Distributed Detection in Tree Topologies with Byzantines

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

Abstract—In this paper, we consider the problem of distributed detection in tree topologies in the presence of Byzantines. The expression for minimum attacking power required by the Byzantines to blind the fusion center (FC) is obtained. More specifically, we show that when more than a certain fraction of individual node decisions are falsified, the decision fusion scheme becomes completely incapable. We obtain closed form expressions for the optimal attacking strategies that minimize the detection error exponent at the FC. We also look at the possible counter-measures from the FC's perspective to protect the network from these Byzantines. We formulate the robust topology design problem as a bi-level program and provide an efficient algorithm to solve it. We also provide some numerical results to gain insights into the solution.

Index Terms—Distributed Detection, Byzantine Attacks, Kullback-Leibler Divergence, Bounded Knapsack Problem, Bi-level Programming

I. INTRODUCTION

Distributed detection has been a well studied topic in the detection theory literature [1] [2] [3] and has traditionally focused on the parallel network topology. In distributed detection with parallel topology, nodes make their local decisions regarding the underlying phenomenon and send them to the fusion center (FC), where a global decision is made. Even though the parallel topology has received significant attention, there are many practical situations where parallel topology cannot be implemented due to several factors, such as, the FC being outside the communication range of the nodes and limited energy budget of the nodes [4]. In such cases, a multi-hop network is employed, where nodes are organized hierarchically into multiple levels (tree networks). With intelligent use of resources across levels, tree networks have the potential to provide a suitable balance between cost, coverage, functionality, and reliability [5]. Some examples of tree networks

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

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

include wireless sensor and military communication networks. For instance, the IEEE 802.15.4 (Zigbee) specifications [6] and IEEE 802.22b [7] can support tree-based topologies. Theses nodes are often deployed in open and unattended environments and are vulnerable to physical tampering.

In recent years, security issues of distributed inference networks are increasingly being studied. One typical attack on such networks is a Byzantine attack. While Byzantine attacks (originally proposed by [8]) may, in general, refer to many types of malicious behavior; our focus in this paper is on data-falsification attacks [9]–[17]. In this type of attack, the compromised node may send false (erroneous) local decisions to the FC to degrade the detection performance. This attack becomes more severe in tree topologies where malicious nodes can alter local decisions of a large part of the network and cause degradation of system performance and may even make the decision fusion schemes to become completely incapable. In this paper, we refer to such a data falsification attacker as a Byzantine.

A. Related Work

Although distributed detection has been a very active field of research in the past [1]–[3], security problems in distributed detection networks gained attention only very recently. In [12], the authors considered the problem of distributed detection in the presence of Byzantines for a parallel topology and determined the optimal attacking strategy which minimizes the detection error exponent. They assumed that the Byzantines know the true hypothesis, which obviously is not satisfied in practice but does provide a bound. In [13], the authors analyzed the same problem in the context of collaborative spectrum sensing. They relaxed the assumption of perfect knowledge of the hypotheses by assuming that the Byzantines obtain knowledge about the true hypotheses from their own sensing observations.

The above work [12], [13] addresses the issue of Byzantines from the attacker's perspective. Schemes to mitigate the effect of Byzantines have also been proposed in the literature. In [13], the authors proposed a simple scheme to identify the Byzantines. The idea was to maintain a reputation metric for every node by comparing each node's local decision to the global decision made at the FC using the majority rule. In [16], the authors proposed another scheme to mitigate the effect of Byzantines in a parallel topology. The idea behind the proposed identification scheme is to compare every node's observed behavior over time with the expected behavior

of an honest node. The nodes whose observed behavior is sufficiently far from the expected behavior are tagged as Byzantines and this information is employed while making a decision at the FC. In [17], the authors investigated the problem of distributed detection in the presence of different types of Byzantine nodes. Each Byzantine type corresponds to a different operating point and, therefore, the problem of identifying different Byzantine nodes along with their operating points was considered. Once the Byzantine operating points are estimated, this information was utilized by the FC to improve global detection performance. The problem of designing the optimal fusion rule and the local sensor thresholds with Byzantines for a parallel topology was considered in [15].

B. Main Contributions

All the approaches discussed so far consider distributed detection with Byzantines for parallel topologies. In contrast to previous work, we study the problem of distributed detection with Byzantines for tree topologies. More specifically, we address the problem of distributed detection in perfect a-ary tree networks in the presence of Byzantine attacks (data falsification attacks). Well structured (or regular) topologies such as a-ary tree topologies are commonly picked by network designers for their simplicity and, therefore, easier network management. For some practical examples of such networks, one may refer to [18] (and references within). Perfect a-ary tree topologies are widely used in peer to peer systems [19]. Also notice that, designing optimal tree topology for various performance metrics is computationally not feasible [20]. In such scenarios, perfect a-ary topologies provide mathematical tractability and valuable insights into the solution. For previous works on perfect a-ary tree networks, please see [21], [22], [23]. We assume that the cost of attacking nodes at different levels is different and analyze the problem under this assumption. In our preliminary work on this problem [14], we analyzed the problem only from an attacker's perspective assuming that the honest and Byzantine nodes are identical in terms of their detection performance. In our current work, we significantly extend our previous work and investigate the problem from both the attacker's and the FC's perspectives. For the analysis of the optimal attack, we allow Byzantines to have different detection performance than the honest nodes and, therefore, provide a more general and comprehensive analysis of the problem compared to our previous work [14]. The main contributions of this paper are as follows.

- We obtain a closed form expression for the minimum attacking power required by the Byzantines to blind the FC in a tree network and show that when more than a certain fraction of individual node decisions are falsified, the decision fusion scheme becomes completely incapable.
- When the fraction of Byzantines is not sufficient to blind the FC, we provide closed form expressions for the optimal attacking strategies for the Byzantines that most degrade the detection performance.
- We also look at the problem from the network designer's (FC) perspective. More specifically, we formulate the
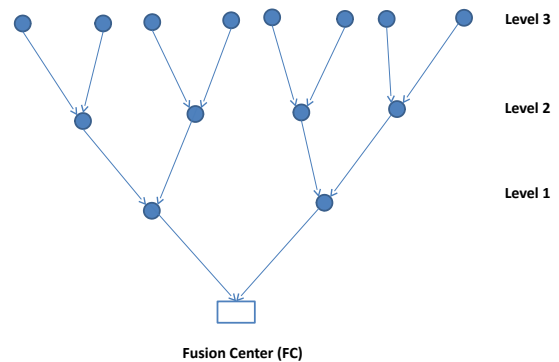

Fig. 1. A distributed detection system organized as a perfect binary tree $T(3,\ 2)$ is shown as an example.

robust tree topology design problem as a bi-level program and provide an efficient algorithm to solve it, which is guaranteed to find an optimal solution, if one exists.

The rest of the paper is organized as follows. Section II introduces our 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 formulate the robust topology design problem as a bi-level program and provide an efficient algorithm to solve it in polynomial time. Finally, Section V concludes the paper.

II. SYSTEM MODEL

We consider a distributed detection system with the topology of a perfect a-tree $T(K,\ a)$ rooted at the FC (See Fig. 1). A perfect a-tree is an a-ary tree in which all the leaf nodes are at the same depth and all the internal nodes have degree 'a'. $T(K,\ a)$ has a set $\mathcal{N} = \{\mathbb{N}_k\}_{k=1}^{K}$ of transceiver nodes, where $|\mathbb{N}_k| = N_k = a^k$ is the total number of nodes at level (or depth) k. We assume that the depth of the tree is $K > 1$ and the number of children is $a \geq 2$. The total number of nodes in the network is denoted as $\sum_{k=1}^{K} N_k = N$. $\mathcal{B} = \{\mathbb{B}_k\}_{k=1}^{K}$ 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 levels $1 \leq k \leq K$ is defined as an attack configuration, i.e., $\{B_k\}_{k=1}^{K} = \{|\mathbb{B}_k|\}_{k=1}^{K}$. Notice that, for the attack configuration $\{B_k\}_{k=1}^{K}$, the total number of corrupted paths (or paths containing Byzantine nodes) from Level k to the FC are $\sum_{i=1}^{k} B_i \frac{N_k}{N_i}$, where $B_i \frac{N_k}{N_i}$ gives the total number of covered[1] nodes at level k by 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. In practice, nodes operate with very limited energy and, therefore, it is reasonable to assume that the packet IDs (or source IDs) are not forwarded in the tree to save energy. Moreover, even in cases where the packet IDs (or source IDs) are forwarded, notice that the packet IDs (or source

---

[1]Node i at level k' covers all its children at levels $k'+1 \leq k \leq K$ and the node i itself and, therefore, the total number of covered nodes by $B_{k'}$, Byzantine at level k', is $\frac{B_{k'}}{N_{k'}} \cdot \sum_{i=k'}^{K} N_i$.

