ON THE PERFORMANCE ANALYSIS OF DATA FUSION SCHEMES WITH BYZANTINES

Bhavya Kailkhura *Swastik Brahma* *Pramod K. Varshney*

Department of EECS, Syracuse University, Syracuse, NY 13244 USA

ABSTRACT

This paper considers the problem of performance analysis of data fusion schemes in the presence of Byzantine attacks. First, we analyze the security performance of data fusion schemes with Byzantines. We show that when more than a certain fraction of Byzantines are present in the network, the raw data fusion schemes become completely incapable (blind). More specifically, we obtain a closed form expression for the lower bound on the fraction of Byzantines needed to blind the fusion center as a function of attacker's strength. Next, we investigate the global detection performance in the presence of Byzantine attacks, and analytically characterize the effect of Byzantines on detection performance. Numerical results provide insights into our analysis.

Index Terms— Distributed Detection, Data Fusion, Byzantine Attacks, Deflection Coefficient, Probability of Error

1. INTRODUCTION

Distributed detection is a well studied topic in detection theory literature [1–3]. The distributed detection framework comprises of a group of spatially distributed nodes which acquire the observations regarding the phenomenon of interest and send them to the fusion center (FC) where a global decision is made. Different fusion schemes can be employed depending on what is transmitted to the FC. For example, in data fusion based schemes, nodes send their raw energy measurements, however, in decision fusion based schemes nodes send their local detection decisions based on their energy measurements. In this paper, our focus is on the data fusion based detection schemes where raw measurements are sent to the FC.

In recent years, such distributed networks have become increasingly vulnerable to security threats. One typical attack is a Byzantine attack or a data falsification attack. Byzantines try to degrade the detection performance of the fusion center by sending falsified information. Recently, the problem of detection in the presence of Byzantine attacks has attracted attention. In [4–16], the authors considered the problem of Byzantine attacks on *decision* fusion schemes. Byzantines, in order to undermine network performance, may alter their one bit local decisions prior to transmission. In addition to the aforementioned contributions that consider Byzantine attacks on decision fusion schemes, a few other papers have considered Byzantine attack on *data* fusion schemes. Byzantine attacks on data fusion schemes in [17–20] aim to degrade the detection performance by manipulating their observed data (e.g., raw energy values) either by increasing or decreasing the signal strength. In such scenarios, it is important to characterize and study system degradation caused by the Byzantines.

The impact of Byzantine attacks on data fusion schemes has been briefly mentioned in [19–21], and some schemes to counter them have been proposed in [17–21]. However, no analytical study has been carried out to investigate the performance of the system. We aim to fill this gap by analyzing the security and detection performance degradation of data fusion based methods under Byzantine attacks. We are interested in an analytical characterization of the ability of Byzantines to affect the decision at the fusion center. The analysis and the discussion in the rest of the paper provide a deeper understanding of the effectiveness of Byzantine attacks. The main contributions of this paper are as follows.

1. We use deflection coefficient to characterize the security performance of a detection system and analyze performance degradation as a function of number of Byzantines.
2. We provide a lower bound on the fraction of Byzantines needed to blind the FC as a function of attack strength.
3. Using probability of detection and probability of false alarm as measures of detection performance, we investigate the detection performance degradation with Byzantines.

2. SYSTEM MODEL

The problem of signal detection is formulated as a binary hypothesis test where the hypothesis H_1 indicates the presence of a signal, while H_0 indicates its absence. Nodes acquire observations that are independent conditioned on the hypotheses. A parallel network topology with N nodes using an energy detection scheme [22] is considered. Nodes directly transmit their summary statistic based on raw energy value to the FC through noise free reporting channels. For the i^{th} node, the received signal x_i at time instant k can be modeled as

$$x_i(k) = \begin{cases} n_i(k), & \text{if } H_0 \\ h_i s_i(k) + n_i(k) & \text{if } H_1 \end{cases}$$

where h_i is the channel gain, $s_i(k)$ is the signal at time instant k, $n_i(k)$ is AWGN, i.e., $n_i(k) \sim N(0, \sigma_i^2)$. $s_i(k)$ and $n_i(k)$ are assumed to be independent of each other. Each node i calculates a summary statistic Y_i based on M samples that are collected over a detection interval of interest, i.e., $Y_i = \sum_{k=1}^{M} (x_i(k))^2$, where M is determined by the time-bandwidth product. Since Y_i is the sum of the square of M Gaussian random variables, $\frac{Y_i}{\sigma_i^2}$ follows a central chi-square distribution with M degrees of freedom under H_0; otherwise, non-central chi-square distribution with M degrees of freedom and parameter η_i.

