Louisiana State University

LSU Digital Commons

LSU Master's Theses | Graduate School

2011

Secure distributed detection in bandwidth-constrained wireless sensor networks

Reza Soosahabi

Louisiana State University and Agricultural and Mechanical College

Follow this and additional works at: https://digitalcommons.lsu.edu/gradschool_theses

Part of the Electrical and Computer Engineering Commons

Recommended Citation

Soosahabi, Reza, "Secure distributed detection in bandwidth-constrained wireless sensor networks" (2011). *LSU Master's Theses*. 1346.
https://digitalcommons.lsu.edu/gradschool_theses/1346

This Thesis is brought to you for free and open access by the Graduate School at LSU Digital Commons. It has been accepted for inclusion in LSU Master's Theses by an authorized graduate school editor of LSU Digital Commons. For more information, please contact gradetd@lsu.edu.

SECURE DISTRIBUTED DETECTION IN BANDWIDTH-CONSTRAINED WIRELESS SENSOR NETWORKS

Thesis

Submitted to the Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Master of Science in Electrical Engineering

in

The Department of Electrical and Computer Engineering

by
Reza Soosahabi
B.S. in Electrical Engineering - Communication
Amirkabir University of Technology (Tehran Polytechnic), Iran, 2009.
August, 2011

To my wonderful family

In memory of my dear granny

Acknowledgements

Firstly I offer my sincerest gratitude to my supervisor, Dr. Morteza Naraghi-Pour, who appointed me as his graduate research assistant for the last two years. I am so grateful for his kind support and guidance that helped me to succeed in my research career. He gave me the main idea of this work and patiently motivated me to complete its analysis. In the fruitful courses I have had with him, he taught me how to approach difficult problems and develop the true research spirit in myself.

I would like to thank Dr's Xue-Bin Liang and Shuangqing Wei for patiently attending my defense session and providing me with their useful comments. I also thank Dr's Bahadir Gunturk, Rajgopal Kannan, Xue-Bin Liang and Shuangqing Wei whose classes had great influence on my knowledge.

My deepest gratitude goes to my parents who always supported me and gifted me the liberty to pursue my interests. They taught me the greatest lesson in my life, to think freely and independently.

Finally I am obliged to many of my colleagues who supported me while I was writing this thesis. I thank Ahsan-Abbas Ali, Iman Khademi, Mahdi Orooji, Erfan Soltanmohammadi and Venkat Patcha for their support during my defense session. I also thank Venkat Patcha for helping me with the formating of this thesis.

Table of Contents

List of Tables

List of Figures

Abstract

Utilizing wireless sensor network (WSN) is a novel idea in a variety of applications. However, the limited resources allocated to the sensor nodes make the design of WSNs a challenging problem. We consider the problem of hypothesis testing in a bandwidth-constrained, low-power wireless sensor network operating over insecure links. Sensors quantize their observations and transmit their decisions to an intended (ally) fusion center (AFC) which combines the received messages to detect the state of an unknown hypothesis.

In many applications the sensor messages are vulnerable to unauthorized eavesdropping. The scarce bandwidth and processing power for the sensors rule out the utilization of advanced encryption techniques. To protect their transmissions from an unauthorized (third party) fusion center (TPFC), the sensors use a simple encryption whereby they randomly flip their quantization outcomes, similarly to what happens in a discrete memoryless channel. It is assumed that AFC is aware of the encryption probabilities (keys) but TPFC is not.

For the AFC the decision rule is formulated as a constrained optimization problem where one constraint is a lower bound on the error probability of TPFC. The optimal decision rules for the two fusion centers are then derived. It is shown that by appropriate design of the encryption probabilities and the AFC decision rule, it is possible to degrade the error probability of the TPFC significantly and still achieve very low probability of error for the AFC. Numerical results are presented to show that it is possible to ensure that TPFC does not gain any information from the observation of sensors transmissions.

Chapter 1

Introduction

Sensor networks have originally emerged from application in military surveillance systems [27]. The sensor networks at that time included a few sensors wired to a central processor which was in charge of all signal processing. Technological advances in electronics and wireless communication, facilitated the emergence of wireless sensor networks (WSNs) involving a multitude of small, low-power sensors which can network themselves to accomplish a variety of tasks in a distributed way. Over the last decade WSNs have contributed to a wide range of applications in environmental monitoring, healthcare control, mechanized agriculture and etc. These are achieved by virtue of distinct features of WSNs, like easy utilization and autonomous operation [1], [13].

The distributed sensing is the idea that has fundamentally shaped WSNs to fit with the current demands. A WSN with a distributed function can be well exemplified by a swarm of ants. The individual ants are very small and of limited capabilities, but their cooperation in the swarm makes them a resilient and intelligent form of life. Similarly the wireless sensors have very limited individual resources for sensing and processing but these are multiplied in a WSN. To build a WSN, a large number of wireless sensors are randomly deployed in the monitoring region, and they form an ad-hoc network according to a program assigned to them so as to communicate their collected data with a central node ($f$usion center) [21]. The fusion center, having information from different geographic locations in the monitoring region, can hence make a reliable decision about the events of interest [25]. In many cases where the location of the event is unknown and the environment is not well suited for communication, having a dense distributed network is preferred to a sparse network of fully-supplied sensors. This can be accounted for the fact that a dense network reduces the chance of blind spot in the monitoring region and can remain connected in the presence of communication obstructions [13].

Sensor networks are usually destined to be used in hostile and unaccessible environments, like bottom of oceans and polluted areas, where designers do not have the luxury of a

wired network to supply sensors and establish direct communication channels. There are also many scenarios where sensors need to be of small size, like in battle fields, to be invisible to an enemy [1]. The production of tiny radio transceivers solved these problems by developing WSNs and made wireless communication an indispensable component of sensor networks. Wireless communication also enables connectivity of mobile sensors, such as the sensors built-in microrobots.

Although WSNs seem to be a panacea for many of today's applications, there are many technical challenges regarding their scarce resources such as power supply, memory, size, bandwidth and processing power. Since the individual sensors usually have no power supply more than their internal batteries, they eventually die and this will continue till the WSN fails to accomplish the distributed tasks. Thus there is a limited lifetime for a WSN which has spurred design of energy-efficient communication protocols for WSNs [32].

1.1 Sensor Design and Network Architecture

As mentioned, individual sensors in a WSN are meant to handle simple tasks. The block diagram of the main components of a sensor node is depicted in Fig. 1.1 [1]. The signal emitted by the phenomenon of interest (for example temperature, light, or a combination of them) is received by the sensing unit and converted to an analog electric signal. Then the analog signal is sent to the ADC unit which samples, quantizes and feeds them to the processor in the form of sample frames. Finally the processor unit processes each frame and converts the result into a binary sequence. Then depending on the transmission schedule, it may either immediately send the bits to the wireless transceiver to be transmitted in as packets, or store them. A processor unit typically has very limited storage and processing capacities (for example processing speed 4 MHz and storage of 128 KB [26]) which are mostly allocated to manage communication. Therefore the processor does not have the resources to control the ADC or the the sensing unit in order to adapt them during the lifetime of the device. All the units are once configured before deployment, and during utilization they are not likely to change their operation routines. The processing speed also limits the data rate can be handled by each sensor node that enforces a bandwidth constraint.

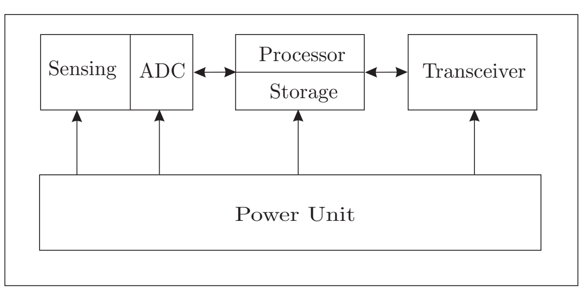

Figure 1.1: The main components of a sensor node

The power unit, as illustrated in Figure 1.1, occupies considerable space in a sensor node. Due to the size constraints the power unit usually includes one or two batteries supplying the other units. Since failure due to lack of power is an inevitable fate of each sensor, a sensor must budget its power during the course of operation. Usually the power consumed by the radio transceiver unit is more significant than the the other units. This is the motivation for developing energy efficient network architecture. To reduce power dissipation in transmission, the sensors are densely scattered in the monitored area such that each node can communicate with multiple nodes within a short range. There are also sleep periods scheduled for each node to switch off its transceiver when not in use [32].

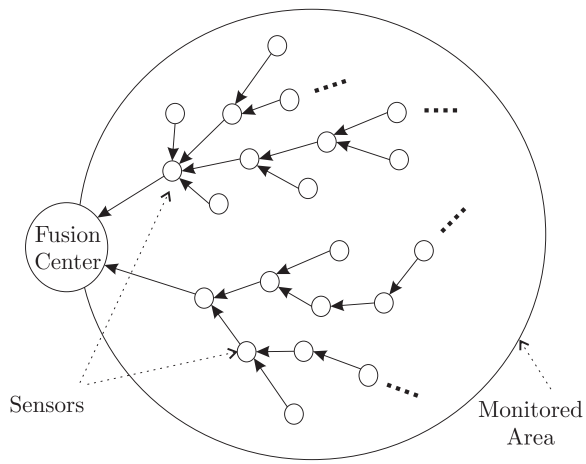

Figure 1.2: The network architecture in WSNs

After the sensors are deployed, each of them tries to reach out its closest neighbors. Then they form a self-organizing tree-structured network, exhibited in Figure 1.2, to deliver their messages (packets) to the fusion center. A routing protocol must then be developed for such networks which must be energy efficient, and robust to topology changes due to link and node failures [15]. Many routing protocols have been developed in recent years and are often based on the shortest-path-tree idea such that each node forwards its own packets together with its received packets to a node among its neighbors which is closest to the fusion center [2].

1.2 Distributed Detection Using Sensor Networks

The tasks of sensor networks include detection, estimation and tracking of a physical quantity such as temperature, sound or light intensity. The complexity of sensor network to handle these tasks respectively increases. For detection, sensors only observe the existence of a certain phenomenon where estimation requires them to measure its qualities. Whereas detection and estimation need observation shots, tracking involves continuous observation of the variations in a phenomenon such that it is sometimes impractical for WSNs. Here we

concentrate on the detection operation appearing in a broad range of WSNs' applications [25].

In the traditional sensor networks, the sensors did not have the processor unit (and neither the power nor transceiver unit in wired cases) compared to the wireless sensors as shown in Figure 1.1. They sent their raw samples to the fusion center which performs the detection operation. This type of detection is called *centralized detection*. Due to the limitations in communication, processing power and power supply mentioned above, centralized detection in WSNs is impractical. Hence the detection scheme tailored to WSNs is named *decentralized detection* where each sensor node partially processes its collected samples and then sends the result to the fusion center using few packets [29, 31].

Depending on the network architecture of a WSN, decentralized detection can be performed in different topologies such as: *star*, *serial* and *tree* [30]. In the serial and tree topology, each sensor processes its own sensed data together with the content of its received packets during the routing. Then it may route only the result of the process [14]. In the star topology sensors' messages are directly routed to the fusion center. The star topology is commonly used in applications where the sensors have very limited processing capability, fusion center needs to immediately detect a target, or the messages from the individual sensors are used to localize a phenomenon. In this work our attention is on the star topology.

Distributed detection using WSNs is a research problem that has been extensively investigated [27]. What is related to our work involves the optimal design of the fusion rule under different conditions of quantization at the individual sensors.

The classical Bayesian detection was used in [27] to draw out the optimal binary detection individually performed by the sensors. Then Chair and Varshney proposed the k-out-of-n rule in [6] as the optimal fusion rule for binary hypothesis testing where the sensors are equipped with identical binary quantizers. In [18] the authors have investigated the optimal fusion rule for the binary hypothesis testing where the sensors make soft local decisions (non-binary quantization). It is worth to note that the communication channel has been assumed to be error-free in the above methods.

In [7] error exponents for probability of error are derived for star networks with capacity constraints. There the authors have analyzed the problem of detecting deterministic signals in the presence of Gaussian noise. They have proved that the information loss in decentralized binary detection can be compensated for by a large number of sensors. Later Tsitsiklis investigated the decentralized detection problem for multiple hypothesis testing in [28, 29]. Having M hypotheses, he proved that a very large set of sensors can be partitioned into $\frac{M(M-1)}{2}$ subsets where the optimal local decision rule is identical for the sensors in each subset. Particularly for binary hypotheses testing, this implies that it is asymptotically optimal to let the sensors make their local decisions based on an identical

likelihood-ratio rule.

The optimal design of decentralized detection schemes in the presence of channel imperfections has been recently studied [24]. Practically channel noise and fading cannot be overlooked in WSNs. The optimal binary fusion rule for identical sensors in generalized Gaussian noise has been discussed in [23]. Dependency of likelihood-ratio based fusion rules on the fading channel information is investigated in [9], where the authors have proposed tow methods to reduce the effect of fading: maximal ratio combining and two-stage Chair-Varshney rule. There the latter method first estimates the channel coefficients and then forms likelihood ratios for detection. There is also the binary fusion rule stated in [19] which only relies on the statistics of Rayleigh fading channels assuming all the sensors experience the same SNR.

1.3 Motivation for This Work

As applications of WSNs become more wide-spread, security issues become more important concerns in mission-critical applications [22]. Examples include surveillance in a hostile or unattended environment such as a battlefield, a protected area, or the site of a (natural or man-made) disaster. While a WSN is on duty, third-parties, which are not authorized participants of the WSN, attempt to attack the WSN to fulfill their own interest. They may either steal the sensitive data collected by the sensors (eavesdropping), or disable the communication between the sensors and the fusion center (jamming) [11]. In many scenarios an attacker takes both actions. Due to the aforementioned resource limitations in WSNs, involving the security precautions makes the design of WSNs even more challenging [12].

In this thesis we consider the problem of distributed detection in a bandwidth-constrained WSN operating over insecure links. Due to the limited power and low bandwidth, we assume that each sensor node transmits a quantized decision of its observation. In addition to the ally (intended) fusion center (AFC), a third-party (unauthorized) fusion center (TPFC) may also be observing the sensor transmissions and attempting to detect the state of the unknown hypothesis. Our goal is to design the system parameters so as to deteriorate the error probability of the unauthorized fusion center while maintaining an acceptable error probability for the intended ally fusion center.

Security encoding is a typical technique to protect the raw messages from the TPFC access. However it increases the packet length which is not tolerable where the bandwidth and energy consumption are strictly limited. Hence to this end, each sensor node uses a simple encryption mechanism whereby its decision result is flipped around (within the possible quantization decisions) with given probabilities, similar to the operation of a discrete memoryless channel. It is assumed that the AFC is aware of the encryption keys (probabilities), and can minimize its probability of error accordingly, whereas the TPFC is

unaware of the encryption keys and can only base its decision on the encrypted bits. This encryption operation was firstly discussed in [4] where the authors considered the problem of decentralized estimation when transmission of sensor decisions is over insecure links. Later Sriram in [25] applied a binary cipher with fixed probabilities to the distributed detection problem where each node sends a binary decision.

