5}$$

Now, from (C.2.3), (C.2.4), and (C.2.5) we can easily show that $\tilde{p}_{fa}^{i} = P_C^{flip}\left(1 - p_{fa}^{i,C}\right) + \left(1 - P_C^{flip}\right) p_{fa}^{i,C}$ and the pmf can be written as

$$f\left(\tilde{I}_i|\mathcal{H}_0; \tilde{p}_{fa}^{i}\right) = \begin{cases} \tilde{p}_{fa}^{i}, & \text{if } \tilde{\mathrm{I}}_{\mathrm{i}} = 1|\mathcal{H}_0 \\ 1 - \tilde{p}_{fa}^{i}, & \text{if } \tilde{\mathrm{I}}_{\mathrm{i}} = 0|\mathcal{H}_0 \end{cases} \tag{C.2.6}$$

In similar manner, we can show that $\tilde{p}_{d}^{i} = P_C^{flip}\left(1 - p_{d}^{i,C}\right) + \left(1 - P_C^{flip}\right) p_{d}^{i,C}$ and the pmf over possible outcomes $\left\{\tilde{I}_i = 1|\mathcal{H}_1\right\}$ and $\left\{\tilde{I}_i = 0|\mathcal{H}_1\right\}$, is given as

$$f\left(\tilde{I}_i|\mathcal{H}_1; \tilde{p}_{d}^{i}\right) = \begin{cases} \tilde{p}_{d}^{i}, & \text{if } \tilde{\mathrm{I}}_{\mathrm{i}} = 1|\mathcal{H}_1 \\ 1 - \tilde{p}_{d}^{i}, & \text{if } \tilde{\mathrm{I}}_{\mathrm{i}} = 0|\mathcal{H}_1 \end{cases} \tag{C.2.7}$$

This concludes the proof. ■

Appendix D

Distributed Detection in Clustered Wireless Sensor Networks

D.1 Introduction

We consider distributed detection[1] in a clustered WSN deployed randomly in a large field for the purpose of intrusion detection. The WSN is modeled by a homogeneous Poisson point process. The sensor nodes (SNs) compute local decisions about the intruder's presence and send them to the cluster heads (CHs). A stochastic geometry framework is employed to derive the optimal cluster-based fusion rule (OCR), which is a weighted average of the local decisions sum of each cluster. Interestingly, this structure reduces the effect of false alarm on the detection performance. Moreover, a generalized likelihood ratio test (GLRT) for cluster-based fusion (GCR) is developed to handle the case of unknown intruder's parameters. Simulation results show that the OCR performance is close to the Chair-Varshney rule. In fact, the latter benchmark can be reached by forming more clusters in the network without increasing the SNs deployment intensity. Simulation results also show that the GCR performs very closely to the OCR when the number of clusters is large enough. The performance is further improved when the SN deployment intensity is increased.

[1]The Acronyms and mathematical symbols used throughout this Appendix are different from previous Chapters and hence are defined here and only valid for this Section.

D.2 Related Work

WSN consists of a large number of geographically distributed low-cost sensor nodes (SNs) forming a network via wireless links. This structure enabled the instrumentation of WSNs in many applications [109]. Detecting an intruder in a monitored region of interest (ROI) is one of the most important applications of WSNs [110,111]. The SNs monitor the ROI to detect abnormal phenomena, which might take the form of temperature, electromagnetic or acoustic disturbances. Such physical signals are usually localized in space, i.e., the signal's power attenuates with the distance between the source and the sensor. The SNs sample the physical signal and then wirelessly communicate their data to a remote fusion center (FC), where the final decision about any intrusion is made. Due to bandwidth and power constraints, the data is often compressed to a single bit representing the local decision of the SN. When the ROI is very large, the WSN is divided into clusters to manage the large number of SNs needed to provide adequate coverage. In each cluster, the SNs send data to a cluster head (CH), which subsequently reports to the FC.

There is a large body of literature studying the problem of distributed detection and decision fusion for a single fusion center network configuration [57,58,62]. Chair and Varshney derived the optimum fusion rule in [64], which requires knowledge of local detection and false alarm probabilities for each SN. Niu and Varshney relaxed the latter requirement leading to the suboptimal counting rule (CR) [112]. The performance of the CR was investigated in [89]. However, the CR suffers from the problem of spurious detection in large WSN. This problem was tackled by using the scan statistic (SS) detector in [113] and [114]. In SS, a moving FC travels across the ROI and scans the SNs. This can be interpreted as sliding a window across the ROI, summing the number of positive local decisions, and continuously testing against a threshold. However, the SS rule is sequential in nature and hence incurs communication and delay penalties. A survey on the context of energy-efficient systems in wearable sensors that allow monitoring a user and its environment is given in [115].

For a cluster-based WSN on the other hand, clustering algorithms for WSN [116] have been extensively studied in various contexts such as energy management [117]

and routing [118]. Clustering and data aggregation in WSNs have been surveyed in [119]. Power-constrained distributed estimation in WSNs was addressed in [120] where network communication was based on the amplify-and-forward scheme. A sequential measurement fusion method is presented to design local estimators for clustered asynchronous sensor networks in [121]. Quantized sensor observations were used in [122, 123] for distributed estimation in a clustered multi-hop WSN.

Decentralized detection in multi-level clustered WSNs has been considered in [124]. Each level of CHs uses a majority-like fusion rule to fuse the data from the level beneath it. The results in [124] (surprisingly) show that clustering decreases the detection performance. The effect of uniform and nonuniform clustering work was studied in [125]. In [126], the authors studied the performance of data fusion in a clustered Zigbee WSN implementation of [124]. The effect of communication errors on distributed detection in multi-hop clustered WSN was considered in [127] where it was shown that the optimal fusion rule is a weighted order statistic filter.

In this Appendix we adopt the network configuration in [112] in which a vast WSN is divided into geographical regions managed by CHs. However, we assume that within each CH, the SNs send a single bit, representing their local decision, to the CH due to bandwidth and power constraints. The CHs then send the sums of the local decisions to the FC where the ultimate detection decision is made. Using a stochastic geometry framework [128, 129], we derive the optimal cluster-based fusion rule (OCR). In contrast to [124], we show that clustering significantly improves the detection performance. In fact, the OCR is shown to have a performance very close to that of the optimal Chair-Varshney fusion rule (CVR) while it does not require the knowledge of the exact SNs locations unlike the CVR. Moreover, using stochastic geometry, we develop a Generalized Likelihood Ratio Test (GLRT) for the clustered-based fusion rule to handle the case of unknown intruder's parameters.

This Appendix is organized as follows. Section D.3 presents models for the intruder, sensing, and communication. In Section D.4, fusion rules for a single fusion point network are reviewed. The optimal fusion rule is presented in Section D.5, which also contains the GLRT development. In Section D.6 the simulation results are presented. Finally, conclusions are given in Section D.7.

D.3 System Model

In this section we present the models for sensing, the sensor network, and communication in the WSN. In addition, a stochastic geometry model is presented for the WSN.

