LLNL-CONF-734905

BYZANTINE-RESILIENT COLLABORATIVE AUTONOMOUS DETECTION

B. Kailkhura, P. Ray, D. Rajan, A. Yen, P. Barnes, R. Goldhahn

July 17, 2017

2017 IEEE International Workshop on Computational
Advances in Multi-Sensor Adaptive Processing
Curaçao, Netherlands
December 10, 2017 through December 13, 2017

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

BYZANTINE-RESILIENT COLLABORATIVE AUTONOMOUS DETECTION

Bhavya Kailkhura, Priyadip Ray, Deepak Rajan, Anton Yen, Peter Barnes, Ryan Goldhahn

Lawrence Livermore National Laboratory

ABSTRACT

Autonomous sensor networks are increasingly being used for detection, classification and tracking applications. Therefore, we need algorithms which optimally combine the data collected at different sensors to produce a global decision without any centralized supervision. Three of the biggest challenges for collaborative autonomous detection are, 1) conventional detection statistics are difficult to implement as they are often nonlinear functions of the observed data, 2) algorithmic overhead increases as the network grows larger, and 3) autonomous sensor networks are very susceptible to adversarial attacks such as data falsification (Byzantine) attacks. In this paper, we propose a new simple-to-implement locally optimum detection algorithm, and present a decentralized implementation using alternating direction method of multipliers (ADMM). We implement our proposed algorithms for the problem of autonomous sensor networks detecting an unknown radioactive source buried in background noise. Results show that algorithm performance approaches the centralized clairvoyant detection algorithm in the low SNR regime, and exhibits excellent convergence rate and scaling behavior (w.r.t. number of nodes). We also derive a low-overhead, robust ADMM algorithm for Byzantine-resilient detection, and demonstrate its robustness to data falsification attacks.

Index Terms— locally optimum detection, data falsification, Byzantines, autonomous networks, ADMM

1. INTRODUCTION

Autonomous vehicles provide sensing platforms which are small, low cost, and maneuverable. Because of size, weight and power restrictions, the sensors onboard are of limited performance. Signal processing and data fusion techniques are thus needed to approach the performance of a capable sensor with a large number of adaptively re-configurable low cost sensors. This work provides a computationally tractable scheme for autonomous detection, applied to the problem of detecting a radioactive source. Detection of radiation from nuclear materials has become an important task due to the increase in nuclear power plants or increasing threats from potential terrorist activities. We propose a system comprising of a network of autonomous sensor collaboratively collecting observations to detect the presence of a radioactive source.

Detection of radioactive sources using sensor networks has received some attention in the literature. In [1], the authors examine the gain in signal-to-noise ratio obtained by a simple combination of data from networked sensors compared to a single sensor. The costs and benefits of using a network of radiation detectors for radioactive source detection are analyzed and evaluated in [2]. In [3], the authors derived a test for the fusion of correlated decisions and obtained optimal sensor thresholds for two sensor case. In [4], the authors considered the problem of detecting a time-inhomogeneous Poisson process buried in the recorded background radiation using sensor networks. However, all these works assume existence of a centralized fusion center (FC) to fuse the data from multiple sensors and to make a global decision.

In many scenarios, a centralized FC may not be available. In large networks, it is a potential vulnerability, and/or can become an information bottleneck that may cause degradation of system performance, and may even lead to system failure. Also, due to the distributed nature of future communication networks and various practical constraints (e.g., absence of the FC, transmit power or hardware constraints and dynamic characteristic of wireless communications), it may be desirable to achieve collaborative decision making by employing peer-to-peer local information exchange to reach a global decision.

Recently, collaborative autonomous detection based on peer-to-peer algorithms has been explored in [5–10]. In autonomous detection approaches, each node communicates only with its neighbors and updates its local state information about the phenomenon (i.e. a summary statistic) by a local fusion rule that employs a weighted combination of its own value and those received from its neighbors. Nodes continue with this process until the whole network converges to a steady-state value which is the global test statistic. However, all these approaches assume a clairvoyant detection where all the parameters of the detection system and signal model are completely known. Note that, for our application of interest (i.e., nuclear radiation detection) the location of the radiation sources is rarely known. Centralized approaches manage this challenge by employing composite hypothesis testing frameworks such as the generalized likelihood ration test (GLRT). The GLRT, the detection procedure replaces unknown parameters in the detection algorithm with their maximum likelihood estimates, which need multiple sensing intervals for a reasonably accurate parameter estimate. This overhead and delay is not desirable in nuclear radiation detection problems especially under weak signal models. Secondly, due to the non-linearity introduced by the estimation step in GLRT, a decentralized implementation of GLRT is non-trivial. Also, a maximizer in the estimation step is not known before hand as it depends on the entire sensed data collected across all the nodes at all times. Hence, as far as communication complexity in the GLRT implementation is concerned, the maximization step incurs the major overhead. In fact, a direct implementation of the GLRT requires access to the entire raw data at all times at the FC. Finally, the implementation of non-linear detectors on low cost UAVs is difficult in practice. Thus, a decentralized solution with a simple implementation for the radiation detection problem with unknown source location is of utmost interest.

