2010

# Adaptive quantization in wireless sensor networks with encryption

Niharika Konakalla
*Louisiana State University and Agricultural and Mechanical College*

# ADAPTIVE QUANTIZATION IN WIRELESS SENSOR NETWORKS WITH ENCRYPTION

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

Department of Electrical and Computer Engineering

by
Niharika Konakalla
B.E. in Electrical and Communication Engineering,Kakatiya University, 2007.
May 20101

# Acknowledgements

I am indebted to my major advisor Dr. Morteza Naraghi-Pour for his exemplary patience, guidance and support. He taught me how to approach problems and inspired me when the progress was slow. It was with his kind support, I overcame all the obstacles on my way towards completing my thesis.

I would also like to thank my committee members, Dr. Xue-Bin Liang and Dr. Shuangqing Wei for their valuable suggestions and kind support. Furthermore, I thank the Dept. of Electrical and Computer Engineering for supporting me financially and making me concentrate on my research without any other deviations.

I wish to endow my earnest gratitude to my parents, who believed in me and have been thorough all the rough times. I also want to thank my entire family and friends for their affection, support and compassion.

I would also want to sincerely thank my brother Priyatam Konakalla, with out whom my stay in the United States would not have been possible. It was with his support, my dreams of Master's degree came true.

# Table of Contents

# List of Figures

# Abstract

We consider the estimation of a deterministic unknown parameter in an encrypted wireless sensor networks. Adaptive quantization is used on the sensor's observation and the outputs of the sensors are then encrypted using a probablisitic cipher. In a conventional fixed quantization scheme, estimation error grows exponentially with the difference between the threshold and the unknown parameter to be estimated. Hence, to avoid this, we used and adaptive quantization scheme where each sensor adaptively adjusts its quantization threshold.

We find the Cramer-Rao Lower Bound for the Ally Fusion Center (AFC) and then find the optimal estimate of the unknown parameter for the AFC. To find this, we first prove that the sequence of thresholds used for the quantization process forms a markov chain and that this chain is recurrent non-null and thus has a stationary distribution. This distribution is then obtained analytically in closed form as well as through numerical methods.

The optimal estimate of the unknown parameter for the AFC is obtained asymptotically in the number of sensors. The performance of the Third Party Fusion Center (TPFC) is only computed through simulation and compared to that of AFC.

# 1 Introduction

## 1.1 Overview

With the recent technological advances, Wireless Sensor Networks (WSNs) are gaining great research interests because of their wide range of applications in both consumer and security fields. The developments in MEMS (Micro Electro Mechanical Systems), wireless communications and digital electronics have made sensors much smaller and cheaper. [1]. This low-cost of sensors made the deployment of a large number of sensors in a geographical area possible. Distributed sensor systems were originally motivated by their applications in military surveillance where they use sensors for command, control and communication, [2] [3], but are now used in wide variety of fields. Some of the application areas include health, military, and security [4]. For example, they can be used to detect foreign elements in atmosphere or water, monitoring of temperature or pressure in environment and so on.

One of the most important constraints in WSNs is the power requirement. Sensor nodes are battery powered. Consequently they have a limited and irreplacable power source which can be exhausted after a while. Therefore, while the traditional WSNs want to achieve high quality of service (QoS), practical application of sensors primarily focus on power conservation [4].

Wireless sensor networks have been studied for *distributed detection* and *distributed estimation* [3]. Here we mainly deal with the fundamentals of decentralized estimation problem. The problem of decentralized estimation has been studied in the context of distributed control [5], [6] and tracking [7] and most recently this has been exteneded to WSNs [8]- [13].

For applications related to multiple-target detection and estimation, decentralized detection and estimation has surfaced. In a classical multi-sensor network model, it is assumed that all the sensors send the data to a central processor (known as the fusion center) that performs the optimal detection/estimation of the data. In a decentralized network, processing of data is carried out at each individual sensor and then ultimately sent to the fusion center [3]. Therefore this means that the network has intelligence at each node [14]. The centralized scheme is not practical and therefore we consider the case of decentralized estimation. This scheme also has advantages like low communication bandwidth, increase in reliability and low cost. In a decentralized system, there is partial information loss due to the processing at individual sensors compared to a centralized system and hence the performance is relatively degraded. However, this performance loss can be made minimal by processing the information at the sensors optimally [15]. Based on the flow of data among the sensors and the fusion center, various topologies have been classified. In general, a distributed sensor network has to address various issues like the choice of topology, existence of communication between sensors, feedback of data from fusion center, and external threats to the system [3].

## 1.2 Topologies

Wireless sensor networks can be catagorized based on the arrangement of sensor nodes and the fusion center in the network. There are three major topologies based on this classification - parallel, serial and tree topologies.

In *parallel* topology, sensors do not communicate with each other. They collect data si-

multaneously from the phenomenon, process it and then transmit this processed data to the fusion center where the decision is made based on the data from all the sensors.

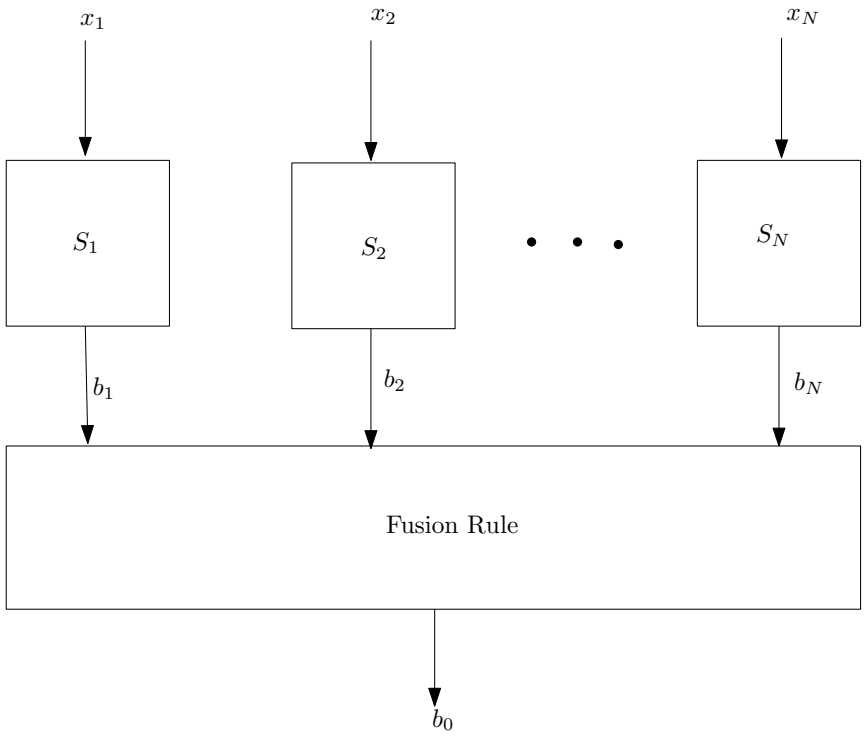


Figure 1.1: Parallel Topology of wireless sensor networks

Fig. 2 shows the serial topology of the WSN. Here, the sensors are connected in series with each other i.e., they communicate with the neighbouring sensor in a unidirectional way. This means that the first sensor processes the data from the phenomenon, makes a decision and transmits this to the second sensor which makes a decision based on this recieved data along with its own observation from the phenomenon. This decision is then transmitted to the adjacent sensor and so on. Here the last sensor in this series can be considered as the fusion center and the decision made by this is the final decision in the network.

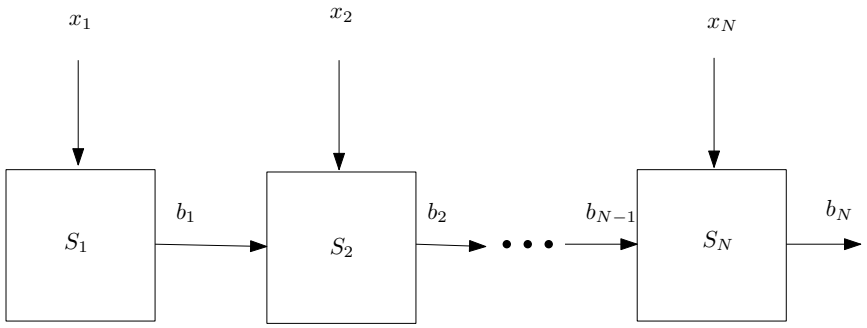


Figure 1.2: Serial Topology of wireless sensor networks

Now the tree topology is nothing but a combination of both series and parallel networks combined together. Here sensors are arranged in various stages and the each stage gets the decision from the preceeding stage and makes a decision based on this along with its own observation. The final stage is the fusion center (also called as the root of the tree) here and gives the final decision.

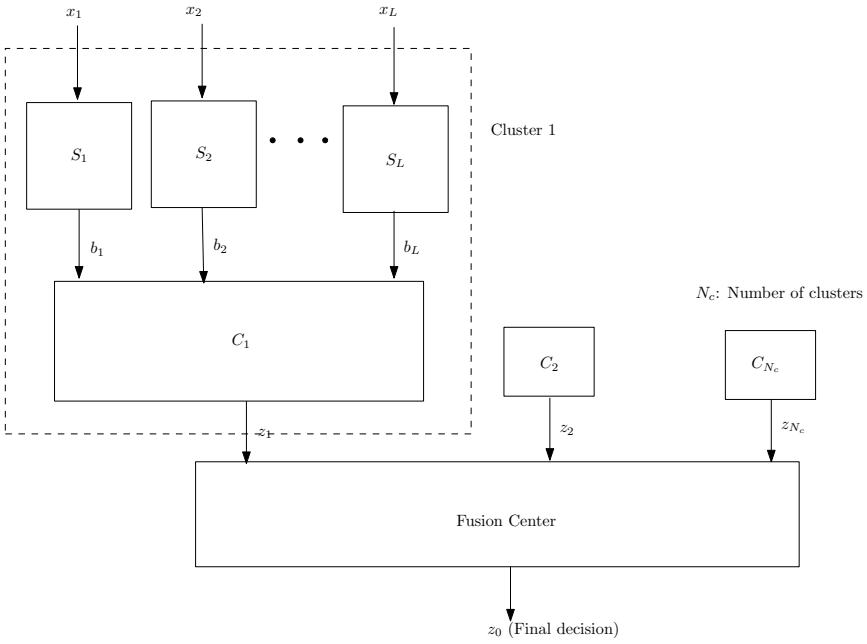


Figure 1.3: Tree Topology of wireless sensor networks

Here in all these networks, the information flow is in only one direction which is nothing but in the direction of the fusion center.