D.3.1 Sensing and Sensor Network Model

Consider a WSN deployed in a certain area, $\mathcal{A} \subset \mathbb{R}^2$ where $\mathcal{A}$ is assumed to be significantly large. The SNs are randomly dispersed in $\mathcal{A}$ according to a uniform distribution, i.e. the coordinate of the ith SN, $\mathbf{x}_i = (x_i, y_i)^T$, is a uniform random variable (RV) in $\mathcal{A}$. Also, the number of the SNs, N, is assumed to be a RV. The random characteristic of N can be justified by SN failure or battery exhaustion.

The WSN is tasked with the detection of any intruder entering the ROI. An intruder at location $\mathbf{x}_0 \in \mathcal{A}$ leaves a signature signal sensed by the SNs. Similar to [112, 114] this signature is assumed to decay with distance according to a power law. Thus the intruder's parameters are given in the vector $\boldsymbol{\theta} = [P_0, \mathbf{x}_0]^T$, where P_0 is the intruder's signal power. The noise-free signal received at the ith SN has the following form:

$$a(\mathbf{x}_i) = \frac{\sqrt{P_0}}{\max(d_0, d_i)} \tag{D.3.1}$$

where d_0 is the reference distance to the node's sensor and $d_i = \|\mathbf{x}_0 - \mathbf{x}_i\|$ is the Euclidean distance between the intruder and the ith SN. Note that the measured signal is saturated if the distance to the target is smaller than d_0. The above model can adequately describe acoustic or electromagnetic signals.

Each SN samples the environment to decide whether an intruder is present. The collected data at the ith SN under the null and alternative hypotheses, $\mathcal{H}_0$ and $\mathcal{H}_1$ respectively, takes the following form:

$$\mathcal{H}_1 : s(\mathbf{x}_i) = a(\mathbf{x}_i) + n(\mathbf{x}_i) \tag{D.3.2}$$

$$\mathcal{H}_0 : s(\mathbf{x}_i) = n(\mathbf{x}_i) \tag{D.3.3}$$

where $n(\mathbf{x}_i)$ is a white Gaussian noise at the SN located at $\mathbf{x}_i$ with zero mean and variance σ_s^2. The noise is assumed to be identically and independently distributed

over all the SNs. The sensing SNR is defined as

$$\text{SNR}_s = \frac{P_0}{\sigma_s^2}. \tag{D.3.4}$$

Each SN computes its binary local decision, $I(\mathbf{x}_i) = \{0, 1\}$, by comparing the collected data with a local decision threshold τ, i.e.,

$$I(\mathbf{x}_i) = \begin{cases} 1, & s(\mathbf{x}_i) \geq \tau \\ 0, & s(\mathbf{x}_i) < \tau \end{cases}. \tag{D.3.5}$$

Here, τ is the same for all SNs. Therefore, the local probabilities of detection and false alarm are given by

$$P_d(\mathbf{x}_i) = Q\left(\frac{\tau - a(\mathbf{x}_i)}{\sigma_s}\right) \tag{D.3.6}$$

$$P_{fa} = Q\left(\frac{\tau}{\sigma_s}\right) \tag{D.3.7}$$

where $Q(\cdot)$ is the Gaussian Q-function given by

$$Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt. \tag{D.3.8}$$

Note, however, that the probability of detection in (D.3.6) depends on the target parameters, P_0 and $\mathbf{x}_0$ through eq. (D.3.1).

D.3.2 Stochastic Geometry Model

The WSN defined above can be elegantly modeled using stochastic geometry [128], which has recently attracted interest in the modeling of wireless networks [130, 131] and cognitive radios [132].

We model the spatial distribution of the SNs as a Poisson Point Process (PPP) $\Phi = \{\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_N\}$ in $\mathcal{A}$. This implies that the $\mathbf{x}_i$'s $\in \Phi$ are uniform RVs and their number $N = |\Phi|$ is a Poisson RV, i.e., $N \sim \text{Pois}(\lambda|\mathcal{A}|)$, where λ is the average number of points (SNs) in a unit area (deployment intensity) and $|\mathcal{A}|$ is the area of $\mathcal{A}$. Φ is assumed to be simple (no two points occupy the same location) and stationary in space, i.e., its statistical properties do not change if Φ is shifted. A PPP is called homogeneous if the intensity, λ, is independent of the location $\mathbf{x}$. Otherwise it is called inhomogeneous.

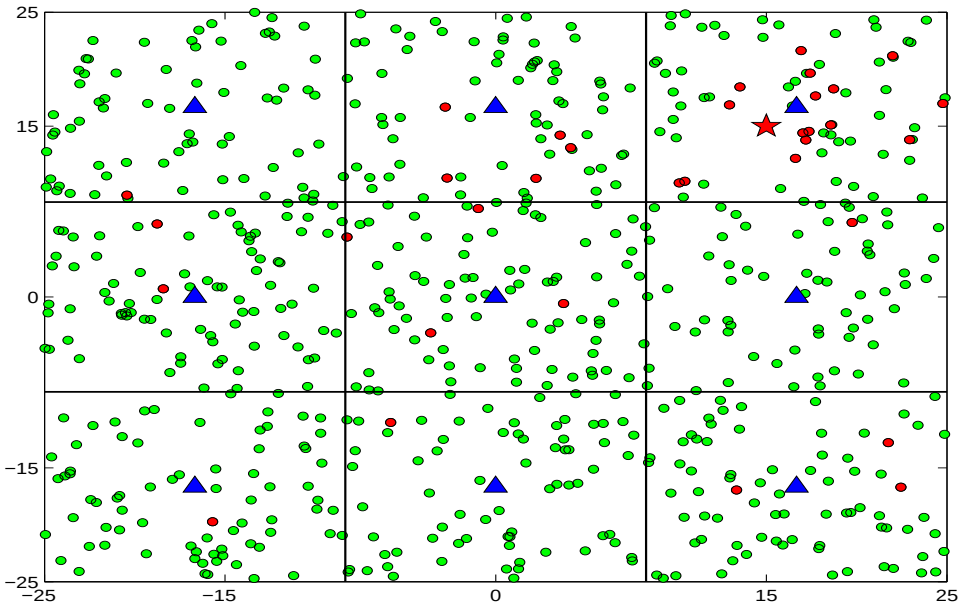

Figure D.1: Poisson field of sensor nodes. Pentagram: intruder, green circle: SN; red circle: detecting SN; blue triangle: CH. The system parameters are $\lambda = 0.3$, $P_0 = 50$, $d_0 = 1$, $\sigma_s^2 = 1$, $P_{fa} = 10^{-2}$, and $\mathbf{x}_0 = (15, 15)^T$.

The thinning of a PPP is the process of removing points from the original PPP that do not adhere to some rule, and hence a point is removed from the PPP with some probability. Thinning can be independent (p-thinning), i.e., the thinning probability does not depend on the location of the point under consideration, or it can be dependent, i.e., the thinning probability depends on the point's location.

Thinning is used here to model the local detection operation. If Φ is thinned to produce Φ_d, the PPP of detecting SNs:

$$\Phi_d = \{\mathbf{x}_i \in \Phi : I(\mathbf{x}_i) = 1\} \tag{D.3.9}$$

The properties of Φ_d are used to derive the optimal fusion rule as given in Section D.5.

D.3.3 Communication Model

Due to vastness of the ROI the WSN is geographically divided into M disjoint zones; $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_M$, where $\mathcal{C}_m \in \mathcal{A}$ for $m = 1, \cdots, M$. Each zone is managed by a CH located at $\mathbf{x}_m \notin \Phi$. The number of clusters is fixed and their locations are also fixed

and known to the WSN. SNs located at $\mathbf{x}_i \in \mathcal{C}_m$ send their decisions to the mth CH. The CHs in turn report back to the FC.

