Scalable PHY-Layer Security for Distributed Detection in Wireless Sensor Networks

Reza Soosahabi, Mort Naraghi-Pour
Department of Electrical and Computer Engineering
Louisiana State University, Baton Rouge, LA 70803
{e-mail: rsoosa1, naraghi@lsu.edu}

***Abstract*—The problem of binary hypothesis testing is considered in a bandwidth-constrained low-power wireless sensor network operating over insecure links. Observations of the sensors are quantized and encrypted before transmission. The encryption method we propose maps the output of the quantizer to one of the possible quantizer output levels randomly according to a probability matrix. This operation is similar to that of a discrete memoryless channel. The intended (ally) fusion center (AFC) is aware of the encryption keys (probabilities) while the unauthorized (third party) fusion center (TPFC) is not. A constrained optimization problem is formulated from the point of view of AFC in order to design its decision rule along with the encryption probabilities. The objective function to be minimized is the error probability of AFC and the constraint is a lower bound on the error probability of TPFC. A good suboptimal solution to this problem is found. Numerical results are presented to show that it is possible to degrade the error probability of TPFC significantly and still achieve very low probability of error for AFC. As the number of levels in the quantizer increases the performance loss of the secure system compared to insecure system is reduced. Compared to the existing data encryption methods, the proposed method is highly scalable since it does not increase the packet overhead or transmit power of the sensors and has very low computational complexity. A scheme is described to randomize the keys so as to defeat any key space exploration attack.**

***Index Terms*—Decentralized detection, decision fusion, soft decision, information security, wireless sensor networks.**

I. Introduction

Wireless sensor networks (WSN) have applications in many military and civilian areas including intrusion detection and surveillance, medical monitoring, emergency response, environmental monitoring, target detection and tracking, and battlefield assessment. Providing security in WSNs is a challenging task. In the sensor nodes the resources such as energy supply, processing power, memory size and communication bandwidth are severely limited. Another difficulty arises from the large number of nodes in the network. Future networks are envisioned to consist of hundreds or thousands of nodes to implement ubiquitous networks. To keep the network cost down, as the number of nodes increases, the cost per node must be reduced. Therefore, it is unlikely that in the near future, technological advances will alleviate the scarcity of resources at the nodes. Despite these difficulties in many applications of WSNs security is as important as performance, if not more [1]. This calls for scalable security protocols with minimal resource requirements and low communication overhead.

Several security protocols have been recently proposed for WSNs [1]–[4]. These schemes are mostly independent of the application at hand and adapt the traditional network security protocols using cryptography, authentication, and key management techniques to provide security at the link and network layer, albeit with more efficient implementation and resource utilization. However, the issue of scalability remains since these techniques provide security at the expense of increased energy consumption and bandwidth [5]. In this paper we consider a specific application of WSNs, namely the problem of distributed detection of the state of a phenomenon in an environment, and propose a security scheme which may be considered a physical layer technique since it only randomizes the content of sensor messages. Our method can be used in conjunction with other security protocols at higher layers to enhance the integrity of the network operation.

Distributed detection using WSNs has been extensively investigated [6]. In particular optimal design of the fusion rule under different conditions of quantization at the individual sensors, topologies of the network, and channel conditions has been investigated in [7]–[11].

In this paper we consider the problem of distributed detection in a large WSN over insecure links. Due to the limited power and low bandwidth, we assume that nodes transmit a quantized version of their observations to their intended (ally) fusion center (AFC). In addition to the AFC, an unauthorized (third-party) fusion center (TPFC) may also be observing the sensor transmissions and attempting to detect the state of the unknown hypothesis. In order to deteriorate the error probability of TPFC, each node uses a simple encryption mechanism whereby it maps the quantizer output level to one the possible output levels randomly similar to the operation of a discrete memoryless channel (DMC). It is assumed that AFC is aware of the encryption probabilities (keys), and can minimize its probability of error accordingly, whereas the TPFC is unaware of the encryption keys and can only assume it has received unencrypted data [12], [13].

The remainder of this paper is organized as follows. In Section II we present the problem under consideration and the optimal decision rules for the TPFC. In Section III we discuss the optimal decision rules for the AFC. Numerical results are presented in Section IV. Finally, concluding remarks are given in Section V.

