1-2-2012

On Noise-Enhanced Distributed Inference in the Presence of Byzantines

Mukul Gagrani
IIT-Kanpur, India

Pranay Sharma
IIT-Kanpur, India

Venkata Sriram Siddhardh Nadendla
Syracuse University, vnadendl@syr.edu

Aditya Vempaty
Syracuse University, avempaty@syr.edu

Pramod Varshney
Syracuse University, varshney@syr.edu

This is an author-produced, peer-reviewed version of this article. The published version of this document can be found online in the Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on (doi: 10.1109/Allerton.2011.6120307) published by *IEEE*.

On Noise-Enhanced Distributed Inference in the Presence of Byzantines

Mukul Gagrani Indian Institute of Technology
Pranay Sharma Indian Institute of Technology
Satish Iyengar Syracuse University
V. Sriram Siddhardh (Sid) Nadendla Syracuse University
Aditya Vempaty Syracuse University
Hao Chen Boise State University
Pramod K. Varshney Syracuse University

ABSTRACT

This paper considers the noise-enhanced distributed detection problem in the presence of Byzantine (malicious) nodes by suitably adding stochastic resonance (SR) noise. We consider two metrics - the minimum number of Byzantines (α_{blind}) needed to blind the fusion center as a security metric and the Kullback- Leibler divergence (D_{KL}) as a detection performance metric. We show that α_{blind} increases when SR noise is added at the honest nodes. When Byzantines also start adding SR noise to their observations, we see no gain in terms of α_{blind}. However, the detection performance of the network does improve with SR. We also consider a game theoretic formulation where this problem of distributed detection in the presence of Byzantines is modeled as a minimax game between the Byzantines and the inference network, and numerically find Nash equilibria. The case when SR noise is added to the signals received at the fusion center (FC) from the sensors is also considered. Our numerical results indicate that while there is no gain in terms of α_{blind}, the network-wide performance measured in terms of the deflection coefficient does improve in this case

I. INTRODUCTION

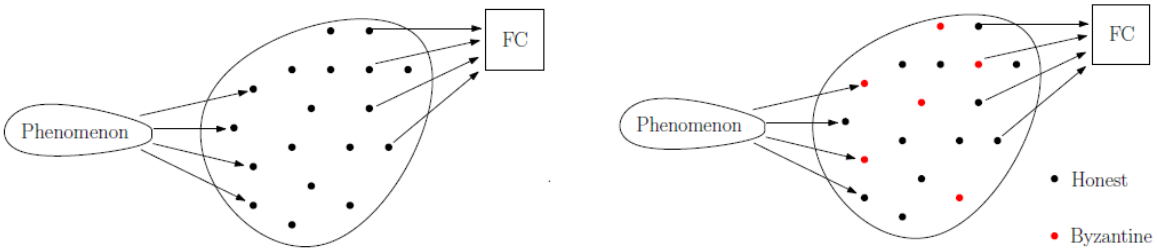
Inference networks have been widely investigated for the past three decades in order to detect or estimate a phenomenon of interest. Specifically, the distributed detection framework has been considered extensively, wherein several nodes sense the surrounding environment and collaboratively make a global inference at the fusion center (FC). It is only in the recent past that the researchers have investigated the problem of security threats in these networks. In this paper, we consider the problem of Data Falsification attacks (in other words, Byzantine attacks) in the context of distributed inference networks. Our primary focus is on designing a technique based on the stochastic resonance (SR) phenomenon to safeguard the network from Byzantine attacks.

SR is a physical phenomenon where the output signals of some nonlinear systems can be amplified by adding noise to the input. This counter-intuitive phenomenon was first observed by Benzi *et al.*, in [1], and, we have, in the past [2], explored and developed the theory of SR for statistical inference problems. For a single sensor detection problem formulated under the Neyman-Pearson (NP) framework, the optimal SR noise to be added to the observations at the input of the detector has a probability density function (pdf) consisting of two Kronecker delta functions each occurring with probability β and ($1-\beta$). For the Bayesian case, a single delta function with unit probability (i.e., a constant) is the optimal SR noise pdf. The formulation was also extended to a distributed detection framework in [3]. Here, we consider the case when some of the sensors deployed in a region of interest (ROI) deliberately report incorrect decisions to a remotely located fusion center, thus causing a reduction in the overall detection performance. Here, we show how one could use SR to counter such Byzantine attacks.

Byzantine attacks (Figure 1) are those attacks in which some of the sensors within the network send false information to the fusion center in order to disrupt the inference process. The Byzantines intend to deteriorate the detection performance of the network and therefore, modify their local decisions before transmitting to the fusion center. Marano *et al.* considered a distributed detection problem for an inference network in the presence of Byzantines in [4] and presented the optimal attacking distribution for the Byzantines under the error exponent framework. In finding the minimum fraction of Byzantines (α_{blind}) needed to make the two hypotheses indistinguishable to the FC, they assumed that the Byzantines have perfect knowledge about the true hypothesis.

Rawat *et al.* in [5] considered the case when Byzantines did not have the knowledge regarding hypothesis present, and gave a closed-form expression for α_{blind} under both independent and collaborative Byzantine attacks.

