Distributed Detection in Tree Networks: Byzantines and Mitigation Techniques

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

***Abstract*— In this paper, the problem of distributed detection in tree networks in the presence of Byzantines is considered. Closed form expressions for optimal attacking strategies that minimize the miss detection error exponent at the fusion center (FC) are obtained. We also look at the problem from the network designer's (FC's) perspective. We study the problem of designing optimal distributed detection parameters in a tree network in the presence of Byzantines. Next, we model the strategic interaction between the FC and the attacker as a leader–follower (Stackelberg) game. This formulation provides a methodology for predicting attacker and defender (FC) equilibrium strategies, which can be used to implement the optimal detector. Finally, a reputation-based scheme to identify Byzantines is proposed and its performance is analytically evaluated. We also provide some numerical examples to gain insights into the solution.**

***Index Terms*— Distributed detection, data falsification, Byzantines, tree networks, error exponent, leader-follower game, reputation based mitigation scheme.**

I. Introduction

DISTRIBUTED detection deals with the problem of making a global decision regarding a phenomenon based on local decisions collected from several remotely located sensing nodes. Distributed detection research has traditionally focused on the parallel network topology, in which nodes directly transmit their observations or decisions to the Fusion Center (FC) [1]–[3]. Despite its theoretical importance and analytical tractability, parallel topology may not always reflect the practical scenario. In certain cases, it may be required to place the nodes outside their communication range with the FC. Then, the coverage area can be increased by forming a multi-hop network, where nodes are organized hierarchically into multiple levels (tree networks). Some examples of tree networks include wireless sensor and military communication networks.

Typically, a network embodies a large number of inexpensive sensors, which are deployed in an open environment to collect the observations regarding a certain phenomenon and, therefore, are susceptible to many kinds of attacks. A typical example is a Byzantine attack. While Byzantine attacks (originally proposed in [4]) may, in general, refer to many types of malicious behavior, our focus in this paper is on data-falsification attacks [5]–[18], where an attacker sends false (erroneous) data to the FC to degrade detection performance. In this paper, we refer to such data falsification attackers as *Byzantines*, and the data thus fabricated as *Byzantine data*.

A. Related Work

Recently, distributed detection in the presence of Byzantine attacks has been explored in [8] and [9], where the problem of determining the most effective attacking strategy for the Byzantines was investigated. However, both works focused only on parallel topology. The problem considered in this paper is most related to our earlier papers [10], [14]. In [10] and [14], we studied the problem of distributed detection in perfect tree networks (all intermediate nodes in the tree have the same number of children) with Byzantines under the assumption that the FC does not know which decision bit is sent from which node and assumes each received bit to originate from nodes at depth k with a certain probability. Under this assumption, the attacker's aim was to maximize the false alarm probability for a fixed detection probability. When the number of nodes is large, by Stein's lemma [19], we know that the error exponent of the false alarm probability can be used as a surrogate for the false alarm probability. Thus, the optimal attacking strategy was obtained by making the error exponent of the false alarm probability at the FC equal to zero, which makes the decision fusion scheme completely incapable (blind). Some counter-measures were also proposed to protect the network from such Byzantines.

There are several notable differences between this paper and our earlier papers [10], [14]. First, in contrast to [10] and [14], in this paper, the problem of distributed detection in regular tree networks[1] with Byzantines is addressed in a practical setup where the FC has the knowledge of which bit

Manuscript received October 7, 2014; revised January 22, 2015; accepted March 16, 2015. Date of publication March 23, 2015; date of current version June 2, 2015. This work was supported by the Center for Advanced Systems and Engineering, Syracuse University, Syracuse, NY, USA. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Vrizlynn L. L. Thing.

B. Kailkhura, S. Brahma, and P. K. Varshney are with the Department of Electrical Engineering and Computer Science, Syracuse University, Syracuse, NY 13244 USA (e-mail: bkailkhu@syr.edu; skbrahma@syr.edu; varshney@syr.edu).

B. Dulek is with the Department of Electrical and Electronics Engineering, Hacettepe University, Ankara 06640, Turkey (e-mail: berkan@ee.hacettepe.edu.tr).

Y. S. Han is with the Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei 10607, Taiwan, and also with the Department of Communication Engineering, National Taipei University, Taipei 10617, Taiwan (e-mail: yshan@mail.ntust.edu.tw).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2015.2415757

[1]For a regular tree, intermediate nodes at different levels are allowed to have different degrees, i.e., number of children.

is transmitted from which node. Note that, in practice, the FC knows which bit is transmitted from which node, e.g., using MAC schemes,[2] and can utilize this information to improve system performance. Next, for the analysis of the optimal attack, we consider nodes residing at different levels of the tree to have different detection performance. We also allow Byzantines residing at different levels of the tree to have different attacking strategies and, therefore, provide a more general and comprehensive analysis of the problem as compared to [10] and [14]. We also study the problem from the network designer's perspective. Based on the information regarding which bit is transmitted from which node, we propose schemes to mitigate the effect of the Byzantines.

B. Main Contributions

In this paper, it is assumed that the FC knows which bit is transmitted from which node. Under this assumption, the problem of distributed detection in tree networks in the presence of Byzantines is considered. The main contributions of this paper are summarized below:

- Detection performance in tree networks with Byzantines is characterized in terms of the error exponent and a closed form expression for the optimal error exponent is derived.
- The minimum attacking power required by the Byzantines to blind the FC in a tree network is obtained. It is shown that when more than a certain fraction of individual node decisions are falsified, the decision fusion scheme becomes completely incapable.
- The problem is also investigated from the network designer's perspective by focusing on the design of optimal distributed detection parameters in a tree network.
- We model the strategic interaction between the FC and the attacker as a Leader-Follower (Stackelberg) game and identify attacker and defender (FC) equilibrium strategies. The knowledge of these equilibrium strategies can later be used to implement the optimal detector at the FC.
- We propose a simple yet efficient reputation based scheme, which works even if the FC is blinded, to identify Byzantines in tree networks and analytically evaluate its performance.

The rest of the paper is organized as follows. Section II introduces the system model. In Section III, we study the problem from Byzantine's perspective and provide closed form expressions for optimal attacking strategies. In Section IV, we investigate the problem of designing optimal distributed detection parameters in the presence of Byzantines. In Section V, we model the strategic interaction between the FC and the attacker as a Leader-Follower (Stackelberg) game and find equilibrium strategies. In Section VII, we introduce an efficient Byzantine identification scheme and analyze its performance. Finally, Section VII concludes the paper.

[2]In practice, one possible way to achieve this is by using the buffer-less TDMA MAC protocol, in which, distinct non-overlapping time slots are assigned (scheduled) to the nodes for communication. One practical example of such a scheme is given in [20].

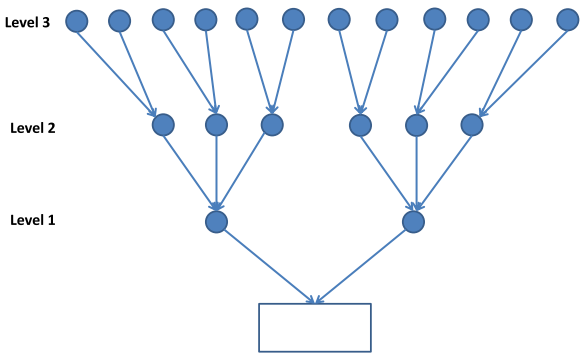

Fig. 1. A distributed detection system organized as a regular tree ($a_1 = 2,\ a_2 = 3,\ a_3 = 2$) is shown as an example.

II. System Model

We consider a distributed detection system organized as a regular tree network rooted at the FC (See Figure 1). For a regular tree, all the leaf nodes are at the same level (or depth) and all the intermediate nodes at level k have degree a_k. The regular tree is assumed to have a set $\mathcal{N} = \{\mathbb{N}_k\}_{k=1}^{K}$ of transceiver nodes, where $|\mathbb{N}_k| = N_k$ is the total number of nodes at level k. We assume that the depth of the tree is $K > 1$ and $a_k \geq 2$. The total number of nodes in the network is denoted as $N = \sum_{k=1}^{K} N_k$ and $\mathcal{B} = \{\mathbb{B}_k\}_{k=1}^{K}$ denotes the set of Byzantine nodes with $|\mathbb{B}_k| = B_k$, where $\mathbb{B}_k$ is the set of Byzantines at level k. The set containing the number of Byzantines residing at each level k, $1 \leq k \leq K$, is referred to as an attack configuration, i.e., $\{B_k\}_{k=1}^{K} = \{|\mathbb{B}_k|\}_{k=1}^{K}$. Next, we define the *modus operandi* of the nodes.

A. Modus Operandi of the Nodes

We consider a binary hypothesis testing problem with two hypotheses H_0 (signal is absent) and H_1 (signal is present). Under each hypothesis, it is assumed that the observations $Y_{k,i}$ at each node i at level k are conditionally independent. Each node i at level k acts as a source in the sense that it makes a one-bit (binary) local decision $v_{k,i} \in \{0, 1\}$ regarding the absence or presence of the signal using the likelihood ratio test (LRT)[3]

$$\frac{p^{(1)}_{Y_{k,i}}(y_{k,i})}{p^{(0)}_{Y_{k,i}}(y_{k,i})} \underset{v_{k,i}=0}{\overset{v_{k,i}=1}{\gtrless}} \lambda_k, \tag{1}$$

where λ_k is the threshold used at level k (it is assumed that all the nodes at level k use the same threshold λ_k) and $p^{(j)}_{Y_{k,i}}(y_{k,i})$ is the conditional probability density function (PDF) of observation $y_{k,i}$ under hypothesis H_j for $j \in \{0, 1\}$. We denote the probabilities of detection and false alarm of a node at level k by $P_d^k = P(v_{k,i} = 1|H_1)$ and $P_{fa}^k = P(v_{k,i} = 1|H_0)$, respectively, which are functions of λ_k and hold for both Byzantines and honest nodes. After making its one-bit local decision $v_{k,i} \in \{0, 1\}$, node i at level k sends

[3]Notice that, under the conditional independence assumption, the optimal decision rule at the local sensor is a likelihood-ratio test [21].

$u_{k,i}$ to its parent node at level $k-1$, where $u_{k,i} = v_{k,i}$ if i is an honest node, but for a Byzantine node i, $u_{k,i}$ need not be equal to $v_{k,i}$. Node i at level k also receives the decisions $u_{k',j}$ of all successors j at levels $k' \in [k+1, K]$, which are forwarded to node i by its immediate children, and forwards[4] them to its parent node at level $k-1$. We assume error-free communication between children and the parent nodes. Next, we present a mathematical model for the Byzantine attack.