We show that when appropriately designed, the proposed method ensures that a high error probability can be imposed on the TPFC to the extent that it cannot gain any information from the sensors' transmissions. Applying the security precautions will also degrade the detection performance at the AFC. However, given enough sensors in the network, an acceptable performance can be achieved by this fusion center. Given the power and bandwidth constraints of WSN, this is an attractive method to protect the sensors' data.

Chapter 2

Secure Distributed Detection Using Binary Decision at the Sensors

In this chapter we first describe the distributed detection problem and the operation of the sensors in the case where the sensors use binary local decisions. Next we discuss the encryption mechanism used by each node and present the error probabilities of both the AFC and TPFC. Similarly to [25] we assume both the sensors and the fusion center perform Bayesian detection. The TPFC, which is unaware of the encryption, presumes that the sensors transmit their raw decisions. Knowing the local decision rule of the sensors, it adjusts its fusion rule in order to minimize its assumed error probability. The AFC can also perform the same optimization and, therefore, is aware of the TPFC's decision rule. Then it investigates the fusion rule and the encryption which minimize its error probability with respect to a lower bound on the TPFC error probability. The solution region for the AFC optimization is considerably reduced in a few steps such that the optimal solution can be analytically evaluated. Finally in the section on numerical results, the deterministic signal detection in the presence of Gaussian noise is examined. The results confirm that for a given lower bound on the TPFC error probability, the AFC error probability can be reduced to any small value.

2.1 System Model

We consider a system of n sensors observing the state of an unknown hypothesis H where $H \in \{H_0, H_1\}$ and with prior probabilities of H_0 and H_1 being q_0 and q_1, respectively. Let X_i denote the observation of the ith sensor, $i = 1, 2, 3, ..., n$. It is assumed that given the hypothesis H_η, $(\eta = 0, 1)$, the observations $X_1, X_2, \cdots, X_n$ are independent and identically distributed. The conditional PDF of X_i under H_η is denoted by $p_\eta(x)$.

Each sensor i, $i = 1, 2, \cdots, n$, makes a decision $u_i \in \{0, 1\}$ regarding the state of the

hypothesis H using the likelihood ratio test

$$\frac{p_1(x)}{p_0(x)} \underset{u_i=0}{\overset{u_i=1}{\gtrless}} \lambda \tag{2.1}$$

where λ is a threshold which is assumed to be identical for all the sensors. The false alarm probability P_0 and the detection probability P_1 of individual sensors are given by

$$P_\eta = P(u_i = 1|H_\eta), \quad \eta = 0, 1 \tag{2.2}$$

For a fixed λ, the binary model in Fig 2.1 exhibits the binary detection process [30].

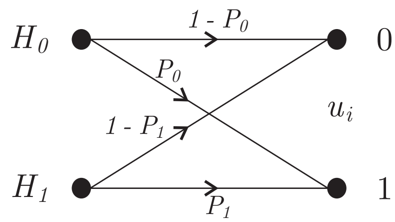

Figure 2.1: Binary model for the sensors' detection rule

In general assuming an identical threshold for local sensors does not lead to an optimum system. However, this assumption has been previously used in the literature in order to make the problem mathematically tractable [10,23,33]. For a two sensor system it is shown in [16] that no optimality is lost when identical thresholds are used. Furthermore, it is shown in [28] and [10] that identical thresholds are asymptotically optimal in the number of sensors n. Relying on these results and in order to make the problem tractable we have also assumed an identical threshold λ for all the local sensors.

The decisions of individual sensors are to be transmitted to the (allied) fusion center which must detect the state of H from the received information. We assume that the channel between the sensors and the FC is error free. This can be achieved using an appropriate error control coding scheme. The transmission of the sensors, however, may be observed by a third party (enemy) fusion center (TPFC) who also wishes to detect the state of H. In order to protect the decisions of the sensors from this unauthorized fusion center during transmission, we employ the following simple, probabilistic cipher. As depicted in Figure 2.2, the decision u_i of sensor i is encrypted to obtain z_i, where $P(z_i = 1|u_i = 0) = \pi_0$ and $P(z_i = 0|u_i = 1) = \pi_1$. This can also be described as $z_i = u_i \oplus v_i$, where $v_i \in \{0, 1\}$, $\{v_i\}_{i=1}^n$ are independent random variables with $P(v_i = 1|u_i = 0) = \pi_0$ and $P(v_i = 1|u_i = 1) = \pi_1$, and where $\oplus$ is the mod-2 addition. The encrypted binary output z_i is then transmitted to the allied fusion center (AFC) and may also be observed by the TPFC. Let

$$\begin{aligned}\theta_0 &\triangleq P(z_i = 0|H_0) = 1 - P_0 - \pi_0 + (\pi_0 + \pi_1)P_0 \\ \theta_1 &\triangleq P(z_i = 0|H_1) = 1 - P_1 - \pi_0 + (\pi_0 + \pi_1)P_1.\end{aligned} \tag{2.3}$$

It is assumed that the AFC has prior knowledge of the values of π_0 and π_1 but not the actual values of $v_1, v_2, \cdots, v_n$. On the other hand, the TPFC has no knowledge of π_0 and π_1 and, in the absence of this information, it can only assume that it has received the original decisions u_i, $i = 1, 2, \cdots, n$.

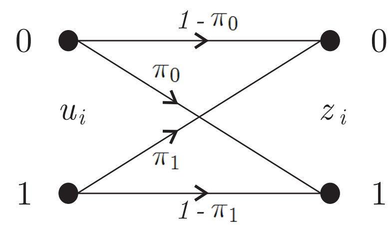

Figure 2.2: Binary model for the encryption

We consider a Bayesian detection problem where the performance criterion for each of the fusion centers is the probability of error. Specifically, our goal is to design the system parameters so as to minimize P_E^a, the probability of error for the AFC, subject to a lower bound on P_E^t, the probability of error for the TPFC.

The likelihood ratio test practiced at each of the fusion centers AFC or TPFC is given by

$$\frac{P(z_1, z_2, \cdots, z_n|H_1)}{P(z_1, z_2, \cdots, z_n|H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \Lambda \tag{2.4}$$

where Λ is a threshold assigned by each fusion center to minimize its error probability. Since the sensors' messages are independent the above ratio is broken down into the product of the likelihood-ratio for individual sensors,

$$\prod_{i=1}^{n} \frac{P(z_i|H_1)}{P(z_i|H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \Lambda. \tag{2.5}$$

Then considering (2.3), the above equation can be rewritten as

$$\frac{\theta_1^{n-m}(1-\theta_1)^m}{\theta_0^{n-m}(1-\theta_0)^m} \underset{H_0}{\overset{H_1}{\gtrless}} \Lambda \tag{2.6}$$

where m is the number of 1's in the sequence of received messages, $z_1, z_2, \cdots, z_n$. In other words, $m = \sum_{i=1}^{n} z_i$. In order to express the decision rule in terms of m, the logarithm is performed on (2.6) to get

$$(n-m)\ln\left(\frac{\theta_1}{\theta_0}\right) + m\ln\left(\frac{1-\theta_1}{1-\theta_0}\right) \underset{H_0}{\overset{H_1}{\gtrless}} \ln\Lambda \tag{2.7}$$

Following a simple rearrangement, we end up with a k-out-of-n rule given by

$$\hat{H} = \begin{cases} H_1, & \text{if } \sum_{i=1}^{n} z_i \geq k \\ H_0, & \text{if } \sum_{i=1}^{n} z_i < k. \end{cases} \tag{2.8}$$

where,

$$k = \left\lceil \frac{\ln \Lambda - n \ln \frac{\theta_1}{\theta_0}}{\ln \frac{\theta_0(1-\theta_1)}{\theta_1(1-\theta_0)}} \right\rceil \tag{2.9}$$

and where $\lceil x \rceil$ denotes the smallest integer no less than x. It is noted that the above decision rule also includes the maximum a posteriori (MAP) rule with $\Lambda = q_0/q_1$ [30]. The block diagram of the above fusion rule is demonstrated in Figure 2.3, where the binary quantizer and binary cipher blocks, respectively, correspond to Figure 2.1 and 2.2.

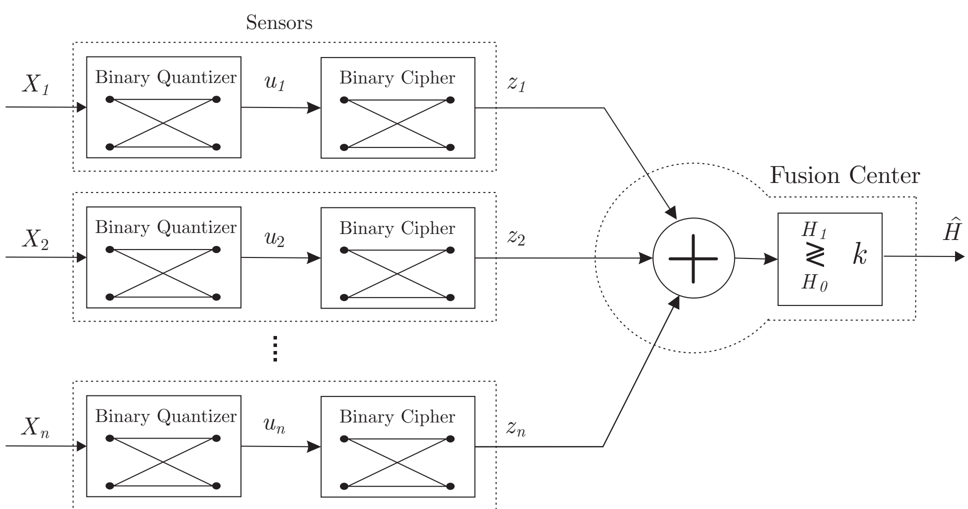

Figure 2.3: Block digram for the binary data fusion

The error probability for the two fusion centers has the same formula given by

$$P_E = q_0 P(\hat{H} = H_1 | H_0) + q_1 P(\hat{H} = H_0 | H_1) \tag{2.10}$$

Using (2.8) and the distribution of z_i given by (2.3) we calculate P_E as

$$P_E(k, \theta_0, \theta_1) = q_0 \psi(k, \theta_0) + q_1(1 - \psi(k, \theta_1)) \tag{2.11}$$

where $\psi(k, \theta)$ is a sum of binomial terms,

$$\psi(k, \theta) \triangleq \sum_{i=k}^{n} \binom{n}{i} (1-\theta)^i (\theta)^{n-i} \tag{2.12}$$

Figure 2.4 depicts the contour plots of $P_E(k, \theta_0, \theta_1)$ as a function of θ_0 and θ_1 for fixed valued of k and q_0. It can be seen that $P_E(k, \theta_0, \theta_1)$ is comprised of four plateaus near the four corner with values 1, q_1, 0 and q_0, in clockwise order beginning from northwest. There is also an inflection point in between which slides along $\theta_1 = \theta_0$ line with respect to the value of k.

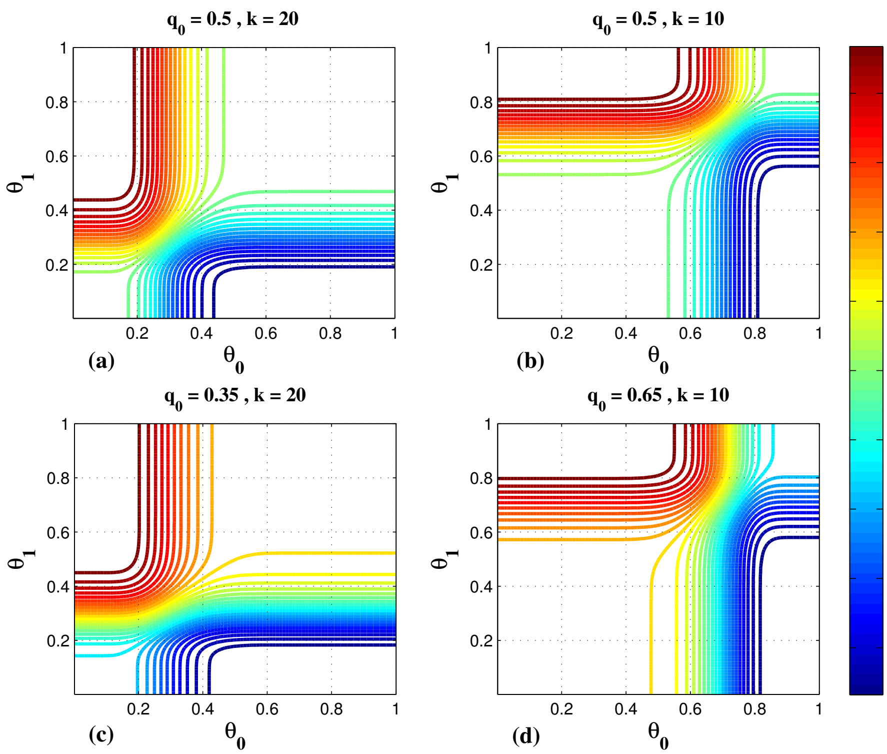

Figure 2.4: Contour plots of P_E with respect to θ_0 and θ_1 for $n = 30$

As evident from (2.10), the formulas for the false alarm and detection probabilities, and the probabilities of error are the same for the two fusion centers AFC and TPFC. However, these two fusion centers have different views of the network and thus their fusion rules are different.

Before studying the error probabilities of AFC and TPFC, we note that θ_0 and θ_1 both depend on P_1 and P_0 whose values in turn depend on the choice of λ. Unlike the cipher parameters, π_0, π_1, which are assigned during message transmission, λ is a built-in sensor parameter usually chosen to minimize the error probability in the absence of any encryp-

tion, i.e., when $\pi_0 = \pi_1 = 0$ [33]. Therefore hereafter we assume that the value of λ is the fixed value calculated accordingly and is known to both fusion centers. This implies that the TPFC can evaluate its fusion threshold, k^t, to minimize its assumed error probability for the corresponding λ. Note that this implies that P_1 and P_0 are also fixed.

2.2 Problem Statement

Both the AFC and TPFC tend minimize their error probabilities as cost functions in the following optimization problems. Note that the constraints in the two problems are different, since the fusion centers have different perspectives of the system.