## 1.3 Literature

In this thesis, we consider the case of serial topology. In the decentralized WSN, because of the bandwidth constraints, the sensors quantize the data before transmitting it further. But this quantization degrades the performance of the system. Therefore, this decentralized network is preferred only when there is bandwidth constraint.

Various kinds of quantization techniques have been formulated. A quantizer maps the real-valued measurements from the phenomenon to a finite set of values $q_i$ based on the thresholds of the sensors $\tau_i$. The quantizers are broadly classified as uniform and non-uniform quantizers based on the step-size (distance between the thresholds). In a uniform quantizer, all the thresholds are equally spaced and the outputs are the center values of the intervals, while in non-uniform quantizer, the thresholds and the output values are optimized based on a cost function.

Quantization for estimation has been studied for a single sensor case by [16] and [17]. The multi-sensor case has been studied in [18] and [19]. Many methods have been formulated for the design of quantizers with the aid of the prior distribution knowledge of the unknown parameter to be estimated. These methods usually require knowledge of joint distribution of this parameter along with the observed signals by the sensors [20]. Another category of methods for quantization treat the unknown parameter as a deterministic value. An example of this case is the fixed quantization approach where there is a common threshold

for all the sensors [20]. The problem with this fixed quantization is that the choice of the threshold value is very sensitive, i.e., the closer the threshold value is to the unknown parameter, the better is the performance of the system. This disadvantage led to research in adaptive quantization, where there is a different threshold value for eash sensor depending on the data observed from the phenomenon. Some adaptive quantization techniques have been proposed in [20] [21].

Many results have been published in the field on WSNs for serial topology. In [26] they provided the necessary and sufficient conditions for the probability of error to go to zero asymptotically for both binary and multiple hypothesis problems. [27] is the first paper which proposed recursive equations for threshold values in serial topology WSN. All the works in serial topology provided all the results asymptotically in the number of sensors. But in [27], they considered a finite number of sensors and compared the probability of detection and probability of false alarm and used an adaptive quantization scheme.

Most of the works in the detection and estimation of the data in distributed systems has not considered the presense of the channel between the sensors which is an important factor. That is, perfect reception of the data is assumed at sensors from the preceeding sensors. This is not practical in general but analysis becomes some times difficult and hence we consider a perfect channel. Here in our case, we consider a perfect channel as solving the equations for a noisy wireless channel is out of our scope for now.

## 1.4 Adaptive Quantization

We consider a decentralized system to estimate an unknown parameter $\theta$ from quantization observations. Suppose we have N sensors distributed spatially and each making an observation of $\theta$

$$x_i = \theta + W_i$$

where $W_i$ denotes the additive i.i.d noise with zero-mean. The 1-bit quantizer used by the $i^{th}$ sensor is given by

$$b_i = Q_i(x_i)$$

### 1.4.1 Adaptive Quantization - Fixed Step-size (AQ-FS)

Adaptive quantization with fixed step-size was introduced in [21]. In this, the first sensor uses an arbitrary threshold, say $\tau_1 = 0$ to generate the quantized bit $b_1$

$$b_1 = sgn\{x_1 - \tau_1\}$$

Now, $b_1$ is broadcasted to all other sensors and the fusion center. Sensor 2 computes $\tau_2 = b_1\Delta$ where, $\Delta(> 0)$ is the step-size. Then, $b_2$ and $\tau_3$ are generated as

$$b_2 = sgn\{x_2 - \tau_2\}$$

$$\tau_3 = \tau_2 + \Delta b_2$$

In general, for the $n^{th}$ sensor

$$\tau_n = \tau_{n-1} + \Delta b_{n-1} = \Delta \sum_{k=1}^{n-1} b_k$$

$$b_n = sgn\{x_n - \tau_n\}$$

In this scheme, it is shown that $\tau_n$ converges to $\theta$ as $n$ increases.

### 1.4.2 Adaptive Quantization - Variable Step-size (AQ-VS)

It can be observed that the determination of the threshold value has 2 stages: *transient phase* which brings $\tau_n$ near $\theta$ and *convergent phase* where $\tau_n$ is around $\theta$. To make the convergence fast, we need to have large step-size, but to reduce the granular noise after convergence, we need to have small $\Delta$ value. Based on this, another scheme is introduced using variable step-size.

Let $b_1$ and $b_2$ be generated in the same way as in AQ-FS. Now at next sensors, previous bits are accumulated and weighted by a VS $\Delta_n$ for $n^{th}$ sensor. Then,

$$\tau_n = \tau_{n-1} + \Delta_n b_{n-1}$$

where $\Delta_n$ is given by

$$\Delta_n = \Delta_{n-1} K^{b_{n-1} b_{n-2}} \qquad n = 3, 4, ...$$

where $K > 1$ is a constant. It is observed that AQ-VS converge faster and stay closer to $\theta$ compared to AQ-FS.

### 1.4.3 Adaptive Quantization - Maximum Likelihood (AQ-ML)

In AQ-VS, the step-size depends only on the previous 2 bits. So we can extend this scheme to use more than two previous bits for a finer value of step-size. In this AQ-ML scheme, we use nonlinear ML estimation to adjust the value of the threshold.

Let $b_1$ be generated by AQ-FS. Then, the sensor 2 after receiving this value, computes $\tau_2 = \Delta b_1$ and sets $b_2 = sgn\{x_2 - \tau_2\}$. Based on $\{b_1, b_2\}$, sensor 3 computes $\tau_3$ as

$$\tau_3 = \arg\max_{\theta} L_3(\theta; b_1, b_2)$$

where $L_3(\theta; b_1, b_2)$ denotes the likelihood function of $\theta$. Here $\tau_3$ is nothing but the ML estimate of $\theta$ based on $b_1$ and $b_2$. Here, the step-size $\Delta$ used by sensor 2 should be large enough so that $b_1$ and $b_2$ have oppostive signs. Else, $\tau_3$ goes to positive or negative infinity and hence should be avoided. Therefore, $\Delta$ should be sufficiently large for this to be satisfied. If, for a chosen $\Delta$, the first two quantized bits have the same sign, the following sensors can use AQ-FS or AQ-VS until they have opposite signs.

In general, for the $n^{th}$ sensor, we have,

$$\tau_n = \arg\max_{\theta} L_n(\theta; b_1, b_2, ..., b_{n-1})$$

where we get the quantized data $\{b_k\}_{k=1}^{n-2}$ from the previous thresholds $\{\tau_k\}_{k=1}^{n-1}$. Here, although sensor $n$ has to perform $n-3$ recursive ML estimations, the complexity is still moderate for Gaussian noise.

In all the three schemes mentioned above, the thresholds used by each scheme only depend

on and can be inferred from the quantized data $\{b_k\}$. No extra bandwidth is needed to communicate the thresholds. AQ-FS and AQ-VS are simple to calculate while AQ-ML offers the best performance among all the three and converges to the best 1-bit quantizer. And we can also note that AQ-FS and AQ-VS require no knowledge of the distribution of data and can be considered as *nonparametric quantizers*. On the other hand, AQ-ML needs the distribution of the sensor observations.

Inspired by this, we use AQ-FS in our system.

### 1.4.4 Motivation for This Work

Most of the previos works in decentralized estimation problem used a fixed quantization technique. The probability of error increase exponentially with the difference between the threshold value and the unknown parameter to be estimated for this case. So in order to minimize this error in estimation, we try to use an adaptive quantization scheme where the quantization threshold value changes according to the observations of all the previous sensors in the system.

In all the previous works, they mainly focussed on the energy or the cost constraints. Security, which is an important issue for the system has been neglected. In a WSN there might be an eavesdropper (Third Party Fusion Center or the Enemy Fusion Center) who try to tap the channel and get the information from the sensor observations and then further estimate the unknown parameter for its own benefit. If it knows the model of the system completely, it might also try to distort the channel between the sensors and the fusion center by sending some jamming signals so that the estimate made by the original (Ally)

fusion center is no more effective. So this physical layer security is an important issue in the design of a WSN. *Aysal et. al.,* first proposed a stochastic encryption scheme so as to improve the security. Inspired from this, we use a similar kind of encryption scheme in this thesis.

Here we thus discuss the performance of the serial wireless sensor network using adaptive quantization with security added. Stochastic enciphers are introduced in the system at the sensors end so that the performance of the AFC is better than that of the TPFC which try to seek information from the network illegally. Hence it is reasonable to assume that probability distribution of the encipher is known only to the AFC.

Here we also assume that the TPFC has no knowledge that there is an encryption process going in the system. Even if it comes to know about the encryption, as it does not the know the probability distribution of the ciphering used, there is always an error in the estimate for TPFC.

# 2 System Model

In this chapter, we will discuss the model of the system we assumed. We consider an encrypted WSN system in our design so as to protect the information against any unauthorized user. In a general WSN, any third-party fusion center (TPFC) can moniter the transmission medium and can have an access to the quantized sensor outputs using which they can perform the same calculations as an ally fusion center (AFC) and find an optimal maximum-likelihood (ML) estimate for the unknown parameter [8]. Hence, we consider a probabilistic encryption scheme in our thesis.

We consider the estimation of a deterministic unknown parameter $\theta$ from quantized observation in an encrypted WSN. Suppose we have N sensors distributed spatially and each making an observation of $\theta$

$$x_i = \theta + W_i \tag{2.1}$$

where $W_i$ denotes the additive noise (i.i.d) with zero-mean. Here we assume that the binary output of the sensor is encrypted probabilistically. We consider symmetric-key encryption where the "0" and "1" enciphering probabilities are equal. We derive the Cramer-Rao lower bound for this estimation problem for the ally fusion center. Further, we also try to analyze the effect of this encryption on the enemy fusion center (Third party fusion center) which does not know that the system is encrypted. The 1-bit quantizer used by the sensor is

$$b_i = Q_i(x_i) \tag{2.2}$$

Now the binary data $b_i$ is encrypted and sent to the fusion center to make an estimate of $\theta$. We assume that the sensors use the channel by time-sharing and transmit the data sequentially [20]. We assume that the data transmitted by each sensor can be heard by every other sensor in the network due to the broadcasting nature of the channel. We further assume that the data is received without any errors and assume that the quantization process is independent of the channel.

## 2.1 Quantization

The sensor 1's 1-bit quantizer uses an arbitrary threshold, say $\tau_1 = 0$, to generate $b_1$ which is encrypted and sent to all other sensors by broadcasting.

$$b_1 = sgn\{x_1 - \tau_1\} \tag{2.3}$$

Here these decisions are transmitted to the fusion center through a wireless channel which can be accessed by any other unauthorized user who can estimate $\theta$ from its observations. In order to degrade the estimation of this unauthorized user, we encrypt the data and then transmit it through the channel so as to make it inaccessible to other users. We use a probabilistic cipher whose distribution is known only to the AFC (Ally Fusion Center).