Due to cost and bandwidth constraints, SNs use on-off keying (OOK) to transmit their binary local decisions to the CH. Only the SNs making positive local decisions report to the CHs. These SNs are assumed to be synchronized to the same time slot. Furthermore, a power control strategy is assumed to be used at the SNs in order to ensure that the powers of the signals received from the SNs at the CH are all equal to the same desired value. This power level is chosen such that the effect of the channel noise is negligible.

Each CH then communicates with the FC over wireless channel that is less restricted in bandwidth. Moreover, the CH encodes its data for protection against errors. This is justified by the argument that the network has only $M \ll N$ CHs, and so it can afford having more sophistication in the CHs.

D.4 Fusion Rules for Single Cluster WSNs

In this section we review fusion rules for distributed detection in a cluster WSN.

In this configuration, all SNs in the network report to a single CH that acts as the FC. The optimal hard decision fusion rule in this case is CVR, which is given by [64]

$$\begin{aligned}\Lambda_{\text{CVR}} = &\sum_{i=1}^{N} I(\mathbf{x}_i) \log\left(\frac{P_d(\mathbf{x}_i)}{P_{fa}}\right) \\ &+ (1 - I(\mathbf{x}_i)) \log\left(\frac{1 - P_d(\mathbf{x}_i)}{1 - P_{fa}}\right).\end{aligned} \tag{D.4.10}$$

This rule requires the complete knowledge of the intruder's parameters in addition to both the number of SNs and their locations. Such conditions are difficult to attain in large WSNs.

Relaxing the above conditions, Niu and Varshney proposed the following suboptimal Counting Rule [112]:

$$\Lambda_{\text{CR}} = \sum_{i=1}^{N} I(\mathbf{x}_i). \tag{D.4.11}$$

As can be seen in (D.4.11), the CR does not require any information about the target or the SNs locations.

However, for a large ROI the problem of spurious detection becomes more prevalent as shown in Figure D.1. The intruder is located in the north-east cluster, in which the number of detecting SNs is relatively large. Whereas the number of detecting SNs in the south-west cluster is small. These positive decisions are mainly due to the sensing noise. This problem was tackled by using the scan statistic (SS) detector proposed in [113]. The SS test statistic is given by

$$\Lambda_{\text{SS}} = \max_{i} \left(\frac{\lambda_1^{SS}}{\lambda_0^{SS}} \right)^{Z_i}, \quad i = 1, \cdots, L \tag{D.4.12}$$

where L is the number of sliding window iterations, Z_i is the number of positive decisions in the ith *window slide iteration*, and λ_0^{SS} and λ_1^{SS} are the mean number of detecting SNs in a typical window under the $\mathcal{H}_0$ and $\mathcal{H}_1$ hypotheses respectively. The Bayesian form of the SS is given by [114]

$$\Lambda_{\text{B-SS}} = \sum_{i=1}^{L} \left(\frac{\lambda_1^{SS}}{\lambda_0^{SS}} \right)^{Z_i}. \tag{D.4.13}$$

The SS was shown to outperform the CR for the case where the WSN has a high node intensity [114].

D.5 Fusion Rules in Clustered WSNs

In this section we present the fusions rules for clustered WSNs in the CH and FC levels. For the purpose of motivation, the majority-like fusion rule [124] is presented first. Then we propose the optimal clustered-based fusion rule followed by the GLRT development.

D.5.1 Decision Fusion in the Cluster Heads

SNs with positive decisions send their local decision to the related CH, which acts as a fusion point for SNs in the cluster as shown in Figure D.2. The fusion rule adopted in each cluster is the CR. In addition to its simplicity, this handles the situation in which information on the SNs is lacking, which is the case in random networks.

Accordingly, the fused data from the mth cluster, Λ_m, takes the following form;

$$\Lambda_m = \sum_{\mathbf{x}_i \in \mathcal{C}_m} I(\mathbf{x}_i). \tag{D.5.14}$$

D.5.2 Majority-like Fusion Rule

We consider the majority-like fusion rule (MFR) with a two-level network, i.e., one level of CHs reporting to a FC, which is the second level. The mth CH uses a majority-like rule to produce the CH's decisions $\tilde{I}_m$ as follows;

$$\tilde{I}_m = \begin{cases} 1, & \Lambda_m \geq k_1 \\ 0, & \Lambda_m < k_1 \end{cases} \tag{D.5.15}$$

where $k_1 = \lceil |\Phi_m|/2 \rceil + 1$ is the first level majority rule threshold and $|\Phi_m|$ is the number of SNs in the mth cluster. The $\tilde{I}_m$'s can be thought of as the one-bit compression of the Λ_m.

However, in random networks the number of SNs in each cluster is not known. Moreover, the source signal is spatially localized leading to a different number of detecting SNs in each cluster. So choosing k_1 as defined previously negatively affects the performance. The $\tilde{I}_m$'s are then sent to the FC for another level of majority rule fusion as described next

$$\Gamma = \sum_{m=1}^{M} \tilde{I}_m \tag{D.5.16}$$

$$I_g = \begin{cases} 1, & \Gamma \geq k_2 \\ 0, & \Gamma < k_2 \end{cases} \tag{D.5.17}$$

where $k_2 = \lceil M/2 \rceil + 1$ is the second level majority rule threshold and I_g is the global decision about the intruder's presence. Note that the MFR virtually uses the CR in the CH and FC levels.

D.5.3 Optimal Cluster-based Fusion Rule

In contrast to MFR, we investigate the optimal scheme to fuse the CHs data, $\{\Lambda_m\}_{m=1}^{M}$. Employing the Neaman-Pearson criterion [78, Chapter 3], the log-likelihood

ratio (LLR) test is expressed as:

$$\Lambda_{\text{OCR}} = \sum_{m=1}^{M} \log\left(\frac{p\left(\Lambda_m; \mathcal{H}_1\right)}{p\left(\Lambda_m; \mathcal{H}_0\right)}\right). \tag{D.5.18}$$

where $p(\Lambda_m; \mathcal{H}_j)$ is the likelihood of Λ_m under hypothesis $\mathcal{H}_j$ for $j = 0, 1$.

To evaluate the LLR test, we investigate the properties of the detecting point process Φ_d in (D.3.9). The statistics of Φ_d under $\mathcal{H}_0$ are given by the following lemma.