2.2.1 Optimization from TPFC's Point of View

As mentioned previously, TPFC is assumed to be unaware of the encryption process and therefore assumes that $\pi_0 = \pi_1 = 0$. However, TPFC is aware of the threshold value λ and chooses its fusion threshold, denoted k^t, to minimize its probability of error. Since λ is also chosen to minimize the probability of error in the absence of any encryption, then the optimal λ and k^t are obtained from the solution of the following problem.

$$\begin{aligned} P1: \quad & \min_{k,\lambda} P_E(k, 1 - P_0(\lambda), 1 - P_1(\lambda)) \\ & \text{subject to:} \quad 0 \le k \le n \end{aligned}$$

where the objective function above is obtained from (2.11) for $\pi_0 = \pi_1 = 0$, ($\theta_i = 1 - P_i(\lambda), i = 0, 1$). We denote the optimal k and λ obtained from P1 by k^t and λ^*, respectively. The AFC can also solve this problem independently and so it is aware of the values of λ^* and k^t. Now in the presence of encryption ($\pi_i \neq 0$, and $\theta_i \neq 1 - P_i(\lambda^*), i = 0, 1$), the actual performance of TPFC is given by

$$P_E^t = P_E(k^t, \theta_0, \theta_1) \tag{2.13}$$

To simplify our notation, hereafter we denote $P_i^* = P_i(\lambda^*)$ for $i = 0, 1$.

2.2.2 Optimization from AFC's Point of View

The allied fusion center must choose its fusion threshold k^a along with the encryption parameters π_0 and π_1 so as to minimize its probability of error. In addition it must ensure that the performance of TPFC is degraded through the application of the encryption process. From (2.3) we can see that the AFC may equivalently choose θ_0 and θ_1 to minimize its probability of error. Therefore AFC attempts to solve the following constrained

optimization problem.

$$
\begin{aligned}
P2: \quad & \min_{k^a,\theta_0,\theta_1} P_E(k^a,\theta_0,\theta_1) && (2.14)\\
& \text{subject to:} \\
& \quad 0 \le k^a \le n && (2.15)\\
& \quad \theta_1 \le \theta_0 && (2.16)\\
& \quad e_{min} \le P_E^t(k^t,\theta_0,\theta_1) \le 0.5 && (2.17)\\
& \quad \theta_0-\theta_1 \le \theta_0 P_1^* - \theta_1 P_0^* && (2.18)\\
& \quad \theta_0 P_1^* - \theta_1 P_0^* \le P_1^* - P_0^*. && (2.19)
\end{aligned}
$$

In the above, (2.16) excludes the cases where $P_E^t(k^a,\theta_0,\theta_1) \geq 0.5$ that are not of interest (see Figure 2.4). In (2.17), e_{min} is a design parameter to ensure a minimum probability of error for TPFC. Moreover, since TPFC makes a binary decision, the case of $P_E^t \geq 0.5$ is not of interest. Finally, (2.18) and (2.19) correspond to the fact that $\pi_1 \geq 0$ and $\pi_0 \geq 0$, respectively. These can be simply derived from (2.3).

Having computed the optimal values of θ_0 and θ_1 from P2, the cipher probabilities π_0 and π_1 can be obtained from (2.3). In the following we pursue analytical solutions to P1 and P2 in the same order.

2.3 Optimization for TPFC

This problem has been investigated in [33] where an algorithm has been proposed that consists of two steps: First, for each $0 \leq k \leq n$ the optimum threshold λ_k, which minimizes P_E, is computed. Then k^t and λ^* are selected as the pair (k, λ_k) that achieves the minimum P_E among all such pairs. The following theorem in [33] shows that gradient based methods can be sued for the computation of the optimum λ_k.

Theorem 1. *Given k, $P_E(k, 1-P_0, 1-P_1)$ is a quasi-convex function of λ and there is a unique λ that minimizes it.*

Proof See [33, Theorm 1]. ■

When n is large, the computational complexity of the above algorithm becomes prohibitive. Below an alternative algorithm is proposed to compute k^t and λ^* by approximating the binomial function in (2.12) with the Q function.

2.3.1 Alternative Algorithm for TPFC Optimization

For large n (e.g $n \geq 20$), $\psi(k,\theta)$ can be well approximated by [20]

$$\psi(k,\theta) \approx Q(\frac{(k-0.5)/n-(1-\theta)}{\sqrt{\theta(1-\theta)/n}}) - Q(\sqrt{\frac{n\theta}{1-\theta}}) \tag{2.20}$$

The following lemma provides justification for gradient-based algorithms for obtaining the optimal solution for k^t.

Lemma 1. *For any θ_0 and θ_1, there is only a unique k that minimizes $P_E(k,\theta_0,\theta_1)$.*

Proof This results from the concavity of the ROC curve corresponding to the k-out-of-n fusion rule and has been discussed in detail in [30]. ∎

Using the approximation in (2.20), the error probability can be written as a function of $\rho \triangleq (k-0.5)/n$ and λ as

$$\begin{aligned} P_E(\rho, 1-P_0(\lambda), 1-P_1(\lambda)) = \; & q_0 \left[Q(\frac{\rho - P_0}{\sqrt{P_0(1-P_0)/n}}) - Q(\sqrt{\frac{n(1-P_0)}{P_0}}) \right] + \\ & q_1 \left[1 - Q(\frac{\rho - P_1}{\sqrt{P_1(1-P_1)/n}}) + Q(\sqrt{\frac{n(1-P_1)}{P_1}}) \right] \end{aligned} \tag{2.21}$$

Then one can calculate the partial derivatives of P_E with respect to ρ and λ and set them to zero. This results in two nonlinear equations that can be solved efficiently using numerical methods. However, since $0 \leq \lambda < \infty$ does not have a finite range, such methods become very sensitive to the initial choice for λ. To overcome this problem, we replace λ by P_0 as the independent variable ($0 \leq P_0 \leq 1$). Then P_1 is a monotone-increasing function of P_0 whose derivative with respect to P_0 can be obtained from the sensors' ROC curve. Thus the following set of equations are used to obtain the optimal P_0 and ρ (denoted P_0^* and ρ^*, respectively).

$$\nabla_{(P_0,\rho)} P_E(\rho, 1-P_0, 1-P_1) = 0 \tag{2.22}$$

Finally, λ^* and k^t can be obtained from P_0^* and ρ^* according to

$$k^t = \lceil 0.5 + n\rho^* \rceil \quad , \quad \lambda^* = \left. \frac{dP_1}{dP_0} \right|_{P_0^*}$$

2.4 Optimization for AFC

The optimization for AFC is more complicated than for TPFC due to the additional constraints. A graphical representation of the constraints is provided below which helps us in obtaining the optimal solution analytically. Given k^t and λ^*, the shaded area in Figure 2.5 demonstrates the feasible values for θ_0 and θ_1 with respect to the constraints in (2.16)-(2.19). As depicted in Figure 2.5, the three constraints in (2.16), (2.18) and

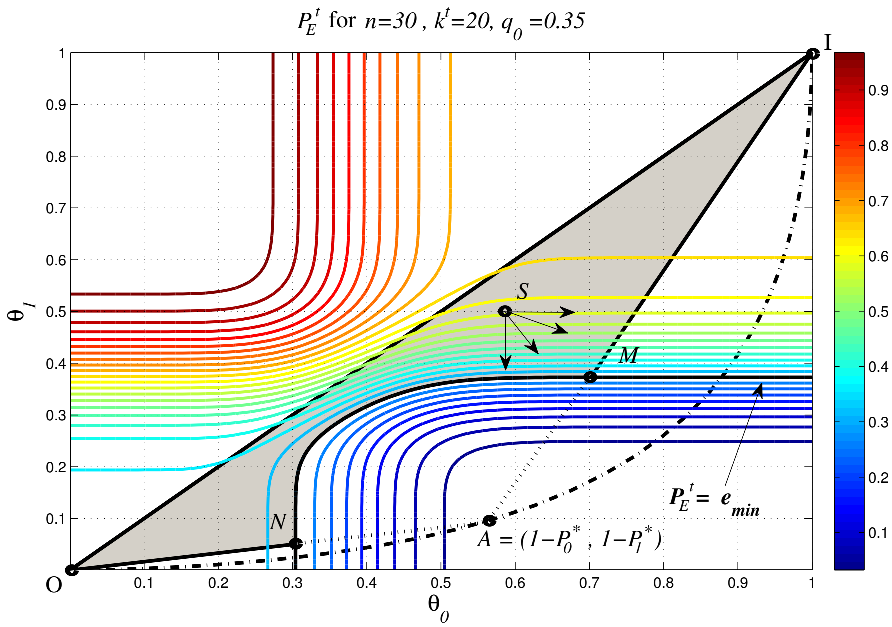

Figure 2.5: The feasible region for AFC optimization

(2.19) form the triangle ΔOIA in which the set of feasible points (θ_0, θ_1) must reside. The dashed trajectory represents the curve $(1 - P_0(\lambda), 1 - P_1(\lambda))$ (as λ varies) and the point A corresponds to λ^*. This triangle is always obtuse and resides above the dashed curve due to the concavity of this curve. The three sides OI, OA, and AI correspond to the boundaries of the three constraints in (2.16) where $\theta_0 = \theta_1$, (2.18) where $\pi_1 = 0$, and (2.19) where $\pi_0 = 0$, respectively. In Figure 1 we have also included the contours of constant P_E^t such that depending on the value of e_{min} in (2.17), one of these contours may play an active role on the set of feasible (θ_0, θ_1). A typical example of such a constraint is indicated by the arc MN in Figure 2.5. Considering this constraint some portion of ΔOIA around the vertex A is excluded from the feasible set of (θ_0, θ_1). Before proposing an analytical optimization, we can further restrict the feasible region through the following lemma.

Lemma 2. *An optimal pair of* (θ_0, θ_1) *meets at least one of the three constraints in* (2.17), (2.18) *and* (2.19), *with equality.*

Proof Consider the point S within the shaded region in Figure 2.5, where all the constraints are met with inequality, and suppose S is an optimal point. Calculating the partial derivatives of $P_E(k, \theta_0, \theta_1)$ with respect to θ_0 and θ_1, we can show that it is a monotone-decreasing function of θ_0 and a monotone-increasing function of θ_1. This is true independent of the value of k. Thus, moving S toward south east in the direction of the arrows in Figure 2.5 will reduce the objective function $P_E(k^a, \theta_0, \theta_1)$. This violates the optimality of S. Clearly, such changes are possible unless S satisfies one of the constraints (2.17)-(2.19) with equality. ■

The above lemma limits the solution region to be along a path such as $ONMI$ in Figure 2.5.

The solution to P2 must satisfy the Karush-Khun-Tucker (KKT) conditions. Avoiding trivial solutions and considering Lemma 2, the augmented objective function is written as

$$\begin{aligned}\boldsymbol{J} =& P_E(k^a, \theta_0, \theta_1) + \zeta_1(e_{min} - P_E(k^t, \theta_0, \theta_1))+ \\ & \zeta_2((1-P_1^*)\theta_0 - (1-P_0^*)\theta_1)+ \\ & \zeta_3((1-\theta_1)P_0^* - (1-\theta_0)P_1^*)\end{aligned} \tag{2.23}$$

where $\zeta_1, \zeta_2, \zeta_3 \geq 0$, are the multipliers corresponding to the constraints in (2.17)-(2.19), respectively. From KKT conditions, $\zeta_i = 0$ implies that the optimal solution meets the corresponding constraint with inequality (inactive constraint) [5]. Then an optimal pair (θ_0, θ_1) must satisfy the following equations along with the constraints.

$$\nabla_{(\theta_0,\theta_1)}\boldsymbol{J} = 0 \tag{2.24}$$

$$k^a(\theta_0, \theta_1) = \left\lceil \frac{\ln\frac{q_0}{q_1} - n\ln\frac{\theta_1}{\theta_0}}{\ln\frac{\theta_0(1-\theta_1)}{\theta_1(1-\theta_0)}} \right\rceil \tag{2.25}$$

$$\frac{\partial \boldsymbol{J}}{\partial \zeta_i} = 0 \qquad \text{for} \quad \zeta_i \neq 0 \tag{2.26}$$

A remark is in order. The KKT condition for k^a cannot be written in terms of derivatives as k^a is integer valued. However, examination of (2.23) reveals that the k^a which minimizes the augmented objective function $\boldsymbol{J}$ is the same as that which minimizes the cost function in (2.14), namely $P_E(k^a, \theta_0, \theta_1)$. On the other hand, the minimizing k^a for $P_E(k^a, \theta_0, \theta_1)$ can be obtained from the maximum a posteriori (MAP) rule from (2.9) and is given by (2.25). Note that (2.24)-(2.26) should be viewed as a set of simultaneous equations for the optimal solution.

The following two lemmas and Theorem 2 completely characterize the optimal solution for (θ_0, θ_1).

Lemma 3. *An optimal* (θ_0, θ_1) *cannot satisfy only* (2.17) *with equality and* (2.18)-(2.19) *with inequality, i.e, in* (2.23) *we cannot have* $\zeta_1 \neq 0$*, and* $\zeta_2 = \zeta_3 = 0$.

Proof Suppose that $P_E(k^t, \theta_0, \theta_1) = e_{min}$ is the only constraint met with equality. Thus the KKT augmented cost function in (2.23) is reduced to the following

$$\boldsymbol{J} = P_E(k^a, \theta_0, \theta_1) + \zeta_1(e_{min} - P_E(k^t, \theta_0, \theta_1)) \tag{2.27}$$

We now set the partial derivatives of $\boldsymbol{J}$ with respect to θ_0 and θ_1 to zero, as in (2.24). This yields the following pair of equations.

$$\begin{aligned} nq_0 \binom{n-1}{k^a-1}(1-\theta_0)^{k^a-1}\theta_0^{n-k^a} &= \\ \zeta_1 nq_0 \binom{n-1}{k^t-1}(1-\theta_0)^{k^t-1}\theta_0^{n-k^t}&. \end{aligned} \tag{2.28}$$

$$\begin{aligned} nq_1 \binom{n-1}{k^a-1}(1-\theta_1)^{k^a-1}\theta_1^{n-k^a} &= \\ \zeta_1 nq_1 \binom{n-1}{k^t-1}(1-\theta_1)^{k^t-1}\theta_1^{n-k^t}&. \end{aligned} \tag{2.29}$$

Then dividing (2.28) by (2.29) we get

$$(\frac{1-\theta_0}{1-\theta_1})^{k^a-k^t} = (\frac{\theta_0}{\theta_1})^{k^a-k^t} \tag{2.30}$$

Since $k^a \neq k^t$, the above equation implies that $\theta_0 = \theta_1$ which, in view of the fact that $\pi_0 + \pi_1 < 1$, cannot hold. Thus it is impossible for the optimal solution to solely meet (2.17) with equality. ■

Using the illustration in Figure 2.5, Lemma 3 implies that if the optimal solution resides on the arc MN, then it can only be at M or N.

Lemma 4. *An optimal* (θ_0, θ_1) *cannot only satisfy either* (2.18) *or* (2.19) *with equality and the remaining constraints with inequality, i.e, in* (2.23) *we cannot have* $\zeta_2 \neq 0, \zeta_1 = \zeta_3 = 0$, *or* $\zeta_3 \neq 0, \zeta_1 = \zeta_2 = 0$.