The encryption method used here is defined as

$$Pr(\tilde{b}_n = 1|b_n = 0) = Pr(\tilde{b}_n = 0|b_n = 1) = p$$

$$Pr(\tilde{b}_n = 0|b_n = 0) = Pr(\tilde{b}_n = 1|b_n = 1) = 1 - p$$

Here note that the performance of the system is degraded due to this encryption process and hence the performance of the non-encrypted network is always better compared to the encrypted one.

Now, sensor 2 receives $\tilde{b}_1$ instead of $b_1$ because of this cipher and it then computes $\tau_2 = \tilde{b}_1\Delta$, where $\Delta$ is a positive number referred to as stepsize. Using this, sensor-2 generates $b_2$ and $\tau_3$ as

$$b_2 = sgn\{x_2 - \tau_2\} \tag{2.4}$$

$$\tau_3 = \tau_2 + \tilde{b}_2\Delta = (\tilde{b}_1 + \tilde{b}_2)\Delta \tag{2.5}$$

In general, for the $n^{th}$ sensor we have

$$\tau_n = \tau_{n-1} + \tilde{b}_{n-1}\Delta = \Delta\sum_{k=1}^{n-1}\tilde{b}_k \tag{2.6}$$

and the sensor generates $b_n$ using this $\tau_n$ as

$$b_n = sgn\{x_n - \tau_n\} \tag{2.7}$$

and transmits $\tilde{b}_n$.

Note that usually sensors are deployed in a large number and so we have resource constraints on WSNs. This restricts the cost of the sensors and power utilization. This, in turn restricts the bandwidth and the number of computations at the sensors. Hence, we considered the most restricted case in our system in which each sensor trasmits a single bit. As the probabilistic enciphering scheme used is just like coin flipping, it does not increase the number of bits, communication costs, or bandwidth utilization. [8]

# 3 Analysis for AFC

In this chapter we try to find the optimal estimate of the unknown parameter $\theta$ for the AFC. For that, we first analyze the distribution of the thresholds of the sensors. We minimize the maximum likelihood function to find the maximum likelihood estimate of $\theta$. In our system, we have seen that AFC has access to the encryption probability $p$.

We first try to find the distribution of the thresholds. We can observe that $b_i \in \{\pm 1\}$. This means, $\tau_n = i\Delta$ implies

$$\tau_{n+1} = \begin{cases} (i+1)\Delta, & if \quad \tilde{b}_n = 1 \\ (i-1)\Delta, & if \quad \tilde{b}_n = -1 \end{cases} \tag{3.1}$$

From which we can find the transition probability as

$$\begin{aligned} P(\tau_{n+1} = (i+1)\Delta | \tau_n = i\Delta) &= P(\tilde{b}_n = 1 | \tau_n = i\Delta) \\ &= P(\tilde{b}_n = 1 | \tau_n = i\Delta, b_n = 1) P(b_n = 1 | \tau_n = i\Delta) \\ &\quad + P(\tilde{b}_n = 1 | \tau_n = i\Delta, b_n = -1) P(b_n = -1 | \tau_n = i\Delta) \\ &= (1-p) P(x_n > i\Delta) + p P(x_n < i\Delta) \\ &= (1-p) F_W(i\Delta - \theta) + p\left[1 - F_W(i\Delta - \theta)\right] \end{aligned}$$

and

$$
\begin{aligned}
P(\tau_{n+1} = (i-1)\Delta | \tau_n = i\Delta) &= P(\tilde{b}_n = -1 | \tau_n = i\Delta) \\
&= P(\tilde{b}_n = -1 | \tau_n = i\Delta, b_n = 1) P(b_n = 1 | \tau_n = i\Delta) \\
&\quad + P(\tilde{b}_n = -1 | \tau_n = i\Delta, b_n = -1) P(b_n = -1 | \tau_n = i\Delta) \\
&= pP(x_n > i\Delta) + (1-p)P(x_n < i\Delta) \\
&= pF_W(i\Delta - \theta) + (1-p)\left[1 - F_W(i\Delta - \theta)\right]
\end{aligned}
$$

Therefore, in general,

$$
P(\tau_{n+1} = j\Delta | \tau_n = i\Delta) = \begin{cases} pF_W(i\Delta - \theta) + (1-p)\left[1 - F_W(i\Delta - \theta)\right], & if \quad j = i-1 \\ (1-p)F_W(i\Delta - \theta) + p\left[1 - F_W(i\Delta - \theta)\right], & if \quad j = i+1 \\ 0, & else \end{cases} \tag{3.2}
$$

From this it can be seen that, $\{\tau_n\}$ is a homogeneous random walk. Let $P_{n,j} \triangleq P(\tau_n = j\Delta)$. Then the pmf of $\tau_n$ is given by

$$
P_{n,j} = P_{n-1,j-1} P(\tau_n = j\Delta | \tau_{n-1} = (j-1)\Delta) + P_{n-1,j+1} P(\tau_n = j\Delta | \tau_{n-1} = (j+1)\Delta) \tag{3.3}
$$

## 3.1 Stationary Distribution

In the following section, we prove that the chain $\tau_n$ is a recurrent non-null and therefore has a stationary distribution. We also find a closed form solution for this stationary distribution.

Let

$$p_{i,j} = P(\tau_{n+1} = j\Delta | \tau_n = i\Delta) \tag{3.4}$$

This is a two-sided random walk. For $p = 0$ or $p = 1$, this reduces to the problem analyzed in [22], [20].

What about $p \neq 0, 1$? Is there a stationary distribution for $\{\tau_n\}$?

$\{\tau_n\}$ is a periodic (period 2) irreducible Markov chain. Thus all states belong to the same class: all transient, all recurrent null or all recurrent non-null.

They can not be all transient. Suppose they are. Then the chain $\tau_n$ must drift to $\pm\infty$, that is, for any $x > 0$

$$\lim_{n\to\infty} P(|\tau_n| < x) = 0 \tag{3.5}$$

This, however, implies that the majority of $X_n$'s must be greater than $x$ in magnitude. Let $\mu_n(x)$ = number of $|X_1|, |X_2|, ..., |X_n|$ that are greater than $x$. Then, the above equation implies that

$$\lim_{n\to\infty} P\left(\frac{\mu_n(x)}{n} > 1/2\right) > 0 \tag{3.6}$$

Let

$$I_i = \begin{cases} 1, & if \quad |X_i| > x \\ 0, & else \end{cases}$$

Then, $\mu_n(x) = \sum_{i=1}^{n} I_i$. This implies,

$$E\mu_n(x) = \sum_{i=1}^{n} EI_i = \sum_{i=1}^{n} P(|X_i| > x)$$

Let $P(|X_i| > x) = \varepsilon(x)$, where $\varepsilon(x)$ is determined by the distribution of $X_n$. Clearly for $x$ large enough, $\varepsilon(x)$ can be made arbitrarily small i.e.,

$$\lim_{x\to\infty} \varepsilon(x) = 0$$

Thus,

$$\frac{E\mu_n(x)}{n} = \frac{n\varepsilon(x)}{n} = \varepsilon(x) \tag{3.7}$$

Now the above equation and the weak law of large numbers implies that

$$\lim_{n\to\infty} P\left(\frac{\mu_n(x)}{n} > 1/2\right) = 0$$

This shows that the chain is not transient. Therefore it is recurrent.

We will try to find a stationary distribution. If such distribution exists, then the chain is recurrent non-null.

Writing the balance equations, we get,

$$\Pi_k p_{k,k+1} = \Pi_{k+1} p_{k+1,k}$$

For $k > 0$,

$$\Pi_{k+1} = \Pi_k \frac{p_{k,k+1}}{p_{k+1,k}} = \Pi_{k-1} \frac{p_{k-1,k}}{p_{k,k-1}} \frac{p_{k,k+1}}{p_{k+1,k}} = .... = \Pi_0 \prod_{i=0}^{k} \frac{p_{i,i+1}}{p_{i+1,i}}$$

For $k < 0$,

$$\Pi_k = \Pi_{k+1} \frac{p_{k+1,k}}{p_{k,k+1}} = .... = \Pi_0 \prod_{i=0}^{k+1} \frac{p_{i,i-1}}{p_{i-1,i}}$$

Let $G_i = \dfrac{p_{i,i-1}}{p_{i-1,i}}$. Then,

$$\begin{aligned} G_i &= \frac{pF_n(i\Delta-\theta)+(1-p)\left[1-F_n(i\Delta-\theta)\right]}{(1-p)F_n((i-1)\Delta-\theta)+p\left[1-F_n((i-1)\Delta-\theta)\right]} \\ &= \frac{(1-p)-(1-2p)F_n(i\Delta-\theta)}{p+(1-2p)F_n((i-1)\Delta-\theta)} \end{aligned}$$

Then, we have

$$\Pi_k = \begin{cases} \Pi_0 \left[\prod_{i=1}^{k} G_i\right]^{-1}; & k>0 \\ \Pi_0; & k=0 \\ \Pi_0 \left[\prod_{i=0}^{k+1} G_i\right]; & k<0 \end{cases} \tag{3.8}$$

Now by choosing

$$\Pi_0 = \left\{1+\sum_{k=1}^{\infty}\left[\prod_{i=1}^{k+1} G_i\right]^{-1} + \sum_{k=-\infty}^{-1}\left[\prod_{i=0}^{k+1} G_i\right]\right\}^{-1}$$

we ensure that $\sum_{-\infty}^{\infty} \Pi_k = 1$ and thus $\Pi_k$ is the stationary distribution.This follows from the following theorem.

**Theorem:** Let $X$ be an irreducible recurrent chain with the transition matrix $P$. Then $\underline{\nu} = \underline{\nu}P$ has a strictly positive solution which is unique to within a constant multiplication.

This theorem and the fact that $\tau_n$ is recurrent implies that $\Pi_0 \neq 0$ and thus $\Pi_k$ is strictly

positive.

It can be proved that for $0 \leqslant p < 0.5$, the Markov chain is recurrent non-null and therefore we have a solution. But for $1 \geqslant p > 0.5$, the chain becomes transient and for $p = 0.5$, it becomes recurrent null. Therefore for $0 \leqslant p < 0.5$, the chain has a stationary distribution.

