Asymptotic Analysis of Distributed Bayesian Detection with Byzantine Data

Bhavya Kailkhura, *Student Member, IEEE*, Yunghsiang S. Han, *Fellow, IEEE*,
Swastik Brahma, *Member, IEEE*, Pramod K. Varshney, *Fellow, IEEE*

Abstract

In this letter, we consider the problem of distributed Bayesian detection in the presence of Byzantine data. The problem of distributed detection is formulated as a binary hypothesis test at the fusion center (FC) based on 1-bit data sent by the sensors. Adopting Chernoff information as our performance metric, we study the detection performance of the system under Byzantine attack in the asymptotic regime. The expression for minimum attacking power required by the Byzantines to blind the FC is obtained. More specifically, we show that above a certain fraction of Byzantine attackers in the network, the detection scheme becomes completely incapable of utilizing the sensor data for detection. When the fraction of Byzantines is not sufficient to blind the FC, we also provide closed form expressions for the optimal attacking strategies for the Byzantines that most degrade the detection performance.

Index Terms

Bayesian detection, Data falsification, Byzantine Data, Chernoff information, Distributed detection

This work was supported in part by ARO under Grant W911NF-13-2-0040 and National Science Council of Taiwan, under grants NSC 99-2221-E-011-158 -MY3, NSC 101-2221-E-011-069 -MY3. Han's work was completed during his visit to Syracuse University from 2012 to 2013.

B. Kailkhura, S. Brahma and P. K. Varshney are with Department of EECS, Syracuse University, Syracuse, NY 13244. (email: bkailkhu@syr.edu; skbrahma@syr.edu; varshney@syr.edu)

Y. S. Han is with EE Department, National Taiwan University of Science and Technology, Taiwan, R. O. C. (email: yshan@mail.ntust.edu.tw)

I. Introduction

Distributed detection is a well studied topic in the detection theory literature [1]–[3]. In distributed detection systems, due to bandwidth and energy constraints, the nodes often make a 1-bit local decision regarding the presence or absence of a phenomenon before sending it to the fusion center (FC). Based on the local decisions transmitted by the nodes, the FC makes a global decision about the presence or absence of the phenomenon of interest. The performance of such systems strongly depends on the reliability of the nodes in the network. The distributed nature of such systems makes them quite vulnerable to different types of attacks. One typical attack on such networks is a Byzantine attack. While Byzantine attacks (originally proposed by [4]) may, in general, refer to many types of malicious behavior, our focus in this letter is on data-falsification attacks [5]–[12].

Distributed detection in the presence of Byzantine attacks has been explored in the past in [7], [8], where the problem of determining the most effective attacking strategy of the Byzantine nodes was explored. In [7], the authors considered the Neyman-Pearson (NP) setup and determined the optimal attacking strategy which minimizes the detection error exponent. This approach, based on Kullback-Leibler divergence (KLD), is analytically tractable and yields approximate results in non-asymptotic cases. They also assumed that the Byzantines know the true hypothesis, which obviously is not satisfied in practice but does provide a bound. In [8], the authors analyzed the same problem in the context of collaborative spectrum sensing under Byzantine Attacks. They relaxed the assumption of perfect knowledge of the hypotheses by assuming that the Byzantines determine the knowledge about the true hypotheses from their own sensing observations. Schemes for Byzantine node identification have been proposed in [8], [12]–[15]. Our focus in this letter is considerably different from Byzantine node identification schemes in that we do not try to authenticate the data; we determine the Byzantine attacking strategies that maximally degrade the detection performance of the network.

All the approaches discussed so far for distributed detection schemes robust to Byzantine attacks consider distributed detection under the Neyman-Pearson (NP) setup. In contrast, we focus on the impact of Byzantine nodes on distributed Bayesian detection, which has not been considered in the past. Adopting Chernoff information as our performance metric, we study the performance of distributed detection systems with Byzantines in the asymptotic regime. We are

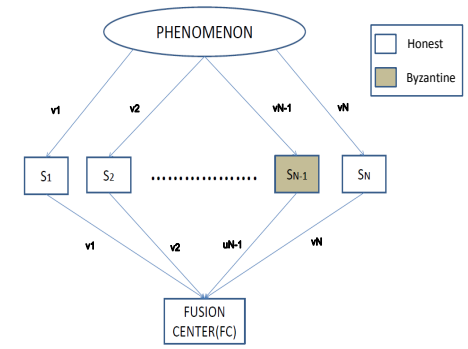


Fig. 1. System Model

interested in answering the following questions.