Lemma D.5.1 *The detecting SN point process Φ_d defined in (D.3.9) under $\mathcal{H}_0$ is a homogeneous PPP with intensity of λP_{fa}.*

Proof: Define the following marked PPP (MPPP):

$$\Phi_m = \{(\mathbf{x}_i, s(\mathbf{x}_i)) : \mathbf{x}_i \in \Phi, s \in \mathcal{S}\} \tag{D.5.19}$$

where the marks are chosen to be the collected data $s(\mathbf{x}_i)$ with the mark space $\mathcal{S}$. Construct the detecting PP Φ_d by thinning Φ_m. Under $\mathcal{H}_0$, however, the probability of $\mathbf{x}_i \in \Phi_d$ is

$$\begin{aligned}\mathbb{P}\left(\mathbf{x}_i \in \Phi_d\right) =& \mathbb{P}\left(I(\mathbf{x}_i) = 1; \mathcal{H}_0\right) \\ =& \mathbb{P}\left(s(\mathbf{x}_i) > \tau; \mathcal{H}_0\right) = P_{fa}\end{aligned} \tag{D.5.20}$$

which is constant across $\mathcal{A}$, and hence the thinning probability is also constant. Therefore, the thinned Φ_d is a homogeneous PPP with intensity given by λP_{fa}. This concludes the proof. ■

Remark: It can be noted that if $\mathcal{A}$ is large the number of detecting SNs is also large. Thus the performance of simple rules such as the CR will suffer degradation and sophisticated rules such as the CVR will burden the network with large communication load. This motivates the use of clusters to divide the ROI into manageable areas with relatively low number of false alarms and communication burden. Similarly, the statistics of Φ_d under $\mathcal{H}_1$ are given in the following lemma.

Lemma D.5.2 *The detecting SN point process Φ_d defined in (D.3.9) under $\mathcal{H}_1$ is an inhomogeneous PPP with intensity $\lambda P_d(\mathbf{x})$.*

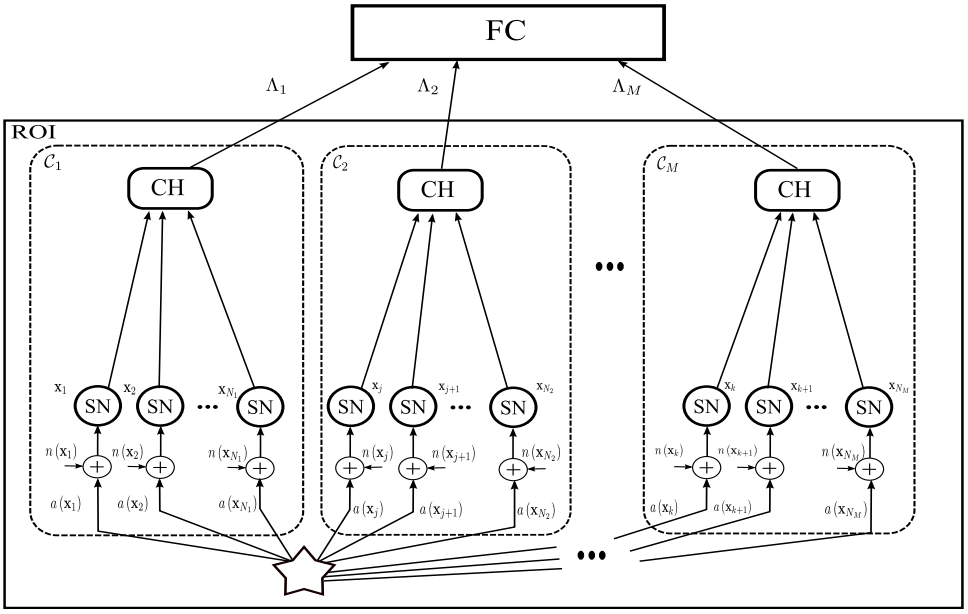

Figure D.2: Functional diagram for the clustered WSN. Pentagram: intruder; $\mathbf{x}_i$: location of ith SN; $a(\mathbf{x}_i)$: intruder's signal at ith SN; $n(\mathbf{x}_i)$: sensing AWGN at ith SN; SN: sensor node, CH: cluster head; FC: fusion center, and $\mathcal{C}_m$: mth cluster.

Proof: Define the detecting PP $\Phi_d = \{\mathbf{x}_i \in \Phi_m : s(\mathbf{x}_i) > \tau\}$. The former is obtained by thinning the MPPP Φ_m defined in (D.5.19) according to the probability

$$\begin{aligned}\mathbb{P}\left(\mathbf{x}_i \in \Phi_d\right) =& \mathbb{P}\left(I(\mathbf{x}_i) = 1; \mathcal{H}_1\right) \\ =& \mathbb{P}\left(s(\mathbf{x}_i) > \tau; \mathcal{H}_1\right) = P_d(\mathbf{x}_i). \end{aligned} \tag{D.5.21}$$

Note that the thinning probability depends on the intruder's parameters as mentioned earlier. Also, the thinning probability depends on $\mathbf{x}_i$ and so results in *dependent thinning*. Dependent thinning in turn produces an inhomogeneous PPP. Under $\mathcal{H}_1$ the mean of the total number of detecting SNs is given by

$$\begin{aligned}\lambda_1 =& \mathbb{E}\left[\sum_{\mathbf{x}_i \in \Phi_d} \mathbf{1}\left(\mathbf{x}_i\right)\right] \\ =& \mathbb{E}\left[\sum_{\mathbf{x}_i \in \Phi'_m} \mathbf{1}\left(s(\mathbf{x}_i) > \tau\right)\right] \end{aligned} \tag{D.5.22}$$

where $\mathbf{1}(A)$ is the indicator function for event A. Applying Campbell's theorem to

find the above mean yields

$$\begin{aligned}\lambda_1 =& \lambda \int_{\mathcal{A}} \int_0^{\infty} \mathbf{1}\left(s(\mathbf{x}) > \tau; \mathcal{H}_1\right) dP(s) dx \\ =& \lambda \int_{\mathcal{A}} \mathbb{P}\left(s(\mathbf{x}) > \tau; \mathcal{H}_1\right) dx \\ =& \lambda \int_{\mathcal{A}} P_d(\mathbf{x}) dx \end{aligned} \tag{D.5.23}$$

where $\mathbb{P}(A)$ is the probability of event A and $P(s)$ is the cumulative distribution function of the mark variable s.

This concludes the proof. ■

The above lemma implies that as the distance from the intruder increases the mean number of detecting SNs decreases due to the nature of the detection probability P_d defined in (D.3.6).

Remark: The detecting intensity of SNs decreases gradually as we move away from the intruder until it reaches the value of λP_{fa}, implying that the intruder's signal has no effect at this point. This fact also motivates the use of clusters since the detecting SNs are much more likely to be close to the intruder. From the above lemmas the distribution of the total number of detecting SNs in the network can be directly inferred as stated in the following corollary.

Corollary D.5.3 *Let the total number of detecting SNs be*

$$\Lambda = \sum_{\mathbf{x}_i \in \Phi_d} \mathbf{1}(\mathbf{x}_i). \tag{D.5.24}$$

Then Λ is Poisson distribution with:

$$\Lambda \sim \begin{cases} \text{Pois}\left(\lambda_0\right), & \mathcal{H}_0 \\ \text{Pois}\left(\lambda_1\right), & \mathcal{H}_1 \end{cases} \tag{D.5.25}$$

where λ_0 are λ_1 are the means number of detecting SNs under $\mathcal{H}_0$ and $\mathcal{H}_1$ respectively and are given by

$$\lambda_0 = \lambda P_{fa} |\mathcal{A}| \tag{D.5.26}$$

$$\lambda_1 = \lambda \int_{\mathcal{A}} P_d(\mathbf{x}) d\mathbf{x}. \tag{D.5.27}$$

Proof: See Lemma D.5.2. ■

Consequently, the distribution of the CR test statistic is directly given by (D.5.25) as it was shown in [133]. Furthermore, the distribution of Λ_m follows directly from the Poisson property of Φ_d as stated by the following corollary.

