2019 American Control Conference (ACC)
Philadelphia, PA, USA, July 10-12, 2019

A Game-theoretic Framework for Security-aware Sensor Placement Problem in Networked Control Systems

Mohammad Pirani, Ehsan Nekouei, Henrik Sandberg and Karl Henrik Johansson

***Abstract*— This paper studies the sensor placement problem in a networked control system for improving its security against cyber-physical attacks. The problem is formulated as a zero-sum game between an attacker and a detector. The attacker's decision is to select f nodes of the network to attack whereas the detector's decision is to place f sensors to detect the presence of the attack signals. In our formulation, the attacker minimizes its visibility, defined as the system L_2 gain from the attack signals to the deployed sensors' outputs, and the detector maximizes the visibility of the attack signals. The equilibrium strategy of the game determines the optimal locations of the sensors. The existence of Nash equilibrium for the attacker-detector game is studied when the underlying connectivity graph is a directed or an undirected tree. When the game does not admit a Nash equilibrium, it is shown that the Stackelberg equilibrium of the game, with the detector as the game leader, can be computed efficiently. Our results show that, under the optimal sensor placement strategy, an undirected topology provides a higher security level for a networked control system compared with its corresponding directed topology.**

I. Introduction

A. Motivation

Applications of distributed control systems, ranging from power grids and smart buildings to intelligent transportation systems, have had a considerable growth. In this direction, the need to do a rigorous research on the control-theoretic approaches to the security of these systems against failures and attacks, considering the physical limitations of the system, is seriously felt [1]. Several approaches have been proposed in the literature to tackle this issue [2]–[7] which are based on the system specifications and the attack strategy. An active line of research in this area is to consider the defense mechanism in the control system as a game between the attacker and the defender and optimize the actions of the defender against possible attack strategies. In this direction, the game objective can be the effect of the attack on the system in which the defender tries to minimize. However, one can use such game-theoretic approaches to increase the visibility and awareness of the attacker's actions, which the defender tries to maximize, and the problem introduced in this paper is of this kind. To improve such an awareness against cyber-physical attacks, typically a set of monitoring sensors are deployed in the network and their outputs are used to monitor the security status of the system.

This work is supported by the Knut and Alice Wallenberg Foundation, the Swedish Foundation for Strategic Research and the Swedish Research Council. Authors are with the Department of Automatic Control, KTH Royal Institute of Technology. E-mail: {pirani,nekouei,hsan,kallej}@kth.se.

In a networked control system, the system designer determines the location of the monitoring sensors (or detectors). However, the security level not only depends on the sensors' locations but also on the nodes selected by the attacker to inject the attack signals. These decisions are made by different entities with conflicting objectives. In this paper, the sensor/attack placement problem is posed as a game between an attacker and a detector and the equilibrium solution of the game is used to determine the location of the sensors. This allows the system designer to anticipate the behavior of the attacker and decides the location of sensors such that the impact of the attacker's decision on the security level is minimized.

B. Related Work

There is a vast literature on game-theoretic approaches to the security and resilience of control systems in the past decade; see [8] and references therein. These approaches vary depending on the structure of the cyber-physical system or the specific type of malicious action acting on the cyber layer. In these earlier approaches, at each layer (physical and cyber) a particular game is defined and the concept of *games-in-games* that reflects two interconnected games emerges where the payoff of each game affects the result of the other one [9], [10]. In other approaches, depending on the type of the adversarial behavior (active or passive), appropriate game strategy, e.g., Nash or Stackelberg, was discussed [11]–[13]. In addition to those studies, the evolution of some network control systems are modeled as cooperative games [14] and the resilience of these cooperative games to the actions of adversarial agents or communication failures are investigated [15]–[17].

C. Contributions

In this paper, we study the sensor placement problem in a leader-follower networked dynamical system[1] for improving its security against cyber-physical attacks. The sensors placement problem is posed as a zero-sum game between a detector and an attacker. The detector's strategy is to place f sensors in f nodes of the network to maximize the visibility of the attacker's action. The attacker strategy is to select f nodes to inject its attack signal with minimum visibility to the sensors. The objective of each player is defined as the L_2 gain of the system from the injected signals to the sensors'

[1]Leader-follower systems have diverse applications from multi-agent formation control and vehicle platooning [18] to opinion dynamics in social networks [19].

978-1-5386-7926-5/$31.00 ©2019 AACC

outputs. The equilibrium strategy of the detector determines the location of the sensors.

Our main contributions can be summarized as follows:

- We characterize the pure Nash equilibrium (NE) strategy of the attacker-detector game for $f = 1$ when the underlying connectivity graph is a directed/undirected tree.
- It is shown that this game may not admit a NE for $f > 1$, and instead Stackelberg game between the attacker and detector is analyzed when the detector acts as the game leader. A low complexity algorithm for computing the Stackelberg equilibrium of the game is proposed for both directed and undirected trees.

Our results indicate that the value of the attacker-detector game over a directed tree is at most equal to that over its corresponding undirected tree. This observation signifies the importance of two-way communication links in improving the security of networked control systems against cyber-physical attacks.

