OPTIMAL DISTRIBUTED DETECTION IN THE PRESENCE OF BYZANTINES

Bhavya Kailkhura[⋆] *Swastik Brahma*[⋆] *Yunghsiang S. Han*[†] *Pramod K. Varshney*[⋆]

[⋆] Department of EECS, Syracuse University
[†]Department of EE, National Taiwan University of Science & Technology

ABSTRACT

This paper considers the problem of optimal distributed detection with independent identical sensors in the presence of Byzantine attacks. By considering the attacker to be strategic in nature, we address the issue of designing the optimal fusion rule and the local sensor thresholds that minimize the probability of error at the fusion center (FC). We first consider the problem of finding the optimal fusion rule under the constraint of fixed local sensor thresholds and fixed Byzantine strategy. Next, we consider the problem of joint optimization of the fusion rule and local sensor thresholds for a fixed Byzantine strategy. Then we extend these results to the scenario where both the FC and the Byzantine attacker act in a strategic manner to optimize their own utilities. We model the strategic behavior of the FC and the attacker using game theory and show the existence of Nash Equilibrium. We also provide numerical results to gain insights into the solution.

Index Terms— Distributed detection, Wireless sensor networks, Byzantines, Game theory

1. INTRODUCTION

Distributed detection with multiple sensors is a well studied topic in detection theory [1]. The design of sensor networks for different applications has been extensively studied in the past decade. Different sensor network topologies have been considered [2] , but in this paper we focus on parallel topology. In [3], [4], the authors considered the design of the optimal fusion rule and local sensor thresholds by minimizing the probability of error at the fusion center (FC) for the parallel topology. Recently, the problem of distributed detection in the presence of Byzantine attacks has attracted attention [5, 6, 7, 8, 9]. Schemes for Byzantine node identification have been proposed in [5, 9]. Analysis of optimal Byzantine attacks is presented in [6, 9, 10]. In [7] and [8], the authors considered the problem of optimization of the fusion rule for a fixed sensor threshold. However, the problem of designing optimal detection parameters in a holistic manner by considering strategic behavior of the FC and the Byzantine is still an area of open research.

In contrast to previous works, in this paper, we consider the problem of designing optimal distributed detection parameters in a holistic manner in the presence of Byzantines and also model the strategic behavior of the FC and the Byzantines using game theory. We analyze the problem under different attacking scenarios and give insights into the practical scenarios where the proposed schemes are useful. The main contributions of this paper are as follows.

This work was supported in part by ARO under Grant W911NF-09-1-0244, AFOSR under Grants FA9550-10-1-0458, FA9550-10-1-0263 and National Science Council of Taiwan, under grants NSC 99-2221-E-011-158 -MY3, NSC 101-2221-E-011-069 -MY3.

1. We consider the problem of joint optimization of the fusion rule and local sensor threshold for a fixed Byzantine strategy.
2. Then we extend these results to the scenario where both the FC and the Byzantine attacker act in a strategic manner to optimize their own utilities and model it using Game Theory.
3. We provide numerical results to gain insights into the solution.

2. SYSTEM MODEL AND PROBLEM FORMULATION

In this section, we present the system model used in this paper. We consider a parallel network with N sensor nodes and a fusion center (FC) trying to detect a phenomenon.

2.1. Distributed detection in sensor networks

Consider a binary hypothesis testing problem with the two hypotheses H_0 (signal is absent) and H_1 (signal is present). Prior probabilities of the two hypotheses H_0 and H_1 are denoted by π_0 and π_1, respectively.

Each node i makes a one-bit local decision $v_i \in \{0, 1\}$ using the likelihood ratio test

$$\frac{p_{Yi}^{(1)}(y_i)}{p_{Yi}^{(0)}(y_i)} \underset{v_i=0}{\overset{v_i=1}{\gtrless}} \lambda \tag{1}$$

where λ is the identical threshold[1] used at all the sensors and $p_{Yi}^{(k)}(y_i)$ is the conditional probability density function (PDF) of observation Yi under the hypothesis H_k. After making its one-bit local decision v_i, node i sends u_i (which may not be the same as v_i) to the FC. We assume error-free communication channels in this paper.