In the past, reputation-based schemes at the fusion center have been suggested to counter these attacks. Rawat *et al.* analysed a similar problem in [5], for the cases of independent attack by individual Byzantines as well as the collaborative attack case. They developed optimal attacking strategies, analyzed limits on the network performance under these attacks and proposed identify-and-eliminate strategies for the fusion center to counter these attacks. Note that this scheme works only when the percentage of Byzantines in the network is less than 50%. On the other hand, the adaptive learning scheme proposed by Vempaty *et al.* in [6] works for any fraction of Byzantines



(a) Honest Network (b) Network with Byzantine nodes

Fig. 1: Byzantine Threat on a Distributed Inference Network

in the network. They learnt the operating points of each and every node in the inference network not only to identify the Byzantines, but also to use the learnt Byzantine parameters in an adaptive fusion rule in order to improve the detection performance over Rawat *et al.*'s scheme [5].

We suggest the use of SR phenomenon to counter these attacks under more severe cases. We explore the optimal SR to be added, where it should be added and under what conditions, it provides improvement in security along with the performance gain, i.e., an increase in α_{blind} along with an improvement in a detection performance metric. We have also considered the attacks in the presence of different types of channels between the phenomenon of interest and the local sensors. We found analytical expressions to quantify the improvement in performance.

The remainder of the paper is organized as follows. Section II presents a general system model and performance metrics that are applicable to the different formulations of the noise-enhanced distributed inference problem, which are later presented in III. We present the two scenarios of SR being employed locally at the sensors and SR being applied at the FC. In Section IV, we present a game-theoretic formulation of the noise-enhanced distributed inference problem in the presence of Byzantines. Next, in Section V, we present numerical results for the different scenarios and formulations presented earlier. Finally, we conclude the work in Section VI with a few comments on our future work.

II. GENERALIZED SYSTEM MODEL

We consider a binary hypotheses testing problem involving hypotheses H_0 and H_1, with prior probabilities π_0 and π_1 respectively. Let the collaborative inference network comprise of N nodes, M of which are Byzantine (malicious) in nature, and a fusion center which makes a global decision based on the observations collected locally at the sensor nodes. The Byzantine nodes send false information to the fusion center in order to deteriorate the performance of the inference network. The inference network tries to employ SR noise as well as counterattack the Byzantines by changing its strategy of decision making in order to reduce the performance deterioration caused by Byzantines.

We denote the i.i.d. observations made at the i^{th} sensor as X_i, and the distribution of X_i conditioned on the hypothesis H_k as $(X_i|H_k), k = 0, 1$. In particular, we consider the signal model $X_i = \theta + n_i$, where θ = 0 under H_0, θ = A under H_1 and $n_i \sim p_n(\cdot)$ for simplicity.

Due to the presence of a suboptimal quantizer at the local sensors, under Scenario-1 (In Scenario-2, SR noise will be added at the FC), SR noise w_i is added to the observations in order to improve the detection performance. Hence, the updated observation at the i^{th} sensor is given by

$$Y_i = X_i + w_i \qquad \forall i = 1, \cdots, N. \tag{1}$$

Here, we denote the pdf of the SR noise w_i added at the honest node as $p_w^H(w)$ and that of the Byzantine node as $p_w^B(w)$. Let z_i, $\forall i = 1, \cdots, N$ be defined as

$$z_i = n_i + w_i \tag{2}$$

Then pdf of z_i can be written as

$$p_z^{<T>}(t) = p_n(t) * p_w^{<T>}(t); \tag{3}$$

where $p_n(t)$is the noise pdf in the channel between the phenomenon and the sensor and $p_w^{<T>}(t)$is the pdf of SR at the sensor of type T (Honest/Byzantine).

We restrict our discussion to a hard quantizer at the local sensors and therefore, if the suboptimal quantization function is given by $\gamma_{<T>}(.)$for a node of type $T\ (T = H/B)$, the operating point of the honest and the Byzantine nodes in the ROC is given by (P_{fa}^H, P_d^H) and (P_{fa}^B, P_d^B)respectively. Note that, in this paper, we focus our discussion on the use of sign detector as the suboptimal quantizer at the local decision-making stage. These operating points can be expressed as follows, for a sign detector employed in the sensor of type T.

$$\begin{aligned} P_d^{<T>} &= P(Y_i \geq 0|H_1) = P(z_i^{<T>} \geq -A) \\ &= \int_{-A}^{\infty} p_n(t) * p_w^{<T>}(t)\, \mathrm{d}t \end{aligned} \tag{4a}$$

$$\begin{aligned} P_{fa}^{<T>} &= P(Y_i \geq 0|H_0) = P(z_i^{<T>} \geq 0) \\ &= \int_{0}^{\infty} p_n(t) * p_w^{<T>}(t)\, \mathrm{d}t \end{aligned} \tag{4b}$$

If α is the probability with which a node is Byzantine, then the effective operating point of any given node, as observed by the FC, is given by

$$\begin{aligned} P_{fa} &= \alpha(1 - P_{fa}^B) + (1 - \alpha)P_{fa}^H \\ P_d &= \alpha(1 - P_d^B) + (1 - \alpha)P_d^H \end{aligned} \tag{5}$$

Note that, empirically, α can be expressed as the fraction ($\frac{M}{N}$) of Byzantine nodes in the inference network. We assume that the fusion center has knowledge about the fraction of Byzantines, $\alpha = \frac{M}{N}$ in the network, but cannot differentiate between the honest and Byzantine sensors (same as Rawat *et al.* in [5]).

Assuming that the channels between the sensors and the FC are ideal, if $\{u_1, \cdots, u_N\}$denote the set of transmitted messages by the sensors to the FC, then a global decision $u_0 \in \{H_0, H_1\}$ is made by fusing these individual local decisions as follows.

$$u_0 = \gamma_0(u_1, \cdots, u_N) \tag{6}$$

A. Performance metrics

In this paper, we consider Kullback Leibler Divergence as the detection performance metric and α_{blind}as the security performance metric, which are described as follows.