IDs) can be tempered too, thereby preventing the FC to be deterministically aware of the source of a message. Therefore, we consider that the FC looks at messages coming from nodes in a probabilistic manner and considers each received bit to originate from nodes at level k with certain probability $\beta_k \in [0, 1]$. This also implies that, from the FC's perspective, received bits are identically distributed. For a $T(K, a)$,

$$\beta_k = \frac{a^k}{N}.$$

A. Distributed detection in a tree topology

We consider a binary hypothesis testing problem with the two hypotheses H_0 (signal is absent) and H_1 (signal is present). Each node i at level k acts as a source in that it makes a one-bit local decision $v_{k,i} \in \{0, 1\}$ and sends $u_{k,i}$ to its parent node at level $k-1$, where $u_{k,i} = v_{k,i}$ if i is an uncompromised (honest) node, but for a compromised (Byzantine) node i, $u_{k,i}$ need not be equal to $v_{k,i}$. It also receives the decisions $u_{k',j}$ of all successors j at levels $k' \in [k+1, K]$, which are forwarded to i by its immediate children. It forwards[2] these received decisions along with $u_{k,i}$ to its parent node at level $k-1$. If node i is a Byzantine, then it might alter these received decisions before forwarding. We assume error-free communication channels between children and the parent nodes. We denote the probabilities of detection and false alarm of a honest node i at level k by $P_d^H = P(v_{k,i} = 1 | H_1, i \notin \mathbb{B}_k)$ and $P_{fa}^H = P(v_{k,i} = 1 | H_0, i \notin \mathbb{B}_k)$, respectively. Similarly, the probabilities of detection and false alarm of a Byzantine node i at level k are denoted by $P_d^B = P(v_{k,i} = 1 | H_1, i \in \mathbb{B}_k)$ and $P_{fa}^B = P(v_{k,i} = 1 | H_0, i \in \mathbb{B}_k)$, respectively.

B. Byzantine attack model

Now a mathematical model for the Byzantine attack is presented. If a node is honest, then it forwards its own decision and received decisions without altering them. However, a Byzantine node, in order to undermine the network performance, may alter its decision as well as received decisions from its children prior to transmission. We define the following strategies $P_{j,1}^H$, $P_{j,0}^H$ and $P_{j,1}^B$, $P_{j,0}^B$ ($j \in \{0, 1\}$) for the honest and Byzantine nodes, respectively:
Honest nodes:

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

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

Byzantine nodes:

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

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

where $P(x = a | y = b)$ is the probability that a node sends a to its parent when it receives b from its child or its actual decision is b. Furthermore, we assume that if a node (at any level) is a Byzantine then none of its ancestors are Byzantines; otherwise, the effect of a Byzantine due to other Byzantines

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

on the same path may be nullified (e.g., Byzantine ancestor re-flipping the already flipped decisions of its successor). This means that any path from a leaf node to the FC will have at most one Byzantine. Thus, we have, $\sum_{k=1}^{K} \alpha_k \leq 1$ since the average number of Byzantines along any path from a leaf to the root cannot be greater than 1.

C. Performance metric

The Byzantine attacker always wants to degrade the detection performance at the FC as much as possible; in contrast, the FC wants to maximize the detection performance. In this work, we employ the Kullback-Leibler divergence (KLD) [24] to be the network performance metric that characterizes detection performance. The KLD is a frequently used information-theoretic distance measure to characterize detection performance. By Stein's lemma, we know that in the Neyman-Pearson setup for a fixed missed detection probability, the false alarm probability obeys the asymptotics

$$\lim_{N \to \infty} \frac{\ln P_F}{N} = -D, \text{ for a fixed } P_M, \quad (5)$$

where P_M, P_F are missed detection and false alarm probabilities, respectively. The KLD between the distributions $\pi_{j,0} = P(z = j | H_0)$ and $\pi_{j,1} = P(z = j | H_1)$ can be expressed as

$$D(\pi_{j,1} || \pi_{j,0}) = \sum_{j \in \{0,1\}} P(z = j | H_1) \log \frac{P(z = j | H_1)}{P(z = j | H_0)}. \quad (6)$$

$$
\begin{aligned}
P(z_i = j | H_0) &= \left[\sum_{k=1}^{K} \beta_k \left(\sum_{i=1}^{k} \alpha_i \right) \right] [P_{j,0}^B (1 - P_{fa}^B) + P_{j,1}^B P_{fa}^B] \quad (7) \\
&+ \left[\sum_{k=1}^{K} \beta_k \left(1 - \sum_{i=1}^{k} \alpha_i \right) \right] [P_{j,0}^H (1 - P_{fa}^H) + P_{j,1}^H P_{fa}^H]
\end{aligned}
$$

$$
\begin{aligned}
P(z_i = j | H_1) &= \left[\sum_{k=1}^{K} \beta_k \left(\sum_{i=1}^{k} \alpha_i \right) \right] [P_{j,0}^B (1 - P_d^B) + P_{j,1}^B P_d^B] \quad (8) \\
&+ \left[\sum_{k=1}^{K} \beta_k \left(1 - \sum_{i=1}^{k} \alpha_i \right) \right] [P_{j,0}^H (1 - P_d^H) + P_{j,1}^H P_d^H]
\end{aligned}
$$

For a K-level network, distributions of received decisions at the FC z_i, $i = 1, .., N$, under H_0 and H_1 are given by (7) and (8), respectively. In order to make the analysis tractable, we assume that the network designer attempts to maximize the KLD of each node as seen by the FC. On the other hand, the attacker attempts to minimize the KLD of each node as seen by the FC.

Next, we explore the optimal attacking strategies for the Byzantines that most degrade the detection performance by minimizing KLD.

III. OPTIMAL BYZANTINE ATTACK

As discussed earlier, the Byzantine nodes attempt to make their KL divergence as small as possible. Since the KLD is always non-negative, Byzantines attempt to choose $P(z = j | H_0)$ and $P(z = j | H_1)$ such that KLD is zero. In this case, an adversary can make the data that the FC receives from the

nodes such that no information is conveyed. This is possible when

$$P(z = j|H_0) = P(z = j|H_1) \qquad \forall j \in \{0, 1\}. \qquad (9)$$

Substituting (7) and (8) in (9) and after simplification, the condition to make the $KLD = 0$ for a K-level network can be expressed as

$$P_{j,1}^B - P_{j,0}^B = \frac{\sum_{k=1}^K [\beta_k (1 - \sum_{i=1}^k \alpha_i)]}{\sum_{k=1}^K [\beta_k (\sum_{i=1}^k \alpha_i)]]} \frac{P_d^H - P_{fa}^H}{P_d^B - P_{fa}^B} (P_{j,0}^H - P_{j,1}^H). \qquad (10)$$

From (1) to (4), we have

$$P_{0,1}^B - P_{0,0}^B = \frac{\sum_{k=1}^K [\beta_k (1 - \sum_{i=1}^k \alpha_i)]}{\sum_{k=1}^K [\beta_k (\sum_{i=1}^k \alpha_i)]]} \frac{P_d^H - P_{fa}^H}{P_d^B - P_{fa}^B} = -(P_{1,1}^B - P_{1,0}^B). \qquad (11)$$

Hence, the attacker can degrade detection performance by intelligently choosing $(P_{0,1}^B, P_{1,0}^B)$, which are dependent on α_k, for $k = 1, \cdots, K$. Observe that,

$$0 \leq P_{0,1}^B - P_{0,0}^B$$

since $\sum_{i=1}^k \alpha_i \leq 1$ for $k \leq K$. To make $KLD = 0$, we must have

$$P_{0,1}^B - P_{0,0}^B \leq 1$$

such that $(P_{j,1}^B, P_{j,0}^B)$ becomes a valid probability mass function. Notice that, when $P_{0,1}^B - P_{0,0}^B > 1$ there does not exist any attacking probability distribution $(P_{j,1}^B, P_{j,0}^B)$ that can make $KLD = 0$. In the case of $P_{0,1}^B - P_{0,0}^B = 1$, there exists a unique solution $(P_{1,1}^B, P_{1,0}^B) = (0, 1)$ that can make $KLD = 0$. For the $P_{0,1}^B - P_{0,0}^B < 1$ case, there exist an infinite number of attacking probability distributions $(P_{j,1}^B, P_{j,0}^B)$ which can make $KLD = 0$.

By further assuming that the honest and Byzantine nodes are identical in terms of their detection performance, i.e., $P_d^H = P_d^B$ and $P_{fa}^H = P_{fa}^B$, the above condition to blind the FC reduces to

$$\frac{\sum_{k=1}^K [\beta_k (1 - \sum_{i=1}^k \alpha_i)]}{\sum_{k=1}^K [\beta_k (\sum_{i=1}^k \alpha_i)]]} \leq 1$$

which is equivalent to

$$\sum_{k=1}^K [\beta_k (1 - 2(\sum_{i=1}^k \alpha_i))] \leq 0. \qquad (12)$$

Recall that $\alpha_k = \frac{B_k}{N_k}$ and $\beta_k = \frac{N_k}{\sum_{i=1}^K N_i}$. Substituting α_k and β_k into (12) and simplifying the result, we have the following proposition.

Proposition 1. *In a tree network with K levels, there exists an attacking probability distribution $(P_{0,1}^B, P_{1,0}^B)$ that can make $KLD = 0$, and thereby blind the FC, if and only if $\{B_k\}_{k=1}^K$ satisfy*

$$\sum_{k=1}^K \left(\frac{B_k}{N_k} \sum_{i=k}^K N_i \right) \geq \frac{N}{2}. \qquad (13)$$

Dividing both sides of (13) by N, the above condition can be written as $\sum_{k=1}^K \beta_k \sum_{i=1}^k \alpha_i \geq 0.5$. This implies that to make the FC blind, 50% or more nodes in the network need to be covered by the Byzantines. Observe that, Proposition 1 suggests that there exist multiple attack configurations $\{B_k\}_{k=1}^K$

that can blind the FC. Also notice that, some of these attacking sets require Byzantines to compromise less than 50% of the nodes in the network. For example, attacking half of the nodes at Level 1 (i.e., $B_1 = \frac{N_1}{2} << \frac{N}{2}$) cover 50% of the nodes in the network and, therefore, the FC becomes blind. This implies that in the tree topology Byzantines have more degrees of freedom to blind the FC as compared to the parallel topology.

Next, to explore the optimal attacking probability distribution $(P_{0,1}^B, P_{1,0}^B)$ that minimizes KLD when (12) does not hold, we explore the properties of KLD.