We denote the probabilities of detection and false alarm of node i by $P_d = P(v_i = 1|H_1)$ and $P_{fa} = P(v_i = 1|H_0)$, respectively, which are assumed to be the same for every node irrespective of whether they are honest or Byzantine nodes. If a node is honest, then it forwards its own decision correctly. However, a Byzantine node, in order to undermine the network performance, may alter these decisions.

2.2. Byzantine attack model

A Byzantine node, in order to undermine the network performance, may alter its decision prior to transmission. Each Byzantine decides to attack independently relying on its own observation and decision regarding the presence of the phenomenon. We define the following strategies $P_{j,1}^H$, $P_{j,0}^H$ and $P_{j,1}^B$, $P_{j,0}^B$ ($j \in \{0, 1\}$) for the honest and Byzantine nodes, respectively: Honest nodes:

[1]It has been shown that the use of identical thresholds is asymptotically optimal [11].

$$P_{1,1}^H = 1 - P_{0,1}^H = P^H(x=1|y=1) = 1 \quad (2)$$

$$P_{1,0}^H = 1 - P_{0,0}^H = P^H(x=1|y=0) = 0 \quad (3)$$

Byzantine nodes:

$$P_{1,1}^B = 1 - P_{0,1}^B = P^B(x=1|y=1) = 0 \quad (4)$$

$$P_{1,0}^B = 1 - P_{0,0}^B = P^B(x=1|y=0) = 1 \quad (5)$$

where $P(x=a|y=b)$ is the probability that a node sends a to the FC when its actual decision is b. We assume that the FC is not aware of the exact set of Byzantine nodes and considers each node i to be Byzantine with a certain probability x.

2.3. Binary Hypothesis Testing at the Fusion Center

We consider a Bayesian detection problem where the performance criterion at the fusion center is the probability of error. We also assume that the FC employs a K-out-of-N fusion rule. Global false alarm and detection probabilities are denoted by Q_F and Q_D, respectively, as

$$Q_F = \sum_{i=K}^{N} \binom{N}{i} (\pi_{10})^i (1-\pi_{10})^{N-i} \quad (6)$$

$$Q_D = \sum_{i=K}^{N} \binom{N}{i} (\pi_{11})^i (1-\pi_{11})^{N-i} \quad (7)$$

where π_{j0} and π_{j1} denote the conditional probabilities of $u_i = j$ given H_0 and H_1, respectively. We can represent π_{10} and π_{11} as

$$\pi_{10} = x(1-P_{fa}) + (1-x)P_{fa} \quad (8)$$

$$\pi_{11} = x(1-P_d) + (1-x)P_d \quad (9)$$

where x denotes the probability that bit u_i received at the FC has been flipped, $i = 1, \cdots, N$. In this paper, we assume that the network is moderately affected by Byzantines and $x \leq 0.5$. The probability of error at the FC is given by

$$P_E = \pi_0 Q_F + \pi_1 (1 - Q_D) \quad (10)$$

The probability of error P_E is a function of parameters (K, λ), which are under the control of the FC and the parameter (x) which is under the control of the attacker. This motivates us to design parameters K and λ given x such that P_E is minimized.

2.4. Problem Formulation

In this subsection, we formulate the Bayesian detection problem and consider the minimization of the probability of error under three different scenarios. First, we consider the problem $P1$ finding the optimal fusion rule (K^*) for a fixed local sensor threshold (λ) and a fixed Byzantine strategy (x). Next, we consider the problem $P2$ of joint optimization of the fusion rule and the local sensor threshold (K, λ) for a fixed Byzantine strategy. Then we extend this result to the problem $P3$ where both the FC and the Byzantine attacker act in a strategic manner to optimize their own utilities and model it as a minimax game. The solution to this minimax game between the FC and the Byzantines is the Nash equilibrium (NE), which is a saddle point in the design metric, P_E. The problems discussed above are formally stated as follows.

$$\text{Problem P1:} \quad \underset{K}{\text{minimize}} \qquad P_E(K, \lambda, x) \quad (11)$$

$$\text{Problem P2:} \quad \underset{K,\lambda}{\text{minimize}} \qquad P_E(K, \lambda, x) \quad (12)$$

$$\text{Problem P3:} \quad \min_{K,\lambda} \max_{x} \qquad P_E(K, \lambda, x) \quad (13)$$

In the next section, we present analytical results that allow us to find the optimal design parameters for the above mentioned formulations.