Corollary D.5.4 *The distribution of* Λ_m *is*

$$\Lambda_m \sim \begin{cases} \text{Pois}\left(\lambda_{0,m}\right), & \mathcal{H}_0 \\ \text{Pois}\left(\lambda_{1,m}\right), & \mathcal{H}_1 \end{cases} \tag{D.5.28}$$

where $\lambda_{0,m}$ *are the* $\lambda_{1,m}$ *are mean numbers of detecting SNs in the* m*th cluster under* $\mathcal{H}_0$ *and* $\mathcal{H}_1$ *respectively and are given by*

$$\lambda_{0,m} = \lambda P_{fa} |\mathcal{C}_m| \tag{D.5.29}$$

$$\lambda_{1,m} = \lambda \int_{\mathcal{C}_m} P_d(\mathbf{x}) d\mathbf{x}. \tag{D.5.30}$$

Proof: Since Λ is a Poisson RV over $\mathcal{A}$ and the Λ_m's are defined in (D.5.14) over the $\mathcal{C}_m$ s that are disjoint areas in $\mathcal{A}$, then Λ_m is a Poisson RV over $\mathcal{C}_m$.
This concludes the proof. ■

Note that if all the $\mathcal{C}_m$'s have the same area, say $|\mathcal{C}|$, then $\lambda_{0,m} = \lambda P_{fa}|\mathcal{C}|$ for all $m = 1, \cdots, M$. Hence, under $\mathcal{H}_0$ all the Λ_m's have the same distribution under $\mathcal{H}_0$.

With this information at hand, the OCR defined earlier in (D.5.18) can be written as

$$\begin{aligned} \Lambda_{\text{OCR}} &= \sum_{m=1}^{M} \log \left(\frac{e^{-\lambda_{1,m}} \left(\lambda_{1,m}^{\Lambda_m} / \Lambda_m!\right)}{e^{-\lambda_{0,m}} \left(\lambda_{0,m}^{\Lambda_m} / \Lambda_m!\right)} \right) \\ &= \sum_{m=1}^{M} \Lambda_m \log \left(\frac{\lambda_{1,m}}{\lambda_{0,m}} \right). \end{aligned} \tag{D.5.31}$$

where the constant term above is ignored in the second line of the equation.

Remark: Note, however, that $\lambda_{1,m}$ is a scaled spatial average of the detection probability in (D.3.6), which is the direct result of applying Campbell's theorem [129, Chapter 2] in (D.5.23). This relieves the OCR from knowing the SNs' positions, in contrast to the CVR. Nonetheless, finding the $\lambda_{1,m}$'s requires knowing the intruder's parameters, P_0 and x_0, a topic that will be discussed later in Subsection D.5.4. Thus, the OCR is a weighted sum of the number of positive decisions in each cluster.

Clusters with larger detecting SNs means, $\lambda_{1,m}$, are given more weight since it is expected that the intruder is in their vicinity. On the other hand, clusters with smaller detecting SNs means are given less weight since the intruder is expected to be far away and hence the detecting SNs in such clusters are due to false alarms. In this sense, the problem of spurious detection is adequately handled.

D.5.4 Generalized Likelihood Ratio Test for Clustered-based Fusion

As mentioned earlier, the OCR requires the knowledge of the $\lambda_{1,m}$'s, which are implicitly dependent on the intruder's parameters, i.e., $\boldsymbol{\theta} = (P_0, \mathbf{x}_0)^T$. Unfortunately, such information is not available in realistic scenarios since the intruder is not cooperative with the network. In this case we resort to the GLRT [78, Chapter 7] method, which consists of replacing the unknown parameters in the LLR by their maximum likelihood estimates.

The data used to estimate $\boldsymbol{\theta}$ is the set $\{\Lambda_m\}_{m=1}^M$ available at the FC. The GLRT for the clustered-based fusion, termed here (GCR), is given by

$$\Lambda_{\text{GCR}} = \max_{\boldsymbol{\theta}\in\boldsymbol{\Theta}} \sum_{m=1}^{M} \Lambda_m \log\left(\frac{\lambda_{1,m}(\boldsymbol{\theta})}{\lambda_{0,m}}\right) \tag{D.5.32}$$

where $\boldsymbol{\Theta} \subset \mathbb{R}^3$ is the space of all $\boldsymbol{\theta}$ values.

Note that the dependence of $\lambda_{1,m}$ on $\boldsymbol{\theta}$ is via the detection probability defined in (D.3.6). The GLRT in (D.5.32) can be interpreted as finding the optimal set of weights that maximize the weighted average of Λ_m's.

However, problem (D.5.32) is a nonlinear three dimensional optimization problem, which is usually solved via numerical techniques. To reduce the complexity, the search space is restricted version of the original, Θ. In particular, the search space for the target's position is restricted to the clusters centroids, $\mathbf{x}_{c,m}$, given by

$$\mathbf{x}_{c,m} = \frac{1}{|\mathcal{C}_m|}\int_{\mathcal{C}_m} \mathbf{x}\, d\mathbf{x}. \tag{D.5.33}$$

for $m = 1, \cdots, M$. Although, the restricted search space is significantly smaller than the original, the corresponding results as shown is Section D.6 are very close to the optimal CVR.

Table D.1: Fusion rules list.

Abbreviation	Equation	Fusion Rule
CVR	(D.4.10)	Chair-Varshney Rule
CR	(D.4.11)	Counting Rule
SS	(D.4.12)	Scan Statistic
B-SS	(D.4.13)	Bayesian SS
MFR	(D.5.17)	Majority-like Fusion Rule
OCR	(D.5.31)	Optimal Clustered-based Fusion Rule
GCR	(D.5.32)	GLRT Clustered-based Fusion Rule

D.6 Simulation Results

We simulate a WSN deployed in a 50×50 ROI. The intruder's power is $P_0 = 1$. The sensing SNR is set to 0 dB. The SNs have a reference distance of $d_0 = 1$ units with a local probability of false alarm of 10^{-2}. We simulate the fusion rules listed in Table D.1 and compare them in using the above setting. The proposed GCR is implemented via a grid search, as stated earlier, on a restricted search space as described next. The values considered for the power P_0 are obtained by linearly the discretizing the interval $[0.1, 1]$; ten values used for the simulations. The discretization of x_0 is done by dividing the ROI into adjacent squares girds with side length of A/N each, where A is the ROI side length ($A = 50$ in our simulation setup) and N is the number of clusters. The centers of those squares in addition to the discretized power values are used to form the restricted search space.