978-1-4673-1881-5/12/$31.00 ©2012 IEEE

II. System Model

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

$$a_\eta(l_j) \triangleq P(\mathcal{Q}(X_i) = l_j | H_\eta) = P(t_{j-1} < X_i \leq t_j | H_\eta) \quad (1)$$

Since the quantization process depends on the sensors' built-in technology, hereafter it is assumed that for $j = 1, 2, \cdots, M$ and $\eta = 0, 1$, $a_\eta(l_j)$ are fixed and known to both the AFC and TPFC. The optimal selection of the quantizer is investigated in [14].

We assume that the channel between the sensors and the FCs is error free. We employ the following simple probabilistic cipher at the sensors where the decision $\mathcal{Q}(X_i)$ of sensor i is randomly encrypted to obtain Y_i, such that

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

for some ϕ_{jk}. The encrypted messages Y_i, $i = 1, 2, \cdots, n$, are then transmitted to AFC over an insecure link. For $\eta = 0, 1$ let $b_\eta(l_j) \triangleq P(Y_i = l_j | H_\eta)$, $j = 1, 2 \cdots, M$. We define

$$\begin{aligned} \boldsymbol{\alpha}_\eta &\triangleq [a_\eta(l_1), a_\eta(l_2), \cdots, a_\eta(l_M)] \ , \\ \boldsymbol{\beta}_\eta &\triangleq [b_\eta(l_1), b_\eta(l_2), \cdots, b_\eta(l_M)] \end{aligned} \quad (3)$$

Then $\boldsymbol{\beta}_\eta = \boldsymbol{\alpha}_\eta \boldsymbol{\Phi}$ where $\boldsymbol{\Phi} \triangleq [\phi_{ij}]$ is an $M \times M$ matrix. It is assumed that AFC has a priori knowledge of the encryption matrix $\boldsymbol{\Phi}$. On the other hand, TPFC does not know $\boldsymbol{\Phi}$ 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 $\boldsymbol{\Phi} = \boldsymbol{I}_{M \times M}$. Our goal is to design $\boldsymbol{\Phi}$ so as to minimize P_E^a, the probability of error for AFC, subject to a lower bound on P_E^t, the probability of error for TPFC.

The optimum decision rule for the two fusion centers is given by the log-likelihood ratio test, [15], where for a received vector $\mathbf{y} = (y_1, y_2, \cdots, y_n)$,

$$T(\mathbf{y}) \triangleq \frac{1}{n} \sum_{i=1}^{n} z_i \quad \underset{H_0}{\overset{H_1}{\gtrless}} \quad \tau \quad (4)$$

where for the AFC

$$\tau = \tau_a, \quad \text{and} \quad z_i \triangleq \log\left(\frac{b_1(y_i)}{b_0(y_i)}\right) \quad (5)$$

and for the TPFC

$$\tau = \tau_r, \quad \text{and} \quad z_i \triangleq \log\left(\frac{a_1(y_i)}{a_0(y_i)}\right). \quad (6)$$

The error probability for the two fusion centers is given by

$$P_E = q_0 P(T(\boldsymbol{Y}) \geq \tau | H_0) + q_1 P(T(\boldsymbol{Y}) < \tau | H_1) \quad (7)$$

where 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. Invoking the central limit theorem, [16], for large n and conditioned on H_η,

$$T(\mathbf{Y}) | H_\eta \sim \mathcal{N}(\delta_\eta, \ \gamma_\eta / n) \quad (8)$$

where for the AFC,

$$\begin{aligned} \delta_\eta &= \mathrm{E}_{\boldsymbol{\beta}_\eta}\left[\log\left(\frac{b_1(Y_i)}{b_0(Y_i)}\right)\right] \triangleq \mu_{a\eta} \ , \\ \gamma_\eta^2 &= \mathrm{Var}_{\boldsymbol{\beta}_\eta}\left[\log\left(\frac{b_1(Y_i)}{b_0(Y_i)}\right)\right] \triangleq \sigma_{a\eta}^2 \end{aligned} \quad (9)$$

and for the TPFC,

$$\begin{aligned} \delta_\eta &= \mathrm{E}_{\boldsymbol{\beta}_\eta}\left[\log\left(\frac{a_1(Y_i)}{a_0(Y_i)}\right)\right] \triangleq \mu_{t\eta} \ , \\ \gamma_\eta^2 &= \mathrm{Var}_{\boldsymbol{\beta}_\eta}\left[\log\left(\frac{a_1(Y_i)}{a_0(Y_i)}\right)\right] \triangleq \sigma_{t\eta}^2 \end{aligned} \quad (10)$$