3. SYSTEM DESIGN IN THE PRESENCE OF BYZANTINES

In this section, we investigate the properties of the probability of error P_E with respect to K, λ and x and use it to solve the optimization problems $(P1), (P2)$ and $(P3)$.

3.1. Optimal Fusion Rule Design

First, we design the optimal fusion rule assuming that the local sensor threshold λ and the Byzantine strategy (x) are fixed and known to FC. [2] Notice that the resulting optimal fusion rule and fixed local sensor threshold pair (K^*, λ) may not be the global minimizer of the probability of error over all possible (K, λ) pairs since λ is assumed fixed during the optimization process. However, this scheme is particularly important in the scenario where the FC wants to avoid the overhead caused by the diffusion of the new local sensor threshold messages to all nodes in the network. We present the solution of Problem $P1$ in the following theorem based on [1].

Theorem 1 *The optimal fusion rule K^* for fixed local sensor threshold λ and Byzantine strategy x is given by*

$$K^* = \frac{\ln\left[(\pi_0/\pi_1)\left\{(1-\pi_{10})/(1-\pi_{11})\right\}^N\right]}{\ln\left[\{\pi_{11}(1-\pi_{10})\}/\{\pi_{10}(1-\pi_{11})\}\right]} \quad (14)$$

where $x < 0.5$. When $x = 0.5$, FC makes the final decision based on the prior probabilities.

As aforementioned, this optimal fusion rule and fixed local sensor threshold pair (K^*, λ) may not be the global minimizer of the probability of error over all (K, λ) pairs. Thus, we next consider the joint optimization of the fusion rule and the local sensor threshold.

3.2. Joint Optimization of Fusion Rule and Sensor Threshold

In this section, we present a procedure to find the optimal fusion rule and local sensor threshold pair (K^*, λ^*) that minimizes the probability of error P_E given a fixed Byzantine strategy x. This scheme is particularly important in the scenario where Byzantine attackers are performing a man-in-the-middle attack and do not have access to the local sensor threshold. We first show that when using the optimal fusion rule (K^*), P_E is a quasi-convex function of the local sensor threshold (λ) under a certain condition.

Lemma 1 *For the optimal K and any fixed x ($x < 0.5$), P_E is a quasi-convex function of λ, if $(d/d\lambda)\left(\lambda^{-1}P_d/P_{fa}\right) \leq 0$.* [3]

Proof A function $f(\lambda)$ is quasi-convex if, for some λ^*, $f(\lambda)$ is non-increasing for $\lambda \leq \lambda^*$ and $f(\lambda)$ is non-decreasing for $\lambda \geq \lambda^*$. In other words, the lemma is proved if $dP_E/d\lambda \leq 0$ (or $dP_E/d\lambda \geq 0$) for all λ, or if for some λ^*, $dP_E/d\lambda \leq 0$ when $\lambda \leq \lambda^*$ and $dP_E/d\lambda \geq 0$ when $\lambda \geq \lambda^*$. Hence, we calculate the partial derivative of P_E with respect to λ. Using the property of ROC's that

[2] In practice, x may be learned by observing u_i-s at FC for a fixed duration; however, this study is beyond the scope of this work.

[3] Various noise distributions satisfy $(d/d\lambda)\left(\lambda^{-1}P_d/P_{fa}\right) \leq 0$ [12].

$dP_d/dP_{fa} = \lambda$, the fact that $d\pi_{11}/d\pi_{10} = \lambda$, we get

$$\begin{aligned}\frac{dP_E}{d\lambda} &= \pi_0 \frac{dQ_F}{d\lambda} - \pi_1 \frac{dQ_D}{d\lambda} \\ &= -\pi_1 \lambda \left(\pi_{10}\right)' N \begin{pmatrix} N-1 \\ K-1 \end{pmatrix} \left(\pi_{11}\right)^{K-1} \left(1-\pi_{11}\right)^{N-K} \\ &\quad + \pi_0 \left(\pi_{10}\right)' N \begin{pmatrix} N-1 \\ K-1 \end{pmatrix} \left(\pi_{10}\right)^{K-1} \left(1-\pi_{10}\right)^{N-K} \end{aligned} \quad (15)$$

where, $(\pi_{10})' = d\pi_{10}/d\lambda = (1-2x)[dP_{fa}/d\lambda] \leq 0$. The inequality follows from the fact that $x \leq 0.5$ and $dP_{fa}/d\lambda \leq 0$. Following an approach similar to [3], [12], we rewrite the above equation as follows.