B. Byzantine Attack Model

We define the following strategies $P^H_{j,1}(k)$, $P^H_{j,0}(k)$ and $P^B_{j,1}(k)$, $P^B_{j,0}(k)$ ($j \in \{0,1\}$ and $k = 1, \cdots, K$) for the honest and Byzantine nodes at level k, respectively:
Honest nodes:

$$P^H_{1,1}(k) = 1 - P^H_{0,1}(k) = P^H_k(x=1|y=1) = 1 \quad (2)$$

$$P^H_{1,0}(k) = 1 - P^H_{0,0}(k) = P^H_k(x=1|y=0) = 0 \quad (3)$$

Byzantine nodes:

$$P^B_{1,1}(k) = 1 - P^B_{0,1}(k) = P^B_k(x=1|y=1) \quad (4)$$

$$P^B_{1,0}(k) = 1 - P^B_{0,0}(k) = P^B_k(x=1|y=0) \quad (5)$$

where $P_k(x=a|y=b)$ is the conditional probability that a node at level k sends a to its parent when it receives b from its child or its actual decision is b. For notational convenience, we use $(P^k_{1,0}, P^k_{0,1})$ to denote the flipping probability of the Byzantine node at level k. Furthermore, we assume that if a node (at any level) is a Byzantine, then none of its ancestors and successors are Byzantine (non-overlapping attack configuration); otherwise, the effect of a Byzantine due to other Byzantines on the same path may be nullified (e.g., Byzantine ancestor re-flipping the already flipped decisions of its successors). This means that every path from a leaf node to the FC will have at most one Byzantine. Notice that, for the attack configuration $\{B_k\}_{k=1}^K$, the total number of corrupted paths (i.e., paths containing a Byzantine node) from level k to the FC are $\sum_{i=1}^k B_i \frac{N_k}{N_i}$, where $B_i \frac{N_k}{N_i}$ is the total number of nodes covered[5] at level k by the presence of B_i Byzantines at level i. If we denote $\alpha_k = \frac{B_k}{N_k}$, then, $\frac{\sum_{i=1}^k B_i \frac{N_k}{N_i}}{N_k} = \sum_{i=1}^k \alpha_i$ is the fraction of decisions coming from level k that encounter a Byzantine along the way to the FC. For a large network, due to the law of large numbers, one can approximate the probability that the FC receives the flipped decision $\bar{x}$ of a given node at level k when its actual decision is x as $\beta^k_{\bar{x},x} = \sum_{j=1}^k \alpha_j P^j_{\bar{x},x}$, $x \in \{0,1\}$.

C. Binary Hypothesis Testing at the Fusion Center

We consider the distributed detection problem under the Neyman-Pearson (NP) criterion. The FC receives decision vectors, $[\mathbf{z_1}, \cdots, \mathbf{z_K}]$, where $\mathbf{z_k}$ for $k \in \{1, \cdots, K\}$ is a decision vector with its elements being $z_1, \cdots, z_{N_k}$, from the nodes at different levels of the tree. Then the FC makes the global decision about the phenomenon by employing the LRT. Due to system vulnerabilities, some of the nodes may be captured by the attacker and reprogrammed to transmit false information to the FC to degrade detection performance. We assume that the only information available at the FC is the probability $\beta^k_{\bar{x},x}$, which is the probability with which the data coming from level k has been falsified. Using this information, the FC calculates the probabilities $\pi^k_{j,0} = P(z_i = j|H_0, k)$ and $\pi^k_{j,1} = P(z_i = j|H_1, k)$, which are the distributions of received decisions z_i originating from level k and arriving to the FC under hypotheses H_0 and H_1. The FC makes its decision regarding the absence or presence of the signal using the following likelihood ratio test

$$\prod_{k=1}^K \left(\frac{\pi^k_{1,1}}{\pi^k_{1,0}}\right)^{s_k} \left(\frac{1-\pi^k_{1,1}}{1-\pi^k_{1,0}}\right)^{N_k - s_k} \underset{H_0}{\overset{H_1}{\gtrless}} \eta \quad (6)$$

where s_k is the number of decisions that are equal to one and originated from level k, and the threshold η is chosen in order to minimize the missed detection probability (P_M) while keeping the false alarm probability (P_F) below a fixed value δ.[6] Using Stein's lemma [19], we know that the Kullback-Leibler divergence (KLD) represents the best error exponent of the missed detection error probability in the NP setup.

Lemma 1 [19]: For a fixed false alarm probability, $P_F \leq \delta$, the missed detection probability for an optimal NP detector asymptotically behaves as

$$\lim_{N\to\infty} \frac{1}{N} \log P_M = -D(H_0 \| H_1)$$

where N is the number of samples used for detection and $D(H_0\|H_1)$ is the Kullback-Leibler divergence (KLD).

A direct consequence of Lemma 1 is that P_M decays, as N grows to infinity, exponentially, i.e.,

$$P_M \approx f(N) e^{-D(H_0\|H_1)},$$

where $f(N)$ is a slow-varying function compared to the exponential, such that $\lim_{N\to\infty} \frac{1}{N} \log f(N) = 0$. Therefore, given a number of observations, the detection performance depends exclusively on the KLD between the hypotheses. We can conclude that the larger the KLD is, the less is the likelihood of mistaking H_0 with H_1 and, therefore, KLD can be used as a surrogate for the probability of missed detection during system design for a large network.[7] Next, we derive a closed form expression for the optimal missed detection error exponent for tree networks in the presence of Byzantines, which will later be used as a surrogate for the probability of missed detection.

Proposition 1: For a K level tree network employing the detection scheme as given in (6), the asymptotic detection

[4]For example, IEEE 802.16j mandates tree forwarding and IEEE 802.11s standardizes a tree-based routing protocol.

[5]Node i at level k' covers (or can alter the decisions of) all its children at levels $k'+1$ to K and itself. In other words, the total number of covered nodes is equivalent to the total number of corrupted paths (i.e., paths containing a Byzantine node) in the network.

[6]This type of problem setup is important, for instance, in Cognitive Radio Networks (CRN). In order to coexist with the primary user (PU), secondary users (SUs) must guarantee that their transmissions will not interfere with the transmission of the PU who have higher priority to access the spectrum.

[7]Kullback-Leibler divergence based detection approaches perform reasonably well even for a small size network as observed in [8] and [22]–[24].

performance (i.e., $N_1 \to \infty$) can be characterized using the missed detection error exponent given below

$$D = \sum_{k=1}^{K} N_k \left[\sum_{j \in \{0,1\}} \pi_{j,0}^k \log \frac{\pi_{j,0}^k}{\pi_{j,1}^k} \right]. \quad (7)$$

Proof: Let $\mathbf{Z} = [\mathbf{Z}_1, \cdots, \mathbf{Z}_{N_1}]$ denote the received decision vectors from the nodes at level 1, where $\mathbf{Z_i}$ is the decision vector forwarded by the node i at level 1 to the FC. Observe that, $\mathbf{Z}_i$ for $i = 1$ to N_1 are independent and identically distributed (i.i.d.). Therefore, using Stein's lemma [19], when $N_1 \to \infty$, the optimal error exponent for the detection scheme as given in (6) is the Kullback-Leibler divergence (KLD) [25] between the distributions $P(\mathbf{Z}|H_0)$ and $P(\mathbf{Z}|H_1)$. The summation term in (7) follows from the additive property of the KLD for independent distributions. ∎

Note that, (7) can be compactly written as $\sum_{k=1}^{K} N_k D_k(\pi_{j,1}^k || \pi_{j,0}^k)$ with $D_k(\pi_{j,1}^k || \pi_{j,0}^k)$ being the KLD between the data coming from node i at level k under H_0 and H_1. The FC wants to maximize the detection performance, while, the Byzantine attacker wants to degrade the detection performance as much as possible which can be achieved by maximizing and minimizing the KLD, respectively. Next, we explore the optimal attacking strategies for the Byzantines that degrade the detection performance most by minimizing the KLD.

III. Optimal Byzantine Attack

As discussed earlier, the Byzantines attempt to make the KL divergence as small as possible or to blind the FC. We say that the FC is blind if an adversary can make the data that the FC receives from the sensors such that no information is conveyed. In other words, the optimal detector at the FC cannot perform better than simply making the decision based on priors. Since the KLD is always non-negative, Byzantines attempt to choose $P(z_i = j|H_0, k)$ and $P(z_i = j|H_1, k)$ such that $D_k = 0, \ \forall k$. This is possible when

$$P(z_i = j|H_0, k) = P(z_i = j|H_1, k) \quad \forall j \in \{0, 1\}, \forall k. \quad (8)$$

Notice that, $\pi_{j,0}^k = P(z_i = j|H_0, k)$ and $\pi_{j,1}^k = P(z_i = j|H_1, k)$ can be expressed as

$$\pi_{1,0}^k = \beta_{1,0}^k (1 - P_{fa}^k) + (1 - \beta_{0,1}^k) P_{fa}^k \quad (9)$$

$$\pi_{1,1}^k = \beta_{1,0}^k (1 - P_d^k) + (1 - \beta_{0,1}^k) P_d^k. \quad (10)$$

with $\beta_{1,0}^k = \sum_{j=1}^{k} \alpha_j P_{1,0}^j$ and $\beta_{0,1}^k = \sum_{j=1}^{k} \alpha_j P_{0,1}^j$. Substituting (9) and (10) in (8) and after simplification, the condition to make the $D = 0$ for a K-level network becomes $\sum_{j=1}^{k} \alpha_j (P_{1,0}^j + P_{0,1}^j) = 1, \ \forall k$. Notice that, when $\sum_{j=1}^{k} \alpha_j < 0.5$, there does not exist any attacking probability distribution $(P_{0,1}^j, P_{1,0}^j)$ that can make $D_k = 0$, and, therefore, the KLD cannot be made zero. In the case of $\sum_{j=1}^{k} \alpha_j = 0.5$, there exists a unique solution $(P_{0,0}^j, P_{1,0}^j) = (1, 1), \forall j$ that can make $D_k = 0, \ \forall k$. For the $\sum_{j=1}^{k} \alpha_j > 0.5$ case, there exist infinitely many attacking probability distributions $(P_{0,1}^j, P_{1,0}^j)$ which can make $D_k = 0, \ \forall k$. Thus, we have the following result.

Lemma 2: In a tree network with K levels, the minimum number of Byzantines needed to make the Kullback-Leibler divergence (KLD) between the distributions $P(\mathbf{Z}|H_0)$ and $P(\mathbf{Z}|H_1)$ equal to zero (or to make $D_k = 0, \ \forall k$) is given by $B_1 = \left\lceil \frac{N_1}{2} \right\rceil$.

Proof: The proof follows from the fact that the condition $\sum_{j=1}^{k} \alpha_j = 0.5, \ \forall k$, is equivalent to $\alpha_1 = 0.5, \ \alpha_k = 0, \ \forall k = 2, \cdots, K$. ∎

Next, we explore the optimal attacking probability distribution $(P_{0,1}^k, P_{1,0}^k)$ that minimizes D_k when $\sum_{j=1}^{k} \alpha_j < 0.5$, i.e., in the case where the attacker cannot make $D = 0$. To analyze the problem, first we investigate the properties of D_k with respect to $(P_{0,1}^k, P_{1,0}^k)$ assuming $(P_{0,1}^j, P_{1,0}^j)$, $1 \leq j \leq k-1$ to be fixed. We show that attacking with symmetric flipping probabilities is the optimal strategy in the region where the attacker cannot make $D_k = 0$. In other words, attacking with $P_{1,0}^k = P_{0,1}^k$ is the optimal strategy for the Byzantines.

Lemma 3: In the region where the attacker cannot make $D_k = 0$, i.e., for $\sum_{j=1}^{k} \alpha_j < 0.5$, the optimal attacking strategy comprises of symmetric flipping probabilities $(P_{0,1}^k = P_{1,0}^k = p)$. In other words, any non zero deviation $\epsilon_i \in (0, p]$ in flipping probabilities $(P_{0,1}^k, P_{1,0}^k) = (p - \epsilon_1, p - \epsilon_2)$, where $\epsilon_1 \neq \epsilon_2$, will result in an increase in D_k.

Proof: Please see Appendix A. ∎

In the next theorem, we present the solution for the optimal attacking probability distribution $(P_{j,1}^k, P_{j,0}^k)$ that minimizes D_k in the region where the attacker cannot make $D_k = 0$.

Theorem 1: In the region where the attacker cannot make $D_k = 0$, i.e., for $\sum_{j=1}^{k} \alpha_j < 0.5$, the optimal attacking strategy is given by $(P_{0,1}^k, P_{1,0}^k) = (1, 1)$.

Proof: Observe that, in the region where the attacker cannot make $D_k = 0$, the optimal strategy comprises of symmetric flipping probabilities $(P_{0,1}^k = P_{1,0}^k = p)$. The proof is complete if we show that D_k is a monotonically decreasing function of the flipping probability p.