First we validate corollaries D.5.3 and D.5.4 by simulation. Figure D.3 shows the results of a Monte Carlo simulation with 10^5 runs to produce the simulated and

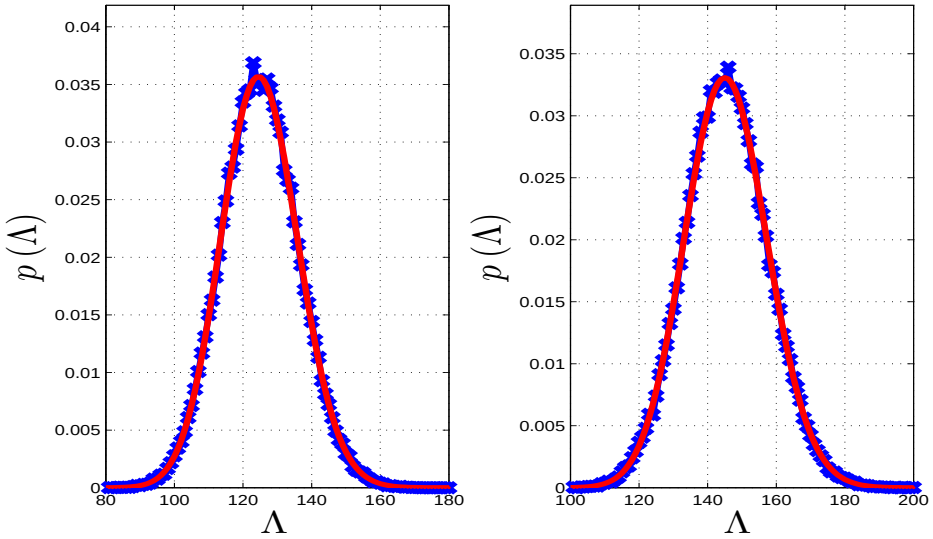

Figure D.3: Distribution of Λ. The system parameters are $\lambda = 5$, $d_0 = 1$, $\text{SNR}_s = 0\text{dB}$, $P_{fa} = 10^{-2}$, and $\mathbf{x}_0 = (20, 20)^T$. 'x' for simulation distribution and solid line for Poisson distribution in Corollary D.5.3.

theoretical distribution of Λ defined in (D.5.24), or that of Λ_{CR} in (D.4.11). The exact Poisson distribution given in Corollary D.5.3 fits the simulation perfectly for both $\mathcal{H}_0$ and $\mathcal{H}_1$. For the same setup, the WSN is divided into four squared-shaped clusters and the distributions of the Λ_m's in the four clusters are shown in Figures D.4 and D.5. Again the theoretical Poisson distributions given in Corollary D.5.4 fit the simulation accurately. Note however, that under $\mathcal{H}_0$ all Λ_m's have the same distribution. Under $\mathcal{H}_1$ on the other hand, Λ_3 differs since the intruder is located in the region monitored by the third cluster. Λ_1, Λ_2 and Λ_4 have a distribution similar to the $\mathcal{H}_0$ case since the intruder is not sensed by SNs in the those clusters.

Figure D.6 show the ROC diagrams for the fusion rules mentioned in Table D.1 for different values of λ, obtained by 10^4 Monte Carlo runs. The OCR uses 25 square-shaped clusters to cover the ROI. The same number of clusters is used for the MFR. The decision threshold for all the CHs in the MFR are the same and are set according to Corollary D.5.4 to provide a cluster level false alarm rate of 0.1 approximately. To make the comparison fair, the SS and the B-SS use a window with

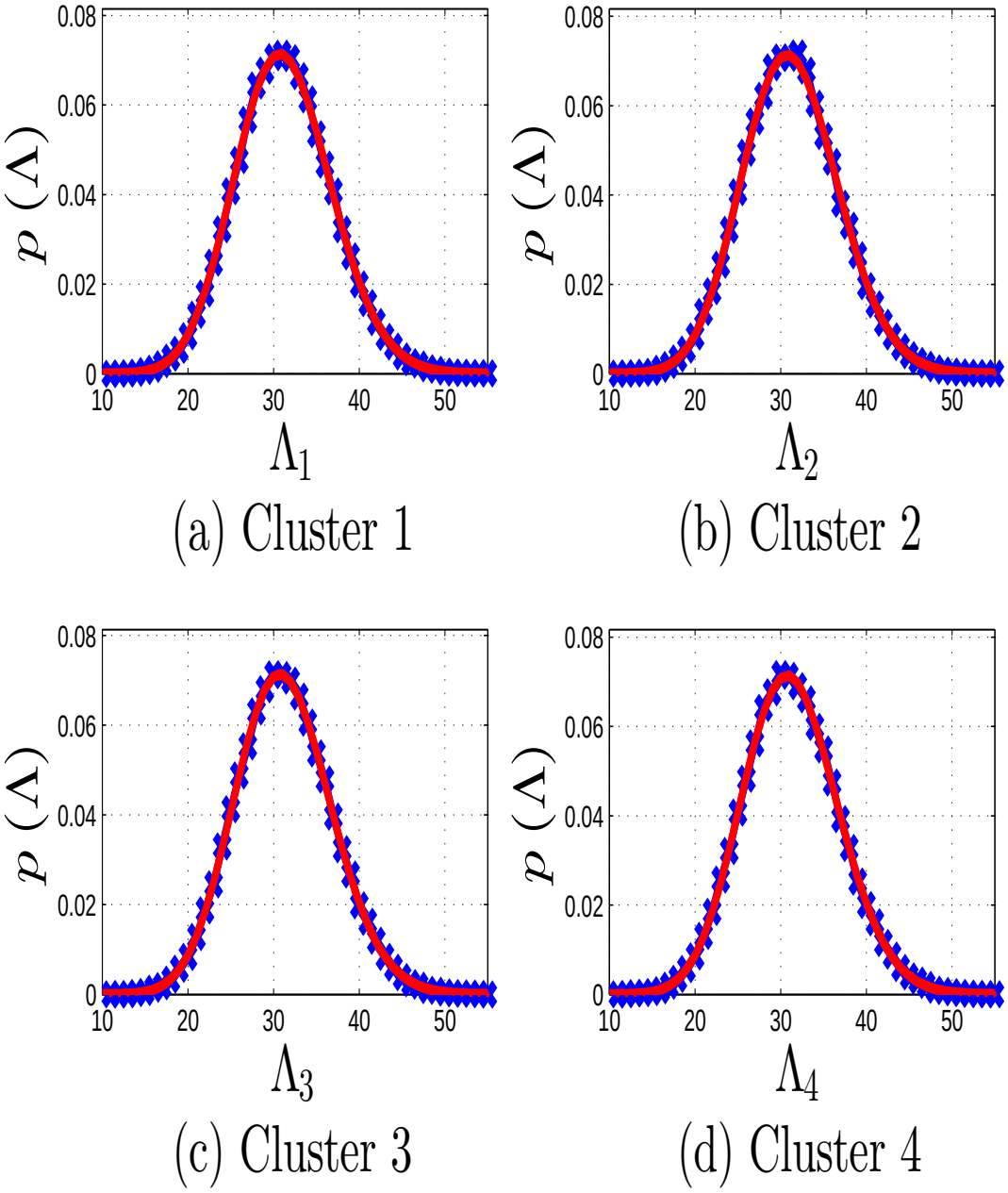

Figure D.4: Distribution of CH data, Λ_m, under $\mathcal{H}_0$ for $\lambda = 5$ and number of clusters $M = 4$. The system parameters are $\lambda = 5$, $d_0 = 1$, $\text{SNR}_s = 0\text{dB}$, $P_{fa} = 10^{-2}$, and $\mathbf{x}_0 = (20, 20)^T$. 'x' for simulated distribution and solid line for Poisson distribution in Corollary D.5.4.

the same size as the clusters used in the OCR. The OCR shows superior performance compared to the rest of the rules. In fact, as λ increases the OCR approaches the optimal performance of the benchmark CVR. The GCR follows a similar trend as