$$\frac{dP_E}{d\lambda} = g\left(\lambda, K, x\right)\left(e^{r(\lambda,K,x)} - 1\right) \quad (16)$$

where

$$g = N \begin{pmatrix} N-1 \\ K-1 \end{pmatrix} \pi_0 (-\pi_{10})' (\pi_{10})^{K-1} (1-\pi_{10})^{N-K} \quad (17)$$

and

$$r = \ln\left(\frac{\lambda\pi_1}{\pi_0}\left(\frac{\pi_{11}}{\pi_{10}}\right)^{(K-1)}\left(\frac{1-\pi_{11}}{1-\pi_{10}}\right)^{(N-K)}\right) \quad (18)$$

Now it can be seen that $g\left(\lambda, K, x\right) \geq 0$. This implies that the sign of $dP_E/d\lambda$ depends on the value of $r\left(\lambda, K, x\right)$. The proof is complete if we show that $r\left(\lambda, K, x\right)$ is either always positive or negative, or there exists a λ^* such that $r\left(\lambda, K, x\right) \leq 0$ for all $\lambda \leq \lambda^*$ and $r\left(\lambda, K, x\right) \geq 0$ for all $\lambda \geq \lambda^*$. Substituting $K = K^*$ given in (14) in equation (18), and dropping K from $r\left(\lambda, K, x\right)$ for ease of notation we get $r(\lambda, x) = \ln\lambda - \ln\left(\pi_{11}/\pi_{10}\right)$. Differentiating $r\left(\lambda, x\right)$ with respect to λ, we get

$$\frac{dr(\lambda,x)}{d\lambda} = \frac{1}{\lambda} + \frac{1}{\pi_{11}}\left[\frac{\pi_{11}}{\pi_{10}} - \lambda\right]\frac{d\pi_{10}}{d\lambda} \quad (19)$$

In the following, we show that $r(\cdot)$ is non-decreasing. Substituting π_{11}, π_{10}, $d\pi_{10}/d\lambda$ in $dr(\lambda, x)/d\lambda \geq 0$,

$$\frac{x}{1-2x} + P_{fa} + \frac{P_{fa} + x/(1-2x)}{P_d + x/(1-2x)}\left(-\lambda^2 \frac{dP_{fa}}{d\lambda}\right) \geq -\lambda\frac{dP_{fa}}{d\lambda},$$

and $P_{fa}/P_d \leq \left(P_{fa} + x/(1-2x)\right)/\left(P_d + x/(1-2x)\right)$ since $P_{fa}/P_d \leq 1$. Therefore, it suffices to show that

$$P_{fa} + \lambda\left(-\lambda\frac{dP_{fa}}{d\lambda}\right)\frac{P_{fa}}{P_d} \geq -\lambda\frac{dP_{fa}}{d\lambda}. \quad (20)$$

The inequality above is equivalent to the condition in the lemma.

From (16) it can be seen that if $r(K, \lambda^*, x) = 0$ for some λ^* then $(P_E)' = 0$ at λ^* and because P_E is quasi-convex for the optimal fusion rule K^*, it is minimized for $\lambda = \lambda^*$. For the optimal fusion rule K^*, $r(K, \lambda, x) = 0$ has a unique positive root and there exist efficient algorithms, which utilize the quasi-convex nature of the problem, to find an optimum (K^*, λ^*) pair that minimizes P_e [13].

Until now we have restricted our analysis to the scenarios where the Byzantine strategy is fixed. Next, we extend the above results to the case where Byzantine attacker also optimizes its strategy against the FC, which results in a game theoretic formulation of the problem.