Autonomous detection schemes are quite vulnerable to different types of attacks. One typical attack on such networks is a Byzantine attack. While Byzantine attacks (originally proposed in [11]) may, in general, refer to many types of malicious behavior, our focus in this paper is on data-falsification attacks [12–18]. Thus far, research on detection in the presence of Byzantine attacks has predominantly focused on addressing these attacks under the centralized model in which information is available at the FC [14, 15, 18, 19]. Several attempts have been made to address the security threats in conventional consensus-based detection schemes in recent research [20–26]. There exist several methods for decentralized consensus optimization, including distributed subgradient descent algorithms [27], dual averaging methods [28], and the alternating direction method of multipliers (ADMM) [29]. Among these, the ADMM has drawn significant attention, as it is well suited for distributed convex optimization and demonstrates fast convergence in many applications. However, the performance analysis of ADMM in the presence of data falsifying Byzantine attacks has thus far not been addressed in the literature.

To overcome the mentioned challenges, in this paper we propose a simple to implement locally optimum detection algorithm to detect radioactive source signal buried in noise. We also devise a robust variant of ADMM algorithm to implement this detection scheme in autonomous networks in the presence of Byzantine attacks. To the best of our knowledge, there have been no existing results on the Byzantine-resilient locally optimum detection in collaborative autonomous sensor networks. The main contributions of the paper are:

- A derivation of a locally optimum test with a simple implementation for the detection of low SNR radioactive sources in background noise.
- A decentralized implementation of the derived test using alternating direction method of multipliers (ADMM) which is robust to Byzantine attacks.
- A study of the robustness of the proposed detection algorithm to Byzantine attacks and a comparison with conventional approaches.

2. SYSTEM MODEL

In this section, we present the signal and network models used in this work. For ease of exposition, and for comparison purposes, we first introduce the clairvoyant setting, in which the source location and intensity are known. In our setting, however, the source location is unknown, which is addressed in detail in subsequent sections.

2.1. Signal Model

Consider two hypotheses H_0 (radioactive source is absent) and H_1 (radioactive source is present). Also, consider a network of N autonomous nodes which must determine which of the two hypotheses is true. The observations received by the node i for $i = 1, \cdots, N$ under both hypotheses are as follows.

$$\begin{aligned} H_0 &: \quad z_i = b_i + w_i \\ H_1 &: \quad z_i = c_i + b_i + w_i \end{aligned} \tag{1}$$

where b_i, c_i and w_i are the background radiation count, source radiation count and measurement noise respectively, at node i located at $\{X_i, Y_i\}$[1]. The background radiation count is assumed to be Poisson distributed with known rate parameter λ_b. The source radiation count at node i is assumed to be Poisson distributed with rate parameter λ_{ci}. We assume an isotropic behavior of radiation in the presence of the source; the rate λ_{ci} is a function of the source intensity I_s and distance of the ith sensor from the source, given by

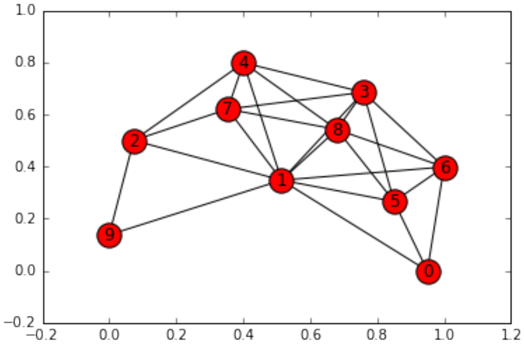

Fig. 1. An sensor network with 10 nodes.

$$\lambda_{ci} = \frac{I_s}{(X_i - X_s)^2 + (Y_i - Y_s)^2}, \tag{2}$$

where $\{X_s, Y_s\}$ represent the source coordinates. The measurement noise w_i is Gaussian distributed with a known variance σ_w^2. The background radiation count b_i and measurement noise w_i are assumed to be independent. We also assume that the observations at any node are conditionally independent and identically distributed given the hypothesis.

2.2. Network Model

We model the network topology as an undirected graph $G = (V, E)$, where $V = \{v_1, \cdots, v_N\}$ represents the set of nodes in the network. Let $|V| = N$, where $|V|$ denotes the cardinality of the set. The set of communication links in the network correspond to the set of edges E. In other words, $\{v_i, v_j\} \in E$ if and only if there is a communication link between v_i and v_j so that v_i and v_j can directly communicate with each other. A representative network topology with 10 nodes in shown in Fig. 1. The adjacency matrix $\mathcal{A}$ of the graph is defined as

$$a_{ij} = \begin{cases} 1 & \text{if } \{v_i, v_j\} \in E, \\ 0 & \text{otherwise.} \end{cases}$$

The neighborhood of a node i is defined as

$$\mathcal{N}_i = \{v_j \in V : \{v_i, v_j\} \in E\}, \forall i \in \{1, 2, \cdots, N\}.$$

The degree d_i of a node v_i is the number of edges in E which include v_i as an endpoint, i.e., $d_i = \sum_{j=1}^{N} a_{ij}$.

The degree matrix D is defined as a diagonal matrix with $\text{diag}(d_1, \cdots, d_N)$ and the Laplacian matrix L is defined as

$$l_{ij} = \begin{cases} d_i & \text{if } j = i, \\ -a_{ij} & \text{otherwise.} \end{cases}$$

In other words, $L = D - \mathcal{A}$.