## 3.2 Asymptotic Distribution of Thresholds

Calculating Cramer-Rao Bound (CRB) using the previous described distribution of thresholds is not so convenient. Therefore, we examine the asymptotic performance of this distribution. We can notice that $\{\tau_n\}$ form a Markov chain with the transition probabilities given above.The convergence in distributions of $\{\tau_{2n}\}$ and $\{\tau_{2n+1}\}$ follows from a stationarity theorem [22]

$$\lim_{n\to\infty} P_{2n,k} = P_{e,k}, \lim_{n\to\infty} P_{2n+1,k} = P_{o,k} \tag{3.9}$$

We can observe that $\tau_{2n}$ takes only odd states $\{\pm\Delta, ...., \pm(2n-1)\Delta\}$ and $\tau_{2n+1}$ takes only even states $\{0, \pm 2\Delta, ...., \pm 2n\Delta\}$ i.e., $P_{e,2i} = 0$ and $P_{o,2i+1} = 0$ for any integer $i$. Thus the chain is periodic with period 2. For a large number of states, we have *atypical states* whose steady-state probability decereases with increase in $n$ value and *typical states* whose steady-state probability remains significant as $n$ increases. These typical states are those threshold values which are relatively close to $\theta$. Here we see the asymptotic analysis by ignoring the atypical states and just considering the typical states. We define a new vector $\Pi$ as

$$\Pi \triangleq [P_{o,-2k}, P_{e,-2k+1}, P_{o,-2k+2}, P_{e,-2k+3}, ...., P_{o,2k}, P_{e,2k+1}]^T \tag{3.10}$$

where $k$ is chosen large enough so as to include all typical states in the Markov chain. By this asymptotic analysis, considering the transition between $\{\tau_{2n}\}$ and $\{\tau_{2n+1}\}$, we can see that

$$P_{e,2j+1} = P_{o,2j}P(\tau_{2n} = (2j+1)\Delta|\tau_{2n-1} = 2j\Delta)+P_{o,2j+2}P(\tau_{2n} = (2j+1)\Delta|\tau_{2n-1} = (2j+2)\Delta)$$

$$P_{o,2j} = P_{e,2j-1}P(\tau_{2n+1} = 2j\Delta|\tau_{2n} = (2j-1)\Delta) + P_{e,2j+1}P(\tau_{2n+1} = 2j\Delta|\tau_{2n} = (2j+1)\Delta)$$

where the transition probability is given by (3.2) and is independent of $n$. We can assume $\{P_{e,\pm 2k_1+1}\}$ and $\{P_{o,\pm 2k_1}\}$ to be zero for $k_1 > k$ if $k$ is large enough to include all typical states. We can write these equations in a matrix form as

$$\Pi = \mathbf{P}\Pi \tag{3.11}$$

where $\mathbf{P}$ is the transition matrix given by

$$\mathbf{P} = \begin{pmatrix} 0 & t_{-2k+1,-2k} & 0 & ... & & & 0 \\ t_{-2k,-2k+1} & 0 & t_{-2k+2,-2k+1} & 0 & ... & & 0 \\ 0 & t_{-2k+1,-2k+2} & 0 & t_{-2k+3,-2k+2} & 0 & ... & 0 \\ \vdots & & & \ddots & & & \vdots \\ 0 & \dots & & & t_{2k-1,2k} & 0 & t_{2k+1,2k} \\ 0 & \dots & & & & t_{2k,2k+1} & 0 \end{pmatrix} \tag{3.12}$$

where, $t_{i,j} \triangleq P(\tau_{n+1} = j\Delta|\tau_n = i\Delta)$.

We see that $\mathbf{P}$ is a sparse matrix and its non-zero entries can be predetermined for the specified values of $\sigma_W$ (the variance of the noise distribution $F_w$) and $\Delta$. Using these equations $\Pi$ can be easily solved.

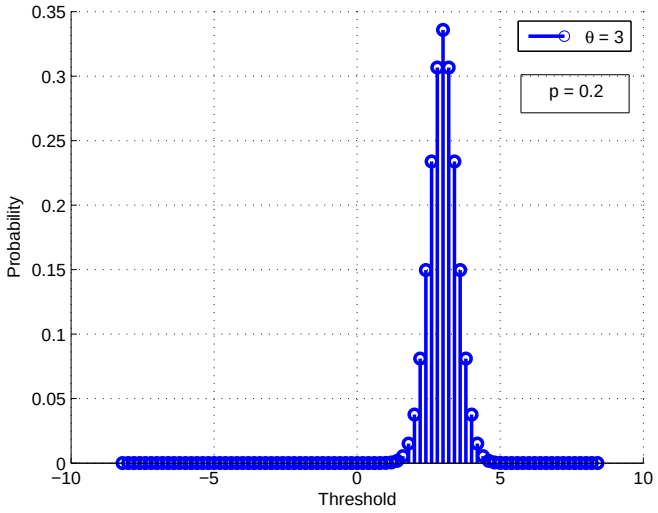


Figure 3.1: Asymptotic distribution of $\tau$ for $\theta = 3$ for Gaussian noise of $mean = 0$ and $\sigma_W = 1$

The above plot is plotted for $\Delta = 0.2$,$p = 0.2$ by using the condition $2k\Delta > |\theta| + 5\sigma_W$ which gives the proper choice of $k$ for Gaussian noise. [20]

## 3.3 Maximum Likelihood Function

We develop the Maximum Likelihood (ML) estimators at the fusion center to estimate the value of $\theta$ based on the binary data $\{\tilde{b}_1, ...., \tilde{b}_N\}$. We can observe that the sequence $\tilde{b}_1, \tilde{b}_2, ..., \tilde{b}_N$ is correlated in general. Now we can write the joint probability mass (pmf) of

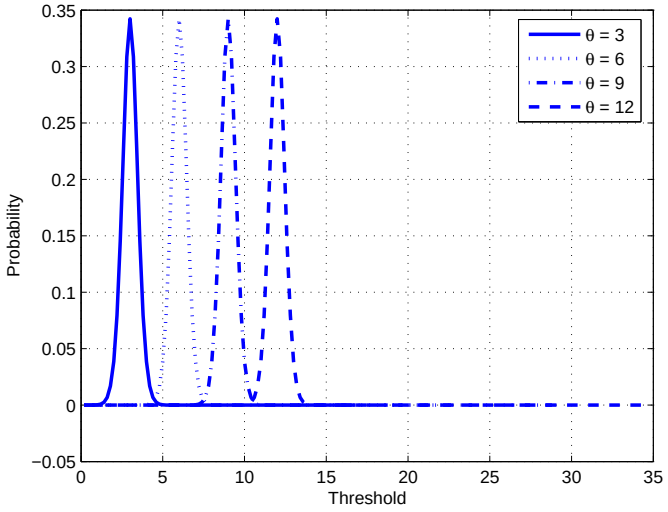


Figure 3.2: Asymptotic distribution of $\tau$ under different values of $\theta$ for Laplacian noise with b = 1

$\tilde{b}_1, \tilde{b}_2, ..., \tilde{b}_N$ as

$$\begin{aligned} P(\tilde{b}_1, ..., \tilde{b}_N; \theta) &= \prod_{n=1}^{N} P(\tilde{b}_n | \tilde{b}_1, ..., \tilde{b}_{n-1}; \theta) \\ &= \prod_{n=1}^{N} P(\tilde{b}_n | \tau_n; \theta) \end{aligned} \tag{3.13}$$

We know the conditional probability of $b_n$ based on the threshold $\tau_n$ is given by

$$P(b_n|\tau_n;\theta) = [F_W(\tau_n - \theta)]^{(1+b_n)/2} \times [1 - F_W(\tau_n - \theta)]^{(1-b_n)/2}$$

We also have,

$$\begin{aligned} P(\tilde{b}_n = 1|\tau_n, \theta) &= [F_W(\tau_n - \theta)](1-p) + [1 - F_W(\tau_n - \theta)](p) \\ &= p + F_W(\tau_n - \theta)(1-2p) \\ &\triangleq q(\theta, \tau_n, p) \end{aligned} \tag{3.14}$$

$$\begin{aligned} P(\tilde{b}_n = -1|\tau_n, \theta) &= [F_W(\tau_n - \theta)](p) + [1 - F_W(\tau_n - \theta)](1-p) \\ &= 1 - q(\theta, \tau_n, p) \end{aligned} \tag{3.15}$$

Now the conditional probability of $\tilde{b}_n$ based on the threshold $\tau_n$ is given by

$$P(\tilde{b}_n|\tau_n; \theta) = [q(\theta, \tau_n, p)]^{(1+\tilde{b}_n)/2} \times [1 - q(\theta, \tau_n, p)]^{(1-\tilde{b}_n)/2} \tag{3.16}$$

Therefore the log-likelihood function can be written as

$$L(\theta) = \sum_{n=1}^{N} \left\{ \left( \frac{1+\tilde{b}_n}{2} \right) \ln[q(\theta, \tau_n, p)] + \left( \frac{1-\tilde{b}_n}{2} \right) \ln[1 - q(\theta, \tau_n, p)] \right\} \tag{3.17}$$

## 3.4 Fisher Information

To evaluate the Cramer-Rao Lower bound (CRLB), we first find the Fisher information as CRLB is just the inverse value of the Fisher information. Fisher information for the estimation problem is given by ( [23])

$$J(\theta) = -\mathbb{E}\left\{ \frac{\partial^2 L(\theta)}{\partial \theta^2} \right\} \tag{3.18}$$

Hence, to evaluate $J(\theta)$, we need to compute $\dfrac{\partial^2 L(\theta)}{\partial \theta^2}$.