After plugging in $(P_{0,1}^k, P_{1,0}^k) = (p, p)$ in (9) and (10), we get

$$\pi_{1,1}^k = [\beta_{1,0}^{k-1}(1 - P_d^k) + (1 - \beta_{0,1}^{k-1}) P_d^k] + [\alpha_k (p - P_d^k(2p)) + P_d^k] \quad (11)$$

$$\pi_{1,0}^k = [\beta_{1,0}^{k-1}(1 - P_{fa}^k) + (1 - \beta_{0,1}^{k-1}) P_{fa}^k] + [\alpha_k (p - P_{fa}^k(2p)) + P_{fa}^k]. \quad (12)$$

Now we show that D_k is a monotonically decreasing function of the parameter p or in other words, $\frac{dD_k}{dp} < 0$. After plugging in $\pi_{1,1}^{k'} = \alpha_k (1 - 2P_d^k)$ and $\pi_{1,0}^{k'} = \alpha_k (1 - 2P_{fa}^k)$ in the expression of $\frac{dD_k}{dp}$ and rearranging the terms, the condition $\frac{dD_k}{dp} < 0$ becomes

$$(1 - 2P_d^k) \left(\frac{1 - \pi_{1,0}^k}{1 - \pi_{1,1}^k} - \frac{\pi_{1,0}^k}{\pi_{1,1}^k} \right) + (1 - 2P_{fa}^k) \log \left(\frac{1 - \pi_{1,1}^k}{1 - \pi_{1,0}^k} \frac{\pi_{1,0}^k}{\pi_{1,1}^k} \right) < 0 \quad (13)$$

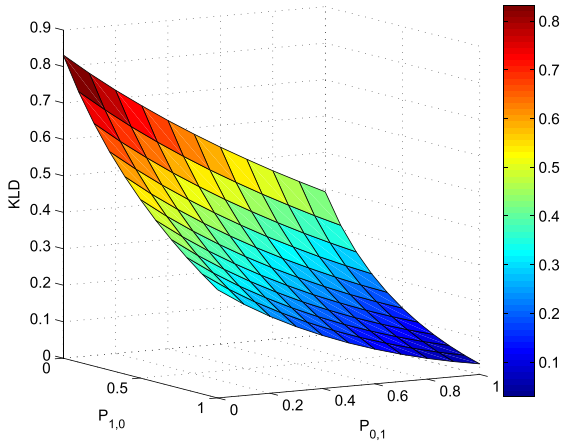

Fig. 2. KLD D_k vs. flipping probabilities when $P_d^k = 0.8$, $P_{fa}^k = 0.2$, and the probability that the bit coming from level k encounters a Byzantine is $\sum_{j=1}^{k} \alpha_j = 0.4$.

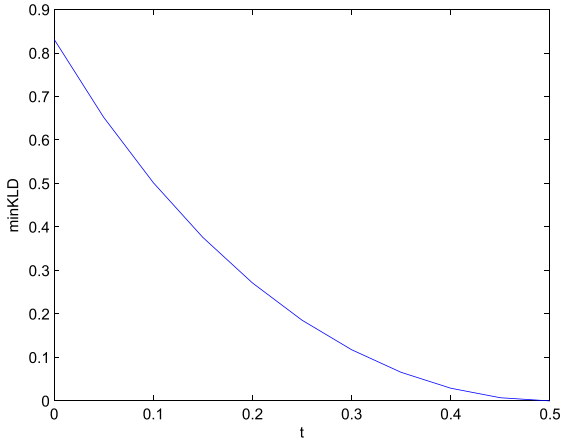

Fig. 3. $\min_{(P_{j,1}^k, P_{j,0}^k)} D_k$ vs probability that the bit coming from level k encounters a Byzantine for $P_d^k = 0.8$ and $P_{fa}^k = 0.2$.

Since $P_d^k > P_{fa}^k$ and $\beta_{\tilde{x},x}^k < 0.5$, we have $\pi_{1,1}^k > \pi_{1,0}^k$. Now, using the fact that $\frac{1-P_d^k}{1-P_{fa}^k} > \frac{1-2P_d^k}{1-2P_{fa}^k}$ and (33), we have

$$\frac{1-2P_d^k}{1-2P_{fa}^k}\left[\frac{1-\pi_{1,0}^k}{1-\pi_{1,1}^k} - \frac{\pi_{1,0}^k}{\pi_{1,1}^k}\right] < (\pi_{1,1}^k - \pi_{1,0}^k)\left[\frac{1}{\pi_{1,1}^k} + \frac{1}{1-\pi_{1,0}^k}\right]$$

$$\Leftrightarrow \frac{1-2P_d^k}{1-2P_{fa}^k}\left[\frac{1-\pi_{1,0}^k}{1-\pi_{1,1}^k} - \frac{\pi_{1,0}^k}{\pi_{1,1}^k}\right] + \left[\frac{\pi_{1,0}^k}{\pi_{1,1}^k} - 1\right] < 1 - \frac{1-\pi_{1,1}^k}{1-\pi_{1,0}^k}. \quad (14)$$

Applying the logarithm inequality $(x-1) \geq \log x \geq \frac{x-1}{x}$, for $x > 0$ to (14), one can prove that (13) is true. ■

Next, to gain insights into the solution, we present some numerical results in Figure 2. We plot D_k as a function of the flipping probabilities $(P_{1,0}^k, P_{0,1}^k)$. We assume that the probability of detection is $P_d^k = 0.8$, the probability of false alarm is $P_{fa}^k = 0.2$, and the probability that the bit coming from level k encounters a Byzantine is $\sum_{j=1}^{k} \alpha_j = 0.4$. We also assume that $P_{0,1}^k = P_{0,1}$ and $P_{1,0}^k = P_{1,0}, \forall k$. It can be seen that the optimal attacking strategy comprises of symmetric flipping probabilities and is given by $(P_{0,1}^k, P_{1,0}^k) = (1, 1)$, which corroborates our theoretical result presented in Lemma 3 and Theorem 1.

We have shown that, for all k,

$$D_k(P_{0,1}^k, P_{1,0}^k) \geq D_k(1, 1). \quad (15)$$

Now, by multiplying both sides of (15) by N_k and summing it over all K we can show that the KLD, D, is minimized by $(P_{0,1}^k, P_{1,0}^k) = (1, 1)$, for all k, in the region $\sum_{k=1}^{K} \alpha_k < 0.5$.

Now, we explore some properties of D_k with respect to $\sum_{j=1}^{k} \alpha_j$ in the region where the attacker cannot make $D_k = 0$, i.e., for $\sum_{j=1}^{k} \alpha_j < 0.5$. This analysis will later be used in exploring the problem from the network designer's perspective.

Lemma 4: $D_k^* = \min_{(P_{j,1}^k, P_{j,0}^k)} D_k(\pi_{j,1}^k || \pi_{j,0}^k)$ is a continuous, decreasing and convex function of $\sum_{j=1}^{k} \alpha_j$ for $\sum_{j=1}^{k} \alpha_j < 0.5$.

Proof: The continuity of $D_k(\pi_{j,1}^k || \pi_{j,0}^k)$ with respect to the involved distributions implies the continuity of D_k^*. To show that D_k^* is a decreasing function of $t = \sum_{j=1}^{k} \alpha_j$, we use the fact that $\arg\min_{(P_{0,1}^k, P_{1,0}^k)} D_k(\pi_{j,1}^k || \pi_{j,0}^k)$ is equal to $(1, 1)$ for $\sum_{j=1}^{k} \alpha_j < 0.5$ (as shown in Theorem 1). After plugging $(P_{0,1}^k, P_{1,0}^k) = (1, 1)$, $\forall k$, in the KLD expression, it can be shown that $\frac{dD_k}{dt} < 0$. Hence, D_k^* is a monotonically decreasing function of $\sum_{j=1}^{k} \alpha_j$ for $\sum_{j=1}^{k} \alpha_j < 0.5$. The convexity of D_k^* follows from the fact that $D_k^*(\pi_{j,1}^k || \pi_{j,0}^k)$ is convex in $\pi_{j,1}^k$ and $\pi_{j,0}^k$, which are affine transformations of $\sum_{j=1}^{k} \alpha_j$ (Note that, convexity holds under affine transformation). ■

It is worth noting that Lemma 4 suggests that minimization/maximization of $\sum_{j=1}^{k} \alpha_j$ is equivalent to minimization/maximization of D_k. Using this fact, one can consider the probability that the bit coming from level k encounters a Byzantine (i.e., $t = \sum_{j=1}^{k} \alpha_j$) in lieu of D_k for optimizing the system performance.

Next, to gain insights into the solution, we present some numerical results in Figure 3. We plot $\min_{(P_{j,1}^k, P_{j,0}^k)} D_k$ as a function of the probability that the bit coming from level k encounters a Byzantine, i.e., t. We assume that the probabilities of detection and false alarm are $P_d^k = 0.8$ and $P_{fa}^k = 0.2$, respectively. Notice that, when $t = 0.5$, D_k between the two probability distributions becomes zero. It is seen that D_k^* is a continuous, decreasing and convex function of the fraction of covered nodes, t, for $t < 0.5$, which corroborates our theoretical result presented in Lemma 4.

Until now, we have explored the problem from the attacker's perspective. In the rest of the paper, we look into the problem from a network designer's perspective and propose techniques to mitigate the effect of Byzantines. First, we study the problem of designing optimal distributed detection parameters in a tree network in the presence of Byzantines.

IV. System Design in the Presence of Byzantines

For a fixed attack configuration $\{B_k\}_{k=1}^K$, the detection performance at the FC is a function of the local detectors used at the nodes in the tree network and the global detector used at the FC. This motivates us to study the problem of designing detectors, both at the nodes at different levels in a tree and at the FC, such that the detection performance is maximized. More specifically, we are interested in answering the question: How does the knowledge of the attack configuration $\{B_k\}_{k=1}^K$ affect the design of optimal distributed detection parameters?

By Stein's lemma [19], we know that in the NP setup for a fixed false alarm probability, the missed detection probability of the optimal detector can be minimized by maximizing the KLD. For an optimal detector at the FC, the problem of designing the local detectors can be formalized as follows:

$$\max_{\{P_d^k, P_{fa}^k\}_{k=1}^K} \sum_{k=1}^{K} N_k \sum_{j\in\{0,1\}} P(z_i = j|H_0, k) \log \frac{P(z_i = j|H_0, k)}{P(z_i = j|H_1, k)}. \tag{16}$$

The local detector design problem as given in (16) is a non-linear optimization problem. Furthermore, it is difficult to obtain a closed form solution for this problem. Next, we show that likelihood ratio tests remain optimal (under the conditional independence assumption) even in the presence of Byzantines and optimal decision rule for each node is independent of Byzantines' parameters.[8] To solve the problem, we need to find the pairs $\{P_d^k, P_{fa}^k\}_{k=1}^K$ which maximize the objective function as given in (16). However, P_d^k and P_{fa}^k are coupled and, therefore, cannot be optimized independently. Thus, we first analyze the problem of maximizing the KLD for a fixed P_{fa}^k. We assume that $P_{fa}^k = y_k$ and $P_d^k = y_k + x_k$. Next, we analyze the properties of KLD with respect to x_k, i.e., $(P_d^k - P_{fa}^k)$ in the region where attacker cannot blind the FC, i.e., for $\sum_{j=1}^k \alpha_j < 0.5$, in order to study the local detector design problem. Notice that, in the region $\sum_{j=1}^k \alpha_j \geq 0.5$, $D_k = 0$ and optimizing over local detectors does not improve the performance.

Lemma 5: For a fixed $P_{fa}^k = y_k$, when $\sum_{j=1}^k \alpha_j < 0.5$, the KLD, D, as given in (7) is a monotonically increasing function of $x_k = (P_d^k - P_{fa}^k)$.