Kullback-Leibler Divergence: D_{KL} has been used as a performance metric for distributed detection systems. It is a measure of the distance between two probability distributions. Here, the two distributions are in the presence of the two hypotheses H_0 and H_1, i.e., $P(u_i|H_0)$ and $P(u_i|H_1)$respectively. As pointed out by Rawat *et al.* in [5], the Byzantines would try to maximize the damage they can cause to the sensing process. This can be done by reducing D_{KL} which results in more decision errors.

$$
\begin{aligned}
D_{KL} &= \frac{1}{N} \cdot \mathbb{E}\left(\log \frac{p(u|H_1)}{p(u|H_0)}\right) \\
&= D(P(u_i|H_1)||P(u_i|H_0)) \\
&= \sum_{j\in\{0,1\}} P(u_i|H_1) \log\left(\frac{P(u_i|H_1)}{P(u_i|H_0)}\right)
\end{aligned} \tag{7}
$$

Blinding fraction of Byzantines: α_{blind} is the minimum fraction of Byzantines needed to degrade the performance of the network (D_{KL} = 0) to the maximum possible extent so that the network is totally *blind* of the phenomenon of interest. Similar to Rawat *et al.*, in [5], this serves as a security metric that defines the level of security, a given system is offering. This can be expressed as follows.

$$
\begin{aligned}
\alpha_{blind} &= \frac{{P_d}^H - {P_{fa}}^H}{[{P_d}^H - {P_{fa}}^H] + [{P_d}^B - {P_{fa}}^B]} \\
&= \frac{\int_{-A}^{0} p_n(t) * p_w^H(t)\, \mathrm{d}t}{\int_{-A}^{0} p_n(t) * \left[p_w^H(t) + p_w^B(t)\right]\, \mathrm{d}t}
\end{aligned} \tag{8}
$$

III. NOISE-ENHANCED DISTRIBUTED INFERENCE IN THEPRESENCE OF BYZANTINES

In this section, we analyze the effect of stochastic resonance on the network performance in the presence of Byzantine attack. Chen *et al.*, in [7], have shown that, for sub-optimal and non-linear systems, SR can be used to improve the detection performance under a constraint on the false alarm rate. Hence, in this paper, we employ SR locally at the sensors in Section III-A and do the same at the FC in Section III-B and analyze the gain in the detection performance.

A. SR employed at the local sensors

We present our results in two different cases. First, we present an ideal case where SR is employed only at the honest nodes, demonstrating the potential of SR effect in terms of the gain in security. Next, we show the most general case when SR is applied at both honest and Byzantine nodes.

1) CASE-1 (SR employed only at the Honest Nodes): Here, we investigate the most favorable case to the network, wherein SR is added only at the honest local sensors and the Byzantines flip their decisions deterministically. One can achieve this system in practice if there is an underlying scheme as proposed by [5] or [6] in the network, which lets the FC identify the Byzantine nodes. The nodes which are tagged *honest*, are later informed to employ SR through some feedback mechanism, while the nodes that are tagged *Byzantine* are left ignorant. Presently, we do not consider the uncertainty involved in the tagging process. This is an important problem which will be addressed in our future work.

We start off with the following lemma where we analyze the behavior of α_{blind} and find the optimal SR pdf that maximizes α_{blind} from honest sensors' perspective.

Lemma 1. *To maximize* α_{blind}, the *optimum SR noise at the honest nodes can be expressed as*

$$
p_{w,opt}^H(t) = \delta(t - t_0)
$$

i.e. 1-peak SR is optimum for obtaining the maximum α_{blind}

Proof: Define $x = P_d^H - P_{fa}^H$ and $a = P_d^B - P_{fa}^B$, for a given P_d^B and P_{fa}^B, *a* is a constant and also *a* > 0. Therefore,

$$\alpha_{blind} = \frac{x}{x+a}$$

$$\frac{d(\alpha_{blind})}{dx} = \frac{a}{(x+a)^2}.$$

Thus, $\alpha_{blind}$is a monotonically increasing function w.r.t x. Therefore, in order to maximize α_{blind}, we must maximize x. This is very similar to the problem of finding the optimal SR noise pdf for Byzantine detection (minimizing P_e), as described in [8], and hence x is maximized by a 1-peak SR. In other words, 1-peak noise is the optimal SR signal that maximizes α_{blind}.

In this case, the network performance improves because the honest nodes' performance is improved, while the Byzantines' performance remains the same. Therefore, we expect an increase in α_{blind}, thereby improving the robustness of the network. We show this phenomenon in the following two examples.

a) Example-1 (Gaussian mixture noise): The channel noise between the primary transmitter and the local sensors is symmetric, Gaussian mixture with pdf,

$$p(x) = \frac{1}{2}\gamma(x; -\mu, \sigma_0^2) + \frac{1}{2}\gamma(x; \mu, \sigma_0^2) \qquad (9)$$

where, $\gamma(x;\mu,\sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}}\exp[-\frac{(x-\mu)^2}{2\sigma^2}]$. Here, we set $\mu = 3$, $A = 1$ and $\sigma_0 = 1$. The distribution of x under H_0 and H_1 hypotheses are,

$$p_0(x) = \frac{1}{2}\gamma(x; -\mu, \sigma_0^2) + \frac{1}{2}\gamma(x; \mu, \sigma_0^2) \qquad (10)$$

and

$$p_1(x) = \frac{1}{2}\gamma(x; -\mu + A, \sigma_0^2) + \frac{1}{2}\gamma(x; \mu + A, \sigma_0^2) \qquad (11)$$

respectively.