We know that $F'_W(x) \triangleq (\partial F_W(x)/\partial x) = -f_W(x)$. So we can write the second derivative of

the log-likelihood function $L(\theta)$ as

$$\begin{aligned}\frac{\partial^2 L(\theta)}{\partial\theta^2} &= \sum_{n=1}^{N}\left\{\left(\frac{1+\tilde{b}_n}{2}\right)\left(\frac{q''_\theta(\theta,\tau_n,p)}{q(\theta,\tau_n,p)}-\frac{[q'_\theta(\theta,\tau_n,p)]^2}{[q(\theta,\tau_n,p)]^2}\right)\right. \\ &\qquad \left.-\left(\frac{1-\tilde{b}_n}{2}\right)\left(\frac{q''_\theta(\theta,\tau_n,p)}{1-q(\theta,\tau_n,p)}+\frac{[q'_\theta(\theta,\tau_n,p)]^2}{[1-[q(\theta,\tau_n,p)]^2]^2}\right)\right\} \qquad (3.19)\\ &\triangleq \sum_{n=1}^{N} A(\tilde{b}_n,\tau_n,\theta)\end{aligned}$$

where $q'_\theta(\theta,\tau_n,p) = \partial q(\theta,\tau_n,p)/\partial\theta$ and $q''_\theta(\theta,\tau_n,p) = \partial q'_\theta(\theta,\tau_n,p)/\partial\theta$ are the derivatives with respect to $\theta$. Now the Fisher information is given by

$$J(\theta) = -\sum_{n=1}^{N}\mathbb{E}_{\tilde{b}_n,\tau_n}\{A(\tilde{b}_n,\tau_n,\theta)\} \qquad (3.20)$$

where $\mathbb{E}_{\tilde{b}_n,\tau_n}$ denotes the expectation with respect to the joint distribution of $\tilde{b}_n$ and $\tau_n$. We have

$$P(\tilde{b}_n,\tau_n;\theta) = P(\tau_n;\theta)P(\tilde{b}_n|\tau_n;\theta) \qquad (3.21)$$

Hence we can write

$$\begin{aligned}J(\theta) &= -\sum_{n=1}^{N}\mathbb{E}_{\tau_n}\{\mathbb{E}_{\tilde{b}_n|\tau_n}[A(\tilde{b}_n,\tau_n,\theta)]\} \\ &= \sum_{n=1}^{N}\mathbb{E}_{\tau_n}\left[\frac{f_W^2(\tau_n-\theta)(1-2p)^2}{[q(\theta,\tau_n,p)][1-q(\theta,\tau_n,p)]}\right] \qquad (3.22)\\ &= \sum_{n=1}^{N}\int P(\tau_n;\theta)G(\tau_n;\theta)d\tau_n\end{aligned}$$

where $\mathbb{E}_{\tau_n}$ denotes the expectation with respect to the distribution $P(\tau_n, \theta)$, $\mathbb{E}_{\tilde{b}_n|\tau_n}$ denotes the expectation with respect to the conditional distribution $P(\tilde{b}_n|\tau_n; \theta)$. We write the first equality based on the fact that $\tilde{b}_n$ is a binary random variable with

$$P(\tilde{b}_n = 1|\tau_n, \theta) = q(\theta, \tau_n, p)$$

$$P(\tilde{b}_n = -1|\tau_n, \theta) = 1 - q(\theta, \tau_n, p)$$

and

$$q'_\theta(\theta, \tau_n, p) = -f_W(\tau_n - \theta)(1 - 2p)$$

where $p$ denotes the probabilistic cipher parameter. Define

$$G(\tau_n; \theta) \triangleq \left[ \frac{f_W^2(\tau_n - \theta)(1 - 2p)^2}{[q(\theta, \tau_n, p)][1 - q(\theta, \tau_n, p)]} \right]$$

We can observe that for symmetrical Gaussian noise or Laplacian noise, $G(\tau_n; \theta)$ is a unimodal, positive and symmetric function achieving its maximum at $\tau_n = \theta$ for any value of the crossover probability $p$ and hence maximizing the Fisher information value when $P(\tau_n; \theta) = \delta()\tau_n - \theta$. This means that the best achievable performance of the AQ (Adaptive Quantization) scheme will not exceed that of the FQ (Fixed Quantization) approach with the optimal threshold ($\tau = \theta$).

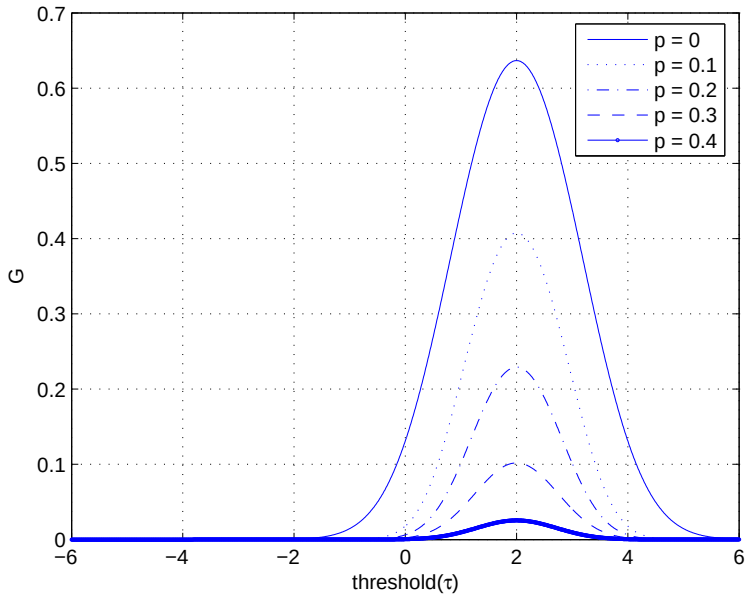


Figure 3.3: Plot of $G(\tau_n;\theta)$ for different values of $p$ for Gaussian noise

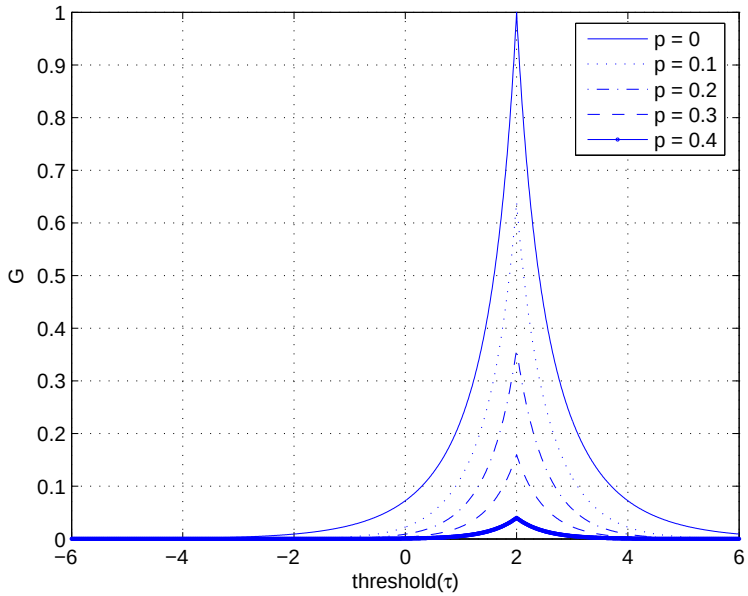


Figure 3.4: Plot of $G(\tau_n;\theta)$ for different values of $p$ for Laplacian noise

## 3.5 Cramer-Rao Bound for AFC

Cramer-Rao Bound (CRB) or Cramer-Rao Lower Bound (CRLB) gives a lower bound on the variance of the estimators of a deterministic parameter. This states that the variance of an estimator is atleast as high as the inverse of the Fisher information [25]. An estimator which achieves this lower bound is said to be efficient. Hence, to see the performance of the estimator we describe later, we first try to evaluate the CRLB value for AFC.

We can rewrite equation (3.21) as the summation of two terms as

$$\begin{aligned} J(\theta) &= \sum_{n=1}^{N} \int P(\tau_n;\theta) G(\tau_n;\theta) d\tau_n \\ &= \sum_{n=1}^{N_c} \int P(\tau_n;\theta) G(\tau_n;\theta) d\tau_n + \sum_{n=N_c+1}^{N} \int P(\tau_n;\theta) G(\tau_n;\theta) d\tau_n \\ &\triangleq J_1 + J_2 \end{aligned} \tag{3.23}$$

where $N_c$ is chosen so that the distribution $P(\tau_n;\theta)$ converges or has negligible difference from the steady-state probability vector $\Pi$ for $n > N_c$. We have

$$N_c \frac{2}{\pi\sigma_n^2} > J_1 > 0 \tag{3.24}$$

and

$$J_2 = \frac{1}{2}(N - N_c)\mathbf{g}^T\Pi \tag{3.25}$$

where the above equality comes from the fact that $P(\tau_n;\theta)$ is discrete and invariant for $n > N_c$. Therefore we have the upper and lower bounds of $CRB^{AFC}$ as

$$\frac{N}{N-N_c}\frac{2}{N\mathbf{g}^T\Pi} > CRB^{AFC}(\theta) > \frac{N}{N+N_c\varepsilon}\frac{2}{N\mathbf{g}^T\Pi} \tag{3.26}$$

where $\varepsilon \triangleq (2/(\pi\sigma_n^2)) - (\mathbf{g}^T\Pi/2)$.

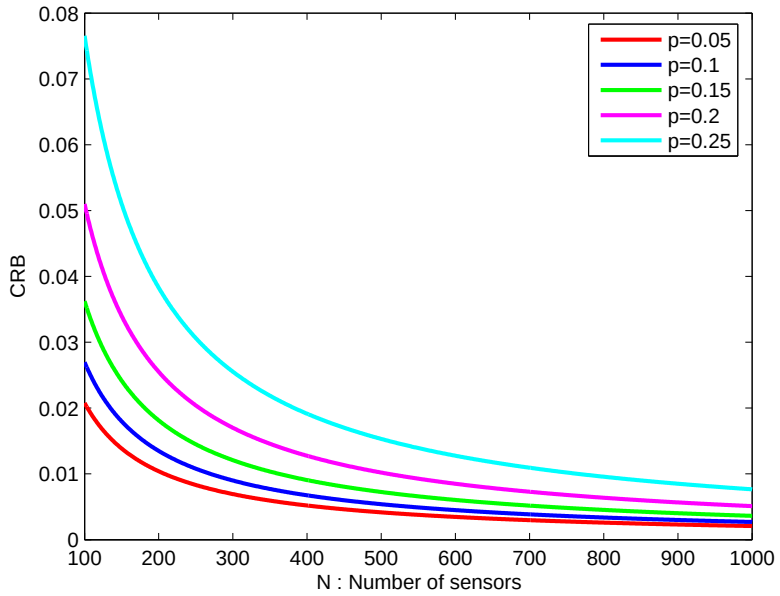


Figure 3.5: CRB as a function of number of sensors for different values of probability $p$ for Gaussian noise