- From the Byzantines' perspective, what is the most effective attacking strategy?
- What is the minimum fraction of Byzantines needed to blind the FC?
- From the FC's perspective, knowing the fraction of Byzantines in the network, or an upper bound thereof, what is the achievable performance not knowing the identities of compromised nodes?

The signal processing problem considered in this letter is most similar to [8]. Our results, however, are not a direct application of those in [8]. While as in [8], we are also interested in the worst distribution pair, our objective function and, therefore, the techniques to find them are different. In contrast to [8], where only optimal strategies to blind the FC were obtained, we also provide closed form expressions for the optimal attacking strategies for the Byzantines that most degrade the detection performance when the fraction of Byzantines is not sufficient to blind the FC. Indeed, finding the optimal Byzantine attacking strategies is only the first step toward designing a robust distributed detection system. The knowledge of optimal attack strategies can be further used to implement the optimal detector at the FC.

II. Distributed detection in the presence of Byzantines

Consider two hypotheses H_0 (signal is absent) and H_1 (signal is present). Also, consider a parallel network (see Figure 1), comprised of a central entity (known as the Fusion Center (FC)) and a set of N sensors (nodes), which faces the task of determining which of the two hypotheses is true. Prior probabilities of the two hypotheses H_0 and H_1 are denoted by P_0 and

P_1, respectively. The sensors observe the phenomenon, carry out local computations to decide the presence or absence of the phenomenon, and then send their local decisions to the FC that makes a final decision U_0 after processing the local decisions. Observations at the nodes are assumed to be conditionally independent and identically distributed. A Byzantine attack on such a system compromises some of the nodes which may then intentionally send falsified local decisions to the FC to make the final decision incorrect. We assume that a fraction α of the N nodes which observe the phenomenon have been compromised by an attacker. We consider the communication channels to be error-free. Next, we describe the modus-operandi of the nodes in detail.

A. *Modus Operandi of the Nodes*

Based on the observations, each node i makes a one-bit local decision $v_i \in \{0, 1\}$ regarding the absence or presence of the phenomenon using the likelihood ratio test

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

where λ is the identical threshold[1] used at all the sensors and $p_{Y_i}^{(k)}(y_i)$ is the conditional probability density function (PDF) of observation y_i under the hypothesis H_k, where $k = 0, 1$.

Each node i, after making its one-bit local decision v_i, sends u_i to the FC, where $u_i = v_i$ if i is an uncompromised (honest) node, but for a compromised (Byzantine) node i, u_i need not be equal to v_i. We denote the probabilities of detection and false alarm of each node i in the network by $P_d = P(v_i = 1|H_1)$ and $P_f = P(v_i = 1|H_0)$, respectively, which hold for both uncompromised nodes as well as compromised nodes.

In this letter, we assume that each Byzantine decides to attack independently relying on its own observation and decision regarding the presence or absence of the phenomenon. Specifically, 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:

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

[1]It has been shown that the use of identical thresholds is asymptotically optimal [16].

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

Byzantine nodes:

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

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

where $P^{H}(x = a|y = b)$ ($P^{B}(x = a|y = b)$) is the probability that an honest (Byzantine) node sends a to the FC when its actual local decision is b. From now onwards, we will refer to Byzantine flipping probabilities simply by $(P_{1,0}, P_{0,1})$. We also assume that the FC is not aware of the identities of Byzantine nodes and considers each node i to be Byzantine with a certain probability α.

B. Performance Criterion

The Byzantine attacker always wants to degrade the detection performance at the FC as much as possible; in contrast, the FC wants to maximize the detection performance. The network detection performance is measured in terms of global probability of error

$$P_E = P_0 P_F + P_1(1 - P_D)$$

where $P_F = P(U_0 = 1|H_0)$ and $P_D = P(U_0 = 1|H_1)$ are global probability of false alarm and global probability of detection, respectively. The probability of error at the FC in the presence of the Byzantines, however, cannot be analyzed easily for the non-asymptotic case. To gain insights into the degree to which an adversary can cause performance degradation, we consider the asymptotic regime and employ the Chernoff information [17] to be the network performance metric that characterizes detection performance.