$$\frac{Y_i}{\sigma_i^2} \sim \begin{cases} \chi_M^2, & \text{if } H_0 \\ \chi_M^2(\eta_i) & \text{if } H_1 \end{cases}$$

where $\eta_i = \frac{E_s |h_i|^2}{\sigma_i^2}$ is the local SNR at the i^{th} node and the quantity $E_s = \sum_{K=1}^{M} |s(k)|^2$ represents transmitted signal energy based on M samples. Note that the local SNR is M times the average SNR at the output of the energy detector, which is $\frac{E_s |h_i|^2}{M\sigma_i^2}$.

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

For data fusion schemes, energy values from different nodes are employed to compute a weighted average with optimized weight coefficients and the decision is made based on the weighted sum:

$$f(Y_1, Y_2 ... Y_N) = \begin{cases} H_1 & \text{if } \sum_{i=1}^{N} w_i Y_i > \lambda \\ H_0 & \text{otherwise} \end{cases}$$

where λ is the global test statistic threshold. By defining $diag(.)$ as a square diagonal matrix with the elements of a given vector on the diagonal, we define: $\Sigma_{H_0} = 2Mdiag^2(\sigma)$,

$\Sigma_{H_1} = 2Mdiag^2(\sigma) + 4diag(\eta)diag^2(\sigma),\ w = [w_1, \cdots, w_N]^T$

$\sigma = [\sigma_1^2, \cdots, \sigma_N^2]^T,\ h = [|h_1|^2, \cdots, |h_N|^2]^T,\ \eta = [\eta_1, \cdots, \eta_N]^T$.
Now, threshold λ with targeted false alarm constraint p is given by

$$\lambda = N\sigma^T w + Q^{-1}(p)\sqrt{w^T \Sigma_{H_0} w}. \quad (1)$$

The optimal weights are given by $w_i = \frac{\eta_i/\sigma_i^2}{\sum_{i=1}^{N} \eta_i/\sigma_i^2}$, where η_i is the local SNR and σ_i^2 is the variance of the measurement noise [23, 24]. According to the central limit theorem, if the number of samples M is large enough (e.g., $M \geq 10$ in practice), the global test statistic, $\Lambda = \sum_{i=1}^{N} w_i Y_i$, is normally distributed with mean

$$mean(\Lambda) = \begin{cases} M\sigma^T w & \text{if } H_0 \\ (M\sigma + E_s h)^T w & \text{if } H_1 \end{cases}$$

and variance

$$Var(\Lambda) = \begin{cases} w^T \Sigma_{H_0} w & \text{if } H_0 \\ w^T \Sigma_{H_1} w & \text{if } H_1. \end{cases}$$

Next, a mathematical model for Byzantine attacks is presented.

3. THE BYZANTINE ATTACK MODEL

The objective of the Byzantines is to degrade the detection performance of the network by falsifying their data. We assume that the fusion center does not know which node is a Byzantine, but it knows that there are α fraction of Byzantines in the network. By assuming that the Byzantines are intelligent and know the true hypothesis, we analyze the performance of the data fusion schemes. This analysis provides the most favorable case from the point of view of the Byzantines and yields the maximum performance degradation that Byzantines can cause. Byzantines tamper their raw data or sensed energy value Y and send $\tilde{Y}$ such that the detection performance will be degraded:

$$\tilde{Y_i} = \begin{cases} Y_i + D_i & \text{if } H_0 \\ Y_i - D_i & \text{if } H_1 \end{cases}$$

where D_i is a constant value which represents the attack strength. As we show later, Byzantine nodes will use a large value of D_i so that the final statistics value is dominated by the Byzantine node's local statistic that will lead to a degraded detection performance.