2.3. Collaborative Autonomous Detection: Clairvoyant Case

For ease of exposition, we first consider the clairvoyant case, i.e., the values of source intensity I_s and source coordinates $\{x_s, y_s\}$ are assumed to be known. The collaborative autonomous detection scheme usually contains three phases: 1) sensing, 2) collaboration,

[1] Note that, the proposed scheme can easily be extended for a three-dimensional setting

and 3) decision making. In the sensing phase, each node acquires the summary statistic about the phenomenon of interest. Next, in the collaboration phase, each node communicates with its neighbors to update/improve their state values (summary statistic) and continues with this process until the whole network converges to a steady state which is the global test statistic. Finally, in the decision making phase, nodes make their own decisions about the presence of the phenomenon using this global test statistic. Next, we describe each of these phases in more detail.

2.3.1. Sensing Phase

In the sensing phase, each node i senses the phenomenon and forms a log likelihood ratio given by

$$\log\left(\frac{f_1(z_i)}{f_0(z_i)}\right)$$

where $f_k(z_i)$ is the conditional probability density function (PDF) of observation z_i at node i under the hypothesis H_k. It is well known that the distribution of the signal model introduced in Section 2.1 can be approximated by the Gaussian distribution [3]. Thus, under H_0, we have

$$f_0(z_i) = N(\lambda_b, \lambda_b + \sigma_w^2).$$

Similarly, under the H_1 hypothesis,

$$f_1(z_i) = N(\lambda_{ci} + \lambda_b, \lambda_{ci} + \lambda_b + \sigma_w^2),$$

where λ_{ci} is a function of the nodes' position relative to the source.

2.3.2. Collaboration Phase

Given individual log likelihood ratios at each node, the optimal test for the scenario considered above is a likelihood ratio test (LRT) given by:

$$\prod_{i=1}^{N}\left(\frac{f_1(z_i)}{f_0(z_i)}\right) \underset{H_0}{\overset{H_1}{\gtrless}} \lambda. \tag{3}$$

In the collaboration phase, the goal of each node is to collaborate with its neighbors to form the global test statistic (LRT). By taking log on both sides of (3), consensus based approaches can be employed to achieve an equivalent test which is the average of log likelihood ratios of all the nodes in the network. It can be shown that for sufficiently large information exchange iterations, the whole network converges to a steady state which is the global test statistic [30].

2.3.3. Decision Making Phase

After the collaboration phase is complete, each node reaches a steady state value x^*, which represents the global test statistic. Next, each node makes its own decision about the hypothesis using a predefined threshold:

$$x^* = \sum_{i=1}^{N}\log\left(\frac{f_1(z_i)}{f_0(z_i)}\right) \underset{H_0}{\overset{H_1}{\gtrless}} \log\lambda$$

where λ is chosen such that the probability of false alarm is constrained below a pre-specified level δ.

2.4. Detection with Unknown Source Location: GLRT

In many practical scenarios, including the focus of this work, the location of the radioactive source is not known and the LRT cannot be implemented. In such scenarios, one of the most popular tests is the Generalized Likelihood Ratio Testing (GLRT). The GLRT has an estimation procedure built into it, where the underlying parameter estimates are used as a plug-in estimate for the test statistic. More specifically, the GLRT test statistic is as follows:

$$\max_{\lambda_{ci}}\sum_{i=1}^{N}\log\left(\frac{f_1(z_i;\lambda_{ci})}{f_0(z_i)}\right) \underset{H_0}{\overset{H_1}{\gtrless}} \log\lambda. \tag{4}$$

As discussed in Section 1, the maximization step in the GLRT introduces delay, overhead and non-linearity, thus, is not amenable for an autonomous setting. Furthermore, the signal of interest in our application is very weak (buried in background clutter) and introduces additional challenges. In the next section, we show that in the low signal to noise ratio (SNR) regime, there exist a locally optimum detection scheme which alleviates the above mentioned difficulties.

3. COLLABORATIVE AUTONOMOUS LOCALLY OPTIMUM DETECTION (CA-LOD)

For ease of exposition, we first derive the new locally optimum detection scheme for a centralized scenario. Then, we present an approach to implement the proposed detection scheme in an decentralized setting.

3.1. Locally Optimum Centralized Detection

Theorem 1 *The locally optimal test statistic is given by*

$$\sum_{i=1}^{N}(z_i - \lambda_b) + \sum_{i=1}^{N}\frac{(z_i - \lambda_b)^2}{2(\lambda_b + \sigma_w^2)} \underset{H_0}{\overset{H_1}{\gtrless}} \gamma \tag{5}$$

where γ is chosen such that the probability of false alarm is constrained below a pre-specified level δ.