Since $N \gg N_c$, we can assume that both upper and lower bound approach to $(2/(N\mathbf{g}^T\Pi))$. Therefore we have

$$CRB^{AFC}(\theta) \to \frac{2}{N\mathbf{g}^T\Pi} \tag{3.27}$$

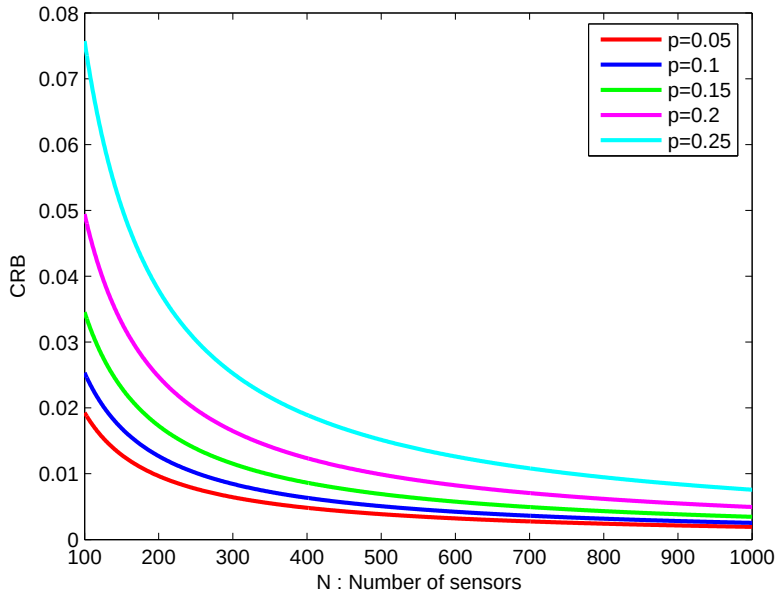


Figure 3.6: CRB as a function of number of sensors for different values of probability $p$ for Laplacian noise

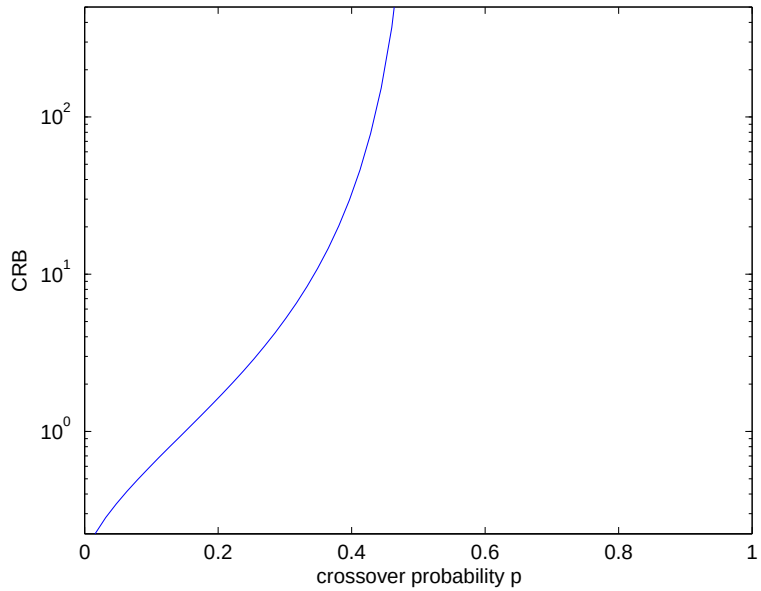


Figure 3.7: CRB as a function of probability $p$ for $N = 200$, $\theta = -1$ with Gaussian noise

where $\mathbf{g}$ is defined as

$$\mathbf{g} \triangleq [G(-2k\Delta;\theta) \;\; G((-2k+1)\Delta;\theta) \;\; ... \;\; G((2k+1)\Delta;\theta)]^T$$

From fig 3.7 we can observe that CRB is an increasing function for $0 < p < 0.5$. As mentioned earlier, we have a solution only for $0 \leqslant p < 0.5$. From fig 3.5 and 3.6 we can also observe that CRB value decreases with the number of sensors deployed for both Gaussian and Laplacian noise.

### 3.5.1 Comparison of CRLB for Adaptive Quantization and Fixed Quantization Schemes

In the previous section we found out the CRLB value for AFC using adaptive quantization scheme. The CRLB value for AFC using fixed quantization is given in [8]. So now in this section, we try to compare these two CRLB values and try to show that the performance of our system is better compared to that of a system using a FQ technique using simulations.

In the above graphs, the continuous plots are for system using FQ and dotted plots are for AQ system. In fig. 3.8, the fixed threshold value for the FQ scheme used is $\tau = 0$ which is quite deviated from the true $\theta$ value which is 1. Here, if we can find an optimal estimate for the unknown parameter for both the systems, the performance of our system is better than that of the system using FQ technique as we can achieve a much lower CRLB value. But in fig 3.9, the fixed threshold value for the FQ scheme used is $\tau = 0.5$ which is closer to $\theta$. Here the performance of system using FQ is better for smaller value of number of

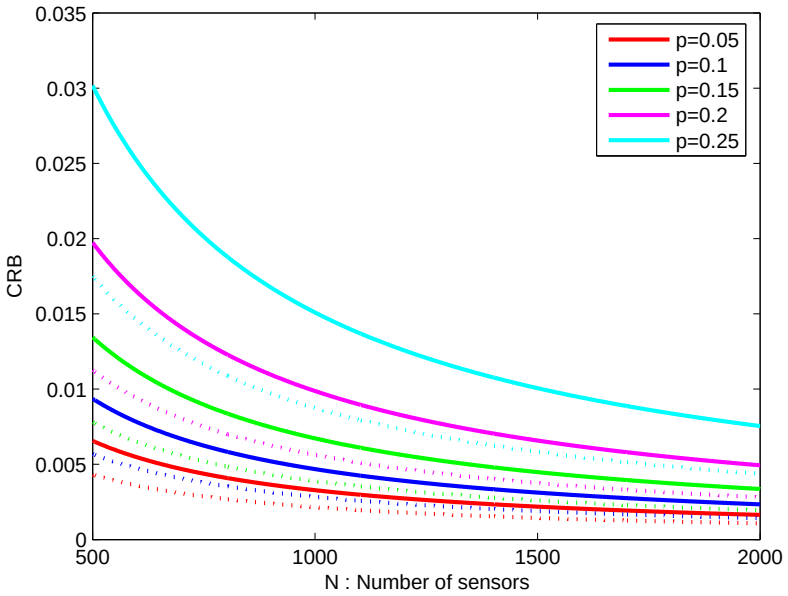


Figure 3.8: CRLB as a function of probability $p$ for $N = 200$, $\theta = -1$ with Gaussian noise and $\tau = 0, \theta = 1$ for fixed quantization

sensors. But as the number of sensors increase asymptotically, the performance of both the systems is nearly the same.

In general, AFC will not know the prior probablities (distribution of $\theta$) of the unknown parameter. Hence, if the choice of the threshold for FQ is very much deviated from the true value of $\theta$, which is the general case, the performace of our system is always better.

## 3.6 Maximum Likelihood Estimate for AFC

Maximum Likelihood estimator (MLE) estimates the value of the unknown parameter $\theta$ that most likely causes a given value of observation to occur. Simply to state, we can get the value of MLE by maximizing the likelihood function. So now we try to find MLE for

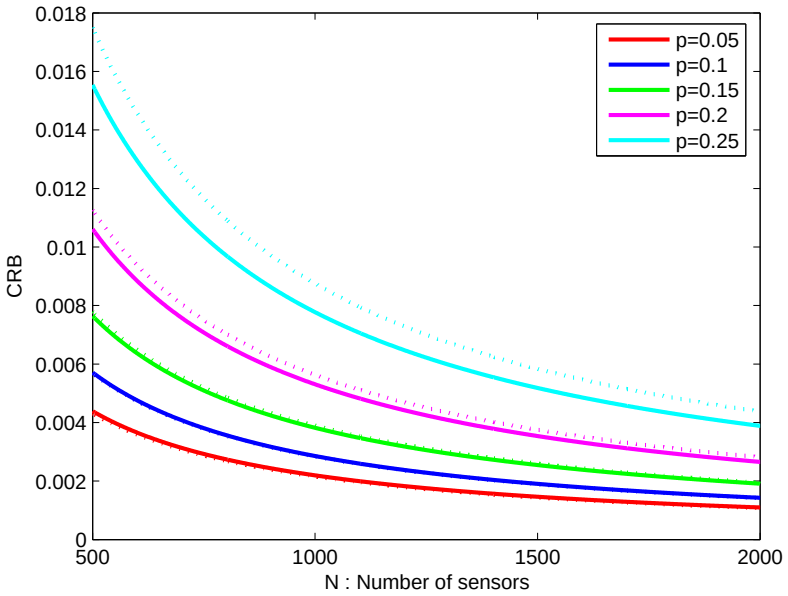


Figure 3.9: CRLB as a function of probability $p$ for $N = 200$, $\theta = -1$ with Gaussian noise and $\tau = 0.5, \theta = 1$ for fixed quantization

the AFC.

We can observe that the ML estimate of $\theta$ for varying $\tau_n$ does not have a closed form solution. Therefore we now try to find out the ML estimate of AFC based on threshold $\tau_n$. We have log-likelihood function given by (3.17). Because for the ML estimate, the likelihood function is maximized, we differentiate this log-likelihood function with respect to $q(\theta, \tau_n, p)$ and equate to zero. Then we get

$$\sum_{n=1}^{N} \hat{q}_{ML}(\theta, \tau_n, p) = \sum_{n=1}^{N} \left( \frac{1 + \tilde{b}_n}{2} \right) \tag{3.28}$$

Now we have,

$$\frac{1}{N}\sum_{n=1}^{N}\hat{q}_{ML}(\theta,\tau_n,p)=\frac{1}{N}\sum_{n=1}^{N}\left(\frac{1+\tilde{b}_n}{2}\right)$$

Since $\tau_n$ is an irreducible Markov chain with stationary distribution $\Pi$, we can write

$$\frac{1}{N}\sum_{n=1}^{N}q(\theta,\tau_n,p)\longrightarrow\mathbb{E}\{q(\theta,\tau,p)\}$$

where $\mathbb{E}\{.\}$ denotes the expectation value and $\tau$ has the distribution $\Pi$.

Note that

$$q(\theta,\tau_n,p)=p+F_W(\tau_n-\theta)(1-2p)$$

. So we can write the expectation value as

$$\mathbb{E}\{q(\theta,\tau,p)\}=p+(1-2p)\sum_i F_w(\tau_i-\theta)\pi_i \tag{3.29}$$

We can approximate the discrete distribution of $\tau_i$ in continuous form. By plotting the $\tau$ distribution and appoximating it with a generalized gaussian distribution, we can write the pdf of $\tau$ as

$$p_{\tau i}(\tau_i)=\frac{\beta}{2\alpha\Gamma(1/\beta)}\exp\left\{-\left(\frac{\tau_i-\mu}{\alpha}\right)^{\beta}\right\} \tag{3.30}$$

where $\beta=2$ is the shape constant and $\alpha$ is the scale constant which varies with the $p$.