If we add 1-peak SR $(p_w^H(t) = \delta(t - c_0))$only at the honest nodes, we can obtain α_{blind} as given in Equation (12).

b) Example 2 (Cauchy Noise): The pdf for cauchy noise is given by

$$p_n(t) = \frac{\lambda}{\lambda + (t-\mu)^2} \qquad (13)$$

We now compute the optimum 1-peak SR for this channel. Following the discussion of [8], the optimal 1-peak SR should satisfy the following equation

$$p_0^X(-c) = p_0^X(-c - A) \qquad (14)$$

$$\text{where } p_o^X(t) = p_n(t) \text{ and } p_w(t) = \delta(t - c) \qquad (15)$$

On solving the above equation, we get

$$c_{opt} = -\mu - \frac{A}{2} \qquad (16)$$

For the case when 1-peak SR is added at the honest nodes only, the α_{blind} expression after substituting (13) is given in Equation (17).

It is easy to see that both the expressions in Equations (12) and (17) are greater than or equal to 0.5.

2) CASE-2 (SR at honest and Byzantine nodes): Both Byzantine and honest sensors apply SR noise to their true observations in order to improve their respective performances. But the Byzantines' choice of the SR signal is the one which reduces the performance of the network to the maximum possible extent, while that of the honest

sensors is to improve the performance of the network. It is easy to see that the optimal SR noise pdf from the Byzantine's perspective is also a one-peak pdf.

When both honest and the Byzantine nodes use the optimal SR to improve their performance, then α_{blind} again turns out to be 0.5, as in the case of *no-SR*. This can be explained from Equation (8) as both the optimal pdfs for SR at the honest and the Byzantine nodes are the same. Intuitively, this can be explained by the fact that the optimal strategy for the Byzantine nodes is to employ the same strategy as that of the honest nodes which employ optimal strategies to improve the performance of the network. The deterministic flipping of data at the Byzantine nodes results in the maximum degradation in the performance of the network.

In the case when the honest nodes have a majority in the network, then one can immediately perceive an improvement in the global detection performance. This is later justified in our numerical results presented in Section V.

B. SR employed at the FC

Next, we consider the addition of SR noise at the fusion center. We assume a Rayleigh fading model to account for the non-ideal transmissions between the local sensors and the fusion center. This model for sensor-to-fusion center channels has been analyzed in the past (See [9]–[11]). In [10], an optimal likelihood ratio (LR)-based fusion was derived assuming full knowledge of the instantaneous channel state information (CSI) and local sensor detection performance indices. In [11], the likelihood ratio based on channel statistics (LRT-CS) was derived and shown to perform well as compared to the optimal LR fusion rule. The test eliminates the need for instantaneous CSI, but still requires knowledge of the channel statistics as well as the performance indices of the local sensors. The fusion rule that requires the least information is the equal gain combiner (EGC) given below.

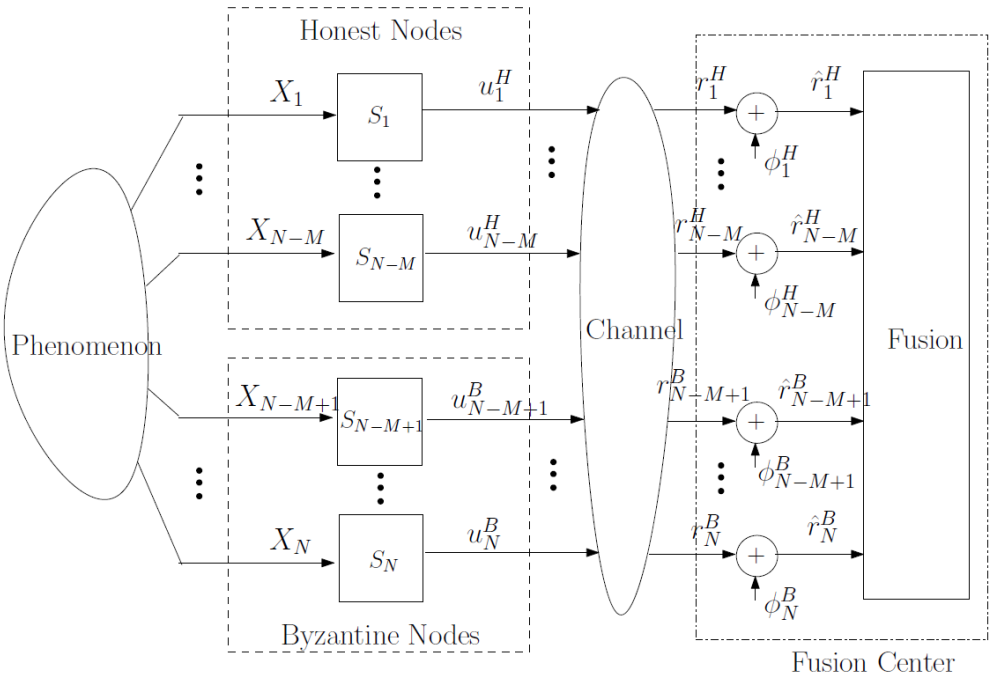


Fig. 2: Inference network model when SR is employed at the FC

$$\Lambda(\hat{\mathbf{r}}) = \frac{1}{N}\sum_{k=1}^{N} \hat{r}_k. \qquad (18)$$

where $\hat{r}_k$ is the signal received from the k^{th} node after the SR noise is added (Refer to Figure 2). It has been shown that the EGC based fusion rule, although suboptimal, performs