First, we show that attacking with symmetric flipping probabilities is the optimal strategy in the region where the attacker cannot blind the FC. In other words, attacking with $P_{1,0} = P_{0,1}$ is the optimal strategy for the Byzantines. For analytical tractability, we assume $P_d^H = P_d^B = P_d$ and $P_{fa}^H = P_{fa}^B = P_{fa}$ in further analysis.

Lemma 1. *In the region where the attacker cannot blind the FC, the optimal attacking strategy comprises of symmetric flipping probabilities. More specifically, any non zero deviation $\epsilon_i \in (0, p)$ in flipping probabilities $(P_{0,1}^B, P_{1,0}^B) = (p - \epsilon_1, p - \epsilon_2)$, where $\epsilon_1 \neq \epsilon_2$, will result in increase in the KLD.*

Proof: Let us denote, $P(z = 1|H_1) = \pi_{1,1}$, $P(z = 1|H_0) = \pi_{1,0}$ and $t = \sum_{k=1}^K \beta_k \sum_{i=1}^k \alpha_i$. Notice that, in the region where the attacker cannot blind the FC, the parameter $t < 0.5$. To prove the lemma, we first show that any positive deviation $\epsilon \in (0, p]$ in flipping probabilities $(P_{1,0}^B, P_{0,1}^B) = (p, p - \epsilon)$ will result in an increase in the KLD. After plugging in $(P_{1,0}^B, P_{0,1}^B) = (p, p - \epsilon)$ in (7) and (8), we get

$$\pi_{1,1} = t(p - P_d(2p - \epsilon)) + P_d \qquad (14)$$
$$\pi_{1,0} = t(p - P_{fa}(2p - \epsilon)) + P_{fa}. \qquad (15)$$

Now we show that the KLD, D, as give in (6) is a monotonically increasing function of the parameter ϵ or in other words, $\frac{dD}{d\epsilon} > 0$.

$$\frac{dD}{d\epsilon} = \pi_{1,1} \left(\frac{\pi_{1,1}'}{\pi_{1,1}} - \frac{\pi_{1,0}'}{\pi_{1,0}} \right) + \pi_{1,1}' \log \frac{\pi_{1,1}}{\pi_{1,0}} \qquad (16)$$
$$+ (1 - \pi_{1,1}) \left(\frac{\pi_{1,0}'}{1 - \pi_{1,0}} - \frac{\pi_{1,1}'}{1 - \pi_{1,1}} \right) - \pi_{1,1}' \log \frac{1 - \pi_{1,1}}{1 - \pi_{1,0}}$$

where $\frac{d\pi_{1,1}}{d\epsilon} = \pi_{1,1}' = tP_d$ and $\frac{d\pi_{1,0}}{d\epsilon} = \pi_{1,0}' = tP_{fa}$ and t is the fraction of covered nodes by the Byzantines. After rearranging the terms in the above equation, the condition $\frac{dD}{d\epsilon} > 0$ becomes

$$\frac{1 - \pi_{1,1}}{1 - \pi_{1,0}} + \frac{P_d}{P_{fa}} \log \frac{\pi_{1,1}}{\pi_{1,0}} > \frac{\pi_{1,1}}{\pi_{1,0}} + \frac{P_d}{P_{fa}} \log \frac{1 - \pi_{1,1}}{1 - \pi_{1,0}}. \qquad (17)$$

Since $P_d > P_{fa}$ and $t < 0.5$, $\pi_{1,1} > \pi_{1,0}$. It can also be

proved that $\frac{P_{fa}}{P_d}\frac{\pi_{1,1}}{\pi_{1,0}} < 1$. Hence, we have

$$1 + (\pi_{1,1} - \pi_{1,0}) > \frac{P_{fa}}{P_d}\frac{\pi_{1,1}}{\pi_{1,0}}$$

$$\Leftrightarrow (\pi_{1,1} - \pi_{1,0})\left[\frac{1 + (\pi_{1,1} - \pi_{1,0})}{\pi_{1,1}(1 - \pi_{1,0})}\right] > \frac{P_{fa}}{P_d}\frac{\pi_{1,1}}{\pi_{1,0}}\left[\frac{\pi_{1,1} - \pi_{1,0}}{\pi_{1,1}(1 - \pi_{1,0})}\right]$$

$$\Leftrightarrow \left[\frac{1 - \pi_{1,0} - (1 - \pi_{1,1})}{1 - \pi_{1,0}} + \frac{(\pi_{1,1} - \pi_{1,0})}{\pi_{1,1}}\right] > \frac{P_{fa}}{P_d}\left[\frac{\pi_{1,1}}{\pi_{1,0}} - \frac{1 - \pi_{1,1}}{1 - \pi_{1,0}}\right]$$

$$\Leftrightarrow \frac{1 - \pi_{1,1}}{1 - \pi_{1,0}} + \frac{P_d}{P_{fa}}\left(1 - \frac{\pi_{1,0}}{\pi_{1,1}}\right) > \frac{\pi_{1,1}}{\pi_{1,0}} + \frac{P_d}{P_{fa}}\left(\frac{1 - \pi_{1,1}}{1 - \pi_{1,0}} - 1\right). \quad (18)$$

To prove that (17) is true, we apply the logarithm inequality $(x - 1) \geq \log x \geq \frac{x - 1}{x}$, for $x > 0$ to (18). First, let us assume that $x = \frac{\pi_{1,1}}{\pi_{1,0}}$. Now, using the logarithm inequality we can show that $\log\frac{\pi_{1,1}}{\pi_{1,0}} \geq 1 - \frac{\pi_{1,0}}{\pi_{1,1}}$. Next, let us assume that $x = \frac{1 - \pi_{1,1}}{1 - \pi_{1,0}}$. Again, using the logarithm inequality it can be shown that $\left[\frac{1 - \pi_{1,1}}{1 - \pi_{1,0}} - 1\right] \geq \log\frac{1 - \pi_{1,1}}{1 - \pi_{1,0}}$. Using these results and (18), one can prove that condition (17) is true. Similarly, we can show that any non zero deviation $\epsilon \in (0, p]$ in flipping probabilities $(P_{1,0}^B, P_{0,1}^B) = (p - \epsilon, p)$ will result in an increase in the KLD, i.e., $\frac{dD}{d\epsilon} > 0$, or

$$\frac{\pi_{1,1}}{\pi_{1,0}} + \frac{1 - P_d}{1 - P_{fa}}\log\frac{1 - \pi_{1,1}}{1 - \pi_{1,0}} > \frac{1 - \pi_{1,1}}{1 - \pi_{1,0}} + \frac{1 - P_d}{1 - P_{fa}}\log\frac{\pi_{1,1}}{\pi_{1,0}}. \quad (19)$$

Since $P_d > P_{fa}$ and $t < 0.5$, $\pi_{1,1} > \pi_{1,0}$. It can also be proved that $\frac{1 - \pi_{1,1}}{1 - \pi_{1,0}} > \frac{1 - P_d}{1 - P_{fa}}$. Hence, we have

$$\frac{1 - \pi_{1,1}}{1 - \pi_{1,0}} > \frac{1 - P_d}{1 - P_{fa}}[1 - (\pi_{1,1} - \pi_{1,0})] \quad (20)$$

$$\Leftrightarrow \frac{1 - \pi_{1,1}}{\pi_{1,0}(1 - \pi_{1,0})} > \frac{1 - P_d}{1 - P_{fa}}\left[\frac{1 - (\pi_{1,1} - \pi_{1,0})}{\pi_{1,0}}\right]$$

$$\Leftrightarrow \frac{1}{\pi_{1,0}(1 - \pi_{1,0})} > \frac{1 - P_d}{1 - P_{fa}}\left[\frac{1 - (\pi_{1,1} - \pi_{1,0})}{\pi_{1,0}(1 - \pi_{1,1})}\right]$$

$$\Leftrightarrow \frac{1}{\pi_{1,1} - \pi_{1,0}}\left[\frac{\pi_{1,1}}{\pi_{1,0}} - \frac{1 - \pi_{1,1}}{1 - \pi_{1,0}}\right] > \frac{1 - P_d}{1 - P_{fa}}\left[\frac{1}{\pi_{1,0}} + \frac{1}{1 - \pi_{1,1}}\right] \quad (21)$$

$$\Leftrightarrow \frac{\pi_{1,1}}{\pi_{1,0}} - \frac{1 - \pi_{1,1}}{1 - \pi_{1,0}} > \frac{1 - P_d}{1 - P_{fa}}\left[\frac{\pi_{1,1} - \pi_{1,0}}{\pi_{1,0}} + \frac{\pi_{1,1} - \pi_{1,0}}{1 - \pi_{1,1}}\right] \quad (22)$$

$$\Leftrightarrow \frac{\pi_{1,1}}{\pi_{1,0}} + \frac{1 - P_d}{1 - P_{fa}}\left[1 - \frac{1 - \pi_{1,0}}{1 - \pi_{1,1}}\right] >$$
$$\frac{1 - \pi_{1,1}}{1 - \pi_{1,0}} + \frac{1 - P_d}{1 - P_{fa}}\left[\frac{\pi_{1,1}}{\pi_{1,0}} - 1\right]. \quad (23)$$

To prove that (19) is true, we apply the logarithm inequality $(x - 1) \geq \log x \geq \frac{x - 1}{x}$, for $x > 0$ to (23). First, let us assume that $x = \frac{1 - \pi_{1,1}}{1 - \pi_{1,0}}$. Now, using the logarithm inequality we can show that $\log\frac{1 - \pi_{1,1}}{1 - \pi_{1,0}} \geq 1 - \frac{1 - \pi_{1,0}}{1 - \pi_{1,1}}$. Next, let us assume that $x = \frac{\pi_{1,1}}{\pi_{1,0}}$. Again, using the logarithm inequality it can be shown that $\left[\frac{\pi_{1,1}}{\pi_{1,0}} - 1\right] \geq \log\frac{\pi_{1,1}}{\pi_{1,0}}$. Using these results and (23), one can prove that condition (19) is true. Condition (17) and (19) imply that any non zero deviation $\epsilon_i \in (0, p]$ in flipping probabilities $(P_{0,1}^B, P_{1,0}^B) = (p - \epsilon_1, p - \epsilon_2)$ will result in an increase in the KLD. ∎

In the next theorem, we present a closed form expression for the optimal attacking probability distribution $(P_{j,1}^B, P_{j,0}^B)$

that minimizes KLD in the region where the attacker cannot blind the FC.