Next, we analyze the security performance of raw data fusion based detection schemes in the presence of Byzantine attacks. We use the Deflection coefficient [25] to characterize the security performance of the detection scheme due to its simplicity and its strong relationship with the global detection performance. Deflection coefficient of the global test statistic, Λ is defined as: $D(\Lambda) = \frac{(\mu_1 - \mu_0)^2}{\sigma_0^2}$, where $\mu_k = \mathbb{E}[\Lambda|H_k]$ is the conditional mean and $\sigma_k^2 = \mathbb{E}[(\Lambda - \mu_k)^2|H_k]$ is the conditional variance. The deflection coefficient is also closely related to other performance measures, e.g., Receiver Operating Characteristics (ROC) curve. In general, the detection performance monotonically increases with increasing value of the deflection coefficient. We define the critical point of the distributed detection network as the minimum fraction of Byzantine nodes needed to make deflection coefficient at the fusion center equal to zero (or blind the network) and denote it by α_{blind}. In Section 4, we use α_{blind} to characterize the security performance of the network. Then in Section 5, we analyze the performance of raw data fusion based detection schemes in the presence of Byzantine attacks. We consider type I and type II error probabilities (equivalently P_f and P_d) as the network performance metrics.

4. SECURITY PERFORMANCE ANALYSIS

In this section, we analyze the security performance of the data fusion schemes in the presence of Byzantines. Next, we determine the minimum fraction of Byzantines needed to make the network blind (or α_{blind}) in data fusion based schemes.

Lemma 1. *For raw data fusion schemes, the minimum fraction of Byzantine nodes needed to blind the network or to make the deflection coefficient zero is given by*

$$\alpha_{blind} = \frac{1}{2} \frac{\sum_{i=1}^{N} (w_i \eta_i \sigma_i^2)}{\sum_{i=1}^{N} (w_i D_i)}.$$

Proof. For large enough M, the local test statistic Y_i is normally distributed with mean

$$mean_i = \begin{cases} M\sigma_i^2 & \text{if } H_0 \\ (M + \eta_i)\sigma_i^2 & \text{if } H_1 \end{cases}$$

and variance $Var_i = \begin{cases} 2M\sigma_i^4 & \text{if } H_0 \\ 2(M + \eta_i)\sigma_i^4 & \text{if } H_1 \end{cases}$

Conditional mean $\mu_k = \mathbb{E}[\Lambda|H_k]$ and conditional variance $\sigma_k^2 = \mathbb{E}[(\Lambda - \mu_k)^2|H_k]$ of the global test statistic, $\Lambda = \sum_{i=1}^{N} w_i \tilde{Y_i}$, are given by:

$$\mu_0 = \sum_{i=1}^{N} [\frac{\alpha w_i}{\sum_{i=1}^{N} w_i}(M\sigma_i^2 + D_i) + \frac{(1-\alpha)w_i}{\sum_{i=1}^{N} w_i}(M\sigma_i^2)] \quad (2)$$

$$\mu_1 = \sum_{i=1}^{N} [\alpha \frac{w_i}{\sum_{i=1}^{N} w_i}((M + \eta_i)\sigma_i^2 - D_i) + (1-\alpha)\frac{w_i}{\sum_{i=1}^{N} w_i}((M + \eta_i)\sigma_i^2)] \quad (3)$$

Byzantine nodes want to make the deflection coefficient as small as possible. Deflection coefficient is always non-negative; so they want to make $D(\Lambda) = \frac{(\mu_1 - \mu_0)^2}{\sigma_0^2} = 0$. After substituting values from (2) and (3), the condition to make $D(\Lambda) = 0$ becomes

$$\sum_{i=1}^{N} [\alpha w_i(\eta_i \sigma_i^2 - 2D_i) + (1-\alpha)w_i(\eta_i \sigma_i^2)] = 0 \quad (4)$$

After simplifying the above equation the condition to blind the FC becomes $\alpha_{blind} = \frac{1}{2}\frac{\sum_{i=1}^{N}(w_i\eta_i\sigma_i^2)}{\sum_{i=1}^{N}(w_iD_i)}$. □

Observe that, α_{blind} is a monotonically decreasing function of the attack strength D_i. In practice, the optimal value of the parameter D_i is dependent on the protection mechanism used by the FC.