Proof The LRT for known λ_{ci} is given by

$$\sum_{i=1}^{N}\log\left(\frac{f_1(z_i;\lambda_{ci})}{f_0(z_i)}\right) \underset{H_0}{\overset{H_1}{\gtrless}} \log\lambda \tag{6}$$

$$\Leftrightarrow \quad \sum_{i=1}^{N}\log f_1(z_i;\lambda_{ci}) - \sum_{i=1}^{N}\log f_0(z_i) \underset{H_0}{\overset{H_1}{\gtrless}} \log\lambda \tag{7}$$

However, since we are considering a weak signal scenario, λ_{ci} tends to zero, and hence linearizing the LRT around $\lambda_{ci} = 0$ results in,

$$\sum_{i=1}^{N}(\lambda_{ci} - 0)\frac{d}{d\lambda_{ci}}\log f_1(z_i;\lambda_{ci})|_{\lambda_{ci}=0} \underset{H_0}{\overset{H_1}{\gtrless}} \log\lambda$$

$$\Leftrightarrow \quad \lambda_{ci}\sum_{i=1}^{N}\frac{d}{d\lambda_{ci}}\Big(-\frac{1}{2}\log(2\pi(\lambda_{ci} + \lambda_b + \sigma_w^2)) - \frac{(z_i - \lambda_{ci} - \lambda_b)^2}{2(\lambda_{ci} + \lambda_b + \sigma_w^2)}\Big)|_{\lambda_{ci}=0} \underset{H_0}{\overset{H_1}{\gtrless}} \log\lambda$$

$$\Leftrightarrow \quad \sum_{i=1}^{N}(z_i - \lambda_b) + \sum_{i=1}^{N}\frac{(z_i - \lambda_b)^2}{2(\lambda_b + \sigma_w^2)} \underset{H_0}{\overset{H_1}{\gtrless}} (\lambda_b + \sigma_w^2)\log\lambda + \frac{N}{2}.$$

The resulting test statistic is independent of the unknown parameter λ_{ci}, and is the *uniformly most powerful* (UMP) test for weak signals.

3.2. Collaborative Autonomous Detection Using ADMM

The LOD test statistic derived in the previous section is of the form below:

$$\frac{1}{N}\sum_{i=1}^{N} f(z_i) \underset{H_0}{\overset{H_1}{\gtrless}} \frac{\gamma}{N}$$

where $f(z_i) = (z_i - \lambda_b) + \frac{(z_i - \lambda_b)^2}{2(\lambda_b + \sigma_w^2)}$. The LOD statistic is separable and the function $f(.)$ is strongly convex. Next, we show that the LOD statistic can be implemented in a distributed manner using ADMM. To apply ADMM, we first formulate a convex optimization problem

$$x^* = \arg\min_{\hat{x}} \sum_{i=1}^{N} \frac{(\hat{x} - f(z_i))^2}{2} \quad (8)$$

i.e., the data average is the solution to a least-squares minimization problem. Next, we reformulate (8) in the ADMM amenable form as below

$$\text{minimize}_{\{x_i\},\{y_{ij}\}} \quad \sum_{i=1}^{N} \frac{(x_i - f(z_i))^2}{2} \quad (9)$$

$$\text{subject to} \quad x_i = y_{ij}, x_j = y_{ij}, \forall (i,j) \in \mathcal{A} \quad (10)$$

where x_i is the local copy of the common optimization variable $\hat{x}$ at node i and y_{ij} is an auxiliary variable imposing the consensus constraint on neighboring nodes i and j. In the matrix form, let us denote $F(\mathbf{x}) = \frac{1}{2}\|\mathbf{x} - f(\mathbf{z})\|_2^2$, then, the optimization problem is

$$\begin{aligned} &\text{minimize}_{\mathbf{x},\mathbf{y}} && F(\mathbf{x}) + G(\mathbf{y}) \\ &\text{subject to} && \mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{y} = \mathbf{0} \end{aligned} \quad (11)$$

where $G(\mathbf{y}) = 0$. Here $\mathbf{B} = [-\mathbf{I}_{|\mathcal{A}|}; -\mathbf{I}_{|\mathcal{A}|}]$ and $\mathbf{A} = [\mathbf{A}_1; \mathbf{A}_2]$ with $\mathbf{A}_k \in \mathbb{R}^{2E\times N}$. If $(i,j) \in \mathcal{A}$ and y_{ij} is the qth entry of $\mathbf{y}$, then the (q,i)th entry of $\mathbf{A}_1$ and the (q,j)th entry of $\mathbf{A}_2$ are 1; otherwise the corresponding entries are 0. The augmented Lagrangian of (11) is given by

$$L_\rho(\mathbf{x}, \mathbf{y}, \lambda) = F(\mathbf{x}) + \langle \lambda, \mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{y}\rangle + \frac{\rho}{2}\|\mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{y}\|_2^2,$$

where $\lambda = [\beta_1; \beta_2]$ with $\beta_1, \beta_2 \in \mathbb{R}^{2E}$ is the Lagrange multiplier and ρ is a positive algorithm parameter. The updates for the ADMM are

$$\begin{aligned} &\mathbf{x}\text{-update} : \nabla F(\mathbf{x}^{k+1}) + \mathbf{A}^T\lambda^k + \rho\mathbf{A}^T(\mathbf{A}\mathbf{x}^{k+1} + \mathbf{B}\mathbf{y}^k) = \mathbf{0} \\ &\mathbf{y}\text{-update} : \mathbf{B}^T\lambda^k + \rho\mathbf{B}^T(\mathbf{A}\mathbf{x}^{k+1} + \mathbf{B}\mathbf{y}^{k+1}) = \mathbf{0} \\ &\lambda\text{-update} : \lambda^{k+1} - \lambda^k - \rho(\mathbf{A}\mathbf{x}^{k+1} + \mathbf{B}\mathbf{y}^{k+1}) = \mathbf{0} \end{aligned} \quad (12)$$

where $\nabla F(\mathbf{x}^{k+1}) = \mathbf{x}^{k+1} - f(\mathbf{z})$ is the gradient of $F(.)$ at $\mathbf{x}^{k+1}$. The global convergence of ADMM was established in [29]. Since our objective function $F(\mathbf{x})$ is strongly convex in $\mathbf{x}$, we obtain x^* equal to the global test statistic as given in (5) as the unique primal solution.