Theorem 1. *In the region where the attacker cannot blind the FC, the optimal attacking strategy is given by* $(P_{0,1}^B, P_{1,0}^B) = (1, 1)$.

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

Let us denote, $P(z = 1|H_1) = \pi_{1,1}$ and $P(z = 1|H_0) = \pi_{1,0}$. After plugging in $(P_{0,1}^B, P_{1,0}^B) = (p, p)$ in (7) and (8), we get

$$\pi_{1,1} = t(p - P_d(2p)) + P_d \quad (24)$$
$$\pi_{1,0} = t(p - P_{fa}(2p)) + P_{fa}. \quad (25)$$

Now we show that the KLD, D, as given in (6) is a monotonically decreasing function of the parameter p or in other words, $\frac{dD}{dp} < 0$. After plugging in $\pi'_{1,1} = t(1 - 2P_d)$ and $\pi'_{1,0} = t(1 - 2P_{fa})$ in the expression of $\frac{dD}{dp}$ and rearranging the terms, the condition $\frac{dD}{dp} < 0$ becomes

$$(1 - 2P_{fa})\left(\frac{1 - \pi_{1,1}}{1 - \pi_{1,0}} - \frac{\pi_{1,1}}{\pi_{1,0}}\right) + (1 - 2P_d)\log\left(\frac{1 - \pi_{1,0}}{1 - \pi_{1,1}}\frac{\pi_{1,1}}{\pi_{1,0}}\right) < 0 \quad (26)$$

Since $P_d > P_{fa}$ and $t < 0.5$, we have $\pi_{1,1} > \pi_{1,0}$. Now, using the fact that $\frac{1 - P_d}{1 - P_{fa}} > \frac{1 - 2P_d}{1 - 2P_{fa}}$ and (21), we have

$$\frac{1}{\pi_{1,1} - \pi_{1,0}}\left[\frac{\pi_{1,1}}{\pi_{1,0}} - \frac{1 - \pi_{1,1}}{1 - \pi_{1,0}}\right] > \frac{1 - 2P_d}{1 - 2P_{fa}}\left[\frac{1}{\pi_{1,0}} + \frac{1}{1 - \pi_{1,1}}\right]$$

$$\Leftrightarrow \frac{\pi_{1,1}}{\pi_{1,0}} + \frac{1 - 2P_d}{1 - 2P_{fa}}\left[1 - \frac{1 - \pi_{1,0}}{1 - \pi_{1,1}}\right] >$$
$$\frac{1 - \pi_{1,1}}{1 - \pi_{1,0}} + \frac{1 - 2P_d}{1 - 2P_{fa}}\left[\frac{\pi_{1,1}}{\pi_{1,0}} - 1\right]. \quad (27)$$

Applying the logarithm inequality $(x - 1) \geq \log x \geq \frac{x - 1}{x}$, for $x > 0$ to (27), one can prove that (26) is true. ∎

Next, to gain insights into the solution, we present some numerical results in Figure 2 that corroborate our theoretical results. We plot KLD as a function of the flipping probabilities $(P_{1,0}^B, P_{0,1}^B)$. We assume that the probability of detection is $P_d = 0.8$, the probability of false alarm is $P_{fa} = 0.2$ and the fraction of covered nodes by the Byzantines is $t = 0.4$. It can be seen that the optimal attacking strategy comprises of symmetric flipping probabilities and is given by $(P_{0,1}^B, P_{1,0}^B) = (1, 1)$, which corroborate our theoretical result presented in Lemma 1 and Theorem 1.

Next, we explore some properties of the KLD with respect to the fraction of covered nodes t in the region where the attacker cannot blind the FC, i.e., $t < 0.5$.

Lemma 2. $D^* = \min_{(P_{j,1}^B, P_{j,0}^B)} D(\pi_{j,1}||\pi_{j,0})$ *is a continuous, decreasing and convex function of fraction of covered nodes by the Byzantines* $t = \sum_{k=1}^{K}[\beta_k(\sum_{i=1}^{k}\alpha_i)]$ *in the region where the attacker cannot blind the FC* $(t < 0.5)$.
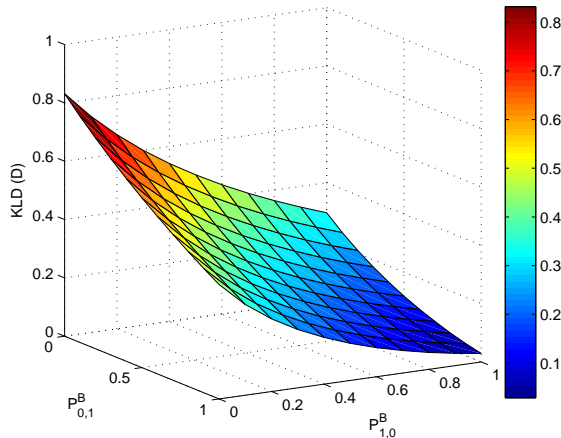
Fig. 2. KL distance vs Flipping Probabilities when $P_d = 0.8$, $P_{fa} = 0.2$, and the fraction of covered nodes by the Byzantines is $t = 0.4$
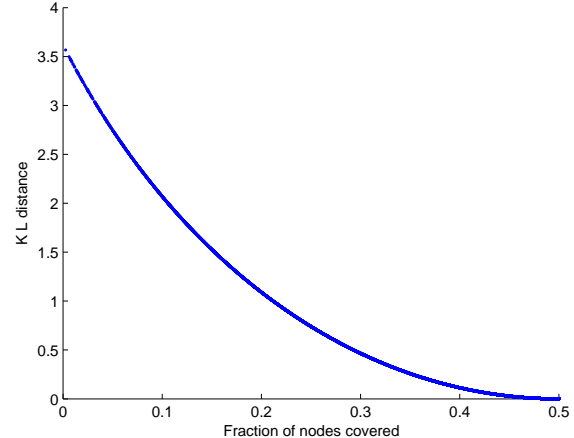

Fig. 3. $\min\limits_{(P_{j,1}^B, P_{j,0}^B)}$ KL distance vs Fraction of nodes covered when $P_d = 0.8$ and $P_{fa} = 0.2$

Proof: The continuity of $D(\pi_{j,1}||\pi_{j,0})$ with respect to the involved distributions implies the continuity of D^*. To show that D^* is a decreasing function of t, we use the fact that $\operatorname*{argmin}\limits_{(P_{0,1}^B, P_{1,0}^B)} D(\pi_{j,1}||\pi_{j,0})$ is equal to $(1,1)$ for $t < 0.5$ (as shown in Theorem 1). After plugging $(P_{0,1}^B, P_{1,0}^B) = (1,1)$ in the KLD expression, it can be shown that the expression for the derivative of D with respect to t, $\dfrac{dD}{dt}$, is the same as (26). Using the results of Theorem 1, it follows that $\dfrac{dD}{dt} < 0$ and, therefore, D^* is a monotonically decreasing function of t in the region where $t < 0.5$. The convexity of D^* follows from the fact that $D^*(\pi_{j,1}||\pi_{j,0})$ is convex in $\pi_{j,1}$ and $\pi_{j,0}$, which are affine transformations of t (Note that, convexity holds under affine transformation). ■

It is worth noting that Lemma 2 suggests that by minimizing/maximizing the fraction of covered nodes t, the FC can maximize/minimize the KLD. Using this fact, from now onwards we will consider fraction of covered nodes t in lieu of the KLD in further analysis in the paper.

Next, to gain insights into the solution, we present some numerical results in Figure 3 that corroborate our theoretical results. We plot $\min\limits_{(P_{j,1}^B, P_{j,0}^B)}$ KLD as a function of the fraction of covered nodes. We assume that the probabilities of detection and false alarm are $P_d = 0.8$ and $P_{fa} = 0.2$, respectively. Notice that, when 50% of the nodes in the network are covered, KLD between the two probability distributions becomes zero and FC becomes blind. It can be seen that D^* is a continuous, decreasing and convex function of the fraction of covered nodes t in the region $t < 0.5$, which corroborate our theoretical result presented in Lemma 2.

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 a technique to mitigate the effect of the Byzantines. More specifically, we explore the problem of designing a robust tree topology considering the Byzantine to incur a cost for attacking the network and the FC to incur a cost for deploying (including the cost of protection, etc.) the network. The FC (network designer) tries to design a perfect a-ary tree topology under its cost budget constraint such that the system performance metric, i.e., KLD is maximized. Byzantines, on the other hand, are interested in attacking or capturing nodes to cause maximal possible degradation in system performance, with the cost of attacking or capturing nodes not to exceed the attacker's budget. This problem can be formulated as a bi-level programming problem where the upper and the lower level problems with conflicting objectives belong to the leader (FC) and the follower (Byzantines), respectively.