If $\mathbf{u}$ is a random vector having N statistically independent and identically distributed components, u_is, under both hypotheses, the optimal detector results in error probability that obeys the asymptotics

$$\lim_{N\to\infty} \frac{\ln P_E}{N} = -C(\pi_{1,1}, \pi_{1,0}), \tag{6}$$

where the Chernoff information C is defined as

$$C = \max_{0 \le t \le 1} -\ln\Big(\sum_{j \in \{0,1\}} \pi_{j0}^{t} \pi_{j1}^{1-t}\Big). \tag{7}$$

π_{j0} and π_{j1} in (7) are the conditional probabilities of $u_i = j$ given H_0 and H_1, respectively. Specifically, $\pi_{1,0}$ and $\pi_{1,1}$ can be calculated as

$$\pi_{1,0} = \alpha(P_{1,0}(1 - P_f) + (1 - P_{0,1})P_f) + (1 - \alpha)P_f \tag{8}$$

$$\pi_{1,1} = \alpha(P_{1,0}(1 - P_d) + (1 - P_{0,1})P_d) + (1 - \alpha)P_d, \tag{9}$$

where α is the fraction of Byzantine nodes.

From the Byzantine attacker's point of view, our goal is to find $P_{1,0}$ and $P_{0,1}$ that minimize Chernoff information C for a given value of α. Observe that, when $\alpha \geq 0.5$, Chernoff information can be minimized by simply making posterior probabilities equal to prior probabilities (we discuss this in more detail later in the letter). However, for $\alpha < 0.5$, a closed form expression for Chernoff information is needed to find $P_{1,0}$ and $P_{0,1}$ that minimize C.

III. Closed Form Expression for the Chernoff Information

In this section, we derive a closed form expression for the Chernoff information, when $\alpha < 0.5$.[2] To obtain the closed form expression for Chernoff information, the solution of an optimization problem is required: $\underset{0 \le t \le 1}{max} -\ln(\sum_{j \in \{0,1\}} \pi_{j0}^{t} \pi_{j1}^{1-t})$. Obtaining a closed form solution for this optimization problem can be tedious. We can find a closed form expression for the Chernoff information for $\alpha < 0.5$.

Lemma 1. *For $\alpha < 0.5$, the Chernoff information between the distributions $\pi_{1,0}$ and $\pi_{1,1}$ (as given in* (8) *and* (9)*, respectively) is given by $C = -\ln(\sum_{j \in \{0,1\}} \pi_{j0}^{t^*} \pi_{j1}^{1-t^*})$ with*

$$t^* = \frac{\ln\left(\dfrac{\ln(\pi_{1,1}/\pi_{1,0})}{\ln((1-\pi_{1,0})/(1-\pi_{1,1}))} \dfrac{\pi_{1,1}}{1-\pi_{1,1}}\right)}{\ln\left(\dfrac{(1/\pi_{1,0})-1}{(1/\pi_{1,1})-1}\right)}. \tag{10}$$

[2]Similar results can be derived for $\alpha \geq 0.5$.

Proof: Observe that the problem of finding the optimal t^* in (7) is equivalent to

$$\min_{0\leq t\leq 1} \ln\Big(\sum_{j\in\{0,1\}} \pi_{j0}^{t}\pi_{j1}^{1-t}\Big) \tag{11}$$

which is a constrained minimization problem. To find t^*, we first perform unconstrained minimization (no constraint on the value of t) and later show that the solution of the unconstrained optimization problem is the same as the solution of the constrained optimization problem. In other words, the optimal t^* is the same for both cases.

By observing that logarithm is an increasing function, the optimization problem as given in (11) is equivalent to

$$\min_{t}[\pi_{1,0}^{t}\pi_{1,1}^{1-t} + (1-\pi_{1,0})^{t}(1-\pi_{1,1})^{1-t}]. \tag{12}$$

Now, performing the first derivative test, we have

$$\begin{aligned} & \frac{d}{dt}[\pi_{1,0}^{t}\pi_{1,1}^{1-t} + (1-\pi_{1,0})^{t}(1-\pi_{1,1})^{1-t}] \\ = \;& (1-\pi_{1,1})\left(\frac{1-\pi_{1,0}}{1-\pi_{1,1}}\right)^{t}\ln\left(\frac{1-\pi_{1,0}}{1-\pi_{1,1}}\right) \\ & +\pi_{1,1}\left(\frac{\pi_{1,0}}{\pi_{1,1}}\right)^{t}\ln\left(\frac{\pi_{1,0}}{\pi_{1,1}}\right). \end{aligned} \tag{13}$$