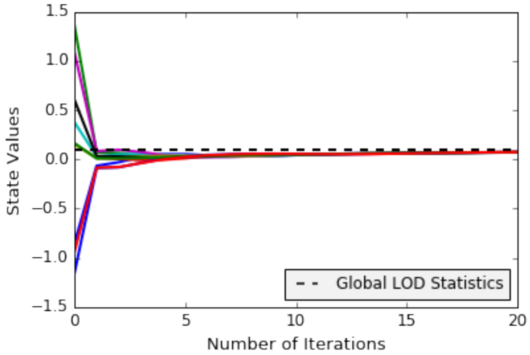

Fig. 2. Convergence of state values of a network with 10 nodes using ADMM based CA-LOD scheme.

The updates in (12) can be further simplified to [31],

$$x_i^{k+1} = \frac{1}{1 + 2\rho|\mathcal{N}_i|}\left(\rho|\mathcal{N}_i|x_i^k + \rho\sum_{j\in\mathcal{N}_i} x_j^k - \alpha_i^k + f(z_i)\right),$$

$$\alpha_i^{k+1} = \alpha_i^k + \rho\left(|\mathcal{N}_i|x_i^{k+1} - \sum_{j\in\mathcal{N}_i} x_j^{k+1}\right) \quad (13)$$

at node i where $\mathcal{N}_i$ denotes the set of neighbors of node i. Note that, the updates in (13) only depend on the data from the neighbors of the node i and can be implemented in a fully autonomous manner. This implies that with these updates, each node can learn the global LOD test statistic only using local information exchanges.

3.3. Illustrative Examples

Next, to gain insight into the solution, we present illustrative examples that corroborate our results. We consider a 10 node network employing the ADMM updates as given in (13) to determine the presence (or absence) of a radioactive source. We assume a mean background radiation with count $\lambda_b = 0.5$ and measurement noise with $\sigma_w^2 = 0.5$. Source and nodes locations and adjacency matrix were generated randomly in a region of interest of dimension 3.0×3.0 units. The ADMM parameter ρ was set to 1.0. We further assume that the prior probability of hypothesis is $P_0 = P_1 = 0.5$ and detection performance is empirically found by performing 1000 Monte-Carlo runs.

3.3.1. Convergence Analysis

To better understand the convergence properties of the proposed approach, we next present an instance of ADMM based CA-LOD in Fig. 2. We assume that each node starts with its local LOD statistic and collaborate with its neighbors to improve its performance. We plot the updated state values (LOD statistic) at each node as a function of information exchange iterations. Fig. 2 shows the state values of each node as a function of the number of iterations. It is observed that the state values converges to the global test statistic within 20 iterations using only local interactions.

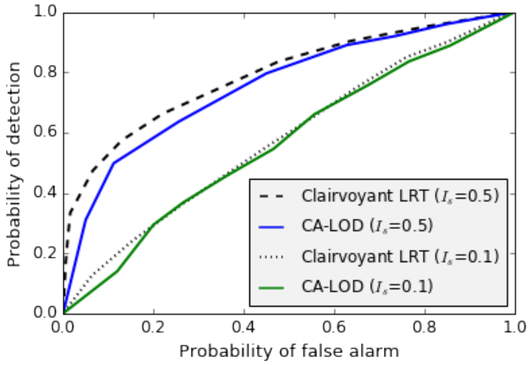

Fig. 3. Performance comparison of CA-LOD with clairvoyant LRT.

3.3.2. *Detection Performance Analysis*

Next, we analyze the detection performance of the proposed scheme. In Fig. 3, we plot steady state receiver operating characteristic (ROC) curves for the proposed CA-LOD approach for different source intensities I_s. We compare the performance of the proposed approach with clairvoyant LRT based approach which has the knowledge of the true source location. It can be seen that for both $I_s = 0.1$ and $I_s = 0.5$, the proposed CA-LOD approach performs almost as good as the clairvoyant LRT based approach.

4. COLLABORATIVE AUTONOMOUS DETECTION IN THE PRESENCE OF BYZANTINE ATTACKS

In this section, we analyze the performance of the proposed detection scheme in the presence of Byzantine attacks. First, we define an attack model for Byzantines. Note that, the objective of the Byzantines is to degrade the detection performance of the network by injecting false data. We assume an independent malicious Byzantine attack model where each Byzantine decides to attack independently relying on its own observation.

4.1. Byzantine Attack Model: Modus Operandi

Note that, the ADMM updates at node i at iteration k is a function of its neighbors' parameters $\{x_j^k\}_{j\in\mathcal{N}_i}$. When there are no adversaries in the network, as seen in the last section, the global statistic can be calculated in an autonomous manner via local interactions. However, instead of broadcasting the true parameters $\{x_i^k\}$, some nodes (referred to as Byzantines) deviate from the prescribed strategies. More specifically, we assume that the Byzantine node j falsifies its data at ADMM iteration k as follows:

$$x_j^k \quad = \quad x_j^k + \delta_j^x$$

where $\delta_j^x \sim \mathcal{N}(\mu_x, \sigma_x^2)$ and (μ_x, σ_x^2) characterize the strength of the attack.