Proof: To prove this, we calculate the partial derivative of D with respect to x_k. By substituting $P_{fa}^k = y_k$ and $P_d^k = y_k + x_k$ into (7), the partial derivative of D with respect to x_k can be calculated as

$$\frac{\partial D}{\partial x_k} = N_k \frac{\partial}{\partial x_k}\left[\pi_{1,0}^k \log\frac{\pi_{1,0}^k}{\pi_{1,1}^k} + (1-\pi_{1,0}^k)\log\frac{1-\pi_{1,0}^k}{1-\pi_{1,1}^k}\right]$$

$$\Leftrightarrow \frac{\partial D}{\partial x_k} = N_k \pi_{1,1}^{k'}\left(\frac{1-\pi_{1,0}^k}{1-\pi_{1,1}^k} - \frac{\pi_{1,0}^k}{\pi_{1,1}^k}\right),$$

where $\pi_{1,0}^k$ and $\pi_{1,1}^k$ are as given in (9) and (10), respectively and $\pi_{1,1}^{k'} = (1 - \beta_{0,1}^k - \beta_{1,0}^k)$. Notice that,

$$\left(\frac{1-\pi_{1,0}^k}{1-\pi_{1,1}^k} - \frac{\pi_{1,0}^k}{\pi_{1,1}^k}\right) > 0 \Leftrightarrow \pi_{1,1}^k > \pi_{1,0}^k.$$

Thus, the condition to make $\frac{\partial D}{\partial x_k} > 0$ simplifies to

$$\pi_{1,1}^{k'} > 0 \Leftrightarrow 1 > (\beta_{0,1}^k + \beta_{1,0}^k) \tag{17}$$

Substituting the values of $\beta_{1,0}^k$ and $\beta_{1,1}^k$, the above condition can be written as:

$$\sum_{j=1}^{k} \alpha_j P_{1,0}^j + \sum_{j=1}^{k} \alpha_j P_{0,1}^j < 1 \tag{18}$$

$$\Leftrightarrow \sum_{j=1}^{k} \alpha_j (P_{1,0}^j + P_{0,1}^j) < 1 \tag{19}$$

The above condition is true for any $0 \leq P_{0,1}^j, P_{1,0}^j \leq 1$ when $\sum_{j=1}^k \alpha_j < 0.5$. This completes the proof. ∎

Lemma 5 suggests that one possible solution to maximize D is to choose the largest possible x_k constrained to $0 \leq x_k \leq 1 - y_k$. The upper bound results from the fact that $\{P_d^k, P_{fa}^k\}_{k=1}^K$ are probabilities and, thus, must be between zero and one. In other words, the solution is to maximize the probability of detection for a fixed value of probability of false alarm. In detection theory, it is well known that the likelihood ratio based test is optimum for this criterion. Thus, under the conditional independence assumption, the likelihood ratio based test as given in (6) is optimal for local nodes, even in the presence of Byzantines, and the optimal operating points $\{P_d^{k*}, P_{fa}^{k*}\}_{k=1}^K$ are independent of the Byzantines' parameters $\{\alpha_k\}_{k=1}^K$.

The above result has the following important consequences: 1) search space is reduced from any arbitrary detector to likelihood ratio based detectors, 2) the threshold in the LRT can be optimized without any prior knowledge about the Byzantines' parameters $\{\alpha_k\}_{k=1}^K$. We further explore the problem from the network designer's (FC) perspective. In our previous analysis, we have assumed that the attack configuration $\{B_k\}_{k=1}^K$ is known and shown that the optimal local detector is independent of $\{\alpha_k\}_{k=1}^K$. However, notice that the KLD is the exponential decay rate of the error probability of the optimal detector. In other words, while optimizing over KLD, we implicitly assumed that the optimal detector, which is a likelihood ratio based detector, is used at the FC. Taking logarithm on both sides of (6), the optimal decision rule simplifies to

$$\sum_{k=1}^{K} [a_1^k s_k + a_0^k (N_k - s_k)] \underset{H_0}{\overset{H_1}{\gtrless}} \log \eta \tag{20}$$

where the optimal weights are given by $a_1^k = \log\frac{\pi_{1,1}^k}{\pi_{1,0}^k}$ and $a_0^k = \log\frac{1-\pi_{1,1}^k}{1-\pi_{1,0}^k}$. To implement the optimal detector, the FC needs to know the optimal weights a_j^k, which are functions of $\{\alpha_k\}_{k=1}^K$. In the next section, we are interested in answering

[8] In other words, under the assumption of conditional independence, an optimal decision rule for each node takes the form of a likelihood ratio test (LRT), with a suitably chosen threshold. In turn, optimization over the set of all thresholds can yield the desired solution.

the question: Is it possible for the FC to predict the attack configuration $\{B_k\}_{k=1}^K$ in the tree? The knowledge of this attack configuration can be used for determining the optimal detector at the FC to improve the system performance. Notice that, learning/estimation based techniques can be used on data to determine the attack configuration. However, the FC has to acquire a large amount of data coming from the nodes over a long period of time to accurately estimate $\{B_k\}_{k=1}^K$.

In the next section, we propose a novel technique to predict the attack configuration by considering the following scenario: The FC, acting first, commits to a defensive strategy by deploying the defensive resources to protect the tree network, while the attacker chooses its best response or attack configuration after surveillance of this defensive strategy. Both, the FC and the Byzantines have to incur a cost to deploy the defensive resources and attack the nodes in the tree network, respectively. We consider both the FC and the attacker to be strategic in nature and model the strategic interaction between them as a Leader-Follower (Stackelberg) game. This formulation provides a framework for identifying attacker and defender (FC) equilibrium strategies, which can be used to implement the optimal detector. The main advantage of this technique is that the equilibrium strategies can be determined *a priori* and, therefore, there is no need to observe a large amount of data coming from the nodes over a long period of time to accurately estimate $\{B_k\}_{k=1}^K$.

V. Stackelberg Game for Attack Configuration Prediction Problems

We model the strategic interaction between the FC and the attacker as a Leader-Follower (Stackelberg) game. We assume that the FC has to incur a cost for deploying the network and the Byzantine has to incur a cost[9] for attacking the network. It is assumed that the network designer or the FC has a cost budget $C_{budget}^{network}$ and the attacker has a cost budget $C_{budget}^{attacker}$[10]. More specifically, the FC wants to allocate the best subset of defensive resources (denoted as $\{\tilde{c}_k\}_{k=1}^K$)[11] from a set of available defensive resources $\mathbb{C} = (c_1, \cdots, c_n)$ (arranged in a descending order, i.e., $c_1 \geq c_2 \cdots \geq c_n$), where $n \geq K$, complying with its budget constraint $C_{budget}^{network}$ to different levels of the tree network. After the FC allocates the defensive resources or budget to different levels of the tree network, an attacker chooses an attack configuration, $\{B_k\}_{k=1}^K$ complying with his budget constraint $C_{budget}^{attacker}$ to maximally degrade the performance of the network.

Next, we formalize the Stackelberg game as a bi-level optimization problem. For our problem, the upper level problem (ULP) corresponds to the FC who is the leader of the game, while the lower level problem (LLP) belongs to the attacker who is the follower.

$$\begin{aligned}
&\underset{\{\tilde{c}_k\}_{k=1}^K \in \mathbb{C}}{\text{maximize}} \; D(\{\tilde{c}_k\}_{k=1}^K) \\
&\text{subject to} \sum_{k=1}^K \tilde{c}_k N_k \leq C_{budget}^{network} \\
&\underset{B_k \in \mathbb{Z}^+}{\text{minimize}} \; D(\{B_k\}_{k=1}^K) \\
&\text{subject to} \sum_{k=1}^K \tilde{c}_k B_k \leq C_{budget}^{attacker} \\
&\qquad 0 \leq B_k \leq N_k, \quad \forall\, k = 1, 2, \ldots, K
\end{aligned} \tag{21}$$

where $\mathbb{Z}^+$ is the set of non-negative integers. Notice that the bi-level optimization problem, in general, is an NP-hard problem. In fact, the LLP is a variant of the packing formulation of the bounded knapsack problem with a non-linear objective function. This is, in general, NP-hard. Using existing algorithms, cost set $\{\tilde{c}_k\}_{k=1}^K$ and attack configuration $\{B_k\}_{k=1}^K$ can be determined at the cost of computational efficiency. In this paper, we identify a special case of the above problem which can be solved in polynomial time to determine the equilibrium strategies. To solve the bi-level optimization problem, we first solve the LLP assuming the solution of the ULP to be some fixed $(\tilde{c}_1, \cdots, \tilde{c}_K)$. This approach will give us a structure of the optimal $\{B_k\}_{k=1}^K$ for any arbitrary $\{\tilde{c}_k\}_{k=1}^K$. Next, using the structure of the optimal $\{B_k\}_{k=1}^K$, the bi-level optimization problem simplifies to finding the solution $\{\tilde{c}_k\}_{k=1}^K$ of the ULP. Finally, we present a polynomial time algorithm to solve the bi-level optimization problem, i.e., to find $\{\tilde{c}_k\}_{k=1}^K$ and, thus, $\{B_k\}_{k=1}^K$.

Next, we discuss the relationships that enable our problem to have a polynomial time solution. We define profit $P(S)$ of an attack configuration $S = \{B_k\}_{k=1}^K$ as follows[12]

$$P(S) = D(\phi) - D(S) = D(\phi) - D(\{B_k\}_{k=1}^K),$$

where $D(\phi)$ is the KLD when there are no Byzantines in the network and $D(S) = D(\{B_k\}_{k=1}^K)$ is the KLD with $\{B_k\}_{k=1}^K$ Byzantines in the tree network. Next, we define the concept of dominance which will be used later to explore some useful properties of the optimal attack configuration $\{B_k\}_{k=1}^K$.

Definition 1: We say that a set S_1 dominates another set S_2 if

$$P(S_1) \geq P(S_2) \quad \text{and} \quad C(S_1) \leq C(S_2), \tag{22}$$

where $P(S_i)$ and $C(S_i)$ denote the profit and cost incurred by using set S_i, respectively. If in (22), $P(S_1) > P(S_2)$, S_1 strictly dominates S_2 and if $P(S_1) = P(S_2)$, S_1 weakly dominates S_2.

[9]Due to variations in hardware complexity and the level of tamper-resistance present in nodes residing at different levels of the tree, the resources required to capture and tamper nodes at different levels may be different and, therefore, nodes have varying costs of being attacked.

[10]In this paper, we assume that the attacker budget $C_{budget}^{attacker}$ is such that $\sum_{k=1}^K \alpha_k < 0.5$, i.e., the attacker cannot make $D_k = 0$, $\forall k$. Notice that, if the attacker can make $D_k = 0$ for some $k = l$, then, it can also make $D_k = 0$, $\forall k \geq l$. Also, $D_k = 0$ implies that $\pi_{1,1}^k = \pi_{1,0}^k$ and, therefore, the weights (a_1^k, a_0^k) in (20) are zero. In other words, the best the FC can do in the case when $D_k = 0$, $\forall k \geq l$ is to ignore or discard the decisions of the nodes residing at level $k \geq l$. This scenario is equivalent to using the tree network with $(l-1)$ levels for distributed detection.

[11]Let $\tilde{c}_k$ denote the resources deployed or budget allocated by the FC to protect or deploy a node at level k.

[12]In this section, we assume that the optimal operating point, i.e., (P_d^{k*}, P_{fa}^{k*}), is the same for all the nodes in the tree network. It has been shown that the use of identical thresholds is asymptotically optimal for parallel networks [26]. We conjecture that this result is valid for tree networks as well and employ identical thresholds.