$$\alpha_{blind} = \frac{Q\left(\frac{\mu+c_0}{\sigma}\right) - Q\left(\frac{A+\mu+c_0}{\sigma}\right) + Q\left(\frac{-\mu+c_0}{\sigma}\right) - Q\left(\frac{A-\mu+c_0}{\sigma}\right)}{Q\left(\frac{\mu+c_0}{\sigma}\right) - Q\left(\frac{A+\mu+c_0}{\sigma}\right) + Q\left(\frac{-\mu+c_0}{\sigma}\right) - Q\left(\frac{A-\mu+c_0}{\sigma}\right) + Q\left(\frac{\mu}{\sigma}\right) - Q\left(\frac{A+\mu}{\sigma}\right) + Q\left(\frac{-\mu}{\sigma}\right) - Q\left(\frac{A-\mu}{\sigma}\right)} \tag{12}$$

$$\alpha_{blind} = \frac{\tan^{-1}\left(\frac{A+\mu+c_0}{\lambda}\right) - \tan^{-1}\left(\frac{\mu+c_0}{\lambda}\right)}{\tan^{-1}\left(\frac{A+\mu+c_0}{\lambda}\right) - \tan^{-1}\left(\frac{\mu+c_0}{\lambda}\right) + \tan^{-1}\left(\frac{A+\mu}{\lambda}\right) - \tan^{-1}\left(\frac{\mu}{\lambda}\right)} \tag{17}$$

reasonably well for most practical SNR values [10]. We, therefore, consider the EGC based fusion rule in this work, and investigate if its performance can be enhanced using SR in the presence of Byzantines. We use the deflection coefficient [12],

$$D(\Lambda) = \frac{\left(\mathbb{E}(\Lambda|H_1) - \mathbb{E}(\Lambda|H_0)\right)^2}{\mathrm{Var}(\Lambda|H_0)} \tag{19}$$

as a performance criterion due to its simplicity and its strong relationship with the actual overall detection performance [13].

IV. GAME-THEORETIC MODEL FOR DISTRIBUTED INFERENCE IN THE PRESENCE OF BYZANTINE NODES

In this section, we will analyse the problem of Byzantine attacks on the network in the presence of SR at the local sensors from a game theoretic perspective. Byzantines and the network are the two players of the game. The aim of the Byzantines is to deteriorate the performance of the network while the network's goal is to survive the Byzantine attack and improve the performance to maximum possible extent.

We formulate a zero-sum game between the Byzantine nodes and the inference network as a two-player zero-sum minimax game between the Byzantine nodes and the network with the utility function as the KL divergence. The set of strategies for the Byzantine node is defined by the p.d.f. of the SR noise, $p_w^H(t)$employed at the Byzantine nodes, while that of the honest nodes is defined by $p_w^H(t)$. Hence, the problem statement is given as follows.

Problem Statement. *Find* $\{p_w^H(w), p_w^B(w)\}$*such that*

$$\begin{aligned} &\min_{p_w^B(w)} \max_{p_w^H(w)} \hat{D}_{KL} = \max_{p_w^H(w)} \min_{p_w^B(w)} \hat{D}_{KL} \\ s.t. \quad &1.\ \int p_w^H(t)dt = 1 \\ &2.\ \int p_w^B(t)dt = 1 \end{aligned} \tag{20}$$

where $\hat{D}_{KL} = D_{KL}$, whenever $P_{fa} \leq P_d$. Otherwise, $\hat{D}_{KL} = -D_{KL}$. This is necessary in order to take into account the performance domination of Byzantines in the game, which the traditional D_{KL} does not provide us due to its non-negativity and symmetry about $P_{fa} = P_d$.

In this paper, we consider an example where $n_i \sim p(x)$ (as given in Equation (9)) is a Gaussian mixture noise with two peaks. Due to the concavity of the log (·) function, one can easily show that the optimal SR noise is again a one-peak SR noise. This is because the optimal strategy in the case of a quasiconcave or a quasiconvex payoff function results in an atomic distribution for the mixed strategy [14]. Therefore, $p_w^H(t) = \delta(t - c_H)$ and $p_w^B(t) = \delta(t - c_B)$.

V. NUMERICAL RESULTS

In this section, we present our numerical results for a network of N = 100 sensors. We consider two different cases to apply SR in the distributed inference network - one is the case when we apply SR only to the observations at the local sensors and the other being the case when SR is employed at the FC. We present these two scenarios in the following subsections.

Note that in order to analyze this system, we consider the following three types of SR noises.

- Optimal 1-peak SR

$$p_w(t) = \delta(t + 3.5) \qquad (21)$$

Note: The optimal 1-peak SR which should be added for this case can be obtained from the discussion of [8].