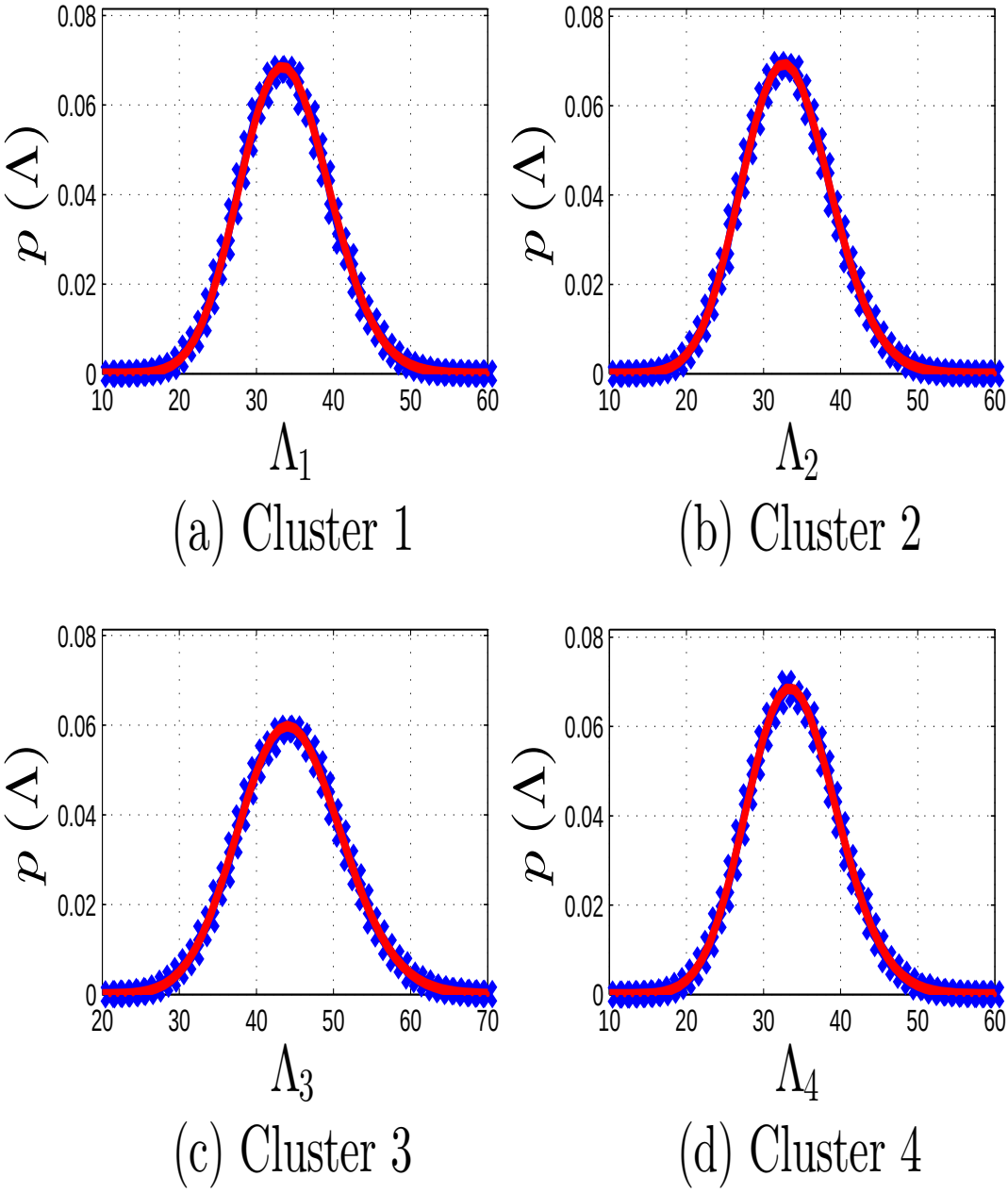

Figure D.5: Distribution of CH data, Λ_m, under $\mathcal{H}_1$ for $\lambda = 5$ and number of clusters $M = 4$. The system parameters are $\lambda = 5$, $d_0 = 1$, $\text{SNR}_s = 0\text{dB}$, $P_{fa} = 10^{-2}$, and $\mathbf{x}_0 = (20, 20)^T$. 'x' for simulated distribution and solid line for Poisson distribution in Corollary D.5.4.

the OCR, in which it can be observed that the GCR rapidly approaches the OCR as λ increases and consequently it performs better than the SS, B-SS, CR, and the MFR. The SS algorithms show better performance when compared to the CR,