To solve the bi-level optimization problem, we first solve the LLP assuming the solution of the ULP to be some fixed $(\tilde{c}_1, \cdots, \tilde{c}_K)$. We refer to LLP as a maximum damage Byzantine attack problem. Observe that, knowing that the FC chooses $(\tilde{c}_1, \cdots, \tilde{c}_K)$, the LLP can be reformulated as follows:

$$\begin{aligned} \underset{B_k \in \mathbb{Z}^+}{\text{minimize}} \ & \sum_{k=1}^{K} N_k D_k(\{B_i\}_{i=1}^{k}) \\ \text{subject to} & \sum_{k=1}^{K} \tilde{c}_k B_k \leq C_{budget}^{attacker} \\ & 0 \leq B_k \leq N_k, \quad \forall k = 1, \cdots, K. \end{aligned}$$

We discuss the relationships that enable maximum damage Byzantine attack problem to admit a polynomial time solution.

A. Analysis of the Optimal Attack Configuration

In this section, we identify a special case of the bounded knapsack problem (LLP) which can be solved in polynomial time. More specifically, we show that if the set of defensive resources $\mathbb{C} = (c_1, \cdots, c_n)$ satisfy the cost structure $c_{max} \leq \left(\min_{k \in \{1, \cdots, K-1\}} \frac{N_{k+1}}{N_k} \right) \times c_{min}$[13] or $c_1 \leq \min_k a_k \times c_n$, then, the optimal solution $\{B_k\}_{k=1}^{K}$ exhibits the properties given in the lemma below.

Lemma 6: Given a K level tree network with cost structure satisfying $c_{max} \leq \left(\min_{k \in \{1, \cdots, K-1\}} \frac{N_{k+1}}{N_k} \right) \times c_{min}$, the best response of an attacker with cost budget $C_{budget}^{attacker}$ is $\{B_k\}_{k=1}^{K}$ with

$$B_1 = \left\lfloor \frac{C_{budget}^{attacker}}{\tilde{c}_1} \right\rfloor$$

and the remaining elements of B_k for $2 \leq k \leq K$ can be calculated recursively.

Proof: Please see Appendix B. ∎

It can also be shown that the solution $\{B_k\}_{k=1}^{K}$ will be non-overlapping and unique under the condition that the attacker cannot make $D_k = 0, \ \forall k$.

B. Bi-Level Optimization Algorithm

Based on Lemma 6, in this section we will present a polynomial time algorithm to solve the bi-level optimization problem, i.e., to find $\{\tilde{c}_k\}_{k=1}^{K}$ and $\{B_k\}_{k=1}^{K}$. Using the cost structure $c_{max} \leq \left(\min_k \frac{N_{k+1}}{N_k} \right) \times c_{min}$, the attack configuration $\{B_k\}_{k=1}^{K}$ as given in Lemma 6 can be determined in a computationally efficient manner. Due to the structure of the optimal $\{B_k\}_{k=1}^{K}$, the bi-level optimization problem simplifies to finding the solution $\{\tilde{c}_k\}_{k=1}^{K}$ of the ULP.

To solve this problem, we use an iterative elimination approach. We start by listing all $\binom{n}{K}$ combinations from the set $\mathbb{C}$, denoted as, $S = \{s_i\}_{i=1}^{\binom{n}{K}}$. Without loss of generality, we assume that the elements of $s_i = \{c_1^i, \cdots, c_K^i\}$ are arranged in descending order, i.e., $c_k^i \geq c_{k+1}^i, \forall k$. Notice that, all these $\binom{n}{K}$ combinations will satisfy $c_k^i \leq \frac{N_{k+1}}{N_k} c_{k+1}^i$, because

$$c_k^i \leq c_{max} \leq \min_j \frac{N_{j+1}}{N_j} c_{min} \leq \min_j \frac{N_{j+1}}{N_j} c_{k+1}^i \leq \frac{N_{k+1}}{N_k} c_{k+1}^i.$$

Next, we discard all those subsets s_i from S which violate the network designer's cost budget constraint. If the set S is empty, then there does not exist any solution for the ULP. Otherwise, the problem reduces to finding the subset s_i which maximizes the KLD. To find the subset s_i which maximizes the KLD, using the dominance relationship we start with assigning the cost $\tilde{c}_1 = \min_{k \in s} c_1^k$, where s has the elements which are solutions of $\arg\min_i \left\lfloor \frac{C_{budget}^{attacker}}{c_1^i} \right\rfloor$. Next, we discard all those subsets s_i from S which do not have $\tilde{c}_1$ as their first element and solve the problem recursively.

The pseudo code of the polynomial time algorithm to find $\{\tilde{c}_k\}_{k=1}^{K}$ and $\{B_k\}_{k=1}^{K}$ is presented as Algorithm 1.

Algorithm 1 Bi-Level Optimization Algorithm

Require: $\mathbb{C} = \{c_k\}_{k=1}^{n}$ with $c_{max} \leq \left(\min_j \frac{N_{j+1}}{N_j} \right) \times c_{min}$

$S \leftarrow$ All K out of n combinations $\{s_i\}_{i=1}^{\binom{n}{K}}$ with elements of s_i arranged in decreasing order
for $i = 1$ **to** $\binom{n}{K}$ **do**
  if $\sum_{k=1}^{K} c_k^i \times N_k > C_{budget}^{network}$ **then**
    $S \leftarrow S / s_i$
  end if
end for
if S is an empty set **then**
  return $(\phi, \ \phi)$
else
  for $k = 1$ **to** K **do**
    $\tilde{c}_k = \min_{j \in s} c_k^j$ where s has elements which are solutions of $\arg\min_i \left\lfloor \frac{C_{budget}^{attacker}}{c_k^i} \right\rfloor$
    $B_k \leftarrow \left\lfloor \frac{C_{budget}^{attacker}}{\tilde{c}_k} \right\rfloor$
    $C_{budget}^{attacker} \leftarrow (C_{budget}^{attacker} - \tilde{c}_k B_k)$
  end for
  return $(\{\tilde{c}_k\}_{k=1}^{K}, \ \{B_k\}_{k=1}^{K})$
end if

C. An Illustrative Example

Let us consider a two-level network with $N_1 = 6$ and $N_2 = 12$. We assume that $\mathbb{C} = \{4, \ 3, \ 2\}$, $C_{budget}^{network} = 60$ and $C_{budget}^{attacker} = 11$. Next, we solve the bi-level optimization problem. Observe that, costs satisfy $c_1 \leq 2 \times c_3$. So the algorithm chooses the solution of the ULP as $(\tilde{c}_1 = 4, \ \tilde{c}_2 = 3)$ and the solution of the LLP as $(B_1 = \lfloor \frac{11}{4} \rfloor = 2, \ B_2 = \lfloor \frac{11 - 2 \times 4}{3} \rfloor = 1)$. To corroborate these results, in Figure 4, we plot the $\min_{P_{1,0}, P_{0,1}}$ KLD for all combinations of

[13] Notice that, in the case of the perfect M-ary tree networks, the proposed cost structure simplifies to $c_{max} \leq M \times c_{min}$.

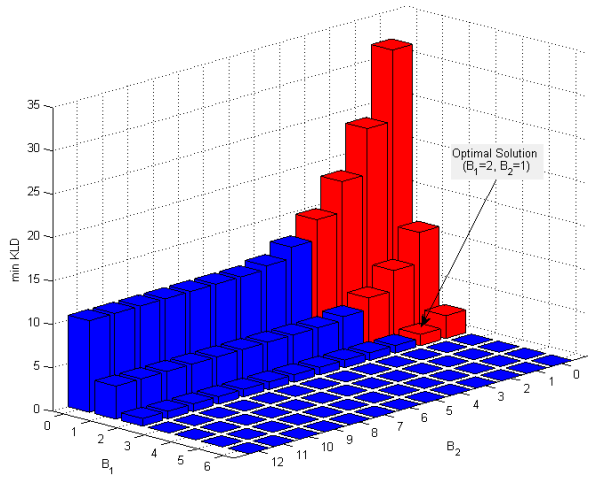

Fig. 4. min KLD vs. attack configuration (B_1, B_2) for $P_d = 0.9$, $P_{fa} = 0.1$.

the parameters B_1 and B_2 in the tree. We vary the parameter B_1 from 0 to 6 and B_2 from 0 to 12. All the feasible solutions are plotted in red and unfeasible solutions are plotted in blue. Figure 4 corroborates the results of our algorithm.

Notice that, the attack configuration $\{B_k\}_{k=1}^{K}$ is the set containing the *number* of Byzantines residing at different levels of the tree. However, the FC cannot identify the Byzantines in the network. Also, notice that when the adversary attacks more than 50% of the nodes at level 1, the decision fusion scheme becomes completely incapable. In these scenarios, where the FC is blind, the knowledge of attack configuration will not incur any performance benefit. Next, we present a reputation-based Byzantine identification/mitigation scheme, which works even when the network is blind, in order to improve the detection performance of the network. We propose a simple yet efficient Byzantine identification scheme and analyze its performance.

VI. An Efficient Byzantine Identification Scheme

In this section, we propose and analyze a Byzantine identification scheme to be implemented at the FC.

A. Byzantine Identification Scheme

We assume that the FC has the knowledge of the attack model and utilizes this knowledge to identify the Byzantines. The FC observes the local decisions of each node over a time window T, which can be denoted by $(k,i) = [u_1(k,i), \ldots, u_T(k,i)]$ for $1 \leq i \leq N_k$ at level $1 \leq k \leq K$. We also assume that there is one honest anchor node with probability of detection P_d^A and probability of false alarm P_{fa}^A present and known to the FC. We employ the anchor node to provide the gold standard which is used to detect whether or not other nodes are Byzantines. The FC can also serve as an anchor node when it can directly observe the phenomenon and make a decision. We denote the Hamming distance between reports of the anchor node and an honest node i at level k over the time window T by $d_H^A(k,i) = ||U^A - U^H(k,i)||$, that is the number of elements that are different between U^A and $U^H(k,i)$. Similarly, the Hamming distance between the reports of the anchor node and a Byzantine node i at level k over the time window T is denoted by $d_B^A(k,i) = ||U^A - U^B(k,i)||$. Since the FC is aware of the fact that Byzantines might be present in the network, it compares the Hamming distance of a node i at level k to a threshold η_k, $\forall i, \forall k$ (a procedure to calculate η_k is discussed later in the paper), to make a decision to identify the Byzantines. In tree networks, a Byzantine node alters its decision as well as received decisions from its children prior to transmission in order to undermine the network performance. Therefore, solely based on the observed data of a node i at level k, the FC cannot determine whether the data has been flipped by the node i itself or by one of its Byzantine parent node. In our scheme, the FC makes the inference about a node being Byzantine by analyzing the data from the node i as well as its predecessor nodes' data. FC starts from the nodes at level 1 and computes the Hamming distance between reports of the anchor node and the nodes at level 1. FC declares node i at level 1 to be a Byzantine if and only if the Hamming distance of node i is greater than a fixed threshold η_1. Children of identified Byzantine nodes $\mathbb{C}(\mathbb{B}_1)$ are not tested further because of the non-overlapping condition. However, if a level 1 node is determined not to be a Byzantine, then, the FC tests its children nodes at level 2. The FC declares node i at level k, for $2 \leq k \leq K$, to be a Byzantine if and only if the Hamming distance of node i is greater than a fixed threshold η_k and Hamming distances of all predecessors of node i is less than equal to their respective thresholds η_j.

In this way, it is possible to counter the data falsification attack by isolating Byzantine nodes from the information fusion process. The probability that a Byzantine node i at level k is isolated at the end of the time window T, is denoted as $P_B^{iso}(k,i)$.