Proof Suppose that (2.18) is the only constraint met with equality implying that $\pi_1(\theta_0, \theta_1) = 0$. Thus the KKT augmented objective function in (2.23) is now given by

$$\boldsymbol{J} = P_E(k^a, \theta_0, \theta_1) + \zeta_2((1 - P_1^*)\theta_0 - (1 - P_0^*)\theta_1) \tag{2.31}$$

Again we calculate the partial derivatives of $\boldsymbol{J}$ with respect to θ_0 and θ_1 and set them to

zero. Dividing the resulting equations as in the proof for Lemma 3 we get

$$\frac{q_0}{q_1}\,(\frac{\theta_0}{\theta_1})^{n-k^a}(\frac{1-\theta_0}{1-\theta_1})^{k^a-1} = \frac{1-P_1^*}{1-P_0^*} \tag{2.32}$$

Moreover from $\pi_1(\theta_0, \theta_1) = 0$ we get

$$\frac{1-P_1^*}{1-P_0^*} = \frac{\theta_1}{\theta_0} \tag{2.33}$$

Therefore,

$$\frac{q_0}{q_1}\,(\frac{\theta_0}{\theta_1})^{n-k^a}(\frac{1-\theta_0}{1-\theta_1})^{k^a-1} = \frac{\theta_1}{\theta_0} \tag{2.34}$$

This, however, implies that

$$\frac{\ln\frac{q_0}{q_1} - n\ln\frac{\theta_1}{\theta_0}}{\ln\frac{\theta_0(1-\theta_1)}{\theta_1(1-\theta_0)}} = k^a - 1 \tag{2.35}$$

which contradicts (2.25). Consequently, the initial assumption is incorrect so (2.18) cannot be the only constraint met with equality by the optimal solution. A similar argument can be used in the case of (2.19). ■

Again Lemma 4 implies that if the optimal solution resides on line ON, (resp. MI), then it must be at N (resp. M). The following theorem summarizes the above lemmas and completely characterizes the optimal solution to (2.14)-(2.19).

Theorem 2. *The optimal solution for* (θ_0, θ_1) *satisfies* (2.17) *and either* (2.18) *or* (2.19) *with equality.*

According to Theorem 2 the optimal solution of P2 lies where $P_E^t = e_{min}$ contour intersects the lines $\pi_0(\theta_0, \theta_1) = 0$ and $\pi_1(\theta_0, \theta_1) = 0$, i.e., the point M or N in Figure 2.5. Depending on the choice of e_{min} there are one or two such intersection points. The contours of $P_E(k^a(\theta_0, \theta_1), \theta_0, \theta_1)$ have been drawn in Figure 2.6, where $k^a(\theta_0, \theta_1)$ is the MAP rule threshold assigned in (2.25). The feasible region indicated in Figure 2.6 is the same as what in Figure 2.5. In Figure 2.6, one can verify that the points M and N are the only points in the feasible region which are likely to produce the least error probability. Therefore, the optimal solution can be obtained by solving the following two nonlinear equations simultaneously using some efficient numerical method.

$$\begin{cases} P_E^t(k^t, \theta_0, \theta_1) = e_{min} \\ \pi_0(\theta_0, \theta_1)\ \pi_1(\theta_0, \theta_1) = 0 \end{cases} \tag{2.36}$$

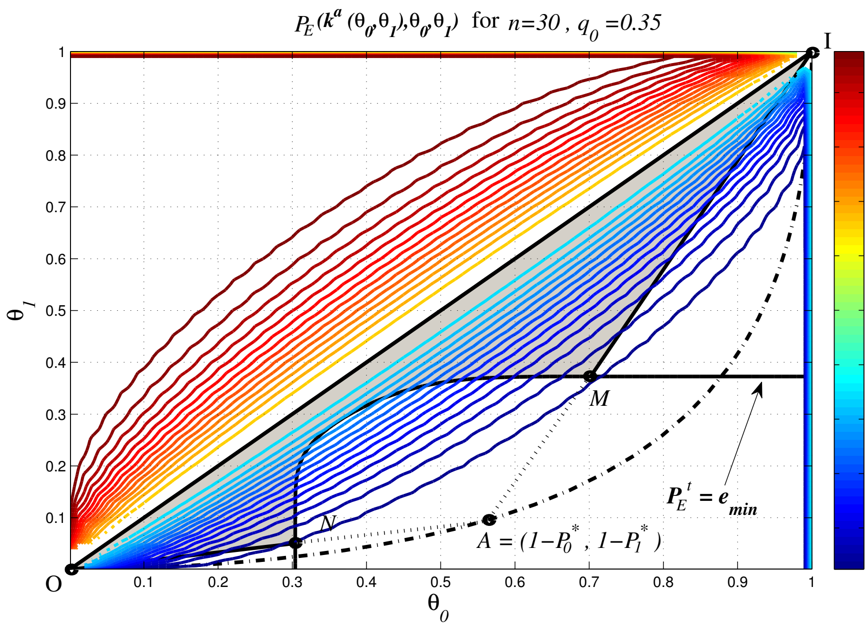

Figure 2.6: The error probability for the MAP rule practicing AFC

where

$$\pi_0(\theta_0, \theta_1) = \frac{(1-\theta_0)P_1 - (1-\theta_1)P_0}{P_1 - P_0} \tag{2.37}$$

$$\pi_1(\theta_0, \theta_1) = \frac{(1-P_0)\theta_1 - (1-P_1)\theta_0}{P_1 - P_0} \tag{2.38}$$

2.5 Numerical Results

Consider the case of additive Gaussian noise where the signal X_i received by sensor i is given by

$$X_i = s + N_i,$$

where $s = d$ under hypothesis H_1, $s = -d$ under hypothesis H_0, and where $\{N_i\}_{i=1}^n$ are iid Gaussian random variables with mean zero and variance σ^2. Then each sensor node makes a decision according to (2.1) with the preassigned threshold λ^*. The detection and the false alarm probabilities for any individual sensor are given by

$$P_0 = Q\left(\frac{\lambda^* + d}{\sigma}\right), \quad P_1 = Q\left(\frac{\lambda^* - d}{\sigma}\right)$$

We define $\gamma = 20\log(d/\sigma)$ as the sensors' detection quality factor. It can be seen that larger γ implies a lower P_0 and a higher P_1 which finally reduces the error probability of

Table 2.1: AFC Optimized Performance

n	γ (dB)	q_0	P_E^t	P_E^a	π_0	π_1	k^a
20	3	0.50	0.30	4.38 e-03	0.48	0	16
20	3	0.30	0.30	3.10 e-03	0	0.48	4
20	6	0.50	0.40	1.76 e-03	0.56	0	18
40	0	0.50	0.50	8.45 e-03	0	0.60	7
40	3	0.50	0.30	9.83 e-05	0	0.47	9
40	3	0.50	0.40	2.38 e-04	0.52	0	33
40	3	0.50	0.50	9.61 e-04	0	0.61	6
40	3	0.30	0.30	6.74 e-05	0	0.45	9
40	6	0.50	0.50	6.82 e-05	0	0.62	5
80	-3	0.50	0.50	7.81 e-04	0	0.45	22
80	0	0.50	0.50	3.05 e-05	0.37	0	50

the fusion centers. Therefore γ may be viewed as the SNR for individual sensors. Table 2.1 shows the performance of the proposed algorithm for several values of n, γ and q_0. It can be seen from Table 2.1 that using the proposed method, very low error probabilities can be achieved at AFC while imposing high error probabilities on TPFC.

Clearly for smaller values of e_{min} the constraint for error probability of TPFC, P_E^t is less stringent. As can be seen, in such cases lower values of P_E^a can be achieved. Furthermore, we note that when $q_0 = 0.30$, the optimization results in $\pi_0 = 0$, which indicates that messages corresponding to H_0 do not need to be encrypted since this event is less likely to happen.

We have assumed that TPFC is aware of the priors q_0 and q_1. Therefore, the worst case error probability for TPFC is given by $P_{\max}^t = \min\{q_0, q_1\}$, which results if TPFC completely ignores the sensors' transmissions and chooses the more likely hypothesis. Table 2.1 shows that this worst case scenario can be imposed on TPFC to ensure that $P_E^t = P_{\max}^t$. This implies that TPFC gains no information from the observation of sensors' transmissions.

In some scenarios it may be possible for TPFC to estimate the encryption keys π_0 and π_1 from the sensor transmissions. To defeat such strategies by TPFC, the sensors can periodically change their key and still impose high probability of error on TPFC. For example in Table 2.1 for the case of $n = 40$, $\gamma = 3$ dB and $q_0 = .50$, the sensors can periodically cycle through the encryption keys $\pi_1 = .47$, $\pi_0 = .52$ and $\pi_1 = .61$ resulting in the error probabilities of $P_E^t = .30, .40$ and $.50$ for TPFC. In this case AFC must also change its decision threshold k^a accordingly.

2.5.1 Computational Issues

When n is large (e.g $n \geq 40$), the first equation in (2.36) become a polynomial equation with very large coefficient that cannot be solved thorough ordinary numerical methods. We can apply approximation to reduce computational complexity. As depicted in Figure 2.5 the contour of $P_E^t = e_{min}$ can be well approximated by flat lines away from $\theta_0 = \theta_1$ line. This can be verified by calculating $\frac{d\theta_0}{d\theta_1}$ which repents the slope of local tangents along the contour of $P_E^t = e_{min}$.

$$\frac{d\theta_0}{d\theta_1} = \frac{q_0(1-\theta_0)^{k-1}\theta_0^{n-k}}{q_1(1-\theta_1)^{k-1}\theta_1^{n-k}} \tag{2.39}$$

When $n \gg 1$ and $0 < k/n < 1$, apparently the above function has a zero and a pole, respectively at $\theta_0 = 1$ and $\theta_1 = 0$ with high multiplicity. This multiplicity allows us to approximate the $P_E^t = e_{min}$ contour with flat lines where $P_E(k^t, 1, \theta_1) = e_{min}$ or $P_E(k^t, \theta_0, 0) = e_{min}$. Considering this together with (2.36) and (2.20), the following set of equation formed to find the intersection points.

$$\begin{cases} (q_0\psi(k^t, \theta_0) - e_{min})(q_1(1 - \psi(k^t, \theta_1)) - e_{min}) = 0 \\ \pi_0(\theta_0, \theta_1)\pi_1(\theta_0, \theta_1) = 0 \end{cases} \tag{2.40}$$

In the above table for $n = 80$ we have used the approximate solution as in (2.40).

Chapter 3

Secure Distributed Detection Using Soft Decision at the Sensors

In this chapter we first describe the distributed detection problem and the operation of the sensors in the case where the sensors quantize their local observations (soft decision). Next we discuss the encryption mechanism used by each node and approximate the error probabilities of both the AFC and TPFC where a large number of sensors are deployed. Similarly to Chapter 2, we assume the fusion centers perform Bayesian detection. The TPFC, which is unaware of the encryption, assumes that the sensors transmit their raw decisions. Knowing the quantization rule of the sensors, it adopts its fusion rule in order to minimize its assumed error probability. The AFC can also perform the same optimization and, therefore, is aware of the TPFC's decision rule. The AFC then explores the fusion rule and the encryption which minimize its error probability, subject to a minimum error probability constraint on the TPFC. The resulting optimization problem is mathematically intractable due to the complexity of the cost function and the constraints. We first deal with the nonlinear constraint belonging to the lower bound on the TPFC error probability. Despite Chapter 2 we try to simplify the problem and suffice to a suboptimal solution. In this regard we formulate a simple optimization problem, similar to section 2.4, whose solution translates the nonlinear constraint into a set of linear constraints. To avoid the complexity in the cost function, we use a simpler cost function which is asymptotically associated with the AFC error probability. Finally in the section on numerical results, the deterministic signal detection in the presence of Gaussian noise is examined using both the binary and soft decision at the sensors. For a given lower bound on the TPFC error probability and identical noise in the sensors, a comparison is made between the numerical results for the two cases error probability. It indicates that the soft decision system is superior, in terms of the AFC error performance and the proportional increase in the AFC error probability for the same TPFC error probability.

3.1 System Model

We consider a system of n sensors observing the state of an unknown hypothesis H where $H \in \{H_0, H_1\}$ and with prior probabilities of H_0 and H_1 being q_0 and q_1, respectively. Let X_i denote the observation of the ith sensor, $i = 1, 2, 3, ..., n$. It is assumed that given the hypothesis H_η, $(\eta = 0, 1)$, the observations $X_1, X_2, \cdots, X_n$ are independent and identically distributed. The conditional PDF of X_i under H_η is denoted by $p_\eta(x)$. It is assumed that sensor i quantizes its observation X_i using an M-level quantizer $\mathcal{Q}$ such that $\mathcal{Q}(X_i) \in \mathcal{L} \triangleq \{l_1, l_2, \cdots, l_M\}$ for $i = 1, 2, \cdots, n$. The quantizer uses the thresholds $t_0, t_1, \cdots, t_M$ such that

$$\mathcal{Q}(x_i) = l_j \quad \text{if} \quad t_{j-1} < X_i \leq t_j,$$

where $t_0 = -\infty$ and $t_M = \infty$. Let

$$a_\eta(l_j) \triangleq P(\mathcal{Q}(X_i) = l_j | H_\eta) = P(t_{j-1} < X_i \leq t_j | H_\eta), \quad j = 1, 2 \cdots, M, \quad \eta = 0, 1 \tag{3.1}$$

An example is depicted in Figure 3.1 for $M = 8$, where the thresholds are uniformly designed. Since the quantization process depends on the sensors' built-in technology, hereafter it is assumed that $a_\eta(l_j)$ for $j = 1, 2, \cdots, M$ are fixed and known to both the AFC and TPFC. The optimal selection of the quantizer is investigated in [18]. The decision rule of the sensors can be modeled as a discrete memoryless model which is exhibited in Figure 3.2 for $M = 4$ [30]. Again we assume that the channel between the sensors and the

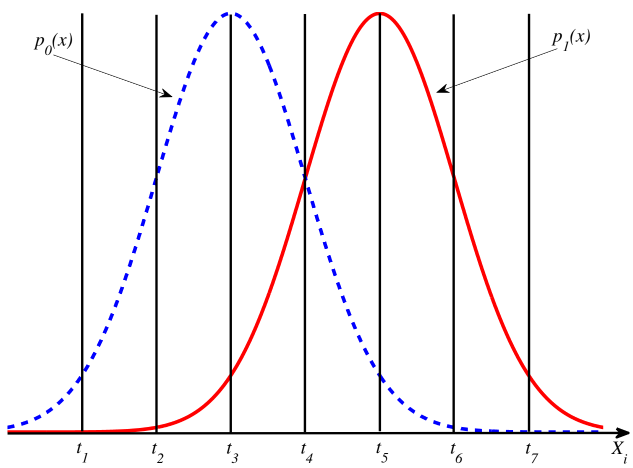

Figure 3.1: 8-level quantizer

FCs is error free which can be achieved using an appropriate error control coding scheme. In order to protect the decisions of the sensors from the TPFC during transmission, we employ the following simple probabilistic cipher at the sensors. As depicted in Figure 3.3,

the decision $\mathcal{Q}(X_i)$ of sensor i is randomly encrypted to obtain Y_i, such that

$$\phi_{jk} \triangleq P(Y_i = l_k | \mathcal{Q}(X_i) = l_j) \qquad j, k = 1, 2, \cdots, M. \tag{3.2}$$