3.3. Minimax Game between the FC and Byzantine Attacker

In this section, we analyze the scenario where both the FC and the Byzantine attacker act strategically to optimize their own utilities. This formulation models the case where Byzantine attackers can compromise and gain full control over the nodes, i.e., the local sensor thresholds. We define a game as follows:

- *Players:* We have two players– the FC and the Byzantine.
- *Strategies:* Strategy set of FC $\triangleq \{K, \lambda\}$; attacker's strategy $\triangleq x$.
- *Utilities:* FC's utility, u_{FC}, and Byzantine's utility, u_B, are the same, i.e., probability of error $P_e(K, \lambda, x)$, which the FC will minimize, and the Byzantine will maximize.

Solution to this game between the FC and the Byzantine is the Nash equilibrium (K^*, λ^*, x^*), which is a saddle point in the design metric P_E and satisfies the condition in the following definition.

Definition (Nash Equilibrium): A strategy (K^*, λ^*, x^*) is a Nash Equilibrium for the game if and only if

1. $u_{FC}(K^*, \lambda^*, x^*) \leq u_{FC}(\hat{K}, \hat{\lambda}, x^*), \forall \hat{K} \neq K^*, \forall \hat{\lambda} \neq \lambda^*$
2. $u_B(K^*, \lambda^*, x^*) \geq u_B(K^*, \lambda^*, \hat{x}), \forall \hat{x} \neq x^*$

Next, we present some analytical results that allow us to find minimax strategies for this formulation. The proofs are omitted due to space constraints.

Lemma 2 *The probability of error, P_E, increases monotonically in x, the attackers parameter,$\forall K$, if $P_d \geq 0.5$ and $P_{fa} \leq 0.5$.*

Lemma 2 suggests that if $P_d \geq 0.5$ and $P_{fa} \leq 0.5$ then attacker's best response will be a pure strategy x_{max}. An optimum design will always satisfy the $P_d \geq 0.5$ and $P_{fa} \leq 0.5$ bounds when $\alpha \leq 0.5$. Theorem 2 is presented as a solution of Problem 3 (see (13)). The minimax game is solved numerically (Section 4).

Theorem 2 *If conditions mentioned in Lemma 1 and Lemma 2 hold, then the saddle-point (K^*, λ^*, x^*) exists in the minimax game formulated between the FC and Byzantine attacker such that*

$$\min_{K,\lambda}\max_{x} P_E(K, \lambda, x) = \max_{x}\min_{K,\lambda} P_E(K, \lambda, x)$$

4. NUMERICAL RESULTS

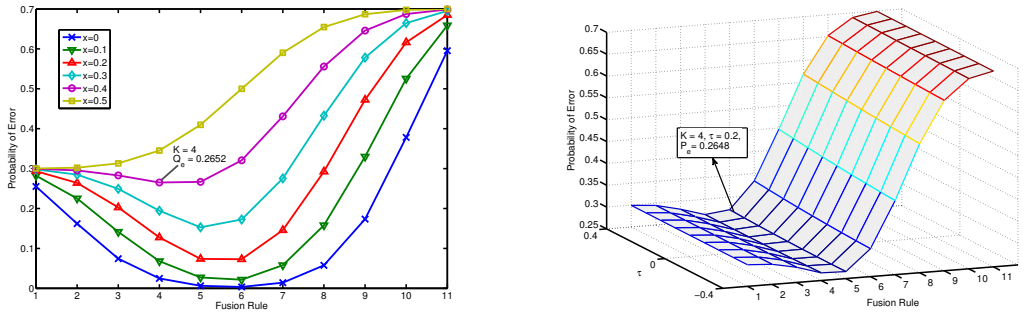
In this section, we consider the detection of known signals in Gaussian noise (cf. [3]). The sensor observation is $y = s_y + n_y$, where $s_y = \pm 1$ is the transmitted signal and $n_y \sim \mathcal{N}(0, 1)$. We denote $\tau = \ln\lambda$ as the log likelihood ratio threshold. Since τ increases monotonically with λ, our results hold when λ is replaced by τ. We consider a parallel topology with odd $(N = 11)$ and even $(N = 10)$ number of nodes. P_e is analyzed as a function of τ, K and x.