B. Performance Analysis

As mentioned earlier, local decisions of the nodes are compared to the decisions of the anchor node over a time window of length T. The probability that an *honest* node i at level k makes a decision that is different from the anchor node is given by

$$\begin{aligned}
&P_{diff}^{AH}(k,i)\\
&= P(u_i^A = 1, u_{k,i}^H = 0, H_0) + P(u_i^A = 0, u_{k,i}^H = 1, H_0)\\
&\quad + P(u_i^A = 1, u_{k,i}^H = 0, H_1) + P(u_i^A = 0, u_{k,i}^H = 1, H_1)\\
&= P_0[(P_{fa}^k + P_{fa}^A) - 2P_{fa}^k P_{fa}^A] + P_1[(P_d^k + P_d^A) - 2P_d^k P_d^A]\\
&\doteq P_0[P_{diff}^{AH}(k,i,0)] + P_1[P_{diff}^{AH}(k,i,1)].
\end{aligned}$$

where the prior probabilities of the two hypotheses H_0 and H_1 are denoted by P_0 and P_1, respectively. The probability that a Byzantine node i at level k sends a decision different from that of the anchor node is given by

$$\begin{aligned}
&P_{diff}^{AB}(k,i)\\
&= P(u_i^A = 1, u_{k,i}^B = 0, H_0) + P(u_i^A = 0, u_{k,i}^B = 1, H_0)\\
&\quad + P(u_i^A = 1, u_{k,i}^B = 0, H_1) + P(u_i^A = 0, u_{k,i}^B = 1, H_1)\\
&= P_0[P_{fa}^A P_{fa}^k + (1 - P_{fa}^A)(1 - P_{fa}^k)]\\
&\quad + P_1[P_d^A P_d^k + (1 - P_d^A)(1 - P_d^k)]\\
&\doteq P_0[P_{diff}^{AB}(k,i,0)] + P_1[P_{diff}^{AB}(k,i,1)].
\end{aligned}$$

The difference between the reports of a node and the anchor node under hypothesis $l \in \{0, 1\}$ (i.e., $d_I^A(k,i,l),\ I \in \{H, B\}$) is a Bernoulli random variable with mean $P_{diff}^{AH}(k,i,l)$ for honest nodes and $P_{diff}^{AB}(k,i,l)$ for Byzantines. FC declares node i at level k to be a Byzantine if and only if the Hamming distance of node i is greater than a fixed threshold η_k and Hamming distances of all predecessors of node i are less than equal to their respective thresholds η_j. The probability that a Byzantine node i at level k is isolated at the end of the time window T can be expressed as

$$\begin{aligned}
&P_B^{iso}(k,i)\\
&= P\Big[(d_B^A(k,i) > \eta_k),\\
&\qquad (d_H^A(k-1,i) \le \eta_{k-1}), \cdots, (d_H^A(1,i) \le \eta_1)\Big]\\
&= \sum_{l\in\{0,1\}} P_l \left[P[d_B^A(k,i,l) > \eta_k] \prod_{m=1}^{k-1} P[d_H^A(m,i,l) \le \eta_m]\right]\\
&= \sum_{l\in\{0,1\}} P_l \sum_{j=\eta_k+1}^{T} \binom{T}{j} (P_{diff}^{AB}(k,i,l))^j (1-P_{diff}^{AB}(k,i,l))^{T-j}\\
&\quad \times \prod_{m=1}^{k-1} \left[\sum_{j=0}^{\eta_m} \binom{T}{j} (P_{diff}^{AH}(m,i,l))^j (1-P_{diff}^{AH}(m,i,l))^{T-j}\right].
\end{aligned}$$

For large T, by using the normal approximation, we get

$$\begin{aligned}
&P_B^{iso}(k,i)\\
&= \sum_{l\in\{0,1\}} P_l Q\left(\frac{\eta_k - T P_{diff}^{AB}(k,i,l)}{\sqrt{(T P_{diff}^{AB}(k,i,l)(1-P_{diff}^{AB}(k,i,l)))}}\right)\\
&\quad \times \prod_{m=1}^{k-1} Q\left(\frac{T P_{diff}^{AH}(m,i,l) - \eta_m}{\sqrt{(T P_{diff}^{AH}(m,i,l)(1-P_{diff}^{AH}(m,i,l)))}}\right).
\end{aligned}$$

This can be written recursively as follows

$$\begin{aligned}
&P_B^{iso}(k+1,i)\\
&= \sum_{l\in\{0,1\}} P_l \left[(1-b(k,l))\left(\frac{a(k+1,l)}{a(k,l)}\right) P_B^{iso}(k,i,l)\right],
\end{aligned} \tag{24}$$

with $P_B^{iso}(k,i) \doteq \sum_{l\in\{0,1\}} P_l[P_B^{iso}(k,i,l)]$, and

$$\begin{aligned}
a(k,l) &= Q\left(\frac{\eta_k - T P_{diff}^{AB}(k,i,l)}{\sqrt{(T P_{diff}^{AB}(k,i,l)(1-P_{diff}^{AB}(k,i,l)))}}\right),\\
b(k,l) &= Q\left(\frac{\eta_k - T P_{diff}^{AH}(k,i,l)}{\sqrt{(T P_{diff}^{AH}(k,i,l)(1-P_{diff}^{AH}(k,i,l)))}}\right).
\end{aligned}$$

One can choose η_k such that the isolation probability of honest nodes at level k based solely on its data under the hypothesis H_l (i.e., $b(k,l)$) is constrained to some value $\delta_k << 0.5$. In other words, we choose η_k such that $\max_{l\in\{0,1\}} b(k,l) = \delta_k$, i.e.,

$$\begin{aligned}
\eta_k = {} & Q^{-1}(\delta_k)\sqrt{T P_{diff}^{AH}(k,i,l^*)(1-P_{diff}^{AH}(k,i,l^*))}\\
&+ T P_{diff}^{AH}(k,i,l^*)
\end{aligned} \tag{25}$$

where $l^* = \arg\max_l b(k,l)$. Now, the expression for $a(k,l)$ can be written as given in (23), as shown at the bottom of this page.

Now using the fact that $\max_l P_{diff}^{AH}(k,i,l) < \min_l P_{diff}^{AB}(k,i,l)$, it can be shown that $(P_{diff}^{AH}(k,i,l^*) - P_{diff}^{AB}(k,i,l)) < 0,\ \forall i$ and, therefore, $\lim_{T\to\infty} a(k,l) = 1$.

Lemma 7: For a K level tree network, for our proposed Byzantine identification scheme, the asymptotic (i.e., $T \to \infty$) probability that a Byzantine node i at level $k+1$, for $1 \le k \le K-1$, is isolated is lower-bounded by,

$$\prod_{j=2}^{k}(1-\delta_j).$$

Proof: Notice that, $\lim_{T\to\infty} a(k,l) = 1$. The asymptotic performance of the proposed scheme can be analyzed as follows:

$$\begin{aligned}
&\lim_{T\to\infty} P_B^{iso}(k+1,i)\\
&= \sum_{l\in\{0,1\}} P_l \lim_{T\to\infty}\left[(1-b(k,l))\left(\frac{a(k+1,l)}{a(k,l)}\right) P_B^{iso}(k,i,l)\right]\\
&\ge (1-\delta_k)\sum_{l\in\{0,1\}} P_l \lim_{T\to\infty}\left[P_B^{iso}(k,i,l)\right]\\
&= \prod_{j=2}^{k}(1-\delta_j).
\end{aligned}$$

■

Notice that, the parallel network topology is a special case of the tree network topology with $K = 1$. For $K = 1$, our scheme can identify all the Byzantines with probability one because $\lim_{T\to\infty} P_B^{iso}(1,i) = \lim_{T\to\infty} \sum_{l\in\{0,1\}} P_l[a(1,l)] = 1$. When $K > 1$, we can choose η_k appropriately such that Byzantines can be identified with a high probability.

Next, to gain insights into the solution, we present some numerical results in Figure 5 that corroborate our theoretical results. We consider a tree network with $K = 5$ and plot $P_B^{iso}(k,i)$, $1 \le k \le 5$, as a function of the time window T. We assume that the operating points (P_d^k, P_{fa}^k), $1 \le k \le 5$, for the nodes at different levels are given by $[(0.8, 0.1), (0.75, 0.1), (0.6, 0.1), (0.65, 0.1), (0.6, 0.1)]$ and

$$a(k,l) = Q\left(\frac{Q^{-1}(\delta_k)\sqrt{P_{diff}^{AH}(k,i,l^*)(1-P_{diff}^{AH}(k,i,l^*))} + \sqrt{T}(P_{diff}^{AH}(k,i,l^*) - P_{diff}^{AB}(k,i,l))}{\sqrt{P_{diff}^{AB}(k,i,l)(1-P_{diff}^{AB}(k,i,l))}}\right) \tag{23}$$

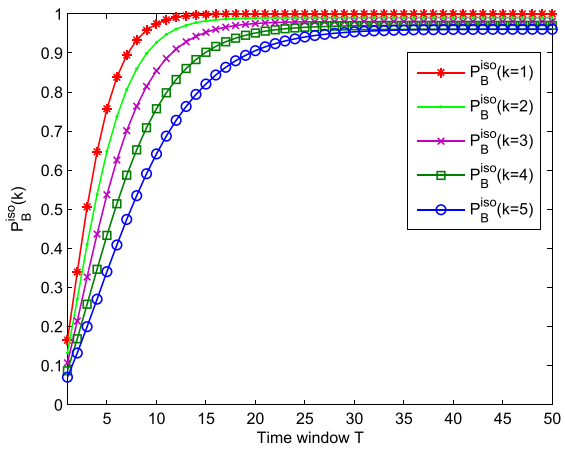

Fig. 5. Isolation probability $P_B^{iso}(k,i)$ vs. time window T.

for anchor node $(P_d^A, P_{fa}^A) = (0.9, 0.1)$. We also assume that the hypotheses are equi-probable, i.e., $P_0 = P_1 = 0.5$, and the maximum isolation probability of honest nodes at level k based solely on its data is constrained by $\delta_k = 0.01, \forall k$. It can be seen from Figure 5 that in a span of only $T = 25$ time windows, our proposed scheme isolates/identifies almost all the Byzantines in the tree network.

VII. Conclusion

In this paper, we considered the problem of optimal Byzantine attacks on distributed detection mechanism in tree networks. We analyzed the performance limit of detection performance with Byzantines and obtained the optimal attacking strategies that minimize the detection error exponent. The problem was also studied from the network designer's perspective. It was shown that the optimal local detector is independent of the Byzantine's parameter. Next, we modeled the strategic interaction between the FC and the attacker as a Leader-Follower (Stackelberg) game and attacker and defender (FC) equilibrium strategies were identified. We also proposed a simple yet efficient scheme to identify Byzantines and analytically evaluated its performance. There are still many interesting questions that remain to be explored in the future work such as analysis of the problem for arbitrary network topologies. The case where Byzantines collude in several groups (collaborate) to degrade the detection performance can also be investigated.

Acknowledgment

The authors would like to thank Aditya Vempaty for his valuable comments and suggestions to improve the quality of the paper.