IV. ROBUST TOPOLOGY DESIGN

In this problem setting, it is assumed that there is a cost associated with attacking each node in the tree (which may represent resources required for capturing a node or cloning a node in some cases). We also assume that the costs for attacking nodes at different levels are different. Specifically, let c_k be the cost of attacking any one node at level k. Also, we assume $c_k > c_{k+1}$ for $k = 1, \cdots, K-1$, i.e., it is more costly to attack nodes that are closer to the FC. Observe that, a node i at level k covers (in other words, can alter the decisions of) all its successors and node i itself. It is assumed that the network designer or the FC has a cost budget $C_{budget}^{network}$ and the attacker has a cost budget $C_{budget}^{attacker}$. Let P_k denote the number of nodes covered by a node at level k. We refer to P_k as the "profit" of a node at level k. Notice that, $P_k = \dfrac{\sum_{i=k+1}^{K} N_i}{N_k} + 1$.

Notice that, in a tree topology, P_k can be written as

$$P_k = a_k \times P_{k+1} + 1 \qquad for \ k = 1, ..., K-1, \qquad (28)$$

where P_k is the profit of attacking a node at level k, P_{k+1} is the profit of attacking a node at level $k + 1$ and a_k is the number of immediate children of a node at level k. For a perfect a-ary tree $a_k = a$, $\forall k$ and $P_k = \dfrac{a^{K-k+1}-1}{a-1}$. The FC designs the network, such that, given the attacker's budget, the fraction of covered nodes is minimized, and consequently a more robust perfect a-ary tree in terms of KLD (See Lemma 2) is generated. Next, we formulate our robust topology design problem.

A. Robust Perfect a-ary Tree Topology Design

Since the attacker aims to maximize the fraction of covered nodes by attacking/capturing $\{B_k\}_{k=1}^K$ nodes within the cost budget $C_{budget}^{attacker}$, the FC's objective is to minimize the fraction of covered nodes by choosing the parameters (K, a) optimally in a perfect a-ary tree topology $T(K, a)$ under its cost budget $C_{budget}^{network}$. This situation can be interpreted as a Bi-level optimization problem, where the first decision maker (the so-called leader) has the first choice, and the second one (the so-called follower) reacts optimally to the leader's selection. It is the leader's aim to find such a decision which, together with the optimal response of the follower, optimizes the objective function of the leader. 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. We assume that the FC has complete information about the attacker's problem, i.e., the objective function and the constraints of the LLP. Similarly, the attacker is assumed to be aware about the FC's resources, i.e., cost of deploying the nodes $\{c_k\}_{k=1}^K$. Next, we formalize our robust perfect a-ary tree topology problem as follows:

$$
\begin{aligned}
\underset{(K,\, a)\in\mathbb{Z}^+}{\text{minimize}} \quad & \frac{\sum_{k=1}^K (a^{K-k+1} - 1) B_k}{a(a^K - 1)} \\
\text{subject to} \quad & a_{min} \le a \le a_{max} \\
& K \ge K_{min} \\
& \sum_{k=1}^K a^k \ge N_{min} \\
& \sum_{k=1}^K c_k a^k \le C_{budget}^{network} \\
\underset{B_k\in\mathbb{Z}^+}{\text{maximize}} \quad & \frac{\sum_{k=1}^K (a^{K-k+1} - 1) B_k}{a(a^K - 1)} \\
\text{subject to} \quad & \sum_{k=1}^K c_k B_k \le C_{budget}^{attacker} \\
& B_k \le a^k, \forall k = 1, 2, \ldots, K
\end{aligned} \tag{29}
$$

where $\mathbb{Z}^+$ is the set of non-negative integers, $a_{min} \ge 2$ and $K_{min} \ge 2$. The objective function in ULP is the fraction of covered nodes by the Byzantines $\frac{\sum_{k=1}^K P_k B_k}{\sum_{k=1}^K N_k}$, where $P_k = \frac{a^{K-k+1} - 1}{a-1}$ and $\sum_{k=1}^K N_k = \frac{a(a^K - 1)}{a-1}$. In the constraint $a_{min} \le a \le a_{max}$, a_{max} represents the hardware constraint imposed by the Medium Access Control (MAC) scheme used and a_{min} represents the design constraint enforced by the FC. The constraint on the number of nodes in the network $\sum_{k=1}^K a^k \ge N_{min}$ ensures that the network satisfies pre-specified detection performance guarantees. In other words, N_{min} is the minimum number of nodes needed to guarantee a certain detection performance. The constraint on the cost expenditure $\sum_{k=1}^K c_k a^k \le C_{budget}^{network}$ ensures that the total expenditure of the network designer does not exceed the available budget.

In the LLP, the objective function is the same as that of the FC, but the sense of optimization is opposite, i.e.,

maximization of the fraction of covered nodes. The constraint $\sum_{k=1}^K c_k B_k \le C_{budget}^{attacker}$ ensures that the total expenditure of the attacker does not exceed the available budget. The constraints $B_k \le a^k$, $\forall k$ are logical conditions, which prevent the attacker from attacking non-existing resources.

Notice that, the bi-level optimization problem, in general, is an NP-hard problem [25]. In fact, the optimization problem corresponding to LLP is the packing formulation of the Bounded Knapsack Problem (BKP) [26], which itself, in general, is NP-hard. Next, we discuss some properties of our objective function that enable our robust topology design problem to have a polynomial time solution.

Lemma 3. *In a perfect a-ary tree topology, the fraction of covered nodes $\frac{\sum_{k=1}^K P_k B_k}{\sum_{k=1}^K N_k}$ by the attacker with the cost budget $C_{budget}^{attacker}$ for an optimal attack is a non-decreasing function of the number of levels K in the tree.*

Proof: Let us denote the optimal attack configuration for a K level *perfect a-ary* tree topology $T(K, a)$ by $\{B_k^1\}_{k=1}^K$ and the optimal attack configuration for a *perfect a-ary* tree topology with $K+1$ levels by $\{B_k^2\}_{k=1}^{K+1}$ given the cost budget $C_{budget}^{attacker}$. To prove the lemma, it is sufficient to show that

$$
\frac{\sum_{k=1}^{K+1} P_k^2 B_k^2}{\sum_{k=1}^{K+1} N_k} \ge \frac{\sum_{k=1}^K P_k^2 B_k^1}{\sum_{k=1}^{K+1} N_k} \ge \frac{\sum_{k=1}^K P_k^1 B_k^1}{\sum_{k=1}^K N_k} \tag{30}
$$

where P_k^1 is the profit of attacking a node at level k in a K level *perfect a-ary* tree topology and P_k^2 is the profit of attacking a node at level k in a $K+1$ level *perfect a-ary* tree topology.

First inequality in (30) follows due to the fact that $\{B_k^1\}_{k=1}^K$ may not be the optimal attack configuration for topology $T(K+1, a)$. To prove the second inequality observe that, an increase in the value of parameter K results in an increase in both the denominator (number of nodes in the network) and the numerator (fraction of covered nodes). Using this fact, let us denote

$$
\frac{\sum_{k=1}^K P_k^2 B_k^1}{\sum_{k=1}^{K+1} N_k} = \frac{x + x_1}{y + y_1} \tag{31}
$$

with $x = \sum_{k=1}^K P_k^1 B_k^1$ with $P_k^1 = \frac{a^{K-k+1} - 1}{a - 1}$, $y = \sum_{k=1}^K N_k = \frac{a(a^K - 1)}{a - 1}$, $x_1 = \sum_{k=1}^K (B_k^1 a^{K-k+1})$ is the increase in the profit by adding one more level to the topology and $y_1 = a^{K+1}$ is the increase in the number of nodes in the network by adding one more level to the topology .

Note that $\frac{x + x_1}{y + y_1} > \frac{x}{y}$ if and only if

$$
\frac{x}{y} < \frac{x_1}{y_1}, \tag{32}
$$

where $x, y, x_1,$ and y_1 are positive values. Hence, it is sufficient to prove that

$$
\frac{a^{K+1} \sum_{k=1}^K \left(\frac{B_k^1}{a^k} \right) - \sum_{k=1}^K B_k^1}{a(a^K - 1)} \le \frac{\sum_{k=1}^K (B_k^1 a^{K-k+1})}{a^{K+1}}.
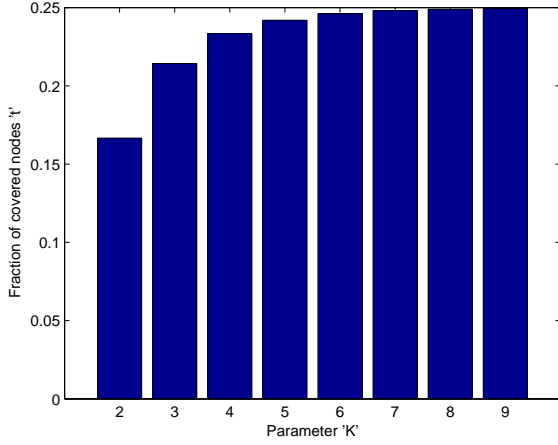$$

Fig. 4. Fraction of nodes covered vs Parameter K when $a = 2$, K is varied from 2 to 9, $[c_1, \cdots, c_9] = [52, 48, 24, 16, 12, 8, 10, 6, 4]$, and $C_{budget}^{attacker} = 50$

The above equation can be further simplified to

$$\sum_{k=1}^{K} \left(\frac{B_k^1}{a^k} \right) \leq \sum_{k=1}^{K} \left(\frac{B_k^1}{a} \right)$$

which is true for all $K \geq 1$. ∎

Next, to gain insights into the solution, we present some numerical results in Figure 4 that corroborate our theoretical results. We plot the fraction of covered nodes by the Byzantines as a function of the total number of levels in the tree. We assume that $a = 2$ and vary K from 2 to 9. We also assume that the cost to attack nodes at different levels are given by $[c_1, \cdots, c_9] = [52, 48, 24, 16, 12, 8, 10, 6, 4]$ and the cost budget of the attacker is $C_{budget}^{attacker} = 50$. For each $T(K, 2)$, we find the optimal attack configuration $\{B_k\}_{k=1}^{K}$ by an exhaustive search. It can be seen that the fraction of covered nodes is a non-decreasing function of the number of levels K, which corroborate our theoretical result presented in Lemma 3.