4.1. Optimal Parameter Design

Figure 1(a) shows the numerical results for $P1$ with $N = 11$ and unequal priors ($\pi_0 = 0.3$, and $\pi_1 = 0.7$). We fix $\tau = \ln\lambda = 0$ and optimize the fusion rule K for different fraction of Byzantine nodes (x). Optimal fusion rule in Figure 1(a) matches our theoretical result given in (14). For example, when $x = 0.4$ and $\tau = 0$, we have $\pi_{10} = 0.4313$ and $\pi_{11} = 0.5683$ from (8) and (9), respectively. The optimal K^* given by (14) is $K^* = 4$ which agrees with Figure 1(a). In Figure 1(b), we fix $x = 0.4$ and jointly optimize fusion rule K and sensor threshold τ. Comparing Figures 1(a) and 1(b), we observe that optimizing the fusion rule alone results in $P_e = 0.2652$ and joint optimization of (K^*, τ^*) results in better $P_e = 0.2648$.

4.2. Equilibrium Analysis of the Minimax Game

Figure 2 plots the minimum probability of error considering FC's best response (joint optimization of K, τ) versus attacker's strategy (fraction of Byzantine nodes). Priors are assumed to be equal.



(a) (b)

Fig. 1. Probability of error (P_e) analysis. (a)P_e with varying fusion rule (K). (b) P_e with varying fusion rule (K) and threshold (τ).

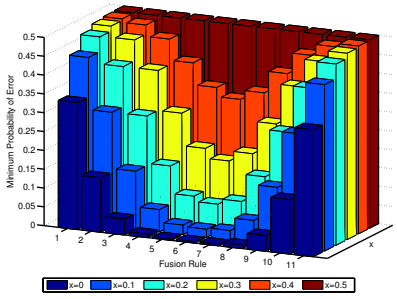


Fig. 2. Minimum probability of error for different x. Odd number of nodes are considered ($N = 11$).

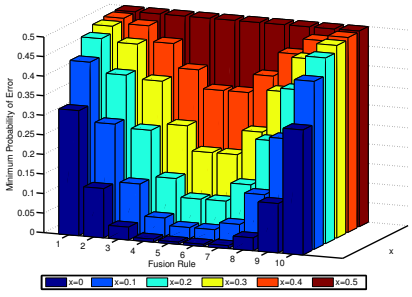


Fig. 3. Minimum probability of error for different x. Even number of nodes are considered ($N = 10$).

Let x_{max} denote the maximum fraction of nodes the Byzantine can compromise. From Figure 2 we can deduce that, *in equilibrium, the Byzantine adopts the pure strategy $x = x_{max}$ (to maxmin the FC), and the FC becomes indifferent to the choice of (k, τ) pairs that solve $\min_{K,\tau} P_e(K, \tau, x_{max})$ and can arbitrarily mix among all such (k, τ) pairs.* This is an equilibrium, since, all (k, τ) pairs that solve $\min_{K,\tau} P_e(K, \tau, x_{max})$ are optimized against the Byzantine's strategy $x = x_{max}$. Also, the Byzantine can not deviate from x_{max} to obtain a higher P_e. Observe that, when $x_{max} < 0.5$, the FC has an unique (k, τ) pair that is a best response to the attacker's strategy $x = x_{max}$, and thus the strategy of the FC degenerates to a pure strategy. Specifically, in this case, the pure strategy Nash Equilibrium (K^*, τ^*, x^*) in the minimax game is given by $(\lceil N/2 \rceil, 0, x_{max})$. However, when $x_{max} = 0.5$, any (k, τ) is a solution to $\min_{K,\tau} P_e(K, \tau, x_{max})$, and thus the FC can arbitrarily mix among all (k, τ) pairs in equilibrium.

In Figure 3, we consider an even number of nodes ($N = 10$) while plotting the minimum probability of error by considering the FC's best response against attacker's strategy. Priors are again assumed to be equal. As can be seen from the figure, probability of error P_e is monotonically increasing function of x. Thus, similar to the case with odd number of nodes, in equilibrium, the Byzantine will again adopt the pure strategy $x = x_{max}$, while the FC can arbitrarily mix among all (k, τ) pairs that solve $\min_{K,\tau} P_e(K, \tau, x_{max})$.