4.1.1. *Performance Analysis of CA-LOD with Byzantines*

In this section, we study the susceptibility of CA-LOD in the presence of Byzantine attacks. We assume a mean background radiation with count $\lambda_b = 0.5$ and measurement noise with $\sigma_w^2 = 0.5$. We further assume that the nodes are observing the phenomena over 1000 time (or detection) intervals. Furthermore, the ADMM parameter ρ was set to 1.0. We assume that there is only 1 Byzantine in the network which is chosen randomly.

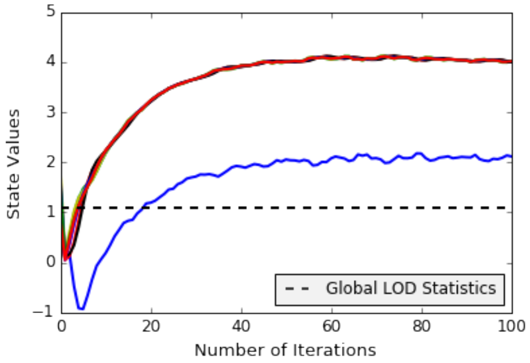

Fig. 4. Convergence of vanilla ADMM based CA-LOD in the presence of Byzantines. Blue curve represents Byzantine's state values.

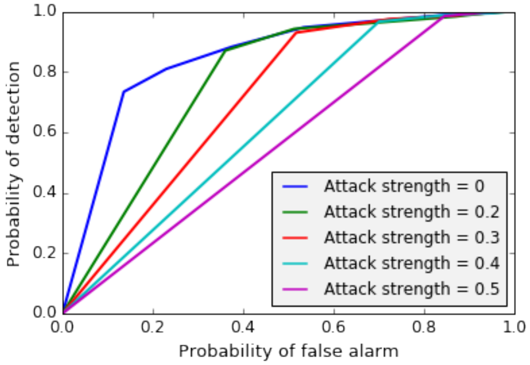

Fig. 5. Susceptibility of CA-LOD to Byzantine attack in terms of ROC.

In Fig. 4, we plot the convergence of the ADMM algorithm with updates as given in (13). We assume the Byzantine's parameters to be $\mu_x = 1.5$ and $\sigma_x^2 = 0.1$. It can be seen that the Byzantine attack can severely degrade the convergence performance. More specifically, it can be seen from Fig. 4 that a single Byzantine can make the rest of the network converge to a state value which is significantly different from the global LOD statistic.

Next, in Fig. 5, we plot the steady state ROC for different values of attack strength μ_x keeping σ_x^2 fixed to 0.1. Observe that, as the attack strength increases, the detection performance degrades severely and an adversary can make the steady state statistic (or data) non-informative. In other words, the optimal detection scheme at each node performs no better than a coin flip detector.

Hence, we can see that Byzantines can severely degrade the detection performance of the CA-LOD. Next, we consider the problem from a network designer's perspective and propose a robust ADMM algorithm to counter Byzantine attacks.

4.2. Robust Collaborative Autonomous Detection using Byzantine-Resilient ADMM

In this section, we propose a Byzantine-resilient ADMM algorithm (R-ADMM) for collaborative autonomous detection. Our approach draws inspiration from robust statistic for anomaly detection to make

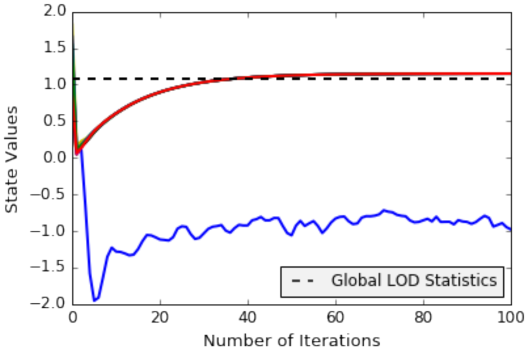

Fig. 6. Convergence of proposed algorithm based CA-LOD in the presence of Byzantine attack. Blue curve represents Byzantines state values.

ADMM resilient to Byzantine attacks. More specifically, proposed robust ADMM updates to tolerate at most p Byzantines are given by

$$x_i^{k+1} = \frac{1}{1+2\rho|\mathcal{N}_i|}\left(\rho|\mathcal{N}_i|x_i^k + \rho\Gamma_p(\{x_j^k\}_{j\in\mathcal{N}_i}) - \alpha_i^k + f(z_i)\right),$$
$$\alpha_i^{k+1} = \alpha_i^k + \rho\left(|\mathcal{N}_i|x_i^{k+1} - \Gamma_p(\{x_j^{k+1}\}_{j\in\mathcal{N}_i})\right) \quad (14)$$

where the sum over neighbors' data in (13) has been replaced by a robust fusion function $\Gamma_p(\{x_j^k\}_{j\in\mathcal{N}_i})$ which operates as follows:
Operation of $\Gamma_p(.)$: *First, sort the elements in* $\mathcal{S} = \{x_j^k\}_{j\in\mathcal{N}_i}$ *in a non-decreasing order (breaking ties arbitrarily), and replace the smallest p values and the largest p values with mean of remaining* $(|\mathcal{N}_i| - 2p)$ *values.*[2] *Next, return the sum of the elements in the new set.*

In other words, it discards the top and bottom p values as potential outliers.