The first derivative (13) is set to zero to find the critical points of the function:

$$\left(\frac{(1/\pi_{1,0})-1}{(1/\pi_{1,1})-1}\right)^{t} = \frac{\ln(\pi_{1,1}/\pi_{1,0})}{\ln((1-\pi_{1,0})/(1-\pi_{1,1}))}\left(\frac{\pi_{1,1}}{1-\pi_{1,1}}\right). \tag{14}$$

After some simplification, t^* which satisfies (14) turns out to be

$$t^* = \frac{\ln\left(\dfrac{\ln(\pi_{1,1}/\pi_{1,0})}{\ln((1-\pi_{1,0})/(1-\pi_{1,1}))}\dfrac{\pi_{1,1}}{1-\pi_{1,1}}\right)}{\ln\left(\dfrac{(1/\pi_{1,0})-1}{(1/\pi_{1,1})-1}\right)}. \tag{15}$$

To determine whether the critical point is a minimum or a maximum, we perform the second

derivative test. Since

$$\begin{aligned} & \frac{d^2}{d^2t}[\pi_{1,0}^t \pi_{1,1}^{1-t} + (1-\pi_{1,0})^t (1-\pi_{1,1})^{1-t}] \\ = \; & (1-\pi_{1,1}) \left(\frac{1-\pi_{1,0}}{1-\pi_{1,1}}\right)^t \left(\ln \frac{1-\pi_{1,0}}{1-\pi_{1,1}}\right)^2 \\ & + \pi_{1,1} \left(\frac{\pi_{1,0}}{\pi_{1,1}}\right)^t \left(\ln \frac{\pi_{1,0}}{\pi_{1,1}}\right)^2 \end{aligned} \tag{16}$$

is greater than zero, t^* as given in (15) minimizes (12). Since $0 \leq t^* \leq 1$ (For proof please refer to [18]), t^* as given in (15) is also the solution of (11). ■

IV. Asymptotic Analysis of Optimal Byzantine Attack

First, we will determine the minimum fraction of Byzantines needed to blind the decision fusion scheme.

A. Critical Power to Blind the Fusion Center

In this section, we determine the minimum fraction of Byzantine nodes needed to make the FC "blind" and denote it by α_{blind}. We say that the FC is blind if an adversary can make the data that the FC receives from the sensors such that no information is conveyed. In other words, the optimal detector at the FC cannot perform better than simply making the decision based on priors.

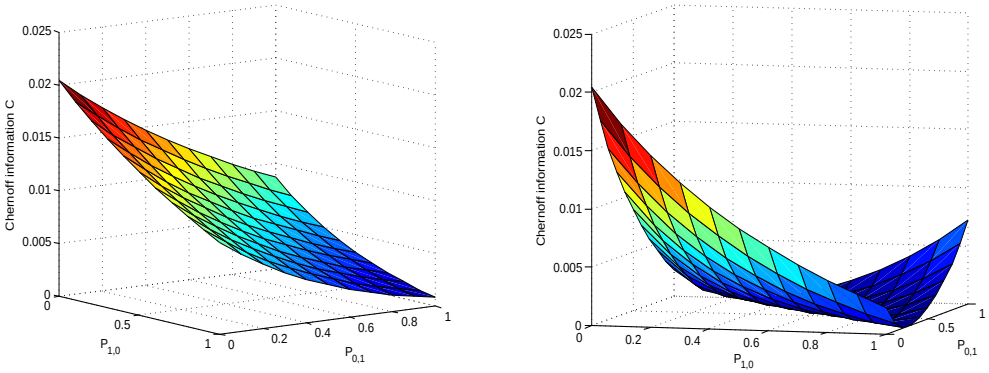
Lemma 2. *In Bayesian distributed detection, the minimum fraction of Byzantines needed to make the FC blind is* $\alpha_{blind} = 0.5$.