Now we can write

$$\sum_i F_w(\tau_i-\theta)\pi_i=\int F_w(\tau-\theta)p_\tau(\tau)d\tau$$

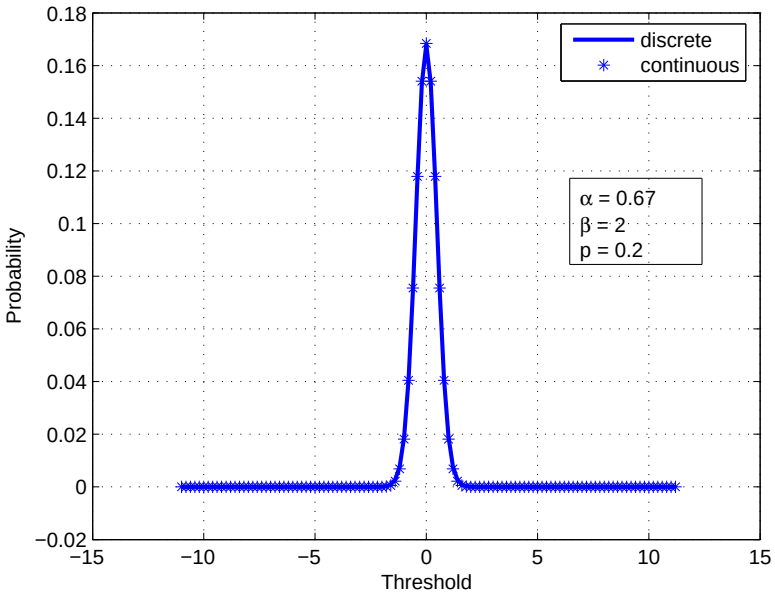


Figure 3.10: Approximation of $\tau$ distribution by a continuous distribution for $p = 0.2$

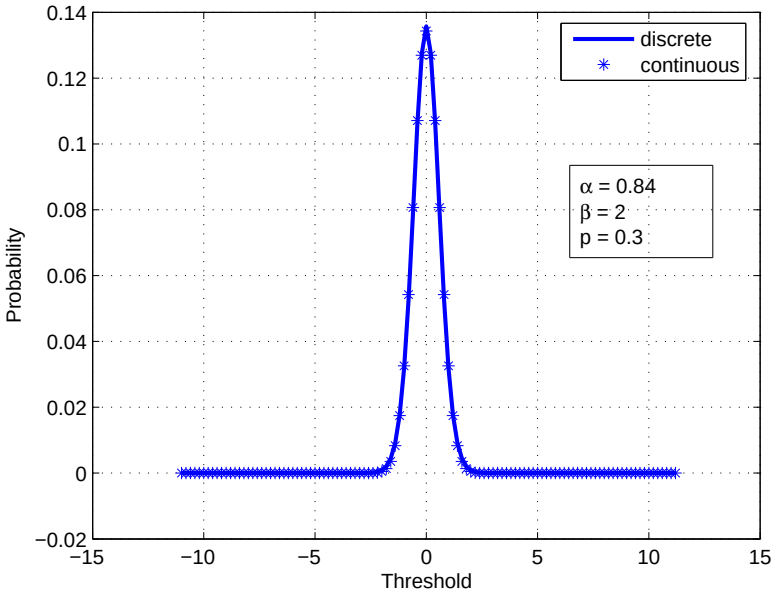


Figure 3.11: Approximation of $\tau$ distribution by a continuous distribution for $p = 0.3$

Let us calculate this integral as follows

$$\begin{aligned}
\int F_w(\tau-\theta)p_\tau(\tau)d\tau &= \int\frac{1}{2}\left\{1-erf\left(\frac{\tau_i-\theta-\mu_1}{\sigma\sqrt{2}}\right)\right\}\frac{\beta}{2\alpha\Gamma(1/\beta)}\exp\left\{-\left(\frac{|\tau_i-\mu_2|^\beta}{\alpha}\right)\right\}d\tau \\
&= \frac{\beta}{4\alpha\Gamma(1/\beta)}\int\left\{1-\left(\frac{\tau_i-\theta-\mu}{\sigma\sqrt{2}}\right)\right\}\exp\left\{-\left(\frac{|\tau_i-\theta-\mu|^\beta}{\alpha}\right)\right\}d\tau \\
&= \frac{\beta}{4\alpha\Gamma(1/\beta)}\int\left(\exp\left\{-\frac{|\tau_i-\theta-\mu|^\beta}{\alpha}\right\}\right. \\
&\qquad \left.-\frac{2}{\sqrt{\pi}}\int_{t=0}^{\frac{\tau_i-\theta-\mu}{\sigma\sqrt{2}}}\exp\{-t^2\}dt.exp\left\{-\frac{|\tau_i-\theta-\mu|^\beta}{\alpha}\right\}\right)d\tau \\
&= \frac{\beta}{4\alpha\Gamma(1/\beta)}\int_{-\infty}^{\infty}\exp\left\{-\frac{|\tau_i-\theta-\mu|^\beta}{\alpha}\right\}\tau_i \\
&\qquad -\frac{\beta}{2\alpha\sqrt{\pi}\Gamma(1/\beta)}\int_{-\infty}^{\infty}\int_{t=0}^{\frac{\tau_i-\theta-\mu}{\sigma\sqrt{2}}}\exp\{-t^2\}.\exp\left\{-\frac{|\tau_i-\theta-\mu|^\beta}{\alpha}\right\}d\tau dt
\end{aligned}$$

Let $c_1=\dfrac{\beta}{4\alpha\Gamma(1/\beta)}$, $c_2=\dfrac{\beta}{2\alpha\sqrt{\pi}\Gamma(1/\beta)}$, the first integral in the above equation be $I_1$ and the second integral be $I_2$. Define $A\triangleq\int F_w(\tau-\theta)p_\tau(\tau)d\tau$.

Now

$$I_2=\int_{-\infty}^{\infty}\exp\left\{-\frac{|\tau_i-\theta-\mu|^\beta}{\alpha}\right\}\left(\int_{t=0}^{\frac{\tau-\theta-\mu}{\sigma\sqrt{2}}}\exp\{-t^2\}dt\right)d\tau \tag{3.31}$$

We can find that

$$\begin{aligned}\int_{t=0}^{\frac{\tau-\theta-\mu}{\sigma\sqrt{2}}} e^{-t^2}dt &= \int_{t=0}^{\infty} e^{-t^2}dt - \int_{\frac{\tau-\theta-\mu}{\sigma\sqrt{2}}}^{\infty} e^{-t^2}dt \\ &= \frac{1}{\sqrt{\pi}}\left\{\frac{1}{2} - Q\left(\frac{\tau-\theta-\mu}{\sigma}\right)\right\}\end{aligned} \tag{3.32}$$

Substituting this in $I_2$, we get,

$$\begin{aligned}I_2 &= \frac{1}{2\sqrt{\pi}}\int_{-\infty}^{\infty}\exp\left\{-\frac{|\tau-\theta-\mu|^\beta}{\alpha}\right\}d\tau \\ &\quad -\frac{1}{\sqrt{\pi}}\int_{-\infty}^{\infty}\exp\left\{-\frac{|\tau-\theta-\mu|^\beta}{\alpha}\right\}Q\left(\frac{\tau-\theta-\mu}{\sigma}\right)d\tau\end{aligned} \tag{3.33}$$

Let the second integral in the above equation be $I_3$. This implies,

$$A = \left(c_1 - \frac{c_2}{2\sqrt{\pi}}\right)I_1 + \frac{c_2}{\sqrt{\pi}}I_3$$

We have already seen that $\beta = 2$ in our case from the previous graphs. Hence, substituting that value and simplifying, we get

$$I_1 = \int_{-\infty}^{\infty}\exp\left\{-\frac{(\tau-\theta-\mu)^2}{\alpha}\right\}d\tau$$

But we know,

$$\frac{1}{b\sqrt{2\pi}}\int_{-\infty}^{\infty}\exp\left\{-\frac{(x-a)^2}{2b^2}\right\}dx = 1$$

for any variable $x$. Hence, we get,

$$I_1 = \sqrt{\pi\alpha} \tag{3.34}$$

Now,

$$I_3 = \int_{-\infty}^{\infty} Q\left(\frac{(\tau-\theta-\mu)}{\sigma}\right)\exp\left\{-\frac{(\tau-\theta-\mu)^2}{\alpha}\right\}d\tau$$

Let $\frac{\tau-\theta-\mu}{\sqrt{\alpha}} = \frac{\psi}{\sqrt{2}}$. Then,

$$\begin{aligned} I_3 &= \int_{-\infty}^{\infty} Q\left(\frac{\psi\sqrt{\alpha}}{\sigma\sqrt{2}}\right)\exp\left\{-\frac{\psi^2}{2}\right\}\sqrt{\frac{\alpha}{2}}\,d\psi \\ &= \sqrt{\frac{\alpha}{2}}\int_{-\infty}^{\infty} Q\left(\frac{\psi\sqrt{\alpha}}{\sigma\sqrt{2}}\right)\exp\left\{-\frac{\psi^2}{2}\right\}d\psi \\ &= \sqrt{\alpha\pi}\,\mathbb{E}_{\psi}\left[Q\left(\frac{\psi\sqrt{\alpha}}{\sigma\sqrt{2}}\right)\right] \end{aligned}$$

Where $\psi \sim \mathcal{N}(0,1)$. To calculate the above equation, we first find the expectation of $Q(x)$ for $x \sim \mathcal{N}(0,1)$ as follows

$$\begin{aligned}
\mathbb{E}_x[Q(x)] &= \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} Q(x)e^{-x^2/2}\,dx \\
&= \frac{1}{2\pi}\int_{-\infty}^{\infty}\int_{x}^{\infty} e^{-\frac{x^2+t^2}{2}}\,dt\,dx \\
&= \frac{1}{2\pi}\int_{-\infty}^{\infty}\int_{0}^{\infty} e^{-\frac{x^2+t^2}{2}}\,dt\,dx \\
&= 1/2
\end{aligned}$$

where we get the second equality from the fact that the curve we are integrating is symmetrical(axial symmetry) and hence the integral will be the same even if we rotate the curve along the z-axis.