4.3. Illustrative Examples

In this section, we analyze the performance of the proposed Byzantine-resilient autonomous detection scheme in the presence of Byzantine attacks. We consider a randomly generated 10 node network employing updates as given in (14) to determine the presence (or absence) of a radioactive source. We assume a mean background radiation with count $\lambda_b = 0.5$ and measurement noise with $\sigma_w^2 = 0.5$. Furthermore, ADMM parameter ρ was set to 1.0. We assume that there is only 1 Byzantine in the network which is chosen randomly. We assume $p = 1$.

4.3.1. Robustness Analysis

In Fig. 6, we plot the convergence of the proposed R-ADMM algorithm with updates as given in (14). We assume the Byzantine's parameters to be $\mu_x = 1.5$ and $\sigma_x^2 = 0.1$. It can be seen that, as opposed to Fig. 4, the state values of the honest nodes converge close to the global LOD statistic despite the presence of Byzantine attack.

Next, in Fig. 7, we compare the steady state ROC for CA-LOD of vanilla ADMM based approach with the R-ADMM based approach. We assume attack parameters to be $\mu_x = 2.5$ and $\sigma_x^2 = 0.1$.

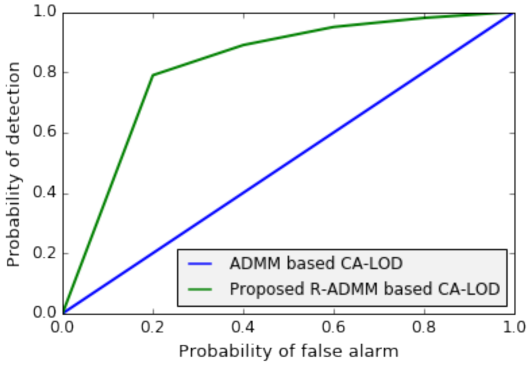

Fig. 7. Detection performance of CA-LOD in the presence of Byzantine attacks.

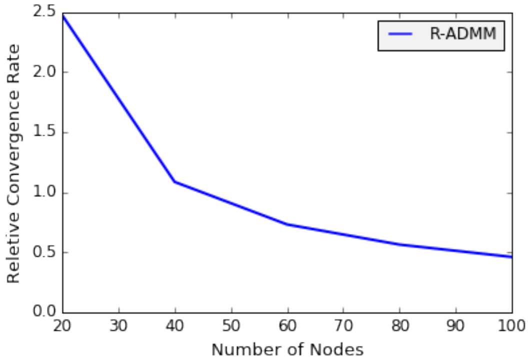

Fig. 8. Scaling behavior of the proposed algorithm for bounded neighborhood size.

It can be seen that the R-ADMM based Byzantine-resilient CA-LOD approach performs significantly better compare to the vanilla ADMM based approach, which breaks down in the the presence of the Byzantine attack.

4.3.2. Scaling Analysis

In Fig. 8, we plot the convergence behavior of R-ADMM based CA-LOD as network grows larger. We consider a practical scenario where we fix the number of nodes (or neighbors) each node can talk to to be 10. This makes the complexity of the sorting step in R-ADMM to be a constant. We plot relative convergence rates defined as T^*/N where T^* is the number of iterations needed to reach within 95% of the global LOD statistic. Note that, the convergence rate T^* increases as number of nodes N increases in the network, however, the relative convergence rate decreases. This implies that the proposed approach retains the excellent scaling properties of ADMM and is amenable for large scale networks.

4.3.3. Overhead Comparison

In Fig. 9, we compare the overhead caused by the R-ADMM based CA-LOD scheme. We consider the case where there is no Byzantine in the network and compare the performance of ADMM based CA-LOD and R-ADMM based CA-LOD in terms of relative convergence rate. It can be seen that the overhead caused by the R-ADMM

[2] We assume that $|\mathcal{N}_i| > 2p, \ \forall i$.

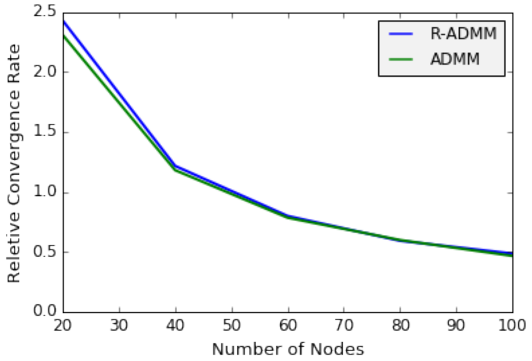

Fig. 9. Overhead comparison in the absence of Byzantine attacks.

based CA-LOD scheme is very small. In practice, this overhead is dominated by the sorting step in R-ADMM algorithm and is a constant for a bounded neighborhood.