Proof: The FC becomes blind if the probability of receiving a given vector $\mathbf{u}$ is independent of the hypothesis present. Using the assumption that observations at the nodes are conditionally independent and identically distributed, the condition to make the FC blind becomes $\pi_{1,1} = \pi_{1,0}$. This is true only when

$$\alpha[P_{1,0}(P_f - P_d) + (1 - P_{0,1})(P_d - P_f)] + (1-\alpha)(P_d - P_f) = 0.$$

Hence, the FC becomes blind if

$$\alpha = 1/(P_{1,0} + P_{0,1}). \tag{17}$$



(a) (b)

Fig. 2. (a) Chernoff information as a function of $(P_{1,0}, P_{0,1})$ for $\alpha = 0.4$. (b) Chernoff information as a function of $(P_{1,0}, P_{0,1})$ for $\alpha = 0.8$.

α in (17) is minimized when $P_{1,0}$ and $P_{0,1}$ both take their largest values, i.e., $P_{1,0} = P_{0,1} = 1$. Hence, $\alpha_{blind} = 0.5$. ■

Next, we find the optimal attacking strategies which minimize the Chernoff information.

B. Minimization of Chernoff Information

First, we minimize Chernoff information for $\alpha < 0.5$. Later in the section, we generalize our results for any arbitrary α. Since logarithm is an increasing function, the problem of minimizing the Chernoff information is equivalent to the following problem:

$$\begin{aligned} \underset{P_{1,0},P_{0,1}}{\text{maximize}} \quad & \pi_{1,0}^{t^*}\pi_{1,1}^{1-t^*} + (1-\pi_{1,0})^{t^*}(1-\pi_{1,1})^{1-t^*} \\ \text{subject to} \quad & 0 \le P_{1,0} \le 1 \\ & 0 \le P_{0,1} \le 1 \end{aligned} \tag{P1}$$

where $\alpha < 0.5$ and t^* is as given in (15).

Let us denote $\tilde{C} = \pi_{1,0}^{t^*}\pi_{1,1}^{1-t^*} + (1-\pi_{1,0})^{t^*}(1-\pi_{1,1})^{1-t^*}$. Observe that, maximization of $\tilde{C}$ is equivalent to the minimization of Chernoff information C. Next, in Lemma 3 we present the properties of Chernoff information C (for the case when $\alpha < 0.5$) with respect to $(P_{1,0}, P_{0,1})$ that enable us to find the optimal attacking strategies in this case.

Lemma 3. *Let $\alpha < 0.5$ and assume that the optimal t^* is used in the expression for the Chernoff information. Then, the Chernoff information, C, is a monotonically decreasing function of $P_{1,0}$*

for a fixed $P_{0,1}$. Conversely, the Chernoff information is also a monotonically decreasing function of $P_{0,1}$ for a fixed $P_{1,0}$.

Proof: Please refer to [18]. ■

Next, using Lemma 3, we present the optimal attacking strategies $P_{1,0}$ and $P_{0,1}$ that minimize the Chernoff information, C, for $0 \leq \alpha \leq 1$.

Theorem 1. *The optimal attacking strategy, $(P^*_{1,0}, P^*_{0,1})$, which minimizes the Chernoff information is*

$$(P^*_{1,0}, P^*_{0,1}) = \begin{cases} (p_{1,0}, p_{0,1}) & \text{if } \alpha \geq 0.5 \\ (1,1) & \text{if } \alpha < 0.5 \end{cases},$$

where, $(p_{1,0}, p_{0,1})$ satisfy $\alpha(p_{1,0} + p_{0,1}) = 1$.

Proof: The minimum value of C is zero and it occurs when $\pi_{1,1} = \pi_{1,0}$. By (8) and (9), $\pi_{1,1} = \pi_{1,0}$ implies

$$\alpha(P_{1,0} + P_{0,1}) = 1. \tag{18}$$

From (18), when $\alpha \geq 0.5$, the attacker can always find flipping probabilities that make the Chernoff information equal to zero. When $\alpha = 0.5$, $P_{1,0} = P_{0,1} = 1$ is the optimal strategy. When $\alpha > 0.5$, any pair which satisfies $P_{1,0} + P_{0,1} = \frac{1}{\alpha}$ is the optimal strategy. However, when $\alpha < 0.5$, (18) cannot be satisfied or in other words Byzantines can not make $C = 0$ since $\pi_{1,1}$ can not be made equal to $\pi_{1,0}$. From Lemma 3, when $\alpha < 0.5$, the optimal attacking strategy, $(P_{1,0}, P_{0,1})$, that minimizes the Chernoff information is $(1, 1)$. ■

Next, to gain insights into Theorem 1, we present some illustrative examples that corroborate our results.