Next, we explore some properties of the fraction of covered nodes with parameter a for a *perfect a-ary* tree topology. Before discussing our result, we define the parameter a_{min} as follows. For a fixed K and attacker's cost budget $C_{budget}^{attacker}$, a_{min} is defined as the minimum value of a for which the attacker cannot blind the network or cover 50% or more nodes. So we can restrict our analysis to $a_{min} \leq a \leq a_{max}$. Notice that, the attacker cannot blind all the trees $T(K, a)$ for which $a \geq a_{min}$ and can blind all the trees $T(K, a)$ for which $a < a_{min}$.

Lemma 4. *In a perfect a-ary tree topology, the fraction of covered nodes $\frac{\sum_{k=1}^{K} P_k B_k}{\sum_{k=1}^{K} N_k}$ by an attacker with cost budget $C_{budget}^{attacker}$ in an optimal attack is a decreasing function of parameter a for a perfect a-ary tree topology for $a \geq a_{min} \geq 2$.*

Proof: As before, let us denote the optimal attack configuration for a K level *perfect a-ary* tree topology $T(K, a)$ by $\{B_k^1\}_{k=1}^{K}$ and the optimal attack configuration for a *perfect*

(a+1)-ary tree topology $T(K, a+1)$ by $\{B_k^2\}_{k=1}^{K}$ given the cost budget $C_{budget}^{attacker}$. To prove the lemma, it is sufficient to show that

$$\frac{\sum_{k=1}^{K} P_k^2 B_k^2}{\sum_{k=1}^{K} N_k^2} < \frac{\sum_{k=1}^{K} P_k^1 B_k^2}{\sum_{k=1}^{K} N_k^1} \leq \frac{\sum_{k=1}^{K} P_k^1 B_k^1}{\sum_{k=1}^{K} N_k^1} \quad (33)$$

where N_k^1 is the number of nodes at level k in $T(K, a)$, N_k^2 is the number of nodes at level k in $T(K, a+1)$, P_k^1 is the profit of attacking a node at level k in $T(K, a)$ and P_k^2 is the profit of attacking a node at level k in $T(K, a+1)$. Observe that, an interpretation of (33) is that the attacker is using the attack configuration $\{B_k^2\}_{k=1}^{K}$ to attack $T(K, a)$. However, one might suspect that the set $\{B_k^2\}_{k=1}^{k=K}$ is not a valid solution. More specifically, the set $\{B_k^2\}_{k=1}^{k=K}$ is not a valid solution in the following two cases:

1. $min(B_k^2, N_k^1) = N_k^1$ *for any k:* For example, if $N_1^1 = 4$ for $T(K, 4)$ and $B_1^2 = 5$ for $T(K, 5)$ then it will not be possible for the attacker to attack 5 nodes at level 1 in $T(K, 4)$ because the total number of nodes at level 1 is 4. In this case, $\{B_k^2\}_{k=1}^{K}$ might not be a valid attack configuration for the tree $T(K, a)$.

2. $\{B_k^2\}_{k=1}^{k=K}$ *is an overlapping set[3] for $T(K, a)$:* For example, for $T(2, 3)$ if $B_1^2 = 2$ and $B_2^2 = 4$, then, B_1^2 and B_2^2 are overlapping. In this case, $\{B_k^2\}_{k=1}^{K}$ might not be a valid attack configuration for the tree $T(K, a)$.

However, both of the above conditions imply that the attacker can blind the network with $C_{budget}^{attacker}$ (See Appendix A), which cannot be true for $a \geq a_{min}$, and, therefore, $\{B_k^2\}_{k=1}^{K}$ will indeed be a valid solution. Therefore, (33) is sufficient to prove the lemma.

Notice that, the second inequality in (33) follows due to the fact that $\{B_k^2\}_{k=1}^{K}$ may not be the optimal attack configuration for topology $T(K, a)$. To prove the first inequality in (33), we first consider the case where attack configuration $\{B_k^2\}_{k=1}^{k=K}$ contains only one node, i.e., $B_k^2 = 1$ for some k, and show that $\frac{P_k^2}{\sum_{k=1}^{K} N_k^2} < \frac{P_k^1}{\sum_{k=1}^{K} N_k^1}$. Substituting $P_k^1 = \frac{a^{K-k+1} - 1}{a - 1}$ for some k and $\sum_{k=1}^{K} N_k^1 = \frac{a(a^K - 1)}{a - 1}$ in the left side inequality of (33), we have

$$\frac{(a)^{K-k+1} - 1}{(a)((a)^K - 1)} > \frac{(a+1)^{K-k+1} - 1}{(a+1)((a+1)^K - 1)}.$$

After some simplification, the above condition becomes

$$(a+1)^{K+1}[(a)^{K-k+1} - 1] - (a)^{K+1}[(a+1)^{K-k+1} - 1]$$
$$+ a[(a+1)^{K-k+1} - 1] - (a+1)[(a)^{K-k+1} - 1] > 0. \quad (34)$$

In Appendix B, we show that

$$(a)[(a+1)^{K-k+1} - 1] - (a+1)[(a)^{K-k+1} - 1] > 0 \quad (35)$$

and

$$(a+1)^{K+1}[a^{K-k+1} - 1] - a^{K+1}[(a+1)^{K-k+1} - 1] \geq 0. \quad (36)$$

[3]We call B_k and B_{k+x} are overlapping, if the summation of B_k^{k+x} and B_{k+x} is greater than N_{k+x}, where B_k^{k+x} is the number of nodes covered by the attack configuration B_k at level $k + x$. In a non-overlapping case, the attacker can always arrange nodes $\{B_k\}_{k=1}^{K}$ such that each path in the network has at most one Byzantine.
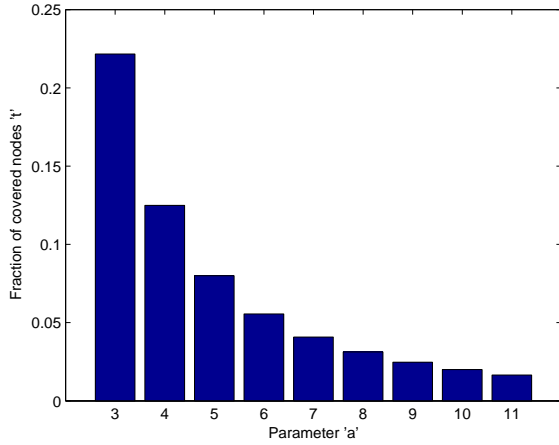
Fig. 5. Fraction of nodes covered vs Parameter a when $K = 6$, parameter a is varied from 3 to 11, $[c_1, \cdots, c_9] = [52, 48, 24, 16, 12, 8, 10, 6, 4]$, and $C_{budget}^{attacker} = 50$

From (36) and (35), condition (34) holds.

Since we have proved that

$$\frac{P_k^2}{\sum_{k=1}^K N_k^2} < \frac{P_k^1}{\sum_{k=1}^K N_k^1} \text{ for all } 1 \leq k \leq K,$$

to generalize the proof for any arbitrary attack configuration $\{B_k^2\}_{k=1}^K$ we multiply both sides of the above inequality with B_k^2 and sum it over all $1 \leq k \leq K$ inequalities. Now, we have

$$\frac{\sum_{k=1}^K P_k^2 B_k^2}{\sum_{k=1}^K N_k^2} < \frac{\sum_{k=1}^K P_k^1 B_k^2}{\sum_{k=1}^K N_k^1}.$$

∎

Next, to gain insights into the solution, we present some numerical results in Figure 5 that corroborate our theoretical results. We plot the fraction of covered nodes by the Byzantines as a function of the parameter a in the tree. We assume that the parameter $K = 6$ and vary a from 3 to 11. We also assume that the cost to attack nodes at different levels are given by $[c_1, \cdots, c_9] = [52, 48, 24, 16, 12, 8, 10, 6, 4]$ and the cost budget of the attacker is $C_{budget}^{attacker} = 50$. For each $T(6, a)$ we find the optimal attack configuration $\{B_k\}_{k=1}^K$ by an exhaustive search. It can be seen that the fraction of covered nodes is a decreasing function of the parameter a, which corroborate our theoretical result presented in Lemma 4. Note that, while deriving the results in Lemma 3 and Lemma 4 we have made no additional assumptions on how the attack configuration $\{B_k\}_{k=1}^K$ is obtained, so that the two lemmas would still hold even if the cost of deploying a node ($c_k^{network}$) is different from the cost of attacking ($c_k^{attacker}$) it. Further, as noted in the paper, Lemma 3 and Lemma 4 suggest that the solution of the upper level problem, i.e., (K, a), is independent of the solution of lower level problem, i.e., $\{B_k\}_{k=1}^K$. In other words, even if $c_k^{network} \neq c_k^{attacker}$, the proposed solution approach would still hold.

Next, based on the above Lemmas we present an algorithm which can solve our robust perfect a-ary tree topology design problem (bi-level programming problem) efficiently.