5. DETECTION PERFORMANCE ANALYSIS

In this section, we analyze the detection performance of the data fusion schemes with Byzantines. In the presence of α fraction of Byzantines, the distribution of $\tilde{Y_i}$ given H_k can be approximated as a Gaussian mixture which comes from $\mathcal{N}((\mu_{1k})_i, (\sigma_{1k})_i^2)$ with probability $(1-\alpha)$ and from $\mathcal{N}((\mu_{2k})_i, (\sigma_{2k})_i^2)$ with probability α, where $\mathcal{N}$ denotes the normal distribution and

$$(\mu_{10})_i = M\sigma_i^2,\ (\mu_{20})_i = M\sigma_i^2 + D_i$$

$$(\mu_{11})_i = (M+\eta_i)\sigma_i^2,\ (\mu_{21})_i = (M+\eta_i)\sigma_i^2 - D_i$$

$$(\sigma_{10})_i^2 = (\sigma_{20})_i^2 = 2M\sigma_i^4,\ \textit{and}\ (\sigma_{11})_i^2 = (\sigma_{21})_i^2 = 2(M+\eta_i)\sigma_i^4$$

Similarly, the PDF of $X_i = w_i\tilde{Y_i}$ conditioned on H_k can be derived

$$\begin{aligned} f(x_i|H_k) &= (1-\alpha)\phi(w_i(\mu_{1k})_i, (w_i(\sigma_{1k})_i)^2) \\ &\quad + \alpha\phi(w_i(\mu_{2k})_i, (w_i(\sigma_{2k})_i)^2) \end{aligned} \quad (5)$$

where $\phi(x|\mu,\sigma^2)$ (for notational convenience denoted as $\phi(\mu,\sigma^2)$) is the PDF of $X \sim \mathcal{N}(\mu,\sigma^2)$ and $\phi(x|\mu,\sigma^2) = \frac{1}{\sigma\sqrt{2\pi}}e^{-(x-\mu)^2/2\sigma^2}$. Next, for clarity of exposition, we first derive our results for a two node network. Later we generalize our results for an arbitrary number of nodes, N.

Notice that, for the two node case, $\tilde{\Lambda} = w_1\tilde{Y_1} + w_2\tilde{Y_2}$, is a summation of independent random variables, $X_i = w_i\tilde{Y_i}$, with conditional PDF given in (5). Notice that, PDF of $(Z = X_1 + X_2)$ is the convolution $(*)$ of $f_{X_1}(x_1) = (1-\alpha)\phi(\mu_1^1, (\sigma_1^1)^2) + \alpha\phi(\mu_1^2, (\sigma_1^2)^2)$ and $f_{X_2}(x_2) = (1-\alpha)\phi(\mu_2^1, (\sigma_2^1)^2) + \alpha\phi(\mu_2^2, (\sigma_2^2)^2)$.

$$f_Z(z) = f_{X_1}(x_1) * f_{X_2}(x_2)$$

$$\begin{aligned} f_Z(z) &= [(1-\alpha)\phi(\mu_1^1, (\sigma_1^1)^2) + \alpha\phi(\mu_1^2, (\sigma_1^2)^2)] * \\ &\quad [(1-\alpha)\phi(\mu_2^1, (\sigma_2^1)^2) + \alpha\phi(\mu_2^2, (\sigma_2^2)^2)] \\ &= (1-\alpha)^2[\phi(\mu_1^1, (\sigma_1^1)^2) * \phi(\mu_2^1, (\sigma_2^1)^2)] \\ &\quad +(\alpha)^2[\phi(\mu_1^2, (\sigma_1^2)^2)) * \phi(\mu_2^2, (\sigma_2^2)^2))] \\ &\quad +\alpha(1-\alpha)[\phi(\mu_1^2, (\sigma_1^2)^2) * \phi(\mu_2^1, (\sigma_2^1)^2)] \\ &\quad +(1-\alpha)\alpha[\phi(\mu_1^1, (\sigma_1^1)^2) * \phi(\mu_2^2, (\sigma_2^2)^2)]. \end{aligned}$$

Now, using the fact that convolution of two Gaussian PDFs $\phi(\mu_1,\sigma_1^2)$ and $\phi(\mu_2,\sigma_2^2)$ is again normally distributed with mean $(\mu_1+\mu_2)$ and variance $(\sigma_1^2+\sigma_2^2)$, we can derive the results below.