Appendix A
Proof of Lemma 3

To prove the lemma, we first show that any positive deviation $\epsilon \in (0, p]$ in flipping probabilities $(P_{1,0}^k, P_{0,1}^k) = (p, p-\epsilon)$ will result in an increase in D_k. After plugging in $(P_{1,0}^k, P_{0,1}^k) = (p, p-\epsilon)$ in (9) and (10), we get

$$\begin{aligned}\pi_{1,0}^k &= [\beta_{1,0}^{k-1}(1-P_{fa}^k) + (1-\beta_{0,1}^{k-1})P_{fa}^k] \\ &\quad + [\alpha_k(p - P_{fa}^k(2p-\epsilon)) + P_{fa}^k] \qquad (26)\\ \pi_{1,1}^k &= [\beta_{1,0}^{k-1}(1-P_d^k) + (1-\beta_{0,1}^{k-1})P_d^k] \\ &\quad + [\alpha_k(p - P_d^k(2p-\epsilon)) + P_d^k]. \qquad (27)\end{aligned}$$

Now we show that D_k is a monotonically increasing function of the parameter ϵ or in other words, $\frac{dD_k}{d\epsilon} > 0$.

$$\begin{aligned}\frac{dD_k}{d\epsilon} &= \pi_{1,0}^k\left(\frac{\pi_{1,0}^{k'}}{\pi_{1,0}^k} - \frac{\pi_{1,1}^{k'}}{\pi_{1,1}^k}\right) + \pi_{1,0}^{k'}\log\frac{\pi_{1,0}^k}{\pi_{1,1}^k} \\ &\quad + (1-\pi_{1,0}^k)\left(\frac{\pi_{1,1}^{k'}}{1-\pi_{1,1}^k} - \frac{\pi_{1,0}^{k'}}{1-\pi_{1,0}^k}\right) \\ &\quad - \pi_{1,0}^{k'}\log\frac{1-\pi_{1,0}^k}{1-\pi_{1,1}^k} \qquad (28)\end{aligned}$$

where $\frac{d\pi_{1,1}^k}{d\epsilon} = \pi_{1,1}^{k'} = \alpha_k P_d^k$ and $\frac{d\pi_{1,0}^k}{d\epsilon} = \pi_{1,0}^{k'} = \alpha_k P_{fa}^k$. After rearranging the terms in the above equation, the condition $\frac{dD_k}{d\epsilon} > 0$ becomes

$$\frac{1-\pi_{1,0}^k}{1-\pi_{1,1}^k} + \frac{P_{fa}^k}{P_d^k}\log\frac{\pi_{1,0}^k}{\pi_{1,1}^k} > \frac{\pi_{1,0}^k}{\pi_{1,1}^k} + \frac{P_{fa}^k}{P_d^k}\log\frac{1-\pi_{1,0}^k}{1-\pi_{1,1}^k}. \qquad (29)$$

Since $P_d^k > P_{fa}^k$ and $\beta_{\bar{x},x}^k < 0.5$, $\pi_{1,1}^k > \pi_{1,0}^k$. It can also be proved that $\frac{P_d^k}{P_{fa}^k}\frac{\pi_{1,0}^k}{\pi_{1,1}^k} > 1$. Hence, we have

$$\begin{aligned}&1 + (\pi_{1,0}^k - \pi_{1,1}^k) < \frac{P_d^k}{P_{fa}^k}\frac{\pi_{1,0}^k}{\pi_{1,1}^k} \\ &\Leftrightarrow (\pi_{1,0}^k - \pi_{1,1}^k)[1 + (\pi_{1,0}^k - \pi_{1,1}^k)] > \frac{P_d^k}{P_{fa}^k}\frac{\pi_{1,0}^k}{\pi_{1,1}^k}(\pi_{1,0}^k - \pi_{1,1}^k) \\ &\Leftrightarrow (\pi_{1,0}^k - \pi_{1,1}^k)\left[\frac{1 + (\pi_{1,0}^k - \pi_{1,1}^k)}{\pi_{1,0}^k(1-\pi_{1,1}^k)}\right] \\ &\qquad > \frac{P_d^k}{P_{fa}^k}\frac{\pi_{1,0}^k}{\pi_{1,1}^k}\left[\frac{\pi_{1,0}^k - \pi_{1,1}^k}{\pi_{1,0}^k(1-\pi_{1,1}^k)}\right] \\ &\Leftrightarrow (\pi_{1,0}^k - \pi_{1,1}^k)\left[\frac{1}{1-\pi_{1,1}^k} + \frac{1}{\pi_{1,0}^k}\right] \\ &\qquad > \frac{P_d^k}{P_{fa}^k}\left[\frac{\pi_{1,0}^k - \pi_{1,0}^k\pi_{1,1}^k + \pi_{1,0}^k\pi_{1,1}^k - \pi_{1,1}^k}{\pi_{1,1}^k(1-\pi_{1,1}^k)}\right] \\ &\Leftrightarrow \left[\frac{1-\pi_{1,1}^k - (1-\pi_{1,0}^k)}{1-\pi_{1,1}^k} + \frac{(\pi_{1,0}^k - \pi_{1,1}^k)}{\pi_{1,0}^k}\right] \\ &\qquad > \frac{P_d^k}{P_{fa}^k}\left[\frac{\pi_{1,0}^k}{\pi_{1,1}^k} - \frac{1-\pi_{1,0}^k}{1-\pi_{1,1}^k}\right] \\ &\Leftrightarrow \frac{1-\pi_{1,0}^k}{1-\pi_{1,1}^k} + \frac{P_{fa}^k}{P_d^k}\left(1 - \frac{\pi_{1,1}^k}{\pi_{1,0}^k}\right) \\ &\qquad > \frac{\pi_{1,0}^k}{\pi_{1,1}^k} + \frac{P_{fa}^k}{P_d^k}\left(\frac{1-\pi_{1,0}^k}{1-\pi_{1,1}^k} - 1\right). \qquad (30)\end{aligned}$$

To prove that (29) is true, we apply the logarithm inequality $(x-1) \geq \log x \geq \frac{x-1}{x}$, for $x > 0$ to (30). First, let us assume that $x = \frac{\pi^k_{1,0}}{\pi^k_{1,1}}$. Now using the logarithm inequality we can show that $\log \frac{\pi^k_{1,0}}{\pi^k_{1,1}} \geq 1 - \frac{\pi^k_{1,1}}{\pi^k_{1,0}}$. Next, let us assume that $x = \frac{1-\pi^k_{1,0}}{1-\pi^k_{1,1}}$. Now using the logarithm inequality it can be shown that $\left[\frac{1-\pi^k_{1,0}}{1-\pi^k_{1,1}} - 1\right] \geq \log \frac{1-\pi^k_{1,0}}{1-\pi^k_{1,1}}$. Using these results and (30), one can prove that condition (29) is true.

Similarly, we can show that any non zero deviation $\epsilon \in (0, p]$ in flipping probabilities $(P^k_{1,0}, P^k_{0,1}) = (p-\epsilon, p)$ will result in an increase in D_k, i.e., $\frac{dD_k}{d\epsilon} > 0$, or

$$\frac{\pi^k_{1,0}}{\pi^k_{1,1}} + \frac{1-P^k_{fa}}{1-P^k_d} \log \frac{1-\pi^k_{1,0}}{1-\pi^k_{1,1}} > \frac{1-\pi^k_{1,0}}{1-\pi^k_{1,1}} + \frac{1-P^k_{fa}}{1-P^k_d} \log \frac{\pi^k_{1,0}}{\pi^k_{1,1}}. \tag{31}$$

Since $P^k_d > P^k_{fa}$ and $\beta^k_{\tilde{x},x} < 0.5$, $\pi^k_{1,1} > \pi^k_{1,0}$. It can also be proved that $\frac{1-\pi^k_{1,0}}{1-\pi^k_{1,1}} < \frac{1-P^k_{fa}}{1-P^k_d}$. Hence, we have

$$\frac{1-\pi^k_{1,0}}{1-\pi^k_{1,1}} < \frac{1-P^k_{fa}}{1-P^k_d}\left[1-(\pi^k_{1,0}-\pi^k_{1,1})\right] \tag{32}$$

$$\Leftrightarrow \frac{1-\pi^k_{1,0}}{\pi^k_{1,1}(1-\pi^k_{1,1})} < \frac{1-P^k_{fa}}{1-P^k_d}\left[\frac{1-(\pi^k_{1,0}-\pi^k_{1,1})}{\pi^k_{1,1}}\right]$$

$$\Leftrightarrow \frac{1}{\pi^k_{1,1}(1-\pi^k_{1,1})} < \frac{1-P^k_{fa}}{1-P^k_d}\left[\frac{1-(\pi^k_{1,0}-\pi^k_{1,1})}{\pi^k_{1,1}(1-\pi^k_{1,0})}\right]$$

$$\Leftrightarrow \frac{1}{\pi^k_{1,0}-\pi^k_{1,1}}\left[\frac{\pi^k_{1,0}-\pi^k_{1,0}\pi^k_{1,1}+\pi^k_{1,0}\pi^k_{1,1}-\pi^k_{1,1}}{\pi^k_{1,1}(1-\pi^k_{1,1})}\right] < \frac{1-P^k_{fa}}{1-P^k_d}\left[\frac{1-(\pi^k_{1,0}-\pi^k_{1,1})}{\pi^k_{1,1}(1-\pi^k_{1,0})}\right]$$

$$\Leftrightarrow \frac{1}{\pi^k_{1,0}-\pi^k_{1,1}}\left[\frac{\pi^k_{1,0}}{\pi^k_{1,1}} - \frac{1-\pi^k_{1,0}}{1-\pi^k_{1,1}}\right] < \frac{1-P^k_{fa}}{1-P^k_d}\left[\frac{1}{\pi^k_{1,1}} + \frac{1}{1-\pi^k_{1,0}}\right] \tag{33}$$

$$\Leftrightarrow \frac{\pi^k_{1,0}}{\pi^k_{1,1}} - \frac{1-\pi^k_{1,0}}{1-\pi^k_{1,1}} > \frac{1-P^k_{fa}}{1-P^k_d}\left[\frac{\pi^k_{1,0}-\pi^k_{1,1}}{\pi^k_{1,1}} + \frac{\pi^k_{1,0}-\pi^k_{1,1}}{1-\pi^k_{1,0}}\right]$$

$$\Leftrightarrow \frac{\pi^k_{1,0}}{\pi^k_{1,1}} - \frac{1-\pi^k_{1,0}}{1-\pi^k_{1,1}} > \frac{1-P^k_{fa}}{1-P^k_d}\left[\frac{\pi^k_{1,0}-\pi^k_{1,1}}{\pi^k_{1,1}} + \frac{1-\pi^k_{1,1}-(1-\pi^k_{1,0})}{1-\pi^k_{1,0}}\right]$$

$$\Leftrightarrow \frac{\pi^k_{1,0}}{\pi^k_{1,1}} + \frac{1-P^k_{fa}}{1-P^k_d}\left[1-\frac{1-\pi^k_{1,1}}{1-\pi^k_{1,0}}\right] > \frac{1-\pi^k_{1,0}}{1-\pi^k_{1,1}} + \frac{1-P^k_{fa}}{1-P^k_d}\left[\frac{\pi^k_{1,0}}{\pi^k_{1,1}} - 1\right]. \tag{34}$$

To prove that (31) is true, we apply the logarithm inequality $(x-1) \geq \log x \geq \frac{x-1}{x}$, for $x > 0$ to (34). First, let us assume that $x = \frac{1-\pi^k_{1,0}}{1-\pi^k_{1,1}}$. Now using the logarithm inequality we can show that $\log \frac{1-\pi^k_{1,0}}{1-\pi^k_{1,1}} \geq 1 - \frac{1-\pi^k_{1,1}}{1-\pi^k_{1,0}}$. Next, let us assume that $x = \frac{\pi^k_{1,0}}{\pi^k_{1,1}}$. Now using the logarithm inequality it can be shown that $\left[\frac{\pi^k_{1,0}}{\pi^k_{1,1}} - 1\right] \geq \log \frac{\pi^k_{1,0}}{\pi^k_{1,1}}$. Using these results and (34), one can prove that condition (31) is true.

APPENDIX B
PROOF OF LEMMA 6

To prove Lemma 6, it is sufficient to show that:

1) KLD is a monotonically decreasing function of B_k, and,
2) Attacking parent nodes is a strictly dominant strategy.

Lemma 4 suggests that the KLD is a monotonically decreasing function of B_k in the region where attacker cannot make $D_k = 0$ and, therefore, (1) is proved. Next, we show that attacking parent nodes is a strictly dominant strategy. In other words, given a cost budget $C^{attacker}_{budget}$, it is more profitable for an attacker to attack the parent nodes. Observe that the KLD at level k is a function of Byzantines' parameter $(B_1, \cdots, B_k)$. Thus, we denote it as $D_k(B_1, \cdots, B_k)$.