The encrypted messages Y_i, $i = 1, 2, \cdots, n$, are then transmitted to the allied fusion center (AFC) over an insecure link. For $\eta = 0, 1$ let

$$b_\eta(l_j) \triangleq P(Y_i = l_j | H_\eta), \quad j = 1, 2 \cdots, M. \tag{3.3}$$

Clearly $b_\eta(l_j) = \sum_{i=1}^{M} a_\eta(l_i)\phi_{ij}$. For ease of notation, let

$$\boldsymbol{\alpha}_\eta \triangleq (a_\eta(l_1), a_\eta(l_2), \cdots, a_\eta(l_M)) \quad , \quad \boldsymbol{\beta}_\eta \triangleq (b_\eta(l_1), b_\eta(l_2), \cdots, b_\eta(l_M))$$

which denote the conditional probability mass functions (p.m.f's) of, respectively, $\mathcal{Q}(X_i)$ and Y_i. This also enables us to view the ciphering process as a linear operation,

$$\boldsymbol{\beta}_\eta = \boldsymbol{\alpha}_\eta \boldsymbol{\Phi} \ , \quad \text{where} \quad \boldsymbol{\Phi} \triangleq \begin{pmatrix} \phi_{11} & \phi_{12} & \cdots & \phi_{1M} \\ \phi_{21} & \phi_{22} & \cdots & \phi_{2M} \\ \vdots & \vdots & \cdots & \vdots \\ \phi_{M1} & \phi_{M2} & \cdots & \phi_{MM} \end{pmatrix}_{M \times M} . \tag{3.4}$$

Similarly to the binary case, it is assumed that the AFC has a priori knowledge of the encryption matrix $\boldsymbol{\Phi}$. On the other hand, TPFC has no knowledge of $\boldsymbol{\Phi}$ and therefore, it can only assume that it has received the original decisions $\mathcal{Q}(X_i)$, $i = 1, 2, \cdots, n$, i.e. it assumes $\boldsymbol{\Phi} = \boldsymbol{I}_{M \times M}$. We again consider a Bayesian detection problem where our goal is to design the system parameters so as to minimize P_E^a, the probability of error for the AFC, subject to a lower bound on P_E^t, the probability of error for the TPFC. The optimum

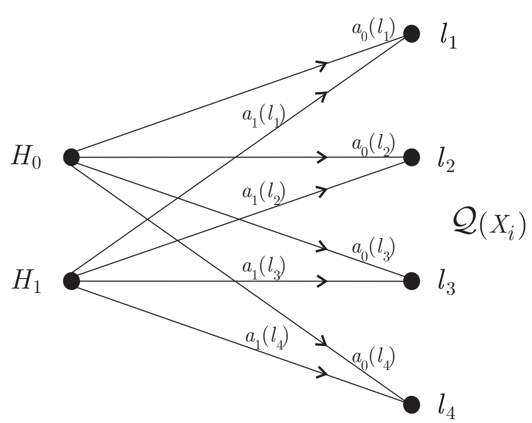

Figure 3.2: Quantization model for $M = 4$

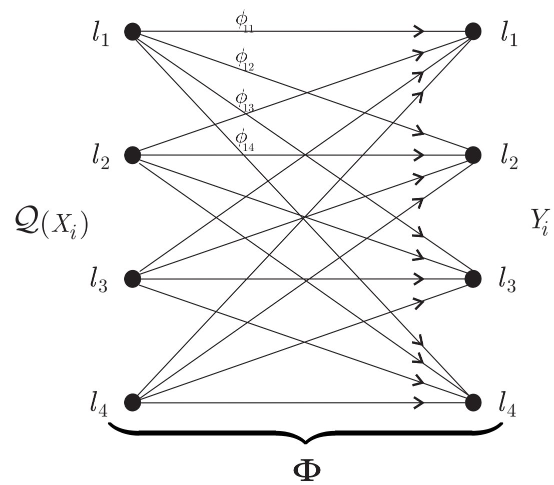

Figure 3.3: Cipher model for $M = 4$

decision rule for the two fusion centers is given by the likelihood ratio test, [30], where for a received $\mathbf{y} = (y_1, y_2, \cdots, y_n)$,

$$T(\mathbf{y}) \triangleq \frac{1}{n}\sum_{i=1}^{n} z_i \quad \underset{H_0}{\overset{H_1}{\gtrless}} \quad \tau \tag{3.5}$$

where for the AFC

$$\tau = \tau^a, \quad \text{and} \quad z_i \triangleq \log\left(\frac{b_1(y_i)}{b_0(y_i)}\right) \tag{3.6}$$

and for the TPFC

$$\tau = \tau^t, \quad \text{and} \quad z_i \triangleq \log\left(\frac{a_1(y_i)}{a_0(y_i)}\right). \tag{3.7}$$

The error probability for the two fusion centers is given by

$$P_E = q_0 P(T(\boldsymbol{Y}) \geq \tau | H_0) + q_1 P(T(\boldsymbol{Y}) < \tau | H_1) \tag{3.8}$$

where the AFC and TPFC use their respective decision statistic $T(\mathbf{Y})$ and threshold τ. It can be seen that the values of the quantization levels, l_j , $j = 1, 2, \cdots, M$ do not affect the error probabilities. The block diagram for the fusion rule is displayed in Figure 3.4, where the log-likelihood-ratio convertor block stands for the operations in (3.6) and (3.7). Invoking the central limit theorem, [20], for the test statistic we get that for large n and

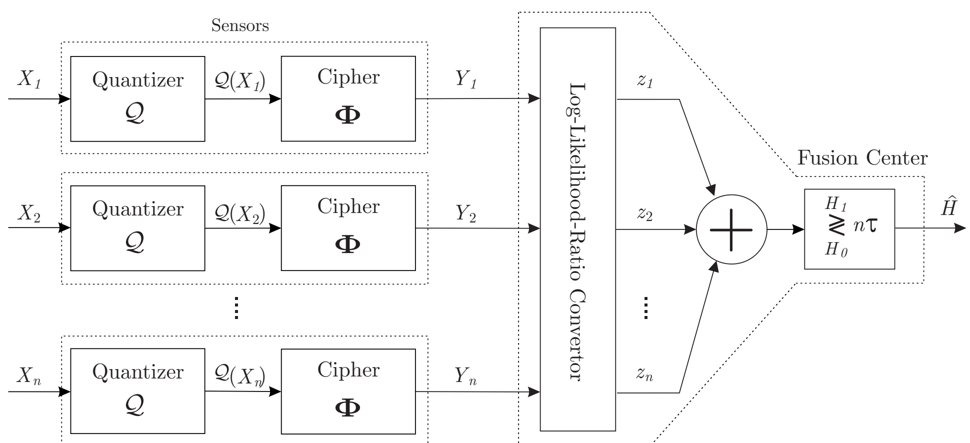

Figure 3.4: Block digram for the soft data fusion

conditioned on H_η,

$$T(\mathbf{Y}|H_\eta) \sim \mathcal{N}(\mu_\eta,\ \sigma_\eta^2/n) \tag{3.9}$$

where,

$$\mu_\eta = \mathrm{E}_{\boldsymbol{\beta}_\eta}\left[\log\left(\frac{b_1(Y_i)}{b_0(Y_i)}\right)\right] \triangleq \mu_\eta^a \quad , \quad \sigma_\eta^2 = \mathrm{Var}_{\boldsymbol{\beta}_\eta}\left[\log\left(\frac{b_1(Y_i)}{b_0(Y_i)}\right)\right] \triangleq (\sigma_\eta^a)^2 \tag{3.10}$$

for the AFC and

$$\mu_\eta = \mathrm{E}_{\boldsymbol{\beta}_\eta}\left[\log\left(\frac{a_1(Y_i)}{a_0(Y_i)}\right)\right] \triangleq \mu_\eta^t \quad , \quad \sigma_\eta^2 = \mathrm{Var}_{\boldsymbol{\beta}_\eta}\left[\log\left(\frac{a_1(Y_i)}{a_0(Y_i)}\right)\right] \triangleq (\sigma_\eta^t)^2 \tag{3.11}$$

for the TPFC, where the subscripts for the operators E and Var indicate the distributions under which these are computed.

However, TPFC does not adjust its fusion rule with respect to μ_η^t and σ_η^t. It assumes $\boldsymbol{\Phi} = \boldsymbol{I}_{M\times M}$ and evaluates its error probability based on the raw statistics.

$$\mu_\eta^r \triangleq \mathrm{E}_{\boldsymbol{\alpha}_\eta}\left[\log\left(\frac{a_1(Y_i)}{a_0(Y_i)}\right)\right] \quad , \quad (\sigma_\eta^r)^2 \triangleq \mathrm{Var}_{\boldsymbol{\alpha}_\eta}\left[\log\left(\frac{a_1(Y_i)}{a_0(Y_i)}\right)\right] \tag{3.12}$$

The probability of error for the two fusion centers can be approximated by

$$P_E \approx P_e(\tau, \mu_0, \mu_1, \sigma_0, \sigma_1) = q_0 Q(\frac{\sqrt{n}(\tau-\mu_0)}{\sigma_0}) + q_1(1 - Q(\frac{\sqrt{n}(\tau-\mu_1)}{\sigma_1})), \tag{3.13}$$

where τ, μ and σ take on the values corresponding to each fusion center.

To see the dependency of the above parameters on $\boldsymbol{\Phi}$ more explicitly, let us define the following functions which take two row vectors as arguments and produce new row vectors of the same length.

$$\boldsymbol{r} \triangleq \xi(\boldsymbol{u}, \boldsymbol{v}) \ , \ \text{where} \ \ r_i = log\left(\frac{u_i}{v_i}\right) \tag{3.14}$$

$$\boldsymbol{s} \triangleq \omega(\boldsymbol{u}, \boldsymbol{v}) \ , \ \text{where} \ \ r_i = log^2\left(\frac{u_i}{v_i}\right). \tag{3.15}$$

The above functions allow us to two rewrite the parameters in (3.10)-(3.12) using (3.4)

$$\mu_\eta^a = \boldsymbol{\alpha}_\eta \boldsymbol{\Phi} \xi(\boldsymbol{\alpha}_1\boldsymbol{\Phi}, \boldsymbol{\alpha}_0\boldsymbol{\Phi})^T \ , \ (\sigma_\eta^a)^2 + (\mu_\eta^a)^2 = \boldsymbol{\alpha}_\eta \boldsymbol{\Phi} \omega(\boldsymbol{\alpha}_1\boldsymbol{\Phi}, \boldsymbol{\alpha}_0\boldsymbol{\Phi})^T \tag{3.16}$$

$$\mu_\eta^t = \boldsymbol{\alpha}_\eta \boldsymbol{\Phi} \xi(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_0)^T \ , \ (\sigma_\eta^t)^2 + (\mu_\eta^t)^2 = \boldsymbol{\alpha}_\eta \boldsymbol{\Phi} \omega(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_0)^T \tag{3.17}$$

$$\mu_\eta^r = \boldsymbol{\alpha}_\eta \xi(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_0)^T \ , \ (\sigma_\eta^r)^2 + (\mu_\eta^r)^2 = \boldsymbol{\alpha}_\eta \omega(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_0)^T \tag{3.18}$$

Remark Technically in many detection problems, such as signal detection in the presence of additive noise, the noise distribution is symmetric which results in the conditional distributions of the observed variables X_i to be symmetric (see Figure 3.1). Hereafter we assume that $p_0(x) = p_1(-x)$. This property leads to a symmetric quantization rule [18], such that

$$a_0(l_j) = a_1(l_{M-j+1}), \quad j = 1, 2, \cdots, M. \tag{3.19}$$

Using (3.18), it can be shown that

$$\mu_1^r = -\mu_0^r \quad \text{, and} \quad \sigma_1^r = \sigma_0^r \tag{3.20}$$

In the following we denote $\bar{\mu} = \mu_1^r$ and $\bar{\sigma} = \sigma_1^r$.

3.2 Problem Statement

Both the AFC and TPFC attempt to minimize their error probabilities as cost functions. The TPFC only optimizes its fusion threshold, whereas the AFC deals with a more complicated problem to optimize both its fusion threshold and the encryption probabilities. The TPFC optimization is stated and solved in the subsection below.

3.2.1 Optimization from TPFC's Point of View

As mentioned previously, the TPFC is assumed to be unaware of the encryption process and therefore assumes that $\phi_{ij} = 1$ for $i = j$, and 0 otherwise. However, the TPFC is aware of the conditional probability mass function (pmf) ,$\boldsymbol{\alpha}_\eta$, and chooses its fusion threshold, τ^t, to minimize its probability of error. Therefore the optimal τ^t is obtained from the solution of the following problem.

$$P1: \qquad \min_{\tau} P_e(\tau, \mu_0^r, \mu_1^r, \sigma_0^r, \sigma_1^r) \tag{3.21}$$

Considering (3.13) and (3.19) and (3.20), $P1$ becomes the classic problem of ML detection in the presence of Gaussian noise for which the optimal threshold is given by

$$\tau^t = \frac{\bar{\sigma}^2}{2n\bar{\mu}} \ln \frac{q_0}{q_1} \tag{3.22}$$

The AFC can also solve this problem independently and so it is aware of the values of τ^t. Now in the presence of encryption where $\Phi \neq I$, the actual performance of TPFC is given by

$$P_E^t = P_e(\tau^t, \mu_0^t, \mu_1^t, \sigma_0^t, \sigma_1^t) \tag{3.23}$$

The performance of the TPFC is degraded due to the fact that neither τ^t is not matched to the mean and variances μ_1^t, μ_1^t, σ_0^t and σ_1^t in (3.23).