The subscripts for the operators E and Var indicate the distributions under which these are computed. However, note that TPFC does not adjust its fusion rule according to the statistics in (9) nor in (10). In the absence of knowledge of $\boldsymbol{\Phi}$ it has to assume that $\boldsymbol{\Phi} = \boldsymbol{I}_{M \times M}$, and it views (8) with the following statistics.

$$\begin{aligned} \delta_\eta &= \mathrm{E}_{\boldsymbol{\alpha}_\eta}\left[\log\left(\frac{a_1(Y_i)}{a_0(Y_i)}\right)\right] \triangleq \mu_{r\eta} \ , \\ \gamma_\eta^2 &= \mathrm{Var}_{\boldsymbol{\alpha}_\eta}\left[\log\left(\frac{a_1(Y_i)}{a_0(Y_i)}\right)\right] \triangleq \sigma_{r\eta}^2 \end{aligned} \quad (11)$$

For ease of notation let $\boldsymbol{\xi} = (\xi_1, \xi_2, \cdots, \xi_M)$ and $\boldsymbol{\omega} = (\omega_1, \omega_2, \cdots, \omega_M)$ where

$$\xi_i \triangleq \log\left(\frac{a_1(l_i)}{a_0(l_i)}\right) \ , \quad \omega_i \triangleq \log^2\left(\frac{a_1(l_i)}{a_0(l_i)}\right) \quad (12)$$

Then for $\eta = 0, 1$ we get,

$$\mu_{t\eta} = \boldsymbol{\beta}_\eta \boldsymbol{\xi}^T \ , \quad \nu_{t\eta}^2 \triangleq \sigma_{t\eta}^2 + \mu_{t\eta}^2 = \boldsymbol{\beta}_\eta \boldsymbol{\omega}^T \quad (13)$$

and

$$\mu_{r\eta} = \boldsymbol{\alpha}_\eta \boldsymbol{\xi}^T \ , \quad \nu_{r\eta}^2 \triangleq \sigma_{r\eta}^2 + \mu_{r\eta}^2 = \boldsymbol{\alpha}_\eta \boldsymbol{\omega}^T \quad (14)$$

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

$$\begin{aligned} P_E \approx P_e(\tau, \delta_0, \delta_1, \gamma_0, \gamma_1) = \ & q_0 Q(\frac{\sqrt{n}(\tau - \delta_0)}{\gamma_0}) + \\ & q_1(1 - Q(\frac{\sqrt{n}(\tau - \delta_1)}{\gamma_1})) \end{aligned} \quad (15)$$

where τ, δ_η and σ_η take on the values corresponding to each fusion center.

A. Optimization from TPFC's Point of View

The TPFC chooses its fusion threshold τ_r to minimize its probability of error. Therefore the optimal τ_r is obtained from the solution of the following problem. Considering (15), optimal threshold τ_r is given by

$$\frac{(\tau_r-\mu_{r0})^2}{2\sigma_{r0}^2}-\frac{(\tau_r-\mu_{r1})^2}{2\sigma_{r1}^2}=\frac{1}{n}\ln\left(\frac{q_0\sigma_{r1}}{q_1\sigma_{r0}}\right). \tag{16}$$

The AFC can also solve this problem independently and so it is aware of the value of τ_r. The actual performance of TPFC, however, is given by

$$P_E^t=P_e(\tau_r,\mu_{t0},\mu_{t1},\sigma_{t0},\sigma_{t1}) \tag{17}$$

The performance of TPFC is degraded since in (17), τ_r is not matched to the mean and variances μ_{t0}, μ_{t1}, σ_{t0} and σ_{t1}.