B. Algorithm for solving Robust Perfect a-ary Tree Topology Design Problem

---
Algorithm 1 Robust Perfect a-ary Tree Topology Design

Require: $c_k > c_{k+1} \quad for \ k = 1, ..., K - 1$
1: $K \leftarrow K_{min}; a \leftarrow a_{max}$
2: **if** $\left(\sum_{k=1}^K c_k a^k > C_{budget}^{network} \right)$ **then**
3:     Find the largest integer $a - \ell$, $\ell \geq 0$, such that $\sum_{k=1}^K c_k (a - \ell)^k \leq C_{budget}^{network}$
4:     **if** $(a - \ell < a_{min})$ **then**
5:         **return** (ϕ, ϕ)
6:     **else**
7:         $a \leftarrow a - \ell$
8:     **end if**
9: **end if**
10: **if** $\left(\sum_{k=1}^K a^k \geq N_{min} \right)$ **then**
11:     **return** (K, a)
12: **else**
13:     $K \leftarrow K + 1$
14:     **return to** Step 2
15: **end if**

Based on Lemma 3 and Lemma 4, we present a polynomial time algorithm for solving the robust perfect a-ary tree topology design problem. Observe that, the robust network design problem is equivalent to designing perfect a-ary tree topology with minimum K and maximum a that satisfy network designer's constraints. In Algorithm 1, we start with the solution candidate (K_{min}, a_{max}). First, the algorithm finds the largest integer $(a_{max} - l)$, $l \geq 0$ that satisfies the cost expenditure constraint. If this value violates the hardware constraint, i.e., $(a_{max} - l) < a_{min}$, we will not have any feasible solution which satisfies the network designer's constraints. Next, the algorithm checks if $(K_{min}, (a_{max} - l))$ satisfies the total number of nodes constraint. If it does, this will be the solution for the problem, otherwise, we increase K_{min} by one, i.e., $K_{min} \leftarrow K_{min} + 1$. Now, we have a new solution candidate $(K_{min} + 1, (a_{max} - l))$ and the algorithm solves the problem recursively in this manner.

This procedure greatly reduces the complexity because we do not need to solve the lower level problem in this case. Next, we prove that Algorithm 1 indeed yields an optimal solution.

Lemma 5. *Robust Perfect a-ary Tree Topology Design algorithm (Algorithm 1) yields an optimal solution* (K^*, a^*), *if one exists.*

Proof: Assume that the optimal solution exists. Let us denote by (K^*, a^*), the optimal solution given by Algorithm 1. The main idea behind our proof is that any solution (K, a) with $K \geq K^*$ and $a \leq a^*$ cannot perform better than (K^*, a^*) as suggested by Lemma 3 and Lemma 4. This property implies that the search should start with the smallest possible K and simultaneously the largest a, i.e., (K_{min}, a_{max}).

Notice that, our algorithm searches for the feasible solution with the smallest K and the largest a. Any feasible solution (K, a) satisfies the following two conditions:

  1) $\sum_{k=1}^K c_k a^k \leq C_{budget}^{network}$;
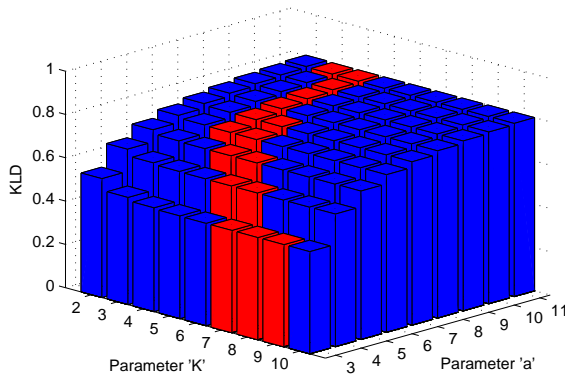 2) $\sum_{k=1}^K a^k \geq N_{min}$.

Fig. 6. KLD vs Parameters K and a when $(P_d, P_{fa}) = (0.8, 0.2)$, $C_{budget}^{network} = 400000$, $C_{budget}^{attacker} = 50$ and $N_{min} = 1400$

By Lemma 4, if (K, a) is a feasible solution, then (K, a') with $a' < a$ will not be a better solution than (K, a). Hence, for a given K, Step 3 only locates the solution with largest a for a given K. Furthermore, if both (K, a) and (K', a') satisfy Condition 1 and $K < K'$, then $a \geq a'$. Hence, for a given K, the largest a in the current iteration satisfying Condition 1 cannot be larger than the a found in the previous iteration. This verifies that $\ell \geq 0$ is a sufficient condition to find the largest a in Step 3.

Next, we prove that Algorithm 1 stops when the first feasible solution has been found. That is, the first feasible solution found by the algorithm is (K^*, a^*). Let (K^1, a^1) be the first feasible solution found by Algorithm 1. It can be observed from the algorithm that $K^* \geq K^1$ since the algorithm increases K from its smallest possible value and has not found a feasible solution until $K = K^1$. It is clear that the next feasible solution (K, a) must have $K > K^1$ and $a \leq a^1$, since, the algorithm increases K and it satisfies Condition 1. As suggested by Lemma 3 and Lemma 4, (K, a) cannot be a better solution than (K^1, a^1). Hence, $K^* = K^1$ and (K^1, a^1) is equal to (K^*, a^*).

It can be seen that if there is no solution, then the algorithm will return $(\emptyset, \emptyset)$. This is due to the fact that if $a - \ell < a_{min}$, then no a can satisfy Condition 1 for current and further iterations. Hence, the algorithm terminates and returns $(\emptyset, \emptyset)$. ∎

Next, to gain insights into the solution, we present some numerical results in Figure 6 that corroborate our theoretical results. We plot the $\min_{P_{1,0}, P_{0,1}}$ KLD for all the combinations of parameter K and a in the tree. We vary the parameter K from 2 to 10 and a from 3 to 11. We also assume that the costs to attack nodes at different levels are given by $[c_1, \cdots, c_{10}] = [52, 50, 25, 24, 16, 10, 8, 6, 5, 4]$, and cost budgets of the network and the attacker are given by $C_{budget}^{network} = 400000$, $C_{budget}^{attacker} = 50$, respectively. The node budget constraint is assumed to be $N_{min} = 1400$. For each $T(K, a)$, we find the optimal attack configuration $\{B_k\}_{k=1}^K$ by an exhaustive search. All the feasible solutions are plotted in red and unfeasible solutions are plotted in blue. Notice

that, $T(K_{min}, a_{max})$ which is $T(2, 11)$ is not a feasible solution and, therefore, if we use Algorithm 1 it will try to find the feasible solution which has minimum possible deviation from $T(K_{min}, a_{max})$. It can be seen that the optimal solution $T(3, 11)$ has minimum possible deviation from the $T(K_{min}, a_{max})$, which corroborate our algorithm.

V. CONCLUSION

In this paper, we have considered distributed detection in perfect a-ary tree topologies in the presence of Byzantines, and characterized the power of attack analytically. We provided closed-form expressions for minimum attacking power required by the Byzantines to blind the FC. We obtained closed form expressions for the optimal attacking strategies that minimize the detection error exponent at the FC. We also looked at the possible counter-measures from the FC's perspective to protect the network from these Byzantines. We formulated the robust topology design problem as a bi-level program and provided an efficient algorithm to solve it. There are still many interesting questions that remain to be explored in the future work such as an analysis of the problem for arbitrary topologies. Note that, some analytical methodologies used in this paper are certainly exploitable for studying the attacks in different topologies. Other questions such as the case where Byzantines collude in several groups (collaborate) to degrade the detection performance can also be investigated.

APPENDIX A

We want to show that the set $\{B_k\}_{k=1}^K$ can blind the FC if any of following two cases is true.
1. $min(B_k, N_k) = N_k$ for any k,
2. $\{B_k\}_{k=1}^{k=K}$ is an overlapping set
In other words, set $\{B_k\}_{k=1}^K$ covers 50% or more nodes. Let us denote by $\tilde{k}$, the k for which $min(B_k, N_k) = N_k$ (there can be multiple such k). Then $\{B_k\}_{k=1}^K$ satisfies

$$\frac{\sum_{k=1}^K P_k B_k}{\sum_{k=1}^K N_k} \geq \frac{P_{\tilde{k}} B_{\tilde{k}}}{\sum_{k=1}^K N_k} \geq \frac{P_{\tilde{k}} N_{\tilde{k}}}{\sum_{k=1}^K N_k} \geq \frac{P_K N_K}{\sum_{k=1}^K N_k}. \quad (37)$$

Similarly, let us assume $B_{k'}$ and $B_{\tilde{k}}$ are overlapping with $\tilde{k} = k' + x$ (there can be multiple overlapping k). Then $\{B_k\}_{k=1}^K$ satisfies

$$\frac{\sum_{k=1}^K P_k B_k}{\sum_{k=1}^K N_k} \geq \frac{P_{\tilde{k}} B_{\tilde{k}} + P_{k'} B_{k'}}{\sum_{k=1}^K N_k} \geq \frac{P_{\tilde{k}} N_{\tilde{k}}}{\sum_{k=1}^K N_k} \geq \frac{P_K N_K}{\sum_{k=1}^K N_k}. \quad (38)$$

Observe that, to prove our claim it is sufficient to show that

$$\frac{P_K N_K}{\sum_{k=1}^K N_k} \geq 0.5 \Leftrightarrow P_K N_K \geq \frac{N}{2}. \quad (39)$$

Using the fact that for a Perfect a-ary tree $P_K = 1$, $N_K = a^K$ and $N = \frac{a(a^K - 1)}{a - 1}$ the condition (39) becomes

$$2 \times a^K \geq \frac{a(a^K - 1)}{a - 1}. \quad (40)$$

When $a \geq 2$, we have

$$
\begin{aligned}
& a \times a^K \geq 2 \times a^K \\
\Leftrightarrow\quad & a + a^{K+1} \geq 2 \times a^K \\
\Leftrightarrow\quad & 2 \times a^{K+1} - 2 \times a^K \geq a^{K+1} - a \\
\Leftrightarrow\quad & 2 \times a^K \geq \frac{a(a^K - 1)}{a - 1}.
\end{aligned}
$$

Hence, (39) holds and this completes our proof.