5. CONCLUSION AND FUTURE WORK

In this paper, we studied the problem of nuclear radiation detection using collaborative autonomous sensors. We proposed a locally optimum detection scheme and implemented it in a fully autonomous setup using ADMM. Furthermore, we devised a robust version of the ADMM algorithm for Byzantine-resilient detection and demonstrated its robustness to data falsification attacks. There are still many interesting questions that remain to be explored in the future work such as analysis and extension of the problem with more realistic signal model and collaborative Byzantine attacks. Theoretical convergence properties of the robust ADMM algorithm can also be investigated.

Acknowledgments

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. LLNL-CONF-734905

6. REFERENCES

[1] S. M. Brennan, A. M. Mielke, and D. C. Torney, “Radioactive source detection by sensor networks,” *IEEE Transactions on Nuclear Science*, vol. 52, no. 3, pp. 813–819, 2005.

[2] D. L. Stephens and A. J. Peurrung, “Detection of moving radioactive sources using sensor networks,” *IEEE Transactions on Nuclear Science*, vol. 51, no. 5, pp. 2273–2278, 2004.

[3] A. Sundaresan, P. K. Varshney, and N. S. V. Rao, “Distributed detection of a nuclear radioactive source using fusion of correlated decisions,” in *2007 10th International Conference on Information Fusion*, July 2007, pp. 1–7.

[4] C. D. Pahlajani, I. Poulakakis, and H. G. Tanner, “Networked decision making for poisson processes with applications to nuclear detection,” *IEEE Transactions on Automatic Control*, vol. 59, no. 1, pp. 193–198, Jan 2014.

[5] 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 2011, pp. 1–6.

[6] F. Pasqualetti, A. Bicchi, and F. Bullo, “Consensus Computation in Unreliable Networks: A System Theoretic Approach,” *Automatic Control, IEEE Transactions on*, vol. 57, no. 1, pp. 90–104, Jan 2012.

[7] G. Xiong and S. Kishore, “Consensus-based distributed detection algorithm in wireless ad hoc networks,” in *Signal Processing and Communication Systems, 2009. ICSPCS 2009. 3rd International Conference on*, Sept 2009, pp. 1–6.

[8] S. Aldosari and J. Moura, “Distributed Detection in Sensor Networks: Connectivity Graph and Small World Networks,” in *Signals, Systems and Computers, 2005. Conference Record of the Thirty-Ninth Asilomar Conference on*, Oct 2005, pp. 230–234.

[9] S. Kar, S. Aldosari, and J. Moura, “Topology for Distributed Inference on Graphs,” *Signal Processing, IEEE Transactions on*, vol. 56, no. 6, pp. 2609–2613, June 2008.

[10] F. Yu, M. Huang, and H. Tang, “Biologically inspired consensus-based spectrum sensing in mobile Ad Hoc networks with cognitive radios,” *Network, IEEE*, vol. 24, no. 3, pp. 26–30, May 2010.

[11] 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

[12] 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.

[13] 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

[14] 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.

[15] 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.

[16] 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.

[17] ——, “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.

[18] 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.

[19] A. Min, K.-H. Kim, and K. Shin, “Robust cooperative sensing via state estimation in cognitive radio networks,” in *New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on*, May 2011, pp. 185–196.

[20] B. Kailkhura, S. Brahma, and P. K. Varshney, "Data falsification attacks on consensus-based detection systems," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 1, pp. 145–158, March 2017.

[21] H. Tang, F. Yu, M. Huang, and Z. Li, "Distributed consensus-based security mechanisms in cognitive radio mobile ad hoc networks," *Communications, IET*, vol. 6, no. 8, pp. 974–983, May 2012.

[22] 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 2009, pp. 1–7.

[23] F. Yu, M. Huang, and H. Tang, "Biologically inspired consensus-based spectrum sensing in mobile Ad Hoc networks with cognitive radios," *Network, IEEE*, vol. 24, no. 3, pp. 26–30, May 2010.

[24] S. Liu, H. Zhu, S. Li, X. Li, C. Chen, and X. Guan, "An adaptive deviation-tolerant secure scheme for distributed cooperative spectrum sensing," in *Global Communications Conference (GLOBECOM), 2012 IEEE*, Dec 2012, pp. 603–608.

[25] 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 2012, pp. 900–908.

[26] Z. Li, F. Yu, and M. Huang, "A Distributed Consensus-Based Cooperative Spectrum-Sensing Scheme in Cognitive Radios," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 1, pp. 383–393, Jan 2010.

[27] A. Nedic and A. Ozdaglar, "Distributed subgradient methods for multi-agent optimization," *IEEE Transactions on Automatic Control*, vol. 54, no. 1, pp. 48–61, 2009.

[28] J. C. Duchi, A. Agarwal, and M. J. Wainwright, "Dual averaging for distributed optimization: Convergence analysis and network scaling," *IEEE Transactions on Automatic Control*, vol. 57, no. 3, pp. 592–606, March 2012.

[29] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Foundations and Trends® in Machine Learning*, vol. 3, no. 1, pp. 1–122, 2011.

[30] R. Olfati-Saber, J. Fax, and R. Murray, "Consensus and Cooperation in Networked Multi-Agent Systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, Jan 2007.

[31] W. Shi, Q. Ling, K. Yuan, G. Wu, and W. Yin, "On the linear convergence of the admm in decentralized consensus optimization." *IEEE Trans. Signal Processing*, vol. 62, no. 7, pp. 1750–1761, 2014.