C. Illustrative Examples

In Figure 2(a), we plot the Chernoff information as a function of $(P_{1,0}, P_{0,1})$ for $(P_d = 0.6, P_f = 0.4)$ and $\alpha = 0.4$. It can be observed that for a fixed $P_{0,1}$ ($P_{1,0}$) the Chernoff information C is a monotonically decreasing function of $P_{1,0}$, $P_{0,1}$ (as has been shown in Lemma 3). In other words, when $\alpha = 0.4$, the attacking strategy, $(P_{1,0}, P_{0,1})$, that minimizes the Chernoff information C is $(1, 1)$.

Similarly, in Figure 2(b), we consider the scenario when the fraction of Byzantines in the network is $\alpha = 0.8$. It can be seen from Figure 2(b) that the minimum value of the Chernoff information in this case is $C = 0$. Notice that, the attacking strategy, $(P_{1,0}, P_{0,1})$ that makes $C = 0$ is not unique in this case. It can be verified that any attacking strategy which satisfies $P_{1,0} + P_{0,1} = \frac{1}{0.8}$ would make $C = 0$. Thus, results presented in Figures 2(a) and 2(b) corroborate our theoretical result presented in Theorem 1.

V. Discussion and Future Work

We considered the problem of distributed Bayesian detection with Byzantine data, and characterized the power of attack analytically. We obtained closed form expressions for the optimal attacking strategies that most degrade the detection performance. The knowledge of optimal attack strategies can be further used to implement the optimal detector at the FC. In the future, we plan to extend our analysis to the non-asymptotic case.

References

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

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

[3] V. Veeravalli and P. K. Varshney, "Distributed inference in wireless sensor networks," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 370, pp. 100–117, 2012.

[4] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982. [Online]. Available: http://doi.acm.org/10.1145/357172.357176

[5] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks," *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 428–445, 2013.

[6] H. Rifà-Pous, M. J. Blasco, and C. Garrigues, "Review of robust cooperative spectrum sensing techniques for cognitive radio networks," *Wirel. Pers. Commun.*, vol. 67, no. 2, pp. 175–198, Nov. 2012. [Online]. Available: http://dx.doi.org/10.1007/s11277-011-0372-x

[7] S. Marano, V. Matta, and L. Tong, "Distributed Detection in the Presence of Byzantine Attacks," *IEEE Trans. Signal Process.*, vol. 57, no. 1, pp. 16 –29, Jan. 2009.

[8] A. Rawat, P. Anand, H. Chen, and P. Varshney, "Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks," *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 774 –786, Feb 2011.

[9] B. Kailkhura, S. Brahma, Y. S. Han, and P. K. Varshney, "Distributed Detection in Tree Topologies With Byzantines," *IEEE Trans. Signal Process.*, vol. 62, pp. 3208–3219, June 2014.

[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] B. Kailkhura, S. Brahma, Y. S. Han, and P. K. Varshney, "Optimal Distributed Detection in the Presence of Byzantines," in *Proc. The 38th International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2013)*, Vancouver, Canada, May 2013.

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

[13] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. 27th Conf. Comput. Commun., Phoenix, AZ*, 2008, pp. 1876–1884.

[14] E. Soltanmohammadi, M. Orooji, and M. Naraghi-Pour, "Decentralized Hypothesis Testing in Wireless Sensor Networks in the Presence of Misbehaving Nodes," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 205–215, 2013.

[15] B. Kailkhura, Y. S. Han, S. Brahma, and P. K. Varshney, "On Covert Data Falsification Attacks on Distributed Detection Systems," in *Communications and Information Technologies (ISCIT), 2013 13th International Symposium on*, Sept 2013, pp. 412–417.

[16] J. N. Tsitsiklis, "Decentralized Detection by a Large Number of Sensors*," *Math. control, Signals, and Systems*, vol. 1, pp. 167–182, 1988.

[17] H. Chernoff, "A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the sum of Observations," *The Annals of Mathematical Statistics*, vol. 23, pp. 493–507, December 1952.

[18] B. Kailkhura, Y. S. Han, S. Brahma, and P. K. Varshney, "Asymptotic Analysis of Distributed Bayesian Detection with Byzantine Data," *CoRR*, vol. abs/1408.3434, 2014. [Online]. Available: http://arxiv.org/abs/1408.3434