APPENDIX B

We skip the proof of (35) and only focus on the proof of (36). To show

$$
(a+1)^{K+1}[(a)^{K-k+1} - 1] - (a)^{K+1}[(a+1)^{K-k+1} - 1] \geq 0 \text{ for } a \geq 2
$$

is equivalent to show

$$
a^{K+1}[(a-1)^{K-k+1} - 1] - (a-1)^{K+1}[a^{K-k+1} - 1] \geq 0 \text{ for } a \geq 3
$$

which can be simplified to

$$
(a(a-1))^{K-k+1}[a^k - (a-1)^k] \geq [a^{K+1} - (a-1)^{K+1}]. \quad (41)
$$

Using binomial expansion, (41) becomes

$$
(a(a-1))^{K-k+1}[a^{k-1} + (a-1)a^{k-2} + \cdots + (a-1)^{k-1}] \geq
$$
$$
[a^K + (a-1)a^{K-1} + \cdots + (a-1)^{K-1}a + (a-1)^K]
$$
$$
\Leftrightarrow\quad (a-1)^{K-k+1}\underbrace{[a^K + (a-1)a^{K-1} + \cdots + (a-1)^{k-1}a^{K-k+1}]}_{k \text{ terms}} \geq
$$
$$
\underbrace{[a^K + (a-1)a^{K-1} + \cdots + (a-1)^{k-1}a^{K-k+1}]}_{k \text{ terms}} +
$$
$$
\underbrace{[(a-1)^k a^{K-k} + \cdots + (a-1)^{K-1}a + (a-1)^K]}_{K-k+1 \text{ terms}}
$$
$$
\Leftrightarrow\quad ((a-1)^{K-k+1} - 1)[a^K + \cdots + (a-1)^{k-1}a^{K-k+1}] \geq
$$
$$
[(a-1)^k a^{K-k} + \cdots + (a-1)^{K-1}a + (a-1)^K]. \quad (42)
$$

Since $a \geq 3$, we have $((a-1)^{K-k+1} - 1) \geq (K-k+1) \geq 1$. Hence,

$$
((a-1)^{K-k+1} - 1)[a^K + \cdots + (a-1)^{k-1}a^{K-k+1}] \geq
$$
$$
((a-1)^{K-k+1} - 1)a^K \geq \underbrace{[(a-1)^k a^{K-k} + \cdots + (a-1)^K]}_{K-k+1 \text{ terms}} \quad (43)
$$

and (42) holds.

REFERENCES

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

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

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

[4] Y. Lin, B. Chen, and P. Varshney, "Decision fusion rules in multi-hop wireless sensor networks," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 41, no. 2, pp. 475 – 488, april 2005.

[5] P. Kulkarni, D. Ganesan, P. Shenoy, and Q. Lu, "Senseye: a multi-tier camera sensor network," in *Proc. 13th annual ACM international conference on Multimedia*, 2005.

[6] Aliance, "Z. Zigbee Specifications," *Zigbee Standard Organisation*, 2008.

[7] IEEE. P802.22b Draft Standard for Wireless Regional Area Networks (WRAN)–Specific requirements Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands Amendment: Enhancement for Broadband Services and Monitoring Applications.

[8] 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

[9] A. Vempaty, L. Tong, and P. Varshney, "Distributed Inference with Byzantine Data: State-of-the-Art Review on Data Falsification Attacks," *Signal Processing Magazine, IEEE*, vol. 30, no. 5, pp. 65–75, 2013.

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

[11] 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

[12] 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.

[13] 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.

[14] B. Kailkhura, S. Brahma, and P. K. Varshney, "Optimal Byzantine Attack on Distributed Detection in Tree based Topologies," in *Proc. International Conference on Computing, Networking and Communications Workshops (ICNC-2013)*, San Diego, CA, January 2013, pp. 227–231.

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

[16] 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.

[17] E. Soltanmohammadi, M. Orooji, and M. Naraghi-Pour, "Decentralized hypothesis testing in wireless sensor networks in the presence of misbehaving nodes," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 205–215, 2013.

[18] S. Liu, M. Chen, S. Sengupta, M. Chiang, J. Li, and P. Chou, "P2P Streaming Capacity under Node Degree Bound," in *Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on*, 2010, pp. 587–598.

[19] S. Karande and H. Radha, "Influence of Graph Properties of Peer-to-Peer Topologies on Video Streaming with Network Channel Coding," in *Multimedia and Expo, 2006 IEEE International Conference on*, 2006, pp. 825–828.

[20] M. R. Garey and D. S. Johnson, *Computers and Intractability; A Guide to the Theory of NP-Completeness*. New York, NY, USA: W. H. Freeman & Co., 1990.

[21] O. Gurewitz, A. de Baynast, and E. W. Knightly, "Cooperative Strategies and Achievable Rate for Tree Networks With Optimal Spatial Reuse," *IEEE Trans. Inf. Theor.*, vol. 53, no. 10, pp. 3596–3614, Oct. 2007. [Online]. Available: http://dx.doi.org/10.1109/TIT.2007.905000

[22] S. Jafarizadeh, "Fastest Distributed Consensus Averaging Problem on Perfect and Complete n-ary Tree networks," *CoRR*, vol. abs/1005.2662, 2010.

[23] V. N. Padmanabhan, H. J. Wang, P. A. Chou, and K. Sripanidkulchai, "Distributing streaming media content using cooperative networking," in *Proc. International Workshop on Network and Operating Systems Support for Digital Audio and Video*, ser. NOSSDAV '02. New York, NY, USA: ACM, 2002, pp. 177–186. [Online]. Available: http://doi.acm.org/10.1145/507670.507695

[24] S. Kullback, *Information Theory and Statistics*. New York:Wiley, 1968.

[25] J. Bard, "Some properties of the bilevel programming problem," *Journal of Optimization Theory and Applications*, vol. 68, no. 2, pp. 371–378, 1991. [Online]. Available: http://dx.doi.org/10.1007/BF00941574

[26] V. G. Deineko and G. J. Woeginger, "A well-solvable special case of the bounded knapsack problem," *Operations Research Letters*, vol. 39, pp. 118–120, 2011.

Bhavya Kailkhura (S'12) received the M.S. degree in electrical engineering from Syracuse University, Syracuse, NY. Since 2012, he has been pursuing the Ph.D. degree with the Department of Electrical Engineering and Computer Science, Syracuse University. His research interests include statistical signal processing, security in sensor networks, compressive sensing, and machine learning.

Swastik Brahma received the B.Tech degree in Computer Science and Engineering from West Bengal University of Technology, Kolkata, India in 2005. He received 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 (EECS) at Syracuse University, Syracuse, NY, as a Research Associate, where he is currently a Research Scientist. His research interests include wireless communications, detection and estimation theory, security, and applied game theory. He serves as a technical program committee member for several conferences. Dr. Brahma won the best paper award in the IEEE Globecom conference in 2008, and was the recipient of the best Ph.D. forum award in the IEEE WoWMoM conference in 2009.

Yunghsiang S. Han (S'90-M'93-SM'08-F'11) was born in Taipei, Taiwan, 1962. He received B.Sc. and M.Sc. degrees in electrical engineering from the National Tsing Hua University, Hsinchu, Taiwan, in 1984 and 1986, respectively, and a Ph.D. degree from the School of Computer and Information Science, Syracuse University, Syracuse, NY, in 1993. He was from 1986 to 1988 a lecturer at Ming-Hsin Engineering College, Hsinchu, Taiwan. He was a teaching assistant from 1989 to 1992, and a research associate in the School of Computer and Information Science, Syracuse University from 1992 to 1993. He was, from 1993 to 1997, an Associate Professor in the Department of Electronic Engineering at Hua Fan College of Humanities and Technology, Taipei Hsien, Taiwan. He was with the Department of Computer Science and Information Engineering at National Chi Nan University, Nantou, Taiwan from 1997 to 2004. He was promoted to Professor in 1998. He was a visiting scholar in the Department of Electrical Engineering at University of Hawaii at Manoa, HI from June to October 2001, the SUPRIA visiting research scholar in the Department of Electrical Engineering and Computer Science and CASE center at Syracuse University, NY from September 2002 to January 2004 and July 2012 to June 2013, and the visiting scholar in the Department of Electrical and Computer Engineering at University of Texas at Austin, TX from August 2008 to June 2009. He was with the Graduate Institute of Communication Engineering at National Taipei University, Taipei, Taiwan from August 2004 to July 2010. From August 2010, he is with the Department of Electrical Engineering at National Taiwan University of Science and Technology as 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 and a Fellow of IEEE. One of his papers won the prestigious 2013 ACM CCS Test-of-Time Award in cybersecurity.

Pramod K. Varshney (S'72-M'77-SM'82-F'97) was born in Allahabad, India, on July 1, 1952. He received the B.S. degree in electrical engineering and computer science (with highest honors), 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.

From 1972 to 1976, he held teaching and research assistantships with the University of Illinois. 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 CASE: Center for Advanced Systems and Engineering. He served as the Associate Chair of the department from 1993 to 1996. He is also an Adjunct Professor of Radiology at Upstate Medical University, Syracuse. 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. He has published extensively. He is the author of Distributed Detection and Data Fusion (New York: Springer-Verlag, 1997). He has served as a consultant to several major companies.

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 the Guest Editor of the Special Issue on Data Fusion of the IEEE PROCEEDINGS January 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. 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.