B. Optimization from AFC's Point of View

The optimization problem for AFC is stated below.

$$P1:\quad \min_{\tau,\mathbf{\Phi}} P_e(\tau,\mu_{a0},\mu_{a1},\sigma_{a0},\sigma_{a1}) \tag{18}$$

subject to:

$$0\le\phi_{ij}\le 1\ \forall i,j,\quad \text{and}\quad \mathbf{\Phi}\mathbf{1}_{M\times1}=\mathbf{1}_{M\times1} \tag{19}$$

$$e_{min}\le P_e(\tau_r,\mu_{t0},\mu_{t1},\sigma_{t0},\sigma_{t1})\le 0.5 \tag{20}$$

where $\mathbf{1}_{M\times1}$ indicates a column vector of all 1's. Note that the threshold τ in (18) is absent from the constraints. Therefore, for any given values of $(\mu_{a0},\mu_{a1},\sigma_{a0},\sigma_{a1})$ the optimal τ can be calculated from the following.

$$\frac{(\tau_a-\mu_{a0})^2}{2(\sigma_{a0})^2}-\frac{(\tau_a-\mu_{a1})^2}{2(\sigma_{a1})^2}=\frac{1}{n}\ln\left(\frac{q_0\sigma_{a1}}{q_1\sigma_{a0}}\right). \tag{21}$$

Generally the optimization problem $P1$ is not mathematically tractable. In the following section we simplify the cost function and trim the feasible region to obtain a good suboptimal solution.

III. Optimization for AFC

A. Reducing the Number of Variables

From (9)-(10), and (18) and (20) the given statistics and the error probabilities are all functions of $\boldsymbol{\beta}_\eta$ which is obtained from a linear transformation of ϕ_{ij}. Since $\boldsymbol{\beta}_\eta$ contains fewer variable, it is more convenient to find the optimal $\boldsymbol{\beta}_\eta$ in $P1$ and compute the optimal $\mathbf{\Phi}$ from it with no loss in optimality. To this end, we need to express the linear constraints in (19) in terms of $\boldsymbol{\beta}_\eta$. The linear constraints in (19) form a *convex polyhedral set* which can be denoted by

$$\mathcal{P}_\phi\triangleq\{\mathbf{\Phi}\mid 0\le\phi_{ij}\le1\ \forall i,j,\ \text{and}\ \ \mathbf{\Phi}\mathbf{1}_{M\times1}=\mathbf{1}_{M\times1}\} \tag{22}$$

According to [17], there is an equivalent (image) convex polyhedral set for $\mathcal{P}_\phi$ in $\boldsymbol{\beta}_\eta$ domain. For $\eta=0,1$, let

$$\mathcal{P}_\beta\triangleq\{\boldsymbol{\beta}_\eta\mid\boldsymbol{\beta}_\eta=\boldsymbol{\alpha}_\eta\mathbf{\Phi}\ ,\ \mathbf{\Phi}\in\mathcal{P}_\phi\} \tag{23}$$

denote the equivalent set. Similar to $\mathcal{P}_\phi$, this is associated with some linear constraints on $\boldsymbol{\beta}_\eta$ which can be simply calculated using the instructions in [17].

B. Simplifying the Constraints

The constraint in (20) is a function of $(\mu_{t0},\mu_{t1},\sigma_{t0},\sigma_{t1})$. Now for a given $(\mu_{t0},\mu_{t1},\sigma_{t0},\sigma_{t1})$ satisfying (20), $\boldsymbol{\beta}_\eta$ only needs to satisfy the linear equations in (13). Since $\mu_{t\eta}$ and $\nu_{t\eta}$ are linear transformation of $\boldsymbol{\beta}_\eta$, similarly to Section III-A, one can find the convex polyhedral set of $\mu_{t\eta}$ and $\nu_{t\eta}$ corresponding to $\mathcal{P}_\beta$,

$$\mathcal{P}_t\triangleq\{\mu_{t\eta},\ \nu_{t\eta}\mid\mu_{t\eta}=\boldsymbol{\beta}_\eta\boldsymbol{\xi}^T,\ \nu_{t\eta}^2=\boldsymbol{\beta}_\eta\boldsymbol{\omega}^T,\ \boldsymbol{\beta}_\eta\in\mathcal{P}_\beta\} \tag{24}$$