- Optimal 2-peak SR

$$p_w(t) = \beta\delta(t + 3.5) + (1 - \beta)\delta(t - 2.5) \qquad (22)$$

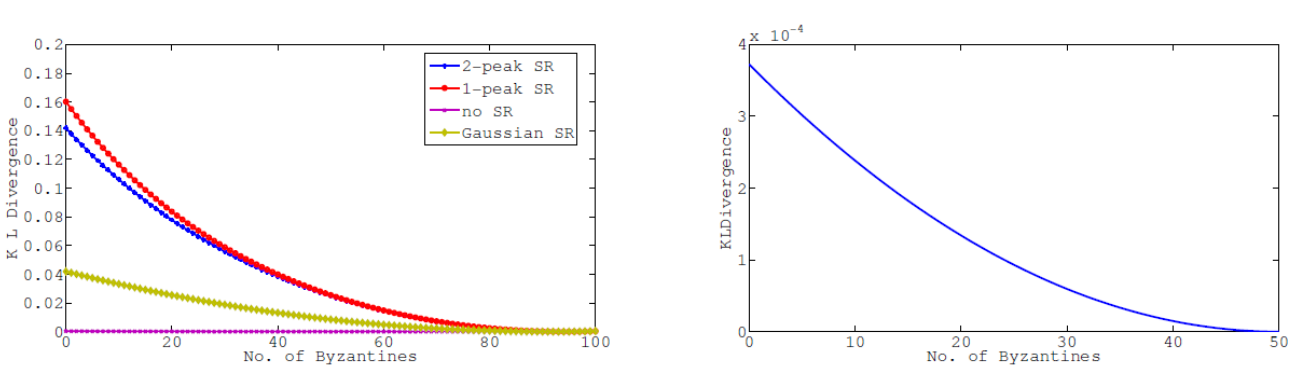
where β = 0.3085

- Optimal Gaussian SR noise

A. Scenario 1: SR applied locally at the nodes

As discussed earlier in Section III, we first present our results for the case when honest nodes alone employ SR, and later present the case when both honest and Byzantine nodes employ SR locally.

CASE-1 (SR employed at the honest nodes alone): First, we assume that all the sensors are identical (i.e., in the absence of SR, all the sensors have the same values of P_D and P_{FA}) and that only the honest sensors add SR. The Byzantines are attacking independently without any collaboration amongst themselves by simply flipping their decisions before sending them to the fusion center.



(a) For no-SR and for 3 different kinds of SR

(b) Only the no SR case

Fig. 3: D_{KL} vs. No. of Byzantines when only honest sensors add SR

Figure 3 shows the performance enhancement obtained by adding SR to honest nodes only. Figure 3a depicts the change in D_{KL} with the no. of Byzantines in the network for the *no- SR* as well as with-SR case. Since the *no-SR* curve is barely visible, it is shown in an expanded view in Figure 3b. Clearly, all the curves follow a similar trajectory with the difference being their magnitudes and the values on the x-axis at which the D_{KL} decays to zero (which correspond to α_{blind} for the different cases - the minimum fraction of Byzantines required to make the fusion center *blind*).

The no SR curve drops to zero when 50% of the sensors are Byzantines (α_{blind}= 0.5), since at this point, both the honest and Byzantine sensors become equally strong. The Gaussian SR noise provides some improvement compared to the *no- SR* case in terms of both relative magnitudes and α_{blind}. The optimal 2-peak SR noise gives further improvement and the performance is maximized by the 1-peak SR noise. As pointed out earlier, the 1-peak SR is the optimal noise to be added. Table I shows the values of α_{blind} for all the cases. We have compared the results obtained from the simulations with our analytical results and both are in close agreement.

SR added	α_{blind} (simulated)	α_{blind} (analytical)
Optimal 1-peak	0.94	0.944
Optimal 2-peak	0.94	0.944
Gaussian	0.91	0.9127
No SR	0.5	0.5

TABLE I: α_{blind} for different types of SR added

Next, we consider the case when the network is heterogeneous. To examine the robustness of the system, we look at the case if the Byzantines have better performance compared to the honest sensors, particularly when the probability of detection (P_D^B) is higher compared to the honest sensors for the same value of probability of false alarm $(P_{fa}^H = P_{fa}^B)$.

Fig. 4 shows the D_{KL} vs. No. of Byzantines plot for this scenario. Optimal 1-peak SR noise is added at the honest local sensors. For the same values of P_{FA}, we plot three curves for three different increasing values of P_D^B. One can see that as the Byzantines become stronger, the network performance deteriorates since D_{KL} drops to zero more rapidly with increasing P_D^B.

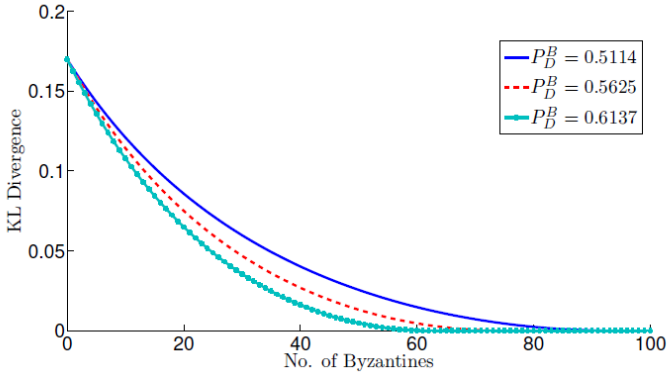


Table II shows the decay in the network performance as P_D increases in the form of decreasing values of α_{blind}.

Byzantine P_Ds	α_{blind} (simulated)	α_{blind} (analytical)
P_{D1} = 0.5114	0.94	0.944
P_{D2} = 0.5625	0.75	0.7531
P_{D3} = 0.6137	0.62	0.6265

TABLE II: α_{blind} for increasing values of P_D

Finally, we present our results for the two examples considered earlier - Gaussian mixture noise and the Cauchy noise. We present the results for the Cauchy noise case alone in Figure 5, while Table III shows the performance comparison in terms of α_{blind} of both the noisy channels.

Figure 5 shows the plot of KL divergence against the number of Byzantines in the network when $\mu = 1$ and $\lambda = 1$. Again, the significant improvement in the network performance after adding SR as compared to the *no-SR* case is articulated through our results.