3.2.2 Optimization from AFC's Point of View

The AFC must choose its fusion threshold τ^a along with the encryption parameters in $\mathbf{\Phi}$, so as to minimize its probability of error. In addition it must ensure that the performance of the TPFC is degraded due to the encryption process. Therefore the AFC attempts to solve the following constrained optimization problem.

$$
\begin{aligned}
P2: \quad & \min_{\tau, \mathbf{\Phi}} P_e(\tau, \mu_0^a, \mu_1^a, \sigma_0^a, \sigma_1^a) && (3.24)\\
& \text{subject to:} \\
& \qquad 0 \leq \mathbf{\Phi} \leq 1 && (3.25)\\
& \qquad \mathbf{\Phi 1}_{M\times 1} = \mathbf{1}_{M\times 1} && (3.26)\\
& \qquad e_{min} \leq P_e(\tau^t, \mu_0^t, \mu_1^t, \sigma_0^t, \sigma_1^t) \leq 0.5 && (3.27)
\end{aligned}
$$

In the above, it is noted that $\mu_\eta^a, \sigma_\eta^a$ and $\mu_\eta^t, \sigma_\eta^t$ depend on $\mathbf{\Phi}$, respectively, according to (3.16) and (3.17). In the equality constraint (3.26) $1_{M\times 1}$ indicates a column vector of all elements equal to 1. It should be considered due to the fact that in (3.4), the rows in $\mathbf{\Phi}$ must add up to 1. The inequalities in (3.25) are obvious since ϕ_{ij} are probabilities. This is included to be used in the sequel. In (3.27), τ^t is available in (3.22) and e_{min} is the lower bound on the TPFC error probability, P_E^t. Moreover, since the TPFC makes a binary decision, the case of $P_E^t \geq 0.5$ is not of interest.

From the complexity viewpoint, the above problem is very complex, particularly because of the nonlinear functions in (3.24) and (3.27). The steep transition of the Q-functions associated with (3.24) and (3.27) makes intractable for many numerical algorithms. By simplifying the cost function and trimming the feasible region, we analytically achieve a reliable suboptimal solution for $\mathbf{\Phi}$ in the following section.

The threshold τ in (3.24) does not contribute in any of the constraints. Therefore, for any given values of $(\mu_0^a, \mu_1^a, \sigma_0^a, \sigma_1^a)$ the optimal threshold for P_e can be either calculated according to the classic ML problem or $\partial P_e / \partial \tau^a = 0$. Both the approaches yield

$$
\frac{(\tau^a - \mu_0^a)^2}{2(\sigma_0^a)^2} - \frac{(\tau^a - \mu_1^a)^2}{2(\sigma_1^a)^2} = \frac{1}{n} \ln\left(\frac{q_0 \sigma_1^a}{q_1 \sigma_0^a}\right). \qquad (3.28)
$$

3.3 AFC Optimization

In this section, we first try to simplify the constraints in $P2$ that leads to a problem similar to the the preceding binary problem. Then we use a surrogate cost function which suits the P_e for a large n. Finally the proposed algorithm is numerically evaluated for an example which verifies its efficiency in terms of the minimum achieved error probability for the AFC.

3.3.1 Simplifying Constraints

The constraint in (3.27) is a function of $(\mu_0^t, \mu_1^t, \sigma_0^t, \sigma_1^t)$. This implies that for a given $(\mu_0^t, \mu_1^t, \sigma_0^t, \sigma_1^t)$ satisfying (3.27), the elements in $\mathbf{\Phi}$ only must satisfy the linear equations in (3.17). Before clarifying this, lets set the following condition on $(\mu_0^t, \mu_1^t, \sigma_0^t, \sigma_1^t)$ to deal only with (μ_0^t, μ_1^t) in our next arguments. Hereafter we choose $(\mu_0^t, \mu_1^t, \sigma_0^t, \sigma_1^t)$ such that

$$(\sigma_\eta^t)^2 + (\mu_\eta^t)^2 = \bar{\sigma}^2 + \bar{\mu}^2 \triangleq \nu^2 \quad , \quad \eta = 0, 1 \tag{3.29}$$

where $\bar{\sigma}$ and $\bar{\mu}$ are as termed after (3.20). Since $\bar{\sigma}$ and $\bar{\mu}$ do not depend on $\mathbf{\Phi}$, the value denoted by ν^2 is a constant. Now lets reformulate $P2$ with (3.27) replaced by a pair of linear constraints,

$$\begin{aligned} P2: \qquad & \min_{\mathbf{\Phi}} P_e(\tau^a, \mu_0^a, \mu_1^a, \sigma_0^a, \sigma_1^a) && (3.30)\\ & \text{subject to:} && \\ & \quad 0 \le \mathbf{\Phi} \le 1 && (3.31)\\ & \quad \mathbf{\Phi} \mathbf{1}_{M\times 1} = \mathbf{1}_{M\times 1} && (3.32)\\ & \quad \boldsymbol{\alpha}_\eta \mathbf{\Phi} \xi(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_0)^T = \mu_\eta^t \quad , \quad \eta = 0, 1 && (3.33)\\ & \quad \boldsymbol{\alpha}_\eta \mathbf{\Phi} \omega(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_0)^T = \nu^2 \quad , \quad \eta = 0, 1 && (3.34)\\ & && (3.35) \end{aligned}$$

where μ_η^t and ν are fixed values such that

$$\boldsymbol{\varepsilon}^t(\tau^t, \mu_0^t, \mu_1^t) \triangleq P_e(\tau^t, \mu_0^t, \mu_1^t, \sqrt{\nu^2 - (\mu_0^t)^2}, \sqrt{\nu^2 - (\mu_1^t)^2}) \ge e_{min}. \tag{3.36}$$

It is clear that μ_0^t and μ_1^t implicitly affect the minimum error probability in (3.30) by shaping the feasible region for $\mathbf{\Phi}$. By virtue of the lemma below we can formulate an optimization problem to assign μ_0^t and μ_1^t somewhat optimally.

Lemma 5. *For any given* $(\mu_\eta^a, \sigma_\eta^a)$ *and* $(\mu_\eta^t, \sigma_\eta^t)$,$\eta = 0, 1$,

$$P_e(\tau^a, \mu_0^a, \mu_1^a, \sigma_0^a, \sigma_1^a) \le P_e(\tau^*, \mu_0^t, \mu_1^t, \sigma_0^t, \sigma_1^t) \tag{3.37}$$

where τ^a *is given in* (3.28) *and similarly* τ^* *is obtained from*

$$\frac{(\tau^* - \mu_0^t)^2}{2(\sigma_0^t)^2} - \frac{(\tau^* - \mu_1^t)^2}{2(\sigma_1^t)^2} = \frac{1}{n} \ln\left(\frac{q_0 \sigma_1^t}{q_1 \sigma_0^t}\right). \tag{3.38}$$

Proof For a fixed matrix $\mathbf{\Phi}$, the minimum achievable error probability according to the MAP rule is represented by $P_e(\tau^a, \mu_0^a, \mu_1^a, \sigma_0^a, \sigma_1^a)$ for the test statistics described in (3.5)-(3.6). On the other hand, $P_e(\tau^*, \mu_0^t, \mu_1^t, \sigma_0^t, \sigma_1^t)$ will be the minimum achievable error prob-

ability where the terms in the test statistic are in (3.7) which do not correspond to the MAP rule anymore. Due to the optimality of the MAP rule, it can be concluded that

$$P_e(\tau^a, \mu_0^a, \mu_1^a, \sigma_0^a, \sigma_1^a) \leq P_e(\tau^*, \mu_0^t, \mu_1^t, \sigma_0^t, \sigma_1^t)$$

■

The upper bound suggested by Lemma 5 explicitly contains μ_0^t and μ_1^t, so can be used to find close to optimal values for μ_0^t and μ_1^t, the optimization problem below can be considered which minimized the upper bound in Lemma 5.

$$P2-1: \quad \min_{\mu_0^t, \mu_1^t} P_e(\tau, \mu_0^t, \mu_1^t, \sqrt{\nu^2 - (\mu_0^t)^2}, \sqrt{\nu^2 - (\mu_1^t)^2}) \tag{3.39}$$

subject to:

$$0 \leq \mathbf{\Phi} \leq 1 \tag{3.40}$$

$$\mathbf{\Phi}\mathbf{1}_{M\times 1} = \mathbf{1}_{M\times 1} \tag{3.41}$$

$$\boldsymbol{\alpha}_\eta \mathbf{\Phi} \xi(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_0)^T = \mu_\eta^t \quad , \quad \eta = 0, 1 \tag{3.42}$$

$$\boldsymbol{\alpha}_\eta \mathbf{\Phi} \omega(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_0)^T = \nu^2 \quad , \quad \eta = 0, 1 \tag{3.43}$$

$$e_{min} \leq \boldsymbol{\varepsilon}^t(\tau^t, \mu_0^t, \mu_1^t) \leq 0.5 \tag{3.44}$$

where the constraint in (3.44) correspond to that one in (3.36). At above, it is obvious that $|\mu_\eta^t| \leq |\nu|$. Here $\mathbf{\Phi}$ does not appear in the cost function. However, $\mathbf{\Phi}$ incorporates in the constraints in (3.40)-(3.43) to form a feasible region for (μ_0^t, μ_1^t). Let $\mathcal{R}$ denote the feasible region for (μ_0^t, μ_1^t) adopted by (3.40)-(3.43). It is easy to investigate that the region $\mathcal{R}$ is convex in the (μ_0^t, μ_1^t) space [5]. Although the $\mathcal{R}$ is convex, it is difficult to formulate the borders of $\mathcal{R}$ and use them to solve $P2-1$. We will limit the choice of (μ_0^t, μ_1^t) to a subregion of $\mathcal{R}$ with linear borders, disregarding the loss of optimality. Such a subregion can be built using a few points within $\mathcal{R}$. It is noted that

$$G = (-\bar{\mu}, \bar{\mu}) \in \mathcal{R} \quad \text{for} \quad \mathbf{\Phi} = I_{M\times M}.$$

Lets assume that

$$\exists m \ , \ 1 \leq m \leq M \ , \ \text{ s.t. } \log\left(\frac{a_1(l_m)}{a_0(l_m)}\right) = \nu \tag{3.45}$$

The above statement depends on the design of the quantization rule which can be simply implemented in $\mathcal{Q}(X_i)$. According to the symmetric property in (3.19), it is immediately concluded that for such an m

$$\log\left(\frac{a_1(l_{(M-m+1)})}{a_0(l_{(M-m+1)})}\right) = -\nu$$

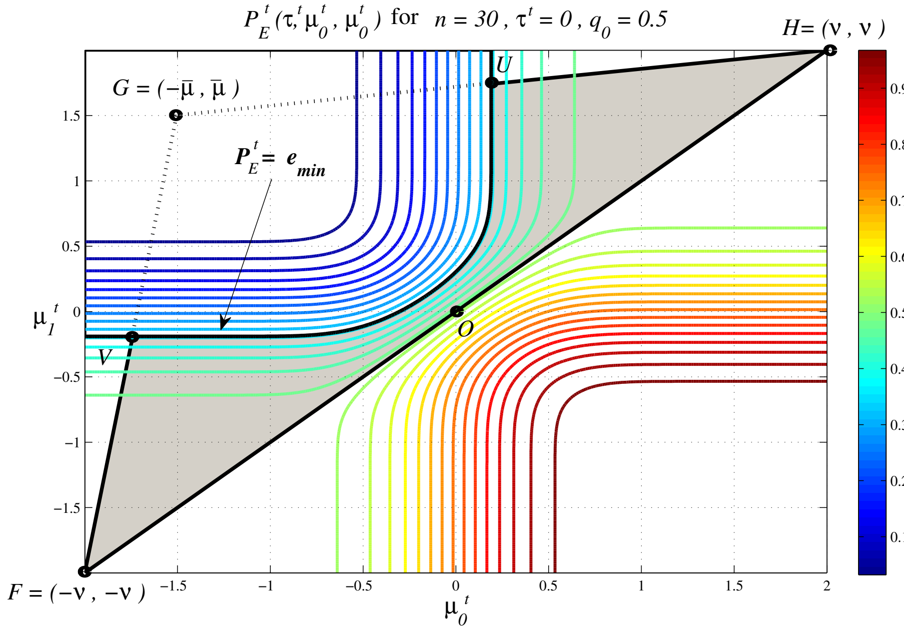

Figure 3.5: The feasible region of interest for $P2-2$ optimization

The above facts reveal two more points in $\mathcal{R}$ such that

$$H = (\nu, \nu) \in \mathcal{R} \text{ for } \mathbf{\Phi} = \begin{cases} \phi_{ij} = 1, & \text{if } j = m \\ \phi_{ij} = 0, & \text{if } j \neq m \end{cases}$$

$$F = (-\nu, -\nu) \in \mathcal{R} \text{ for } \mathbf{\Phi} = \begin{cases} \phi_{ij} = 1, & \text{if } j = M - m \\ \phi_{ij} = 0, & \text{if } j \neq M - m \end{cases}$$

It is straightforward to validate the above statements. Now we form the triangle ΔFGH in $\mathcal{R}$. Since $\mathcal{R}$ is convex, every pair (μ_0^t, μ_1^t) residing in ΔFGH also belongs to $\mathcal{R}$. We will limit our attention only to the points laying in ΔFGH (see Figure 3.5). Finally we are able to eliminate $\mathbf{\Phi}$ from the constraints in $P2-1$ and reorganize it as follows.

$$P2-2: \quad \min_{\mu_0^t, \mu_1^t} P_e(\tau, \mu_0^t, \mu_1^t, \sqrt{\nu^2 - (\mu_0^t)^2}, \sqrt{\nu^2 - (\mu_1^t)^2}) \tag{3.46}$$

subject to:

$$\mu_1^t \leq \mu_0^t \tag{3.47}$$

$$(\mu_0^t - \bar{\mu})(\nu - \bar{\mu}) \leq (\mu_1^t + \bar{\mu})(\nu + \bar{\mu}) \tag{3.48}$$

$$(\mu_0^t - \bar{\mu})(\nu + \bar{\mu}) \leq (\mu_1^t + \bar{\mu})(\nu - \bar{\mu}) \tag{3.49}$$

$$e_{min} \leq \boldsymbol{\varepsilon}^t(\tau^t, \mu_0^t, \mu_1^t) \leq 0.5 \tag{3.50}$$

where the constraints in (3.47) and (3.48) and (3.49) are met with equality, respectively

at sides FH, HG and GF. This has been illustrated in Figure 3.5 where the contour $\boldsymbol{\varepsilon}^t(\tau^t, \mu_0^t, \mu_1^t) = e_{min}$ is plotted such that the shaded area indicates the reduced feasible region for $P2-2$. Viewing Figure 3.5, one can see a remarkable correlation between this problem and the AFC optimization problem in Chapter 2. The following theorem, similar to the Theorem 2 in Chapter 2, completely characterizes the solution to $P2-2$.

Theorem 3. *the optimal solution* (μ_0^t, μ_1^t) *satisfies either* (3.48) *or* (3.49) *with equality.*

Proof Let

$$\boldsymbol{\varepsilon}^a(\tau, \mu_0^t, \mu_1^t) \triangleq P_e(\tau, \mu_0^t, \mu_1^t, \sqrt{\nu^2 - (\mu_0^t)^2}, \sqrt{\nu^2 - (\mu_1^t)^2}).$$

It is easy to investigate that $\boldsymbol{\varepsilon}^a(\tau, \mu_0^t, \mu_1^t)$ is monotone increasing in μ_1^t, and monotone decreasing in μ_0^t. Thus similarly to Lemma 2 the optimal solution cannot land on line $\mu_1^t = \mu_0^t$.