For $\mu_{t\eta}$, $\nu_{t\eta}\in\mathcal{P}_t$, let us define

$$\boldsymbol{\varepsilon}(\tau,\mu_{t\eta},\nu_{t\eta})\triangleq P_e(\tau,\mu_{t0},\mu_{t1},\sigma_{t0},\sigma_{t1}) \tag{25}$$

Thus the constraint in (20) can be replaced with

$$e_{min}\le\boldsymbol{\varepsilon}(\tau_r,\mu_{t\eta},\nu_{t\eta})\le0.5 \tag{26}$$

Our goal is to select $\mu_{t\eta}$ and $\nu_{t\eta}$ to satisfy 26. However, this selection sets additional constraints on $\boldsymbol{\beta}_\eta$ instead of (20). As a result the optimal cost function in (18) may not be achievable. In fact with these new constraints the computed cost function may be far from optimal. A "wise" choice for $\mu_{t\eta}$ and $\nu_{t\eta}$ is needed to ensure that the suboptimal solution computed with the new constraints is close to the optimal. The lemma below allows us to formulate an upper bound on the cost function based on $\mu_{t\eta}$ and $\nu_{t\eta}$.

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

$$P_e(\tau_a,\mu_{a0},\mu_{a1},\sigma_{a0},\sigma_{a1})\le\boldsymbol{\varepsilon}(\tau^*,\mu_{t\eta},\nu_{t\eta}) \tag{27}$$

where τ_a is given in (21) and τ^* is obtained from

$$\frac{(\tau^*-\mu_{t0})^2}{2(\sigma_{t0})^2}-\frac{(\tau^*-\mu_{t1})^2}{2(\sigma_{t1})^2}=\frac{1}{n}\ln\left(\frac{q_0\sigma_{t1}}{q_1\sigma_{t0}}\right). \tag{28}$$

Proof: For a fixed $\boldsymbol{\beta}_\eta$, the minimum achievable error probability according to the MAP rule is represented by $P_e(\tau_a,\mu_{a0},\mu_{a1},\sigma_{a0},\sigma_{a1})$ for the test statistics described in (4)-(5). On the other hand, $\boldsymbol{\varepsilon}(\tau^*,\mu_{t\eta},\nu_{t\eta})$ will be the minimum achievable error probability where the terms in the test statistic are given in (6). However, this does not correspond to the MAP rule. Due to the optimality of the MAP rule, the inequality in (27) holds. ■

The "wise" choice of $(\mu_{t\eta},\nu_{t\eta})$ denoted $(\mu_{t\eta}^*,\nu_{t\eta}^*)$ is now computed using the following optimization problem.

$$P1-1:\quad\min_{\mu_{t\eta},\nu_{t\eta}}\boldsymbol{\varepsilon}(\tau^*,\mu_{t\eta},\nu_{t\eta}) \tag{29}$$

subject to:

$$\mu_{t\eta},\nu_{t\eta}\in\mathcal{P}_t \tag{30}$$

$$e_{min}\le\boldsymbol{\varepsilon}(\tau_r,\mu_{t\eta},\nu_{t\eta})\le0.5 \tag{31}$$

Considering the fact that $\boldsymbol{\varepsilon}(\tau^*,\mu_{t\eta},\nu_{t\eta})$ is monotonic with respect to $\mu_{t\eta}$ and $\nu_{t\eta}$, the above problem can be efficiently solved using KKT method. These optimal values are then used in the optimization problem in the next section.

C. Simplifying Cost Function

For large n, P_E^a is a decreasing function of μ_{a1} and an increasing function of μ_{a0}. It can also be inferred that for large n, the impact of $\sigma_{a\eta}$ becomes small compared to $\mu_{a\eta}$. Thus one is motivated to maximize $\mu_{a1} - \mu_{a1}$ instead of the cost function in $P1$. In [14] the same idea is used to find the optimal quantizer $\mathcal{Q}$ without the security issue. From (9), it can be seen that μ_{a1} and μ_{a1} are associated with Kullback-Leibler divergence.

$$\mu_{a0} = -\mathcal{D}(\boldsymbol{\beta}_0||\boldsymbol{\beta}_1) \quad , \quad \mu_{a1} = \mathcal{D}(\boldsymbol{\beta}_1||\boldsymbol{\beta}_0) \tag{32}$$