CASE-2 (SR employed at both honest and Byzantine nodes): We present this case for three different types of SR signals. Fig. 6 shows the D_{KL} vs. No. of Byzantines curve. The curves

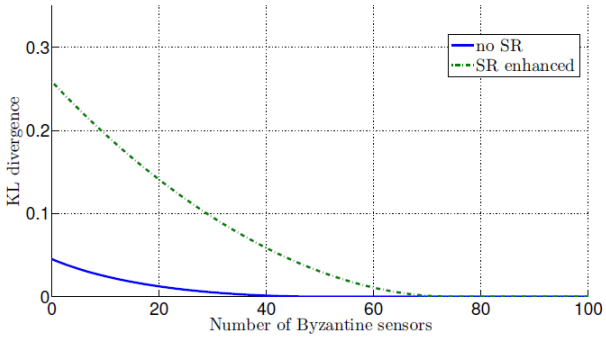


Fig. 5: D_{KL} vs. No. of Byzantines curve when SR employed at honest nodes alone for the Cauchy channel

	analytical	simulation
Gaussian mixture noise channel	0.944	0.94
Cauchy channel	0.742	0.75

TABLE III: α_{blind} comparison between analytical and simulation results

start from the same point on the y-axis as in the SR-only-at-honest sensors case. However, all the three curves decay quite rapidly and reach zero when 50% of the sensor population becomes Byzantines. This happens in the same way as we had in the no SR case where D_{KL} dropped to zero when Byzantines became as strong as the honest sensors. So, the result is intuitively correct. For all the three cases, we get α_{blind} = 0.5.

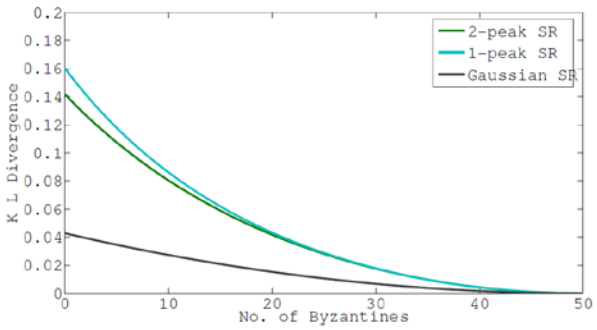


Fig. 6: D_{KL} vs. No. of Byzantines. SR is added at all the sensors, both honest and Byzantines

Although this case did not provide the necessary robustness in terms of security, later in the paper, we will analyze the problem from a game-theoretic perspective in order to find the optimal strategies employed by the Byzantine nodes and the inference network.

B. Scenario 2: SR applied at the FC

In this scenario, we consider a simple example where a one-peak noise is applied at the FC. We simulate the example scenario for about 100,000 Monte-Carlo runs and calculate the deflection coefficient as given by Equation (19). Figure 7 shows how the deflection coefficient varies with increasing number of Byzantines in the network. It is evident from the figure that SR provides detection performance improvement, but since the deflection coefficient becomes zero when $\alpha = \alpha_{blind}$ = 0.5, there is no improvement in the design from a security perspective. This can be attributed to the fact that SR is employed at both the Byzantine and the honest sensors. In the future, we will investigate the case where SR is applied to the honest nodes' receptions alone at the FC.

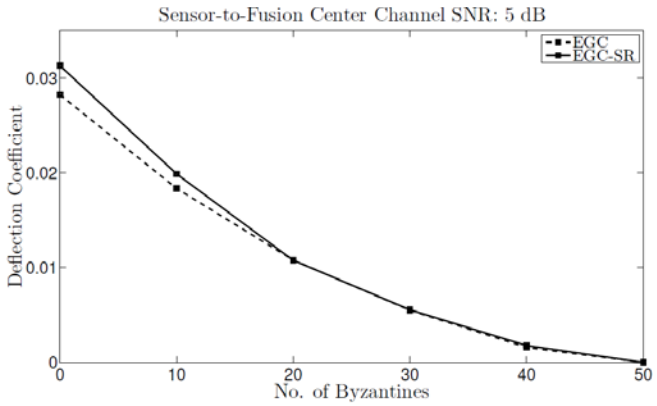


Fig. 7: Deflection Coefficient as a function of the number of Byzantines when SR is employed at the Rayleigh-faded FC's receptions.

C. Game-Theoretic Formulation of Inference in the presence of SR and Byzantine attacks

In this paper, we present results only for the example in which $p_0, p_1 = 0.5$, $\mu_1 = -3$, $\mu_2 = 3$, and $\sigma_1^2 = \sigma_2^2 = 1$ and as discussed earlier, the SR noise w_i is a one-peak noise with p.d.f. given by $\delta(t - c_{<T>})$ for a node of type *T* (Example considered by Chen *et al.*, in [7]). Here, *T* = *H/B*, where *H* stands for Honest and *B* stands for Byzantine. Note that we focus on finding those saddle points that minimize $\hat{D}_{KL}$ with respect to c_B, while maximize the same with respect to c_H. Figure 8 depicts how the contours of $\hat{D}_{KL}$ vary with the SR noise parameters c_H and c_B respectively, when α = 0.5. In this case, we find that when $c_H = c_B = 0$ (the case when no SR is applied at either the honest or the Byzantine node), the network is blinded since $\hat{D}_{KL} = 0$. One can clearly observe that, for a given SR signal at the honest node, a deviation in c_B from zero results in a performance degradation and vice versa. Also, note that the Nash equilibria are the points (-3.5, -3.5), (-3.5, 2.5), (2.5, -3.5) and (2.5, 2.5). These are very similar to the optimal SR signals computed by Chen *et al.*, in [7] when SR is not applied locally at the sensors. Due to symmetry in the example considered in Figure 8, all the equilibria correspond to $\hat{D}_{KL} = 0$.