Interestingly, when $x_{max} < 0.5$, the FC has two (k, τ) pairs[4] that are best responses to the attacker's strategy $x = x_{max}$, which is in contrast to the scenario with odd number of nodes. Thus, in equilibrium the FC can mix between the two pairs of (k, τ) that minimize P_e when $x = x_{max} < 0.5$. Specifically, in this case, the Nash Equilibrium strategy profile is $((N/2) + 1, -\epsilon, x_{max})$ and $(N/2, \epsilon, x_{max})$, where $\epsilon > 0$. Similar to the case with odd number of nodes, when $x_{max} = 0.5$, any (k, τ) is a solution to $\min_{K,\tau} P_e(K, \tau, x_{max})$, and thus the FC can arbitrarily mix among all (k, τ) pairs in equilibrium.

[4]In Figure 3, these two (k, τ) pairs are $(6, -\epsilon)$ and $(5, \epsilon)$ with $\epsilon = 0.3,\ 0.3,\ 0.4,\ 0.4,\ 0.2$ for $x = 0,\ 0.1,\ 0.2,\ 0.3\ , 0.4$, respectively.

5. CONCLUSION AND FUTURE WORK

In this paper, we considered the problem of optimal fusion rule and threshold design in the presence of Byzantine attackers. First, we considered the problem of finding optimal fusion rule (K^*) under the constraint of fixed local sensor thresholds (λ) and fixed Byzantine strategy (x). Next, we considered the problem of joint optimization of fusion rule and local sensor threshold ($K,\ \lambda$) for a fixed Byzantine strategy. Then we extended these results to the scenario where the FC and the Byzantine act in a strategic manner and modelled it as a minimax game. We numerically analyzed the game, showing the existence of Nash Equilibrium and also illustrated the equilibrium strategy profile. In future, we will investigate enhancing distributed detection performance in the presence of Byzantine attackers by suitably adding stochastic resonance (SR) noise, while considering probability of error as a detection performance metric.

6. REFERENCES

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

[2] R. Viswanathan and P. Varshney, "Distributed detection with multiple sensors I. Fundamentals," *Proceedings of the IEEE*, vol. 85, no. 1, pp. 54 –63, jan 1997.

[3] 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.

[4] W. Shi, T. W. Sun, and R. D. Wesel, "Optimal binary distributed detection," in *Proceedings of the 33rd Asilomar Conference on Signals, Systems, and Computers*, 1999, pp. 24–27.

[5] A. Vempaty, K. Agrawal, H. Chen, and P. Varshney, "Adaptive learning of byzantines' behavior in cooperative spectrum sensing," in *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, march 2011, pp. 1310 –1315.

[6] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of byzantine attacks," *Signal Processing, IEEE Transactions on*, vol. 57, no. 1, pp. 16 –29, jan. 2009.

[7] H. Wang, L. Lightfoot, and T. Li, "On phy-layer security of cognitive radio: Collaborative sensing under malicious attacks," in *Information Sciences and Systems (CISS), 2010 44th Annual Conference on*, March 2010, pp. 1 –6.

[8] M. Abdelhakim, L. Zhang, J. Ren, and T. Li, "Cooperative sensing in cognitive networks under malicious attack," in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*, May 2011, pp. 3004 –3007.

[9] A. Rawat, P. Anand, H. Chen, and P. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *Signal Processing, IEEE Transactions on*, vol. 59, no. 2, pp. 774 –786, Feb 2011.

[10] B. Kailkhura, S. Brahma, and P. K. Varshney, "Optimal byzantine attack on distributed detection in tree based topologies," in *Proc. International Conference on Computing, Networking and Communications Workshops (ICNC-2013)*, San Diego, CA, January 2013, pp. 227–231.

[11] J. N. Tsitsiklis, "Decentralized detection by a large number of sensors*," *Mathematics of control, Signals, and Systems*, vol. 1, pp. 167–182, 1988.

[12] M. Naraghi-Pour and V. Nadendla, "Secure detection in wireless sensor networks using a simple encryption method," in *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, March 2011, pp. 114 –119.

[13] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes: The Art of Scientific Computing*, 3rd ed. Cambridge University Press, 2007.