In order to prove that attacking parent nodes is a strictly dominant strategy, it is sufficient to show that the attack configuration $S_1 = (B_1, \cdots, B_j, B_{j+1}, \cdots, B_K)$ strictly dominates the attack configuration $S_2 = (B_1, \cdots, B_j - \delta, B_{j+1} + \delta\frac{N_{j+1}}{N_j}, \cdots, B_K)$ for $\delta \in \{1, \cdots, B_j\}$. In other words, we want to show that $P(S_1) > P(S_2)$ and $C(S_1) \leq C(S_2)$. From the cost inequality it follows that $C(S_1) \leq C(S_2)$ because $c_{max} \leq (\min_k N_{k+1}/N_k) \times c_{min} \Rightarrow \tilde{c}_j \leq (N_{j+1}/N_j) \times \tilde{c}_{j+1}$. Also, note that if the attack configuration S_1 strictly dominates the attack configuration S_2, then, it will also strictly dominate any attack configuration $\tilde{S}_2$ with $\tilde{S}_2 = (B_1, \cdots, B_j - \delta, B_{j+1} + \delta\gamma, \cdots, B_K)$, where $\gamma \leq \frac{N_{j+1}}{N_j}$. Next, we show that $P(S_1) > P(S_2)$.

Since $D_j(B_1, \cdots, B_{j-1}, B_j) < D_j(B_1, \cdots, B_{j-1}, B_j - \delta)$, for $\delta \in \{1, \cdots, B_j\}$, $\forall j$, it follows that

$$D_j(B_1, \cdots, B_{j-1}, B_j) < D_j(B_1, \cdots, B_{j-1}, B_j - \delta)$$

$$\Leftrightarrow \sum_{k=1}^{j} D_k(B_1, \cdots, B_k) < \sum_{k=1}^{j-1} D_k(B_1, \cdots, B_k) + D_j(B_1, \cdots, B_{j-1}, B_j - \delta)$$

$$\Leftrightarrow \sum_{k=1}^{K} D_k(B_1, \cdots, B_k) < \sum_{k=1}^{j-1} D_k(B_1, \cdots, B_k) + D_j(B_1, \cdots, B_{j-1}, B_j - \delta) + \sum_{k=j+1}^{K} D_k(B_1, \cdots, B_j - \delta, B_{j+1} + \delta\frac{N_{j+1}}{N_j}, B_{j+2}, \cdots, B_k),$$

where the last inequality follows from the fact that $\frac{B_j}{N_j} + \frac{B_{j+1}}{N_{j+1}} = \frac{B_j - \delta}{N_j} + \frac{B_{j+1} + \frac{N_{j+1}}{N_j}\delta}{N_{j+1}}$ and, therefore,

$$D_k(B_1, \cdots, B_j, B_{j+1}, \cdots B_k) = D_k(B_1, \cdots, B_j - \delta, B_{j+1} + \frac{N_{j+1}}{N_j}\delta, \cdots, B_k).$$

This implies that S_1 strictly dominates S_2. From Lemma 4, we know that the profit is an increasing function of attack nodes. Lemma 4 in conjunction with the fact that attacking parent nodes is a strictly dominant strategy implies Lemma 6.

REFERENCES

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

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

[3] V. V. Veeravalli and P. K. Varshney, "Distributed inference in wireless sensor networks," *Philosoph. Trans. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 370, no. 1958, pp. 100–117, Jan. 2012.

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

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

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

[7] H. Rifà-Pous, M. J. Blasco, and C. Garrigues, "Review of robust cooperative spectrum sensing techniques for cognitive radio networks," *Wireless Pers. Commun.*, vol. 67, no. 2, pp. 175–198, Nov. 2012.

[8] 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.

[9] 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, Feb. 2011.

[10] B. Kailkhura, S. Brahma, and P. K. Varshney, "Optimal Byzantine attacks on distributed detection in tree-based topologies," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, San Diego, CA, USA, Jan. 2013, pp. 227–231.

[11] B. Kailkhura, S. Brahma, Y. S. Han, and P. K. Varshney, "Optimal distributed detection in the presence of Byzantines," in *Proc. IEEE 38th Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, Vancouver, BC, Canada, May 2013, pp. 2925–2929.

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

[13] 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, Jan. 2013.

[14] B. Kailkhura, S. Brahma, Y. S. Han, and P. K. Varshney, "Distributed detection in tree topologies with Byzantines," *IEEE Trans. Signal Process.*, vol. 62, no. 12, pp. 3208–3219, Jun. 2014.

[15] B. Kailkhura, Y. S. Han, S. Brahma, and P. K. Varshney, "Asymptotic analysis of distributed Bayesian detection with Byzantine data," *IEEE Signal Process. Lett.*, vol. 22, no. 5, pp. 608–612, May 2015.

[16] B. Kailkhura, Y. S. Han, S. Brahma, and P. K. Varshney, "On covert data falsification attacks on distributed detection systems," in *Proc. 13th Int. Symp. Commun. Inf. Technol. (ISCIT)*, Sep. 2013, pp. 412–417.

[17] B. Kailkhura, S. Brahma, and P. K. Varshney, "On the performance analysis of data fusion schemes with Byzantines," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2014, pp. 7411–7415.

[18] B. Kailkhura, Y. S. Han, S. Brahma, and P. K. Varshney. (2013). "Distributed Bayesian detection with Byzantine." [Online]. Available: http://arxiv.org/abs/1307.3544

[19] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 1991.

[20] W.-Z. Song, R. Huang, B. Shirazi, and R. LaHusen, "TreeMAC: Localized TDMA MAC protocol for real-time high-data-rate sensor networks," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, Mar. 2009, pp. 1–10.

[21] S. C. A. Thomopoulos, R. Viswanathan, and D. K. Bougoulias, "Optimal distributed decision fusion," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 25, no. 5, pp. 761–765, Sep. 1989.

[22] W. P. Tay, "Decentralized detection in resource-limited sensor network architectures," Ph.D. dissertation, Dept. Elect. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, Feb. 2008.

[23] U. Rogers and H. Chen, "Heterogeneous sensor networks with convex constraints," in *Proc. IEEE Aerosp. Conf.*, Mar. 2013, pp. 1–10.

[24] J. Font-Segura, G. Vazquez, and J. Riba, "Asymptotic error exponents in energy-detector and estimator-correlator signal detection," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 3676–3680.

[25] S. Kullback, *Information Theory and Statistics*. New York, NY, USA: Dover, 1968.

[26] J. N. Tsitsiklis, "Decentralized detection by a large number of sensors," *Math. Control, Signals, Syst.*, vol. 1, no. 2, pp. 167–182, 1988.

Bhavya Kailkhura (S'12) received the M.S. degree in electrical engineering from Syracuse University, Syracuse, NY, where he is currently pursuing the Ph.D. degree with the Department of Electrical Engineering and Computer Science. His research interests include high-dimensional data analysis, signal processing, machine learning, and their applications to solve inference problems with security and privacy constraints.

Swastik Brahma (S'09–M'14) received the B.Tech. degree in computer science and engineering from the West Bengal University of Technology, Kolkata, India, in 2005, and the M.S. and Ph.D. degrees in computer science from the University of Central Florida, Orlando, FL, in 2008 and 2011, respectively. In 2011, he joined the Department of Electrical Engineering and Computer Science, Syracuse University, Syracuse, NY, as a Research Associate, where he is currently a Research Scientist. His research interests include communication systems, detection and estimation theory, cyber-security, and game theory. He was a recipient of the best paper award at the IEEE Globecom Conference in 2008, and the Best Ph.D. Forum Award at the IEEE WoWMoM Conference in 2009. He serves as a Technical Program Committee Member for several conferences.

Berkan Dulek (S'11–M'13) received the B.S., M.S., and Ph.D. degrees in electrical and electronics engineering from Bilkent University, in 2003, 2006, and 2012, respectively. From 2007 to 2010, he was with the Tubitak Bilgem Iltaren Research and Development Group. From 2012 to 2013, he was a Post-Doctoral Research Associate with the Department of Electrical Engineering and Computer Science, Syracuse University, Syracuse, NY, USA. Since 2014, he has been with the Department of Electrical and Electronics Engineering, Hacettepe University, where he is currently an Assistant Professor. His research interests are in statistical signal processing, detection and estimation theory, and communication theory.

Yunghsiang S. Han (S'90–M'93–SM'08–F'11) was born in Taipei, Taiwan, in 1962. He received the B.Sc. and M.Sc. degrees in electrical engineering from National Tsing Hua University, Hsinchu, Taiwan, in 1984 and 1986, respectively, and the Ph.D. degree from the School of Computer and Information Science, Syracuse University, Syracuse, NY, in 1993. He was a Lecturer with Ming-Hsin Engineering College, Hsinchu, from 1986 to 1988. He was a Teaching Assistant from 1989 to 1992, and a Research Associate with the School of Computer and Information Science, Syracuse University, from 1992 to 1993. He was an Associate Professor with the Department of Electronic Engineering, Hua Fan College of Humanities and Technology, Taipei, from 1993 to 1997. He was with the Department of Computer Science and Information Engineering, National Chi Nan University, Nantou, Taiwan, from 1997 to 2004. He was promoted to Professor in 1998. He was a Visiting Scholar with the Department of Electrical Engineering, University of Hawaii at Manoa, HI, in 2001, the SUPRIA Visiting Research Scholar with the Department of Electrical Engineering and Computer Science and the CASE Center, Syracuse University, from 2002 to 2004 and 2012 to 2013, and a Visiting Scholar with the Department of Electrical and Computer Engineering, University of Texas at Austin, TX, from 2008 to 2009. He was with the Graduate Institute of Communication Engineering, National Taipei University, Taipei, from 2004 to 2010. Since 2010, he has been with the Department of Electrical Engineering, National Taiwan University of Science and Technology, as the Chair Professor. His research interests are in error-control coding, wireless networks, and security.

Dr. Han was a winner of the 1994 Syracuse University Doctoral Prize. One of his papers received the prestigious 2013 ACM CCS Test-of-Time Award in cyber security.

Pramod K. Varshney (S'72–M'77–SM'82–F'97) was born in Allahabad, India, in 1952. He received the B.S. degree (Hons.) in electrical engineering and computer science and the M.S. and Ph.D. degrees in electrical engineering from the University of Illinois at Urbana—Champaign, in 1972, 1974, and 1976, respectively.

He held teaching and research assistantships with the University of Illinois at Urbana—Champaign from 1972 to 1976. Since 1976, he has been with Syracuse University, Syracuse, NY, where he is currently a Distinguished Professor of Electrical Engineering and Computer Science and the Director of the Center for Advanced Systems and Engineering. He served as the Associate Chair of the Department of Electrical Engineering and Computer Science from 1993 to 1996. He is an Adjunct Professor of Radiology with Upstate Medical University, Syracuse. He has served as a Consultant to several major companies. He has published extensively. He is the author of *Distributed Detection and Data Fusion* (New York: Springer-Verlag, 1997). His current research interests are in distributed sensor networks and data fusion, detection and estimation theory, wireless communications, image processing, radar signal processing, and remote sensing.

Dr. Varshney was a James Scholar, a Bronze Tablet Senior, and a Fellow while at the University of Illinois. He is a member of Tau Beta Pi and is the recipient of the 1981 ASEE Dow Outstanding Young Faculty Award. He was elected to the grade of Fellow of the IEEE in 1997 for his contributions in the area of distributed detection and data fusion. He was a Guest Editor of the Special Issue on Data Fusion of the IEEE PROCEEDINGS in 1997. In 2000, he received the Third Millennium Medal from the IEEE and Chancellor's Citation for exceptional academic achievement at Syracuse University. He is the recipient of the IEEE 2012 Judith A. Resnik Award and Doctor of Engineering degree honoris causa from Drexel University in 2014. He is on the Editorial Boards of the *Journal on Advances in Information Fusion* and *IEEE Signal Processing Magazine*. He was the President of International Society of Information Fusion during 2001.