Figure 9 plots the contours of $\hat{D}_{KL}$ against c_H and c_B, when α = 0.2. Note that the equilibria points are very close to those in the case of α = 0.5 case (with a slight skew), but the detection performance at the equilibria in terms of $\hat{D}_{KL}$ improved with decreasing α.

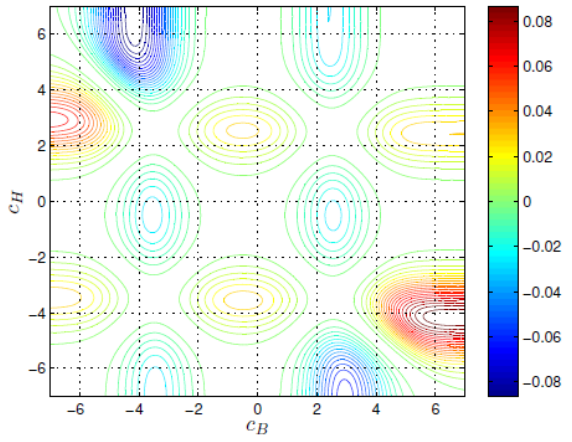


Fig. 8: Contour plots of $\hat{D}_{KL}$ as a function of c_H and c_B in the presence of Gaussian mixture noise for $\alpha = 0.5$.

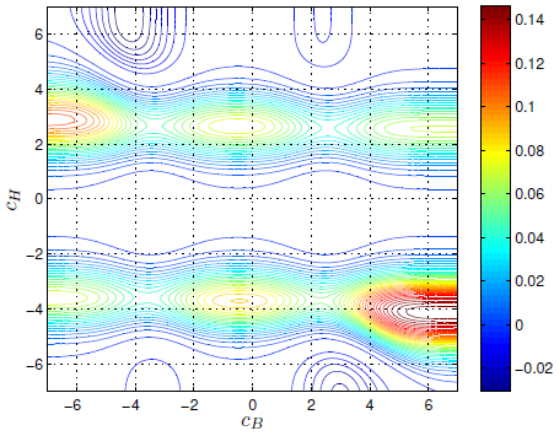


Fig. 9: Contour plots of $\hat{D}_{KL}$ as a function of c_H and c_B ir the presence of Gaussian mixture noise when $\alpha = 0.2$.

VI. CONCLUSION AND FUTURE WORK

In this paper, we have shown that SR phenomenon provides robustness to the designs along with the performance improvement, especially when the scenario is favorable to the inference network. If the Byzantines simply attack by flipping their decisions and not employ SR noise in their designs, then the α_{blind} increased beyond 50%, providing us with better security. In the case when Byzantines are equally powerful with SR being employed in the designs, then the robustness is not different from the *no-SR* case, but we found a performance improvement in terms of detection if the honest nodes form the majority. We also found that the p.d.f. of the optimal SR noise in the presence of Byzantine attackers is the same as that of the results given by Chen *et al.*, in [7], when there are no Byzantines in the network.

Future work will involve the case when SR is employed at both local sensors and the FC. Also, we will investigate other channel-aware fusion strategies. Another important problem that we will look at is the problem of SR at honest nodes when the Byzantine-identification scheme is *not* error-free. It will also be interesting to investigate the different game-theoretic formulations, such as the case where SR is employed at FC and Bayesian game models are considered with incomplete information.

REFERENCES

[1] R. Benzi, A. Sutera, and A. Vulpiani, "The mechanism of stochastic resonance," *Journal of Physics A: Mathematical and General*, vol. 14, p. L453.L457, 1981.

[2] H. Chen, "Noise enhanced signal detection and estimation," Ph.D. dissertation, Syracuse University, 2007.

[3] B. Liu, S. Iyengar, H. Chen, J. H. Michels, and P. K. Varshney, "Sensor fusion enhancement via optimized stochastic resonance at local sensors," in *Proc. 10th Int Information Fusion Conf*, 2007, pp. 1–5.

[4] 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, 2009.

[5] A. S. Rawat, P. Anand, H. Chen, and P. K. 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, 2011.

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

[7] H. Chen, P. K. Varshney, S. M. Kay, and J. H. Michels, "Theory of the stochastic resonance effect in signal detection - part 1: Fixed detectors," *IEEE Trans. Signal Process.*, vol. 55, no. 7, pp. 3172–3184, 2007.

[8] S. Kay, J. H. Michels, H. Chen, and P. K. Varshney, "Reducing probability of decision error using stochastic resonance," *IEEE Signal Process. Lett.*, vol. 13, no. 11, pp. 695–698, 2006.

[9] S. Thomopoulos and L. Zhang, "Distributed decision fusion with networking delays and channel errors," *Information Science*, vol. 66, pp. 91–118, December 1992.

[10] B. Chen, R. Jiang, T. Kasetkasem, and P. K. Varshney, "Channel aware decision fusion in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 52, no. 12, pp. 3454–3458, 2004.

[11] R. Niu, B. Chen, and P. K. Varshney, "Fusion of decisions transmitted over rayleigh fading channels in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 54, no. 3, pp. 1018–1027, 2006.

[12] S. Kay, *Fundamentals of Statistical Signal Processing, Volume II: Detection Theory*. Prentice Hall, 1993.

[13] B. Picinbono, "On deflection as a performance criterion in detection," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 31, no. 3, pp. 1072–1081, 1995.

[14] D. Fudenberg and J. Tirole, *Game Theory*. The MIT Press, 1991