$$\begin{aligned} f_Z(z) &= (1-\alpha)^2[\phi(\mu_1^1+\mu_2^1, (\sigma_1^1)^2 + (\sigma_2^1)^2)] \\ &\quad +(\alpha)^2[\phi(\mu_1^2+\mu_2^2, (\sigma_1^2)^2 + (\sigma_2^2)^2)] \\ &\quad +\alpha(1-\alpha)[\phi(\mu_1^2+\mu_2^1, (\sigma_1^2)^2 + (\sigma_2^1)^2)] \\ &\quad +(1-\alpha)\alpha[\phi(\mu_1^1+\mu_2^2, (\sigma_1^1)^2 + (\sigma_2^2)^2)]. \end{aligned}$$

Let I denote the set of all combinations of node strategies:

$$I = \{\{B_1, B_2\}, \{H_1, B_2\}, \{B_1, H_2\}, \{H_1, H_2\}\}$$

where by B_i we mean that node i is a Byzantine and by H_i we mean that node i is an honest node. Let $A_t \in J$ denote the indices of honest nodes in the strategy combination t.

$$J = \{A_1 = \{\phi\}, A_2 = \{1\}, A_3 = \{2\}, A_4 = \{1,2\}\}$$

$$J^c = \{A_1^c = \{1,2\}, A_2^c = \{2\}, A_3^c = \{1\}, A_4^c = \{\phi\}\}$$

We use $\{\phi\}$ to denote the null set and m to denote the cardinality of subset $A_t \in J$. Using these notations, we generalize our results for any arbitrary N.

Lemma 2. *The global test statistic $\tilde{\Lambda} = \sum_{i=1}^{N} w_i\tilde{Y_i}$ is a Gaussian mixture with PDF*

$$f(\tilde{\Lambda}|H_k) = \sum_{A_t\in J}(\alpha)^{N-m}(1-\alpha)^m\phi(\tilde{\Lambda}|(\mu_k)_{A_t}, \sum_{i=1}^{N}(w_i(\sigma_{1k})_i)^2))$$

$$\textit{with}\ (\mu_k)_{A_t} = \sum_{j\in A_t} w_j(\mu_{1k})_j + \sum_{j\in A_t^c} w_j(\mu_{2k})_j.$$

The performance of the detection scheme in the presence of Byzantines can be represented in terms of the probability of detection and the probability of false alarm of the network.

Proposition 1. *The probability of detection and the probability of false alarm of the network in the presence of Byzantines can be represented as*

$$P_d = \sum_{A_t\in J}(\alpha)^{N-m}(1-\alpha)^m Q\left(\frac{\lambda - (\mu_1)_{A_t}}{\sqrt{\sum_{i=1}^{N}(w_i(\sigma_{11})_i)^2)}}\right),$$

$$P_f = \sum_{A_t\in J}(\alpha)^{N-m}(1-\alpha)^m Q\left(\frac{\lambda - (\mu_0)_{A_t}}{\sqrt{\sum_{i=1}^{N}(w_i(\sigma_{10})_i)^2)}}\right).$$

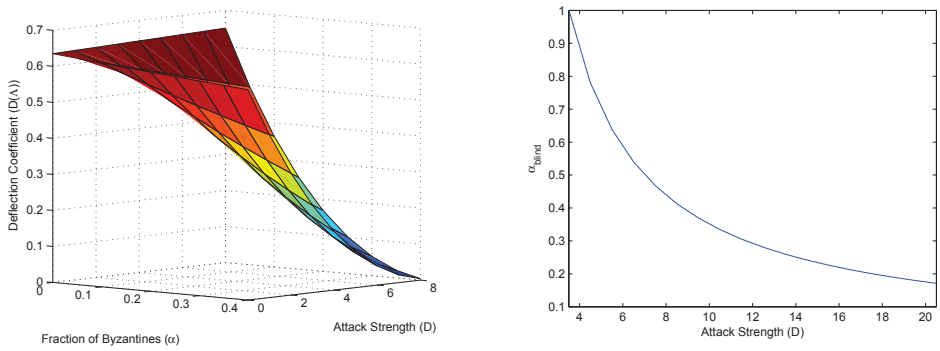
Remark 1. *Notice that, the expressions of probability of detection P_d and probability of false alarm P_f for the N-node case involves 2^N combinations (cardinality of J is 2^N). It, however, can be represented compactly by vectorizing the expressions,i.e.,*