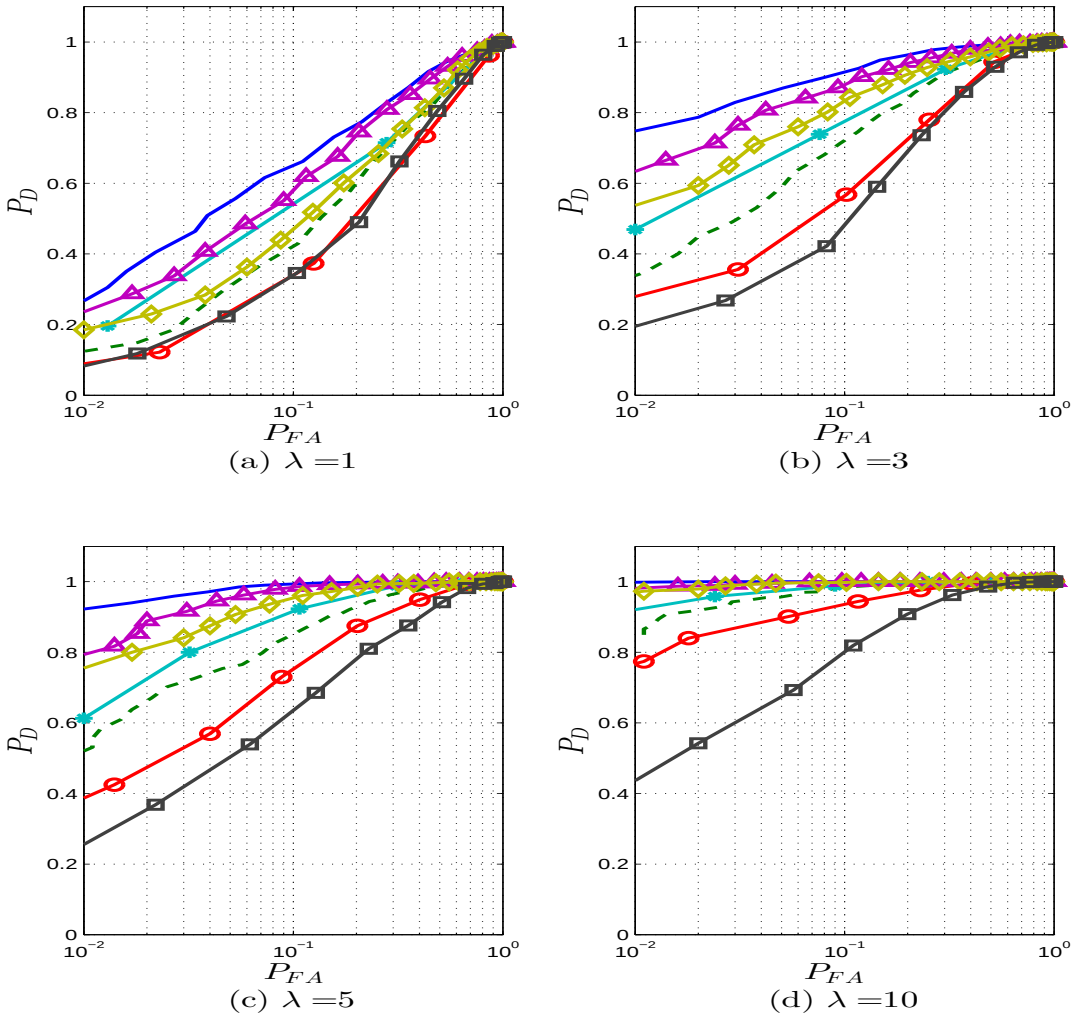

Figure D.6: ROC diagrams for a network with 25 clusters. The system parameters are $d_0 = 1$, $\text{SNR}_s = 0\text{dB}$, $P_{fa} = 10^{-2}$, and $\mathbf{x}_0 = (0,0)^T$. CVR: Solid line, CR: dashed line, OCR: '$\triangle$', GCR: '$\diamond$', MFR: '$\square$', SS: '$*$', and B-SS: '$\circ$'.

which shows a relatively slow improvement as λ increases. The MFR performs the worst among all rules, this is due to utilizing the least amount of information when compared to the other rules.

Figure D.7 illustrates the effect of increasing M, the number of clusters, on the performance of the fusion rules[2]. It is noted that when the number of clusters is small, the OCR resembles the CR in performance. This result is intuitive since the

[2]The B-SS is not shown in the case of $M = 4$ due to a severely bad performance.

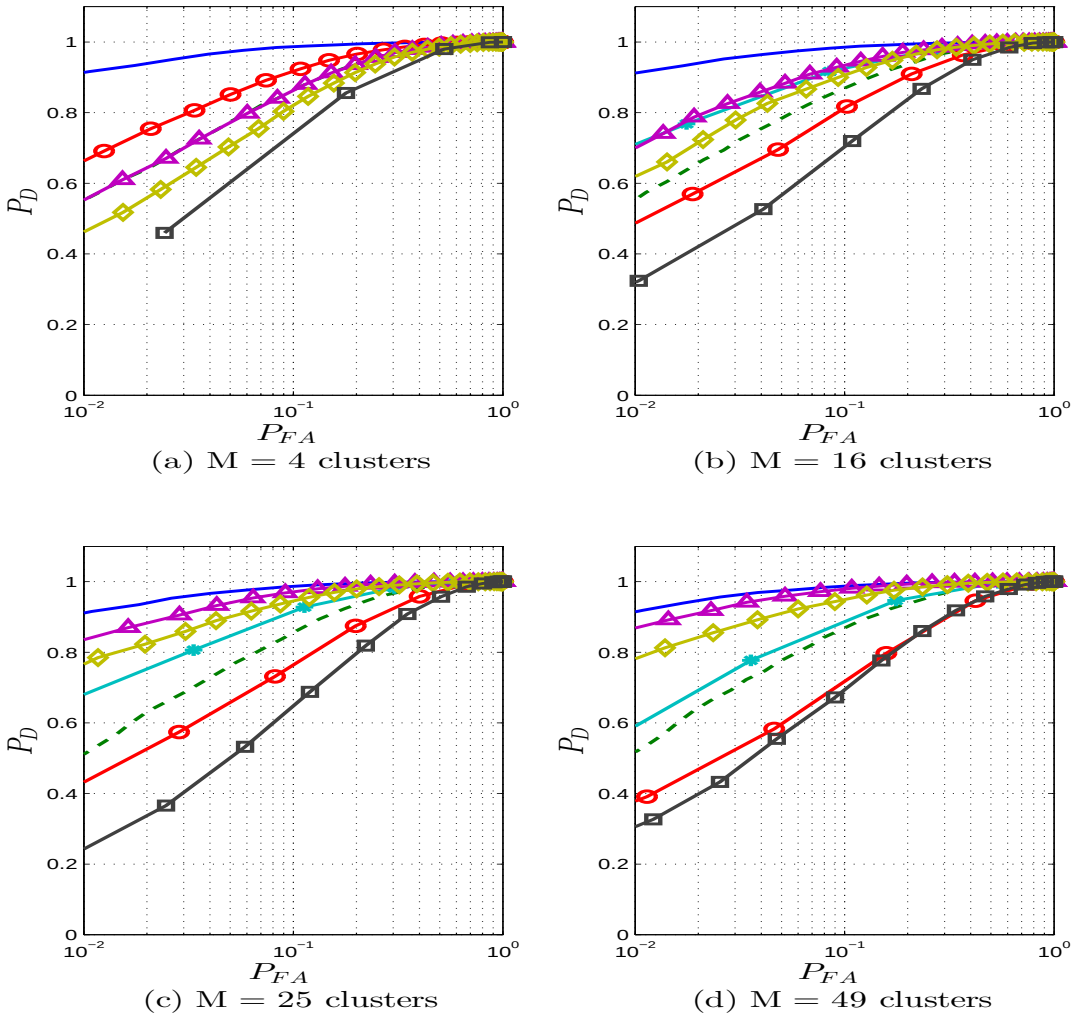

Figure D.7: ROC diagrams for a network with $\lambda = 5$. The system parameters are $d_0 = 1$, $\text{SNR}_s = 0\text{dB}$, $P_{fa} = 10^{-2}$, and $\mathbf{x}_0 = (0, 0)^T$. CVR: Solid line, CR: dashed line, OCR: '$\triangle$', GCR: '$\diamond$', MFR: '$\square$', SS: '$*$', and B-SS: '$\circ$'.

limit case of a single cluster is equivalent to the CR. The SS algorithms perform better because they use more information for fusion. However, as M increases the OCR and GCR outperform the rest of the rules and ultimately reach the benchmark performance of the CVR. This behavior can be explained by the fact that as the number of clusters increases the detecting SNs due to the intruder's presence are contained in clusters that are given large weights. On the other hand, clusters containing the spurious detection are given small weights, hence improving the detection performance.

D.7 Conclusions

We have studied fusion rules for distributed detection in random clustered WSNs. In each cluster the CH collects the local decisions of the SNs and sends the sum to the FC. Using stochastic geometry, we derived the optimal cluster-based fusion rule (OCR), which is the weighted average of the sums of local decisions at each cluster. The weights are shown to depend on the mean number of detecting SNs under the null and alternative hypotheses. In contrast to the optimal Chair-Varshney rule, the OCR does not require the locations of the SNs to be known. Furthermore, a reduced-complexity GLRT for cluster-based fusion (GCR) is developed to handle the case of unknown intruder's parameters. Simulation results have shown that the performance of the OCR approaches that of the Chair-Varshney rule. Results also showed that as the number of clusters increases the performance rapidly reaches the Chair-Varshney benchmark for fixed SNs deployment intensity. In other words, optimal detection can be achieved by forming more clusters in the network, in contrast to adding more sensor nodes to it. Finally, the performance of the GCR was shown to approach that of the OCR when the number of clusters is large enough.