Then $\mu_{a1} - \mu_{a1}$ can be written in form of J-divergence [14]

$$\mu_{a1} - \mu_{a0} = \mathcal{J}(\boldsymbol{\beta}_1||\boldsymbol{\beta}_0) \tag{33}$$

Finally using the results from Sections III-A and III-B, the optimization problem is stated as:

$$\tilde{P1}: \quad \max_{\boldsymbol{\beta}_0,\boldsymbol{\beta}_1} \mathcal{J}(\boldsymbol{\beta}_1||\boldsymbol{\beta}_0) \tag{34}$$

$$\text{subject to:} \tag{35}$$

$$\boldsymbol{\beta}_\eta \in \mathcal{P}_\beta \quad , \quad \eta = 0, 1 \tag{36}$$

$$\boldsymbol{\beta}_\eta \xi^T = \mu^*_{t\eta}, \quad \boldsymbol{\beta}_\eta \omega^T = (\nu^*_{t\eta})^2 \quad , \quad \eta = 0, 1 \tag{37}$$

Theorem 1. *$\mathcal{J}(\boldsymbol{\beta}_1||\boldsymbol{\beta}_0)$ is a convex function with respect to $\boldsymbol{\beta}_0$ and $\boldsymbol{\beta}_1$.*

To prove the above theorem one needs to show that the Hessian matrix $[\nabla^2_{\boldsymbol{\beta}_0,\boldsymbol{\beta}_1} \mathcal{J}(\boldsymbol{\beta}_1||\boldsymbol{\beta}_0)]$ is positive definite. It is easy to show that it is a tridiagonal matrix with all positive eigenvalues.

Let $\mathcal{R}$ represent the feasible region for $\boldsymbol{\beta}_\eta$ determined by the constraints in (36)-(37). It is easy to verify that $\mathcal{R}$ is still a convex polyhedral set. Now our goal is to maximize a convex function within a polyhedral region. This maximum must be explored among the extreme points in the region [18]. In other words, we only need to examine the vertices of $\mathcal{R}$ to find the global maximum [19]. In [20] an efficient algorithm is proposed to trace all the vertices of a convex polyhedral set. Having computed the optimal $\boldsymbol{\beta}_0$ and $\boldsymbol{\beta}_1$, the optimal $\boldsymbol{\Phi}$ can now be calculated. There are many solutions for $\boldsymbol{\Phi}$ and we choose the one with the fewest number of nonzero elements so as to minimize the storage requirements. Next we obtain τ^a from (21).

IV. 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 quantizes X_i with M levels according to a quantization rule designed in [14]. We define $\gamma = 20\log(d/\sigma)$ as the sensors' SNR.

Table I shows the performance of both binary and soft decision systems for several values of n, γ and q_0. Therein P^a_{Eb} and P^{min}_{Eb} are, in turn, the minimum error probability for the binary quantizer, and the minimum achievable error probability for the insecure case. As Table I shows, as M grows the performance improves.