$$P_d = \mathbf{1^T}\left(\mathbf{b}\otimes Q\left(\frac{\boldsymbol{\lambda} - \boldsymbol{\mu_1}}{\sqrt{\sum_{i=1}^{N}(w_i(\sigma_{10})_i)^2)}}\right)\right)$$

with $\boldsymbol{\mu_1} = A\boldsymbol{w\mu_{11}} + A^c\boldsymbol{w\mu_{21}}$, $B = (1-\alpha)A + \alpha A^c$ and $\mathbf{b} = [\mathbf{B^1}\otimes\cdots\otimes\mathbf{B^N}]$, where boldface letters represent vectors, $\otimes$ symbol represents element-wise multiplication, $Q(\cdot)$ represents element wise Q function operation, i.e., $Q(x_1,\cdots,x_N) = [Q(x_1),\cdots,Q(x_N)]^T$, $\mathbf{B^i}$ is i^{th} column of matrix B, $\boldsymbol{w\mu_{j1}} = [w_1\mu_{j1}^1,\cdots,w_N\mu_{j1}^N]^T$, matrix $A_{(2^N*N)}$ is the binary representation of decimal numbers from 0 to $N-1$ and A^c is the matrix after interchanging 1 and 0 in matrix A.

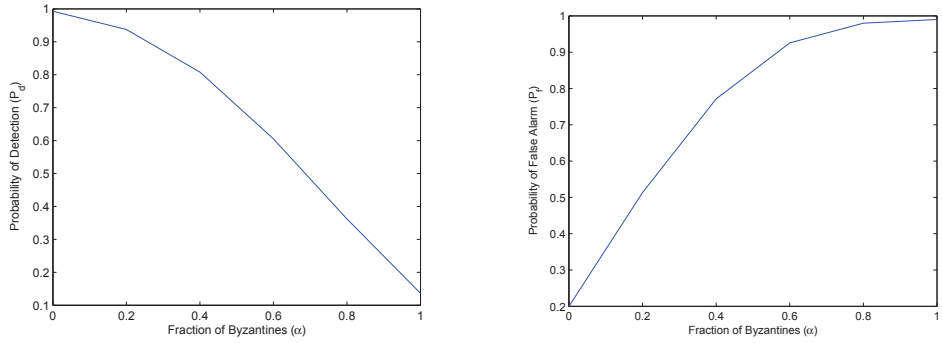
6. NUMERICAL RESULTS

In this section, we numerically evaluate the security and detection performance of the system in the presence of Byzantines. We consider a network of $N = 8$ nodes with channel gains $h = [0.8, 0.8, 0.7, 0.71, 0.72, 0.61, 0.69, 0.9]$. For simplicity, we assume that the nodes are detecting a known signal under AWGN with $s(k) = 1$ and noise variance $\sigma_i = 1, \forall i$. Each node i calculates a summary statistic Y_i based on $M = 12$ samples.



(a) (b)

Fig. 1. Security performance analysis. (a) Effect of Byzantines on Deflection Coefficient. (b) Effect of Attack Strength on α_{blind}.



(a) (b)

Fig. 2. Detection performance analysis. (a) Effect of Byzantines on Prob. of Detection. (b) Effect of Byzantines on Prob. of False Alarm.

6.1. Security Performance Evaluation

Figure 1(a) shows the effect of Byzantine attacks on the deflection coefficient for the data fusion scheme. We plot the deflection coefficient as a function of the fraction of Byzantines, α, and the attack strength, D_i, which is assumed to be the same for all the Byzantines, i.e., $D_i = D,\ \forall i$. We can see from the figure that only 40 percent Byzantines attacking with the attack strength $D = 8$ can blind the FC, which corroborates our theoretical result presented in Lemma 1. Another observation to make is that the deflection coefficient $D(\Lambda)$ decreases as D increases. This implies that the minimum fraction of Byzantines needed to make the deflection coefficient equal to zero is dependent on the attack strength.