Therefore, we have

$$\mathbb{E}_\psi\left[Q\left(\frac{\psi\sqrt{\alpha}}{\sigma\sqrt{2}}\right)\right] = 1/2$$

Substituting all these values in $A$ and simplifying, we get

$$A = c_1\sqrt{\pi\alpha}$$

Now using the fact that $\beta = 2$ and $\Gamma(1/2) = \sqrt{\pi}$, we get

$$A = 1/2\sqrt{\alpha}$$

Hence,

$$\mathbb{E}q(\theta, \tau, p) = p + (1-2p).(1/2\sqrt{\alpha}) \tag{3.35}$$

Rearraging and expressing $\theta$ in terms of $q(\theta, \tau_n, p)$, we get

$$\theta = \tau_n - F_W^{-1}\left(\frac{q(\theta,\tau_n,p)-p}{1-2p}\right)$$

We know that the ML estimate of a transformed parameter $\alpha = g(\theta)$, where $g(.)$ is a one-to-one function, is given as $\hat{\alpha} = g(\hat{\theta})$ [8].Here $q(\theta,\tau_n,p)$ is a one-to-one function of $\theta$. This gives us the ML estimate of $\theta$ for AFC as

$$\begin{aligned}\hat{\theta}_{ML}^{AFC} &= \tau_n - F_W^{-1}\left(\frac{\hat{q}(\theta,\tau_n,p)-p}{1-2p}\right) \\ &= \tau_n - F_W^{-1}(1/2\sqrt{\alpha})\end{aligned} \tag{3.36}$$

for $p \neq 0.5$. Here $F_W^{-1}$ denotes the inverse complementary cumulative distribution function(CCDF) of noise.

# 4 Analysis for TPFC

In this chapter we consider the effects of using an encrypted WSNs for the TPFC or the enemy/unauthorized fusion center. It is assumed that the TPFC has access to the output values of the sensors and the adaptive quantization scheme employed but has no knowledge about the encryption being used in the WSN. Note that the performance of TPFC would further deteriorate if these parameters are unknown.

For an unencrypted system, the log-likelihood function is given by [20]

$$L(\theta) = \sum_{n=1}^{N} \left\{ \left( \frac{1+b_n}{2} \right) \ln[F_W(\tau_n - \theta)] + \left( \frac{1-b_n}{2} \right) \ln[1 - F_W(\tau_n - \theta)] \right\} \tag{4.1}$$

As TPFC has no knowledge of this encryption, it assumes $\tilde{b}_n$ to $b_n$. Therefore, the log-likelihood function for TPFC is

$$L_{TPFC}(\theta) = \sum_{n=1}^{N} \left\{ \left( \frac{1+\tilde{b}_n}{2} \right) \ln[F_W(\tau_n - \theta)] + \left( \frac{1-\tilde{b}_n}{2} \right) \ln[1 - F_W(\tau_n - \theta)] \right\} \tag{4.2}$$

The analysis for TPFC would be exactly like in [20] except for the fact that it uses $\tilde{b}_n$ instead of $b_n$ and hence the performance is degraded. The MLE for this given by

$$\hat{\theta}_{ML}^{TPFC} = \arg\max_{\theta} L_{TPFC}(\theta) \tag{4.3}$$

In general, the above equation has no closed form solution and hence we can use a searching algorithm to compute numerically. For Gaussian noise, it can be shown that the above

likelihood function is concave in nature and therefore, any one-dimensional graidient based search algorithms with a random initial estimate would converge to the global maximum [20].

# 5 Conclusions and Future Work

We proposed a secure adaptive quantization scheme for a tandem sensor network where each sensor's quantization threshold value is adaptively adjusted according to the incoming data from both the sensor's observation and its previous sensor's transmission.

We first showed that chain of thresholds represented in the topological order of the network form a stationary distribution for AFC design. This stationary distribution is then obtained in closed form analytically as well as through numerical methods. Using this, we found the CRB and the optimal estimate for AFC. We showed that the performance of the system using adaptive quantization is better than that of the system using fixed quantization if the system does not know about the prior distribution of the unknown parameter and hence using a fixed threshold value which is quite deviated from the true value of the unknown parameter by comparing their CRLB values.

Although we discussed about the analysis of TPFC, we could not provide an analytical optimal estimate of the unknown parameter for the TPFC. We would try to get some numerical results for the estimates using some one-dimensional graidient based search algorithm for both AFC and TPFC so that we can compare the performance of both systems and analyze the effectiveness of this encryption scheme.

After having accomplished the mentioned results, many interesting extensions can be forseen, some of which are listed below.

As an immediate extension to our present formulation, we would like to analyze our AFC design using a more complicated encryption scheme where the cipher deterministically hops

from one distribution to another with in a pool of a known set of distributions. Another interesting extension is to consider a variable step-size adaptive quantization scheme with encryption so as to improve the rate of convergence of the threshold to the unknown paramater.

Another important extension is to provide an analytical solution to the TPFC's estimate, its variance and the performance gain guarenteed at AFC over TPFC. On can also envision optimal search algorithms to estimate the unknown parameter with better performance in terms of computational complexity.

Another very interesting problem is to analyze the performance of AFC in the presence of compromised (misbehaving) sensor nodes with a constraint on the performance of TPFC. The presence of misbehaving nodes in a tandem sensor network has a tremendous impact on the convergence of thresholds to the unknown parameter.

# References


[1] K.S.J. Pister and B. Warneke, "Mems for distributed wireless sensor networks," In *9th Intl Conf. on Electronics, Circuits and Systems*, Dubrovnik,Croatia, Sep. 2002.

[2] Z. Chair and P. K. Varshney, "Optimal data fusion in multiple sensor detection systems," *IEEE Trans. Aerospace Elect. Syst.,* vol. AES-22, pp. 98-101, Jan. 1986.

[3] R. Viswanathan and P. K. Varshney, "Distributed detection with multiple sensors: Part I- Fundamentals," *Proc. of the IEEE,* vol. 85, no. 1, pp. 54-63, Jan. 1997.

[4] I. F. Akyildiz, W. Su, Y. Sankasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," *Computer Networks,* vol. 38, pp. 393-422, 2002.

[5] D. Castanon and D. Teneketzis, "Distributed estimation algorithms for nonlinear systems," *IEEE Trans. Autom. Control,* vol. AC-30, no. 5, pp. 418-425, May 1985.

[6] J. L. Speyer, "Computation and transmission requirements for a decentralized linear-quadratic-Gaussian control problem," *IEEE Trans. Autom. Control,* vol. AC-24, no. 2, pp. 266-269, Apr. 1979.

[7] A. S. Willsky, M. Bello, D. Castanon, B. Levy, and G. Verghese, "On the complexity of decentralized decision making and detection problems," *IEEE Trans. Autom. Control,* vol. AC-27, no.4, pp. 799-813, Aug. 1982.

[8] T. C. Aysal and K. E. Barner, "Sensor Data Cryptography in Wireless Sensor Networks," *IEEE Trans. Inf. forensics and security.,* vol.3, no.2, pp. 273-289, June 2008.

[9] P. K. Varshney, *Distributed Detection and Data Fusion.* New York: Springer-Verlag, 1997.

[10] A. Ribeiro and G. B. Giannakis, "Bandwidth-constrained distributed estimation for wireless sensor networks-Part I: Gaussian case," *IEEE Trans. Signal Process.,* vol. 54, no. 3, pp. 1131-1143, Mar. 2006.

[11] A. Ribeiro and G. B. Giannakis, "Bandwidth-constrained distributed estimation for wireless sensor networks-Part II: Unknown probability density function," *IEEE Trans. Signal Process.,* vol. 54, no. 7, pp. 2784-2796, Jul. 2006.

[12] Z.-Q. Luo, "Universal decentralized estimation in a bandwidth constrained sensor networks," *IEEE Trans. Inf. Theory,* vol. 51, no. 6, pp. 2210-2219, Jun. 2005.

[13] Z.-Q. Luo, "An isotropic universal decentralized estimation scheme for a bandwidth constrained *ad hoc* sensor network," *IEEE J. Sel. Areas Commun.,* vol. 23, no. 4, pp. 735-744, Apr. 2005.

[14] S. S. Iyengar, R. L. kashyap, and R. N. Madan, "Distributed sensor networks-Introduction to the special section," *IEEE Trans. Syst., Man Cybern.,* vol.21, pp. 1027-1031, Sept. 1991.

[15] J. N. Tsitsiklis, "Decentralized detection," *Advances in Statistical Signal Process.,* vol. 2, pp. 297344, 1993.

[16] Y. Ephraim and R. M. Gray, "A unified approach for encoding clean and noisy sources by means of waveform and autoregressive model vector quantization," *IEEE Trans. Inform. Theory,* vol. 34, pp. 826-834, July 1988.

[17] E. Ayanoglu, "On optimal quantization of noisy sources," *IEEE Trans. Inf. Theory,* vol. 36, pp. 1450-1452, Nov. 1990.

[18] W. M. Lam and A. R. Reibman, " Design of quantizers for decentralized estimation systems," *IEEE Trans. Commun.,* vol. 41, pp. 1602-1605, Nov. 1993.

[19] J. Gubner, "Distributed estimation and quantization," *IEEE Trans. Inf. Theory,* vol. 39, pp. 1456-1459, Jul. 1993.

[20] H. Li and J. Fang, "Distributed adaptive quantization for wireless sensor networks: From Delta modulation to maximum likelihood," *IEEE Trans. Signal Process.,* vol.56, pp. 5246-5257, Oct. 2008.

[21] H. Li and J. Fang, "Distributed adaptive quantization and estimation for wireless sensor networks," *IEEE Trans. Signal Process. Lett.,* vol. 14, pp. 669-672, Oct. 2007.

[22] T. L. Fine, "The response of a particular nonlinear system with feedback to each of two random processes," *IEEE Trans. Inf. Theory,* vol. IT-14, pp. 255-264, Mar. 1968.

[23] S. M. Kay, *Fundamentals of Statistical Signal Process.:Estimation Theory,* Upper Saddle River, NJ: Prentice-Hall, 1993.

[24] W. H. Greene, *Econometric Analysis*, 5th ed. Upper Saddle River, NJ:Prentice-Hall, 2003.

[25] H. L. Van Trees, *Detection, Estimation, and Modulation theory - Part 1*, 1st ed. , John Wiley  Sons Inc., 2001.

[26] J. D. Papastavrou and M. Athans, "Distributed detection by a large team of sensors in tandem," *IEEE Trans. Aerospace Elect. Syst.,* vol. AES-28, no. 3, pp. 630-653, Jul. 1992.

[27] P. F. Swaszek, "On the performance of serial networks in distributed detection," *IEEE Trans. Aerospace Elect. Syst.,* vol. AES-29, no. 1, pp. 254-260, Jan. 1993.

# Vita

Niharika Konakalla was born in March, 1986 in Warangal, Andhra Pradesh, India. She graduated with her Bachelor of Technology in Electronics and Communication Engineering from Kakatiya University, Warangal, India in the year 2007. She is presently enrolled in master's program in Electrical Engineering at Louisiana State University and is expected to graduate in May 2010. Her research interests include Digital/Wireless Communications and networking and her present focus is on security issues in wireless sensor networks.

She worked as a teaching assistant in the Department of Electrical Engineering, Louisiana State University. She is a graduate student member of IEEE. She intends to pursue a doctoral degree after working for few years and gaining some practical experience.