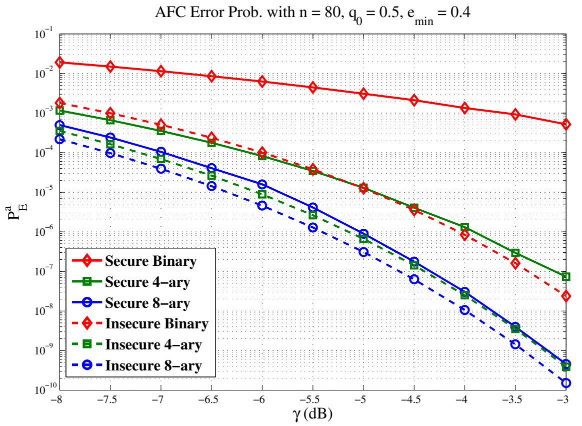

Fig. 1. Comparing the AFC error performance versus SNR

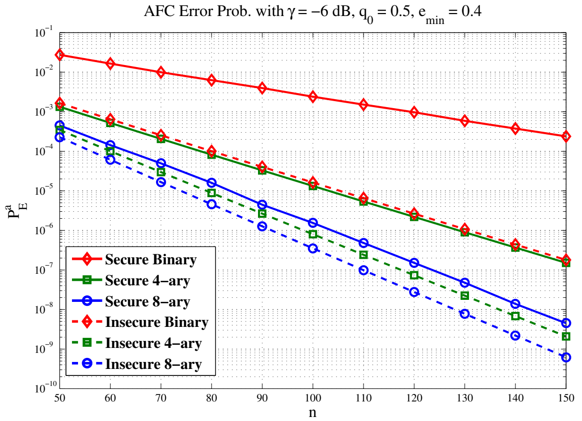

Fig. 2. Comparing the AFC error performance versus n

In Fig. 1 the soft decision system with $M = 4$ performs close to the insecure binary system and for $M = 8$ the secure system outperforms the insecure binary system. Moreover, as M increases, the loss in error probability of AFC due to the encryption at the sensors is reduced. Fig. 1 shows AFC's error probability vs. the number of nodes n. The soft decision system with $M = 4$ performs similarly to the insecure binary case and the system with $M = 8$ outperforms the insecure binary system.

In Table I $K(M)$ stands for the number of nonzero elements of $\boldsymbol{\Phi}$ where the soft decision with M levels is employed, i.e., $K(M)$ can be thought as the hash to store the encryption parameters. Although there are initially M^2 parameters in $\boldsymbol{\Phi}$, the hash for the optimal $\boldsymbol{\Phi}$ does not follow the square law.

The sensors are recommended to periodically cycle their encryption keys so as to defeat any strategies used by TPFC to estimate the encryption parameters from sensor transmissions. For example in Table I, for $n = 40$ and $q_0 = 0.5$ we have shown three solutions (keys) $c5$, $c6$ and $c7$ for the optimal $\boldsymbol{\Phi}$. After each observation of the hypothesis H, the sensors can

TABLE I
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}	$K(4)$	$K(8)$
$c1$	20	0	0.5	0.3	1.52 e-02	3.89 e-04	1.16 e-05	2.32 e-04	09	12
$c2$	20	0	0.3	0.3	1.37 e-02	1.11 e-04	8.49 e-06	2.50 e-04	07	15
$c3$	20	3	0.5	0.4	6.66 e-03	1.28 e-06	2.97 e-09	4.43 e-07	08	12
$c4$	40	-3	0.5	0.5	2.80 e-02	4.79 e-05	9.07 e-06	2.01 e-04	09	17
$c5$	40	0	0.5	0.3	1.15 e-03	5.59 e-08	4.83 e-10	3.17 e-07	09	12
$c6$	40	0	0.5	0.4	2.28 e-03	1.28 e-07	3.59 e-10	3.17 e-07	07	12
$c7$	40	0	0.5	0.5	7.58 e-03	1.14 e-06	1.43 e-09	3.17 e-07	08	12
$c8$	40	0	0.3	0.3	9.64 e-04	4.14 e-06	9.74 e-10	5.24 e-07	09	13
$c9$	40	3	0.5	0.5	1.15 e-03	3.18 e-12	3.35 e-17	1.37 e-12	08	12
$c10$	80	-6	0.5	0.5	1.40 e-02	4.82 e-05	1.40 e-05	1.00 e-04	08	18
$c11$	80	-3	0.5	0.5	1.83 e-03	3.22 e-08	7.37 e-10	2.38 e-08	09	17

choose one key (pseudo) randomly to encrypt their decision before transmission to AFC according to a schedule mandated by the AFC. This can be implemented for example by using a pseudo noise (PN) sequence generated by a long maximal length (linear feedback) shift register (MLSR). All the sensor nodes and AFC must be equipped with identical MLSRs which start with the same initial state.

V. CONCLUSIONS

The problem of binary hypothesis testing is considered in a bandwidth-constrained low-power wireless sensor network operating over insecure links. Observations of the sensors are quantized and encrypted before transmission. The encryption method maps the output of the quantizer to one of the quantizer output levels randomly according to a probability matrix similar to the operation of a discrete memoryless channel. The ally fusion center (AFC) is aware of the encryption keys (probabilities) and can design its decision rule along with the encryption probabilities so as to impose a high probability of error on the unauthorized fusion center (TPFC). A fusion rule is derived from the viewpoint of the two fusion centers and the encryption keys are designed so as to achieve a small probability of error for AFC with a lower bound on the error probability of TPFC. It is shown that by appropriate selection of the encryption parameters it is possible to impose a high error probability on TPFC while achieving low error probability for AFC. The proposed method which may be considered a PHY-layer security scheme for distributed detection is highly scalable due its low computational complexity and no communication overhead.