In Figure 1(b), we plot α_{blind} as a function of the attack strength, D. It can be seen that the minimum fraction of Byzantines needed to make the deflection coefficient zero is a monotonically decreasing function of D. In other words, Byzantines can minimize α_{blind} to an arbitrary value by increasing D. Observe that, when $D < 3.5$, the Byzantines cannot make $D(\Lambda) = 0$. However, for $D \geq 3.5$, the value of α_{blind} decreases as D increases and at $D = 20.5$, α_{blind} is less than 0.2.

6.2. Detection Performance Evaluation

In this subsection, we evaluate the detection performance of the data fusion schemes in the presence of Byzantine attackers.

Figure 2(a) shows the effect of Byzantine attacks on the global probability of detection P_d for Data Fusion schemes. We use the threshold at the FC given in (1) such that $p = 0.2$ or constraining the probability of false alarm below 0.2. We assume that the attack strength, D_i, is the same for all the Byzantines, i.e., $D_i = 8,\ \forall i$. Notice that, as the fraction of Byzantines in the network increases, the global probability of detection P_d decreases.

In Figure 2(b), we plot the effect of Byzantine attacks on the global probability of false alarm P_f in Data Fusion schemes. We use the threshold at the FC given in (1) such that $p = 0.2$ or constraining the probability of missed detection below 0.2. We assume that the attack strength, D_i, is the same for all attackers, i.e., $D_i = 8,\ \forall i$. Notice that, as the number of Byzantines in the network increases, the global probability of false alarm P_f decreases.

As can be seen from both the figures (Figs. 1 and 2), as the number of Byzantines in the network increases, network wide detection performance degrades significantly. In the future, we plan to extend this work to the scenarios where both the FC and the Byzantine attacker act in a strategic manner to optimize their own utilities.

7. 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," *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] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 428–445, 2013.

[5] 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

[6] A. Vempaty, L. Tong, and P. Varshney, "Distributed inference with byzantine data: State-of-the-art review on data falsification attacks," *Signal Processing Magazine, IEEE*, vol. 30, no. 5, pp. 65–75, 2013.

[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, 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.

[10] 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.

[11] 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*, 2013, pp. 412–417.

[12] ——, "Distributed bayesian detection with byzantine data," *CoRR*, vol. abs/1307.3544, 2013.

[13] B. Kailkhura, S. Brahma, Y. S. Han, and P. K. Varshney, "Distributed detection in tree topologies with byzantines," *CoRR*, vol. abs/1309.4513, 2013.

[14] 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.

[15] 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.

[16] M. Barni and B. Tondi, "Multiple-observation hypothesis testing under adversarial conditions," in *IEEE International Workshop on Information Forensics and Security (WIFS)*, Nov 2013, pp. 91–96.

[17] A. Min, K. Shin, and X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," in *Network Protocols, 2009. ICNP 2009. 17th IEEE International Conference on*, Oct., pp. 294–303.

[18] N. Nguyen-Thanh and I. Koo, "An enhanced cooperative spectrum sensing scheme based on evidence theory and reliability source evaluation in cognitive radio context," *IEEE Commun. Lett.*, vol. 13, no. 7, pp. 492–494, 2009.

[19] F. Yu, H. Tang, M. Huang, Z. Li, and P. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *Military Communications Conference, 2009. MILCOM 2009. IEEE*, Oct., pp. 1–7.

[20] F. Zhu and S.-W. Seo, "Enhanced robust cooperative spectrum sensing in cognitive radio," *Communications and Networks, Journal of*, vol. 11, no. 2, pp. 122–133, 2009.

[21] Q. Yan, M. Li, T. Jiang, W. Lou, and Y. Hou, "Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks," in *INFOCOM, 2012 Proceedings IEEE*, March, pp. 900–908.

[22] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE*, vol. 55, no. 4, pp. 523–531, 1967.

[23] Z. Quan, S. Cui, and A. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 28–40, 2008.

[24] W. Zhang, Z. Wang, Y. Guo, H. Liu, Y. Chen, and J. Mitola, "Distributed cooperative spectrum sensing based on weighted average consensus," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, Dec., pp. 1–6.

[25] S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume 2: Detection Theory*. ser. Prentice Hall Signal Processing Series, A. V. Oppenheim, Ed. Prentice Hall PTR, 1998.