The solution to $P2-1$ must stisfy the Karush-Khun-Tucker (KKT) conditions. We form the KKT augmented objective function which includes KKT multipliers for each of the constraints. If we avoid trivial solutions, the augmented cost function will be

$$\begin{aligned}\mathcal{C} = \ & \boldsymbol{\varepsilon}^a(\tau, \mu_0^t, \mu_1^t) + \zeta_3(e_{min} - \boldsymbol{\varepsilon}^t(\tau^t, \mu_0^t, \mu_1^t)) \\ & \zeta_2((\mu_0^t - \bar{\mu})\vartheta_0 - (\mu_1^t + \bar{\mu})\vartheta_1) + \zeta_1((\mu_0^t - \bar{\mu})\vartheta_1 - (\mu_1^t + \bar{\mu})\vartheta_0)\end{aligned} \tag{3.51}$$

where

$$\vartheta_0 \triangleq \nu - \bar{\mu} \quad , \quad \vartheta_1 \triangleq \nu + \bar{\mu}$$

It is clear that $0 \leq \vartheta_0 \leq \vartheta_1$. In (3.51), the variables $\zeta_1, \zeta_2, \zeta_3 \geq 0$, are respectively the multipliers belonging to the constraints in (3.48), (3.48) and (3.50). Then an optimal pair (μ_0^t, μ_1^t) must satisfy the following equations along with the previous constraints.

$$\nabla_{(\mu_0^t, \mu_1^t)} \mathcal{C} = 0 \tag{3.52}$$

$$\frac{\partial \mathcal{C}}{\partial \zeta_i} = 0 \qquad \text{for} \quad \zeta_i \neq 0 \tag{3.53}$$

It has been noted that τ and τ^t are obtained from MAP rule which also hold in

$$\frac{\partial \boldsymbol{\varepsilon}^a(\tau,\mu_0^t,\mu_1^t)}{\partial \tau}=0 \ \text{ results } \ \frac{Q'(\sqrt{n}\frac{\tau-\mu_0^t}{\sqrt{\nu^2-(\mu_0^t)^2}})}{Q'(\sqrt{n}\frac{\tau-\mu_1^t}{\sqrt{\nu^2-(\mu_1^t)^2}})}=\frac{q_1}{q_0}\sqrt{\frac{\nu^2-(\mu_0^t)^2}{\nu^2-(\mu_1^t)^2}} \tag{3.54}$$

$$\frac{\partial \boldsymbol{\varepsilon}^t(\tau^t,\mu_0^t,\mu_1^t)}{\partial \tau^t}=0 \ \text{ results } \ \frac{Q'(\sqrt{n}\frac{\tau^t-\mu_0^t}{\sqrt{\nu^2-(\mu_0^t)^2}})}{Q'(\sqrt{n}\frac{\tau^t-\mu_1^t}{\sqrt{\nu^2-(\mu_1^t)^2}})}=\frac{q_1}{q_0}\sqrt{\frac{\nu^2-(\mu_0^t)^2}{\nu^2-(\mu_1^t)^2}} \tag{3.55}$$

(3.56)

where $Q'(.)$ represents the derivative of the Q-function. The τ in (3.54) is also optimal for the augmented cost function $\mathcal{C}$ since it does not contribute to any constraint. The claim in Theorem 3 can be split into the two parts which are separately investigated.

I) Suppose that (3.50) is the only constraint met with equality, i.e, $\zeta_3 \neq 0, \zeta_1=\zeta_2=0$. Thus the KKT augmented cost function in (3.51) is reduced to

$$\mathcal{C}_1=\boldsymbol{\varepsilon}^a(\tau,\mu_0^t,\mu_1^t)+\zeta_3(e_{min}-\boldsymbol{\varepsilon}^t(\tau^t,\mu_0^t,\mu_1^t)) \tag{3.57}$$

Then

$$\frac{\partial \mathcal{C}_1}{\partial \mu_\eta^t}=0\ , \quad \eta=0,1 \tag{3.58}$$

Considering (3.58) together with (3.54) and (3.55) will lead to the contradiction that $\mu_1^t=\mu_0^t$. Thus (3.50) cannot be the only constraint met with equality.

II) Suppose that (3.48) is the only constraint met with equality, i.e, $\zeta_1 \neq 0, \zeta_2=\zeta_3=0$. Thus the KKT augmented cost function in (3.51) is reduced to

$$\mathcal{C}_2=\boldsymbol{\varepsilon}^a(\tau,\mu_0^t,\mu_1^t)+\zeta_1((\mu_0^t-\bar{\mu})\vartheta_1-(\mu_1^t+\bar{\mu})\vartheta_0) \tag{3.59}$$

Then

$$\frac{\partial \mathcal{C}_2}{\partial \mu_\eta^t}=0\ , \quad \eta=0,1 \tag{3.60}$$

Considering (3.60) together with (3.54) and (3.55) will lead to the contradiction that $\mu_1^t=\mu_0^t$. Thus (3.48) cannot be the only constraint met with equality. Similarly the case where $\zeta_2 \neq 0, \zeta_1=\zeta_3=0$ is also impossible.

Combining the cases I and II, it is concluded that $\zeta_1=0,\zeta_2\neq 0,\zeta_3\neq 0$ and $\zeta_2=0,\zeta_1\neq 0,\zeta_3\neq 0$ are the only possible scenarios. ■

The above theorem states that the optimal point located where the contour $\boldsymbol{\varepsilon}^t(\tau^t, \mu_0^t, \mu_1^t) = e_{min}$ intersects the sides of ΔFGH, i.e the point U or V in Figure 3.5. Depending on the choice of e_{min} there are one or two such intersection points. Let (μ_0^{t*}, μ_1^{t*}) denote the optimal solution for (μ_0^t, μ_1^t). Thus it can be computed through the following pair of simultaneous equations.

$$\begin{cases} P_e(\tau^t, \mu_0^{t*}, \mu_1^{t*}, \sqrt{\nu^2 - (\mu_0^{t*})^2}, \sqrt{\nu^2 - (\mu_1^{t*})^2}) = e_{min} \\ (\mu_1^{t*} - \bar{\mu})(\nu - \bar{\mu}) = (\mu_0^{t*} + \bar{\mu})(\nu + \bar{\mu}) \quad \text{or} \\ (\mu_1^{t*} - \bar{\mu})(\nu + \bar{\mu}) = (\mu_0^{t*} + \bar{\mu})(\nu - \bar{\mu}) \end{cases}$$

Having (μ_0^{t*}, μ_1^{t*}), we can drop (3.36) in $P2$ and pursue the solution of the following problem with linear constraints.

$$P2-3: \qquad \min_{\mathbf{\Phi}} P_e(\tau^a, \mu_0^a, \mu_1^a, \sigma_0^a, \sigma_1^a) \tag{3.61}$$

subject to:

$$0 \le \mathbf{\Phi} \le 1 \tag{3.62}$$

$$\mathbf{\Phi 1}_{M\times 1} = \mathbf{1}_{M\times 1} \tag{3.63}$$

$$\boldsymbol{\alpha}_\eta \mathbf{\Phi} \xi(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_0)^T = \mu_\eta^{t*} \quad , \quad \eta = 0,1 \tag{3.64}$$

$$\boldsymbol{\alpha}_\eta \mathbf{\Phi} \omega(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_0)^T = \nu^2 \quad , \quad \eta = 0,1 \tag{3.65}$$

3.3.2 Simplifying Cost Function

After simplifying the constraints, we need to find a simpler substitute for the cost function in $P2-3$. Viewing (3.8) for large n, it is noted that P_E^a is decreasing in μ_1^a and increasing in μ_0^a. It also can be inferred that comparing to μ_η^a, the impact of σ_η^a becomes small. Thus one can be motivated to maximize $\mu_1^a - \mu_1^a$ instead of the cumbersome P_e in $P2$. The authors in [18] have utilized the same idea to find the optimal quantizer $\mathcal{Q}$ without the security issue. Reviewing (3.16), it can be seen that μ_1^a and μ_1^a are associated with Kullback-Leibler divergence.

$$\mu_0^a = -\mathcal{D}(\boldsymbol{\alpha}_0\mathbf{\Phi}||\boldsymbol{\alpha}_1\mathbf{\Phi}) \quad , \quad \mu_1^a = \mathcal{D}(\boldsymbol{\alpha}_1\mathbf{\Phi}||\boldsymbol{\alpha}_0\mathbf{\Phi}) \tag{3.66}$$

where $\mathcal{D}(.||.)$ denotes Kullback-Leibler divergence. For given p.m.f's $\boldsymbol{p} = (p_1, p_2, \cdots, p_N)$ and $\boldsymbol{q} = (q_1, q_2, \cdots, q_N)$,

$$\mathcal{D}(\boldsymbol{p}||\boldsymbol{q}) \triangleq \sum_{i=1}^{N} p_i \log\left(\frac{p_i}{q_i}\right) \tag{3.67}$$

Then Then $\mu_1^a - \mu_1^a$ can be written in form of J-divergence (special case of Jensen-Shannon divergence).

$$\mu_1^a - \mu_0^a = 2\mathcal{J}(\boldsymbol{\alpha}_1\boldsymbol{\Phi}||\boldsymbol{\alpha}_0\boldsymbol{\Phi}) \triangleq \mathcal{D}(\boldsymbol{\alpha}_1\boldsymbol{\Phi}||\boldsymbol{\alpha}_0\boldsymbol{\Phi}) + \mathcal{D}(\boldsymbol{\alpha}_0\boldsymbol{\Phi}||\boldsymbol{\alpha}_1\boldsymbol{\Phi}) \tag{3.68}$$

Finally, the optimization problem below can be solved for optimal $\boldsymbol{\Phi}$

$$\hat{P}2: \quad \max_{\boldsymbol{\Phi}} \mathcal{J}(\boldsymbol{\alpha}_1\boldsymbol{\Phi}||\boldsymbol{\alpha}_0\boldsymbol{\Phi}) \tag{3.69}$$

subject to:

$$0 \leq \boldsymbol{\Phi} \leq 1 \tag{3.70}$$

$$\boldsymbol{\Phi}\mathbf{1}_{M\times 1} = \mathbf{1}_{M\times 1} \tag{3.71}$$

$$\boldsymbol{\alpha}_\eta\boldsymbol{\Phi}\xi(\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_0)^T = \mu_\eta^{t*} \quad , \quad \eta = 0,1 \tag{3.72}$$

$$\boldsymbol{\alpha}_\eta\boldsymbol{\Phi}\omega(\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_0)^T = \nu^2 \quad , \quad \eta = 0,1 \tag{3.73}$$

In [18] the convexity of J-divergence with respect to its arguments has been investigated. Since in (3.68) the arguments of J-divergence will be the linear combinations of the elements in $\boldsymbol{\Phi}$ the convexity still applies to the optimization with respect to $\boldsymbol{\Phi}$. The above problem can be efficiently solved by means of Lagrange multiplier technique or other classical iterative algorithms.

After computing the optimum $\boldsymbol{\Phi}$, we can obtain τ^a from (3.28).

3.4 Numerical Results and Comparison

Consider again the case of additive Gaussian noise where the signal X_i received by sensor i is given by

$$X_i = s + N_i,$$

where $s = d$ under hypothesis H_1, $s = -d$ under hypothesis H_0, and where $\{N_i\}_{i=1}^n$ are iid Gaussian random variables with mean zero and variance σ^2. Then each sensor quantizes X_i with M levels according to a quantization rule designed in [18] (designed to obtain minimum error without the encryption) such that the condition in (3.45) is also satisfied. We define $\gamma = 20\log(d/\sigma)$ as the sensors' SNR.

Table 3.1 shows the performance of both the binary and soft decision systems for several values of n, γ and q_0. Therein P_{Eb}^a and P_{Eb}^{min} are, in turn, the minimum error probability for the binary AFC and the minimum achievable error for a binary AFC without P_E^t constraint. In the entire cases presented in Table 3.1, the soft decision systems achieve lower AFC error probabilities compared to the binary system. This is better illustrated in Figure 3.6 and 3.7, where insecure cases are referred to the AFC error probability minimization without

Table 3.1: AFC Optimized Error Performance (Soft-Decision vs. Binary)

Case	n	γ (dB)	q_0	P_E^t	P_{Eb}^a	$P_E^a(M=4)$	$P_E^a(M=8)$	P_{Eb}^{min}
$c1$	20	0	0.5	0.3	1.52 e-02	2.14 e-03	1.47 e-04	2.32 e-04
$c2$	20	0	0.3	0.3	1.37 e-02	1.04 e-03	1.14 e-04	2.50 e-04
$c3$	20	3	0.5	0.4	6.66 e-03	7.82 e-06	2.86 e-06	4.43 e-07
$c4$	40	-3	0.5	0.5	2.80 e-02	1.17 e-03	5.66 e-05	2.01 e-04
$c5$	40	0	0.5	0.3	1.15 e-03	2.34 e-05	1.34 e-07	3.17 e-07
$c6$	40	0	0.5	0.4	2.28 e-03	5.24 e-05	1.34 e-07	3.17 e-07
$c7$	40	0	0.5	0.5	7.58 e-03	8.18 e-05	2.13 e-07	3.17 e-07
$c8$	40	0	0.3	0.3	9.64 e-04	9.76 e-06	1.84 e-07	5.24 e-07
$c9$	40	3	0.5	0.5	1.15 e-03	4.57 e-08	5.88 e-12	1.37 e-12
$c10$	80	-6	0.5	0.5	1.40 e-02	1.11 e-03	1.55 e-05	1.00 e-04
$c11$	80	-3	0.5	0.5	1.83 e-03	3.85 e-06	6.28 e-10	2.38 e-08

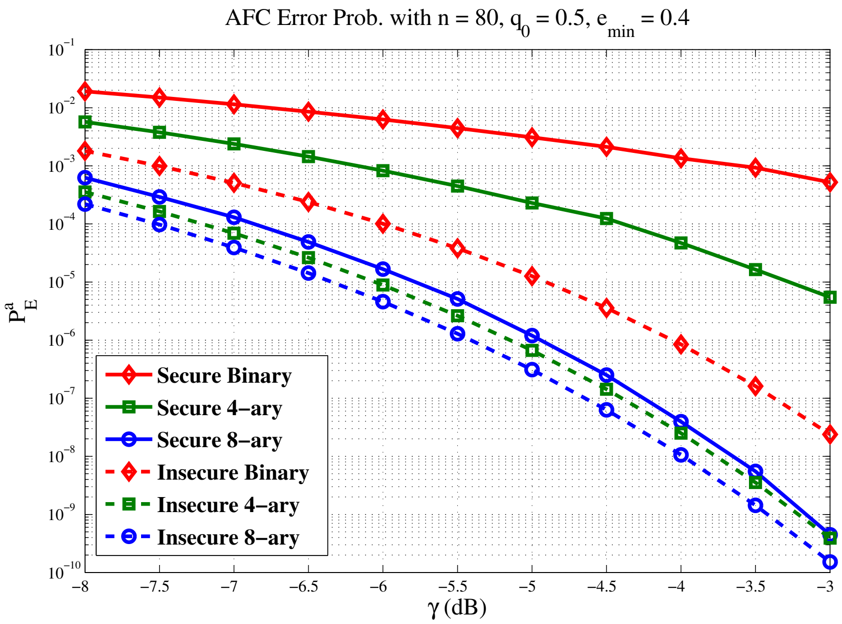

Figure 3.6: Comparing the AFC error performance versus SNR

protection against the TPFC.