REFERENCES

[1] Y. Wang, G. Attebury, and B. Ramamurthy, “A survey of security issues in wireless sensor networks,” *Communications Surveys Tutorials, IEEE*, vol. 8, no. 2, pp. 2 –23, quarter 2006.

[2] X. Du and H.-H. Chen, “Security in wireless sensor networks,” *Wireless Communications, IEEE*, vol. 15, no. 4, pp. 60 –66, aug. 2008.

[3] S. C. Karlof, N and D. Wagner, “Tinysec: a link layer security architecture for wireless sensor networks,” in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, nov. 2004, pp. 162–175.

[4] Y.-T. Wang and R. Bagrodia, “Sensec: A scalable and accurate framework for wireless sensor network security evaluation,” in *Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference on*, june 2011, pp. 230 –239.

[5] X. Chen, K. Makki, K. Yen, and N. Pissinou, “”Sensor network security: a survey”,” *Communications Surveys Tutorials, IEEE*, vol. 11, no. 2, pp. 52 –73, mar 2009.

[6] R. Tenney and N. Sandell, “”Detection with distributed sensors”,” *Aerospace and Electronic Systems, IEEE Transactions on*, vol. AES-17, no. 4, pp. 501 –510, jul 1981.

[7] Q. Zhang, P. Varshney, and R. Wesel, “”Optimal bi-level quantization of i.i.d. sensor observations for binary hypothesis testing”,” *Information Theory, IEEE Transactions on*, vol. 48, no. 7, pp. 2105 –2111, jul 2002.

[8] Z. Chair and P. Varshney, “”Optimal data fusion in multiple sensor detection systems”,” *Aerospace and Electronic Systems, IEEE Transactions on*, vol. AES-22, no. 1, pp. 98 –101, jan. 1986.

[9] B. Chen, R. Jiang, T. Kasetkasem, and P. Varshney, “”Channel aware decision fusion in wireless sensor networks”,” *Signal Processing, IEEE Transactions on*, vol. 52, no. 12, pp. 3454 – 3458, dec. 2004.

[10] R. Niu, B. Chen, and P. Varshney, “”Fusion of decisions transmitted over rayleigh fading channels in wireless sensor networks”,” *Signal Processing, IEEE Transactions on*, vol. 54, no. 3, pp. 1018 – 1027, mar 2006.

[11] W. Shi, T. Sun, and R. Wesel, “”Quasi-convexity and optimal binary fusion for distributed detection with identical sensors in generalized gaussian noise”,” *Information Theory, IEEE Transactions on*, vol. 47, no. 1, pp. 446 –450, jan 2001.

[12] 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.

[13] T. Aysal and K. Barner, “”Sensor data cryptography in wireless sensor networks”,” *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 2, pp. 273 –289, june 2008.

[14] C.-C. Lee and J.-J. Chao, “”Optimum local decision space partitioning for distributed detection”,” *Aerospace and Electronic Systems, IEEE Transactions on*, vol. 25, no. 4, pp. 536 –544, jul 1989.

[15] P. Varshney, *“Distributed Detection and Data Fusion”*. Springer New York, Inc., 1997.

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

[17] A. Barvinok, “Lattice points, polyhedra, and complexity,” *Geometric Combinatorics, IAS/Park City Mathematics Series*, vol. 13, pp. 19–62, 2007. [Online]. Available: http://www.math.lsa.umich.edu/ barvinok/lectures.pdf

[18] G. Nash, S and A. Sofer, *Linear and Nonlinear Programming”*, 1st ed. McGraw-Hill, NY, 1995.

[19] A. Boyd and L. Vandenberghe, *”Convex Optimization”*, 1st ed. Cambridge University Press, UK, 2004.

[20] M. L. Balinski, “An algorithm for finding all vertices of convex polyhedral sets,” *SIAM J. Appl. Math.*, vol. 9, pp. 72–88, 1961.