In Figure 3.6 for $n = 80$, $q_0 = 0.5$, $e_{min} = 0.4$, the soft decision system with $M = 4$ and $M = 8$ evidently outperform the binary detection system for different SNRs. There the system with $M = 8$ outperforms even the insecure binary detection system. This confirms that for a fixed AFC error probability and number of sensors the soft decision system can work in lower SNRs. Similarly in Figure 3.6 for $\gamma = -6dB$, $q_0 = 0.5$, $e_{min} = 0.4$, the soft decision system with $M = 4$ and $M = 8$ can achieve the same AFC error probability

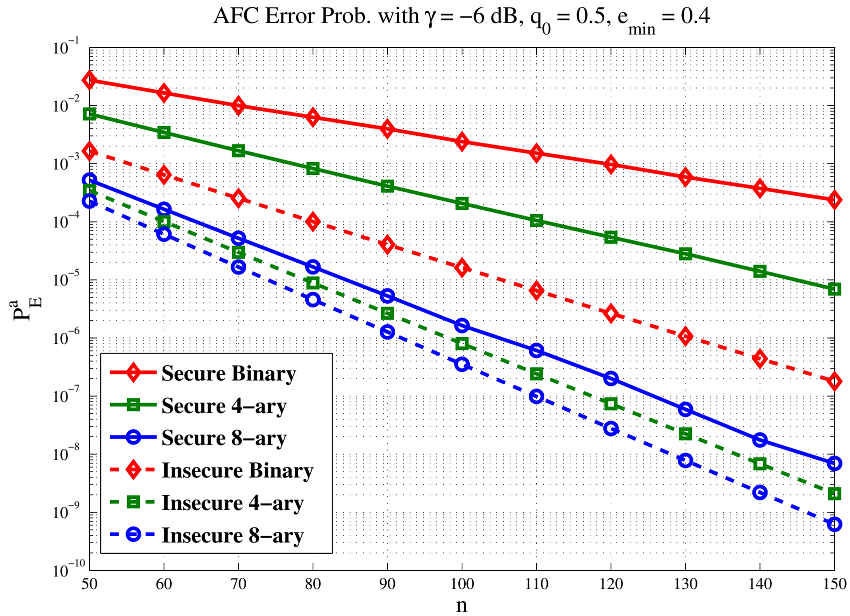

Figure 3.7: Comparing the AFC error performance versus n

using fewer sensors that the binary detection system. There the system with $M = 8$ again outperforms even the insecure binary detection system.

We now introduce the *cost-of-security* (CS) which indicates the increase in the AFC error probability due to the protection against the TPFC for the soft decision system with M levels.

$$CS(M) \triangleq \log_{10}\left(\frac{P_E^a(M)}{P_E^{min}(M)}\right) \tag{3.74}$$

where $P_E^{min}(M)$ is the minimum achievable error probability with no encryption and $M = 2$ refers to the binary case. Obviously the smaller CS, the more efficient the method. The factor CS in Table 3.2 has been calculated for the cases in Table 3.1. It can be seen that applying encryption to the binary case drastically increases the AFC error probability, P_{Eb}^a, compared to minimum achievable error P_{Eb}^{min} (large CS). On the other hand, having soft decision performed at the sensors helps us to tolerate less loss in the AFC error performance due to protection against the TPFC.

In Table 3.2 K stands for the number of nontrivial (nonzero or one with 0.01 precision) elements of $\mathbf{\Phi}^*$ where the soft decision with M levels is applied to cases in Table 3.1, i.e. $K(M)$ can be thought as the hash to store the encryption parameters. Although there are initially M^2 parameters in $\mathbf{\Phi}$, the hash for the optimal $\mathbf{\Phi}$ does not follow the square law.

Similarly to the binary case, the sensors are recommended to periodically cycle their en-

Table 3.2: AFC Efficiency (Soft Decision vs. Binary)

Case	$CS(2)$	$CS(4)$	$CS(8)$	$K(4)$	$K(8)$
$c1$	1.8	1.2	0.1	09	13
$c2$	1.7	0.9	0.1	09	11
$c3$	4.1	0.6	0.2	10	14
$c4$	2.1	1.4	0.2	08	15
$c5$	3.6	2.4	0.2	09	12
$c6$	3.9	2.7	0.2	09	13
$c7$	4.4	2.9	0.4	10	12
$c8$	3.2	1.9	0.4	09	12
$c9$	8.9	3.2	0.1	10	11
$c10$	2.1	2.0	0.5	09	27
$c11$	4.9	3.9	0.6	09	12

cryption keys so as to defeat the strategies used by the TPFC to estimate the encryption parameters from sensor transmissions. For example in Table 3.1, for $n = 40$, $q_0 = 0.5$ computes the optimal $\mathbf{\Phi}$'s for the three cases $c5$, $c6$ and $c7$ and gives them to the sensors. Then the senors can shuffle $\mathbf{\Phi}$'s according a schedule defined by the AFC.

Chapter 4

Conclusion and Future Work

We have considered the problem of hypothesis testing in a bandwidth-constrained, low-power wireless sensor network operating over insecure links. Sensors quantize their observations and transmit their decisions to an ally fusion center (AFC) which combines the received messages to detect the state of an unknown hypothesis. The problem of protecting the wireless sensors' messages against the unauthorized access of third-party fusion center (TPFC) has been investigated. Since the sensors possess limited bandwidth and processing power, applying the simple probabilistic cipher is a suitable solution.

In this scenario the AFC enables the sensors to randomly flip their observation according to preassigned probabilities. The encryption operation incorporates a controlled uncertainty in the transmitted messages. this uncertainty deteriorates the performance of both the fusion centers. For a given lower bound on the TPFC error probability, the AFC seeks the cipher probabilities which minimize its own error probability. It is worth to note that the increase in the AFC error probability (compared to the unsecured network) can be compensated for by adding a few more sensor nodes to the network which is a quite affordable solution.

For the binary case (binary decision sensors) we have attained an analytical solution for the AFC optimization problem. However, the AFC optimization problem in the non-binary case (soft decision sensors) is very complicated. In this case we have obtained a suboptimal solution. The numerical results verified that, in identical conditions, the soft decision systems will have a far better error performance for the AFC than the binary system.

Since we have considered error free channel in the above problem, the first extension to this work is to involve the channel impairments in the AFC optimization. Although this problem will be more occurring in practice, the analytical complexity may derive one to only suffice to numerical optimization.

The proposed algorithm can be accounted as a quintessential mathematical optimization where the calculus techniques had the key rules. This problem can be also discussed from the information theory point of view that may help one to more generalize this idea.

Bibilography

[1] I.F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci. "A survey on sensor networks". *Communications Magazine, IEEE*, 40(8):102 – 114, aug 2002.

[2] J.N. Al-Karaki and A.E. Kamal. "Routing techniques in wireless sensor networks: a survey". *Wireless Communications, IEEE*, 11(6):6 – 28, dec. 2004.

[3] S. Appadwedula, V.V. Veeravalli, and D.L. Jones. "Energy-efficient detection in sensor networks". *Selected Areas in Communications, IEEE Journal on*, 23(4):693 – 702, april 2005.

[4] T.C. Aysal and K.E. Barner. "Sensor data cryptography in wireless sensor networks". *Information Forensics and Security, IEEE Transactions on*, 3(2):273 –289, june 2008.

[5] A. Boyd and L. Vandenberghe. *"Convex Optimization"*. Cambridge University Press, UK, 1st edition, 2004.

[6] Z. Chair and P.K. Varshney. "Optimal data fusion in multiple sensor detection systems". *Aerospace and Electronic Systems, IEEE Transactions on*, AES-22(1):98 –101, jan. 1986.

[7] J.-F. Chamberland and V.V. Veeravalli. "Decentralized detection in sensor networks". *Signal Processing, IEEE Transactions on*, 51(2):407 – 416, feb 2003.

[8] J.-F. Chamberland and V.V. Veeravalli. "Asymptotic results for decentralized detection in power constrained wireless sensor networks". *Selected Areas in Communications, IEEE Journal on*, 22(6):1007 – 1015, aug. 2004.

[9] Biao Chen, Ruixiang Jiang, T. Kasetkasem, and P.K. Varshney. "Channel aware decision fusion in wireless sensor networks". *Signal Processing, IEEE Transactions on*, 52(12):3454 – 3458, dec. 2004.

[10] Po-Ning Chen and A. Papamarcou. "New asymptotic results in parallel distributed detection". *Information Theory, IEEE Transactions on*, 39(6):1847 –1863, nov 1993.

[11] Xiangqian Chen, K. Makki, Kang Yen, and N. Pissinou. ”Sensor network security: a survey”. *Communications Surveys Tutorials, IEEE*, 11(2):52 –73, mar 2009.

[12] V. Cionca, T. Newe, and V. Dadarlat. ”Setting up secure wireless sensor networks”. In *Intelligent Computer Communication and Processing, 2009. ICCP 2009. IEEE 5th International Conference on*, pages 335 –338, aug. 2009.

[13] D. Estrin, L. Girod, G. Pottie, and M. Srivastava. ”Instrumenting the world with wireless sensor networks”. In *Acoustics, Speech, and Signal Processing (ICASSP '01), 2001 IEEE International Conference on*, volume 4, pages 2033 –2036 vol.4, 2001.

[14] E. Fasolo, M. Rossi, J. Widmer, and M. Zorzi. ”In-network aggregation techniques for wireless sensor networks: a survey”. *Wireless Communications, IEEE*, 14(2):70 –87, apr 2007.

[15] Cyril Gavoille. ”Routing in distributed networks: Overview and open problems”. *ACM SIGACT News*, 32:36 –52, 2001.

[16] W.W. Irving and J.N. Tsitsiklis. ”Some properties of optimal thresholds in decentralized detection”. *Automatic Control, IEEE Transactions on*, 39(4):835 –838, apr 1994.

[17] Yee Wei Law and P.J.M. Havinga. ”How to secure a wireless sensor network”. In *International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, pages 89 – 95, dec 2005.

[18] C.-C. Lee and J.-J. Chao. ”Optimum local decision space partitioning for distributed detection”. *Aerospace and Electronic Systems, IEEE Transactions on*, 25(4):536 –544, jul 1989.

[19] Ruixin Niu, Biao Chen, and P.K. Varshney. ”Fusion of decisions transmitted over rayleigh fading channels in wireless sensor networks”. *Signal Processing, IEEE Transactions on*, 54(3):1018 – 1027, mar 2006.

[20] A. Papoulis and S.U. Pillai. *”Probabilty, Random Variables and Stochastic Processes”*. McGraw-Hill New York, Inc., 4th edition, 2009.

[21] G.J. Pottie. ”Wireless sensor networks”. In *Information Theory Workshop, 1998*, pages 139 –140, jun 1998.

[22] E. Shi and A. Perrig. ”Designing secure sensor networks”. *Wireless Communications, IEEE*, 11(6):38 – 43, dec. 2004.

[23] Wei Shi, T.W. Sun, and R.D. Wesel. ”Quasi-convexity and optimal binary fusion for distributed detection with identical sensors in generalized gaussian noise”. *Information Theory, IEEE Transactions on*, 47(1):446 –450, jan 2001.

[24] R. Srinivasan. "Designing distributed detection systems". *Radar and Signal Processing, IEE Proceedings F*, 140(3):191 –197, jun 1993.

[25] V. Sriram S. N. "Secure distributed detection in wireless sensor networks via encryption of sensor decisions". Master's thesis, Department of Electrical and Computer Engineering, Louisiana State University (LSU), Baton Rouge, LA, aug 2009.

[26] Ankur Suri, S.S. Iyengar, and Eungchun Cho. "Ecoinformatics using wireless sensor networks: an overview". In *Ecological Informatics, 4th International Conference on*, volume 1, pages 287 – 293, nov 2006.

[27] R.R. Tenney and N.R. Sandell. "Detection with distributed sensors". *Aerospace and Electronic Systems, IEEE Transactions on*, AES-17(4):501 –510, jul 1981.

[28] J. Tsitsiklis. "Decentralized detection by a large number of sensors". *Math. Control, Signals, System*, 1(2):167 –182, 1988.

[29] J. Tsitsiklis. "Decentralized detection". *Advances in Statist. Signal Processing*, 2:297 –344, 1993.

[30] P.K. Varshney. *"Distributed Detection and Data Fusion"*. Springer New York, Inc., 1997.

[31] R. Viswanathan and P.K. Varshney. "Distributed detection with multiple sensors-part I: fundamentals". *Proceedings of the IEEE*, 85(1):54 –63, jan 1997.

[32] Wei Ye, J. Heidemann, and D. Estrin. "An energy-efficient MAC protocol for wireless sensor networks". In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 3, pages 1567 – 1576, 2002.

[33] Qian Zhang, P.K. Varshney, and R.D. Wesel. "Optimal bi-level quantization of i.i.d. sensor observations for binary hypothesis testing". *Information Theory, IEEE Transactions on*, 48(7):2105 –2111, jul 2002.

Vita

Reza Soosahabi was born in June, 1988, in Tehran, Iran. He received his Bachelor of Science in Electrical Engineering (Communication Systems) with distinction from Amirkabir University of Technology (Theran Polytechnic), Tehran, Iran, in 2008. He is presently pursing his Master of Science in Electrical Engineering at Louisiana State University (LSU) and is expected to graduate in August 2011. His research interests include wireless communication, cognitive radios, wireless sensor networks and signal processing for communication.

He was appointed as a design engineer in Nik Partow Pardaz Inc, Theran, Iran, 2009 where he was working on amplifier compensator for the repeaters used in a long-haul software radio system. He also worked as a graduate research/teaching assistant at LSU from 2009 to present. He has been working with Dr. Morteza Naraghi-Pour and has submitted one IEEE transaction and two papers in Global Communications Conference, Houston, Texas, 2011. He has been IEEE student member (2008-2010) and lifetime member of Torr (International High IQ Society).