Remark 1: Our analytically results are established by deriving a closed-form expression for the system L_2 gain of a networked control system, via graph-theoretic interpretations of its underlying connectivity graph, for both directed and undirected trees. □

D. Notation and Definitions

We use $\mathcal{G}_u = \{\mathcal{V}, \mathcal{E}\}$ to denote an unweighted undirected graph where $\mathcal{V}$ is the set of vertices (or nodes) and $\mathcal{E}$ is the set of undirected edges where $(v_i, v_j) \in \mathcal{E}$ if an only if there exists an undirected edge between v_i and v_j. Moreover $\mathcal{G}_d = \{\mathcal{V}, \mathcal{E}\}$ denotes an unweighted directed graph where $\mathcal{E}$ is the set of directed edges, i.e., $(v_i, v_j) \in \mathcal{E}$ if an only if there exists a directed edge from v_i to v_j. In this paper, directed graphs only have unidirectional edges, i.e., if there exists a direct edge from v_i to v_j in $\mathcal{G}_d$, then there is no direct edge from v_j to v_i. Let $|\mathcal{V}| = n$ and define the adjacency matrix for $\mathcal{G}_d$, denoted by $A_{n\times n}$, to be a binary matrix where $A_{ij} = 1$ if and only if there is an edge from v_j to v_i in $\mathcal{G}_d$ (the adjacency matrix will be a symmetric matrix when the graph is undirected). The *neighbors* of vertex $v_i \in \mathcal{V}$ in the graph $\mathcal{G}_d$ are denoted by the set $\mathcal{N}_i = \{v_j \in \mathcal{V} \mid (v_j, v_i) \in \mathcal{E}\}$. We define the in-degree (or just degree for undirected network) for node v_i as $d_i = \sum_{v_j \in \mathcal{N}_i} A_{ij}$. The Laplacian matrix of an undirected graph is denoted by $L = D - A$, where $D = \mathrm{diag}(d_1, d_2, ..., d_n)$. We use $\mathbf{e}_i$ to indicate the i-th vector of the canonical basis.

E. Organization Of The Paper

The structure of the paper is as follows. In Section II we introduce the mathematical formulation of the attacker-detector game in a leader-follower consensus dynamics. We then analyze equlibriums for this game when the underlying network is an undirected tree, Section III, or a directed tree, Section IV. Section V concludes the paper.

II. Problem Definition

In this section, we propose a game-theoretic approach to the security of a leader-follower networked control system. Consider a connected network $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ comprised of a leader (or reference) agent, denoted by v_ℓ, and a set of follower agents denoted by F . The state of each follower agent $v_j \in F$ evolves based on the interactions with its neighbors as

$$\dot{x}_j(t) = \sum_{v_i \in \mathcal{N}_j} (x_i(t) - x_j(t)). \tag{1}$$

The state of the leader (which should be tracked by the followers) evolves with an exogenous reference signal $u(t)$ as

$$x_\ell(t) = u(t). \tag{2}$$

If the graph is connected, the states of the follower agents will track the reference signal $u(t)$ [20]. We assume without loss of generality that the leader agent is placed last in the ordering of the agents. The updating rule of each agent is prone to an intrusion (or attack).[2] More particularly, there exists an attacker which chooses f nodes in the network to inject the attack signals to.[3] Hence, if the dynamics of follower v_j is influenced by an attacker, it will be in the following form

$$\dot{x}_j(t) = \sum_{v_i \in \mathcal{N}_j} (x_i(t) - x_j(t)) + w_j(t), \tag{3}$$

where $w_j(t) > 0$ represents the attack signal. To detect the presence of the attackers, a defender deploys f dedicated sensors (or detectors) at f specific follower nodes, denoted by $\mathcal{D}$. Thus we have

$$y_i(t) = x_i(t) \quad \text{if} \quad v_i \in \mathcal{D}. \tag{4}$$

where $y_i(t)$ is the output of the sensor (detector) deployed at follower v_i. Aggregating the states of all followers into a vector $x_F(t) \in \mathbb{R}^{n-1}$, and aggregating the attack signals to $\boldsymbol{w}(t)$, equations (1) and (2) along with the output measurement yield the following dynamics

$$\begin{bmatrix} \dot{\boldsymbol{x}}_F(t) \\ \dot{x}_\ell(t) \end{bmatrix} = -\underbrace{\begin{bmatrix} L_g & L_{12} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}}_{L} \begin{bmatrix} \boldsymbol{x}_F(t) \\ x_\ell(t) \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \dot{u}(t) + \begin{bmatrix} B \\ 0 \end{bmatrix} \boldsymbol{w}(t),$$
$$\boldsymbol{y}(t) = C\boldsymbol{x}_F(t), \tag{5}$$

where L_g is called the grounded Laplacian matrix (formed by removing the row and the column corresponding to the leader), the submatrix L_{12} of the graph Laplacian captures the influence of the leader on the followers, $B_{n\times f} = [\mathbf{e}_1, \mathbf{e}_2, ..., \mathbf{e}_f]$, and $C_{f\times n} = [\mathbf{e}_1^T; \mathbf{e}_2^T; ...; \mathbf{e}_f^T]$. In words, for matrices B and C which specify the actions of the attacker and the detector, respectively, there is a single 1 in the i-th row (column) of matrix B (C) if the i-th node is under

[2]We assume that the leader is not affected by the attacks.

[3]The number of nodes under attack in practice is unknown and we can assume f is an upper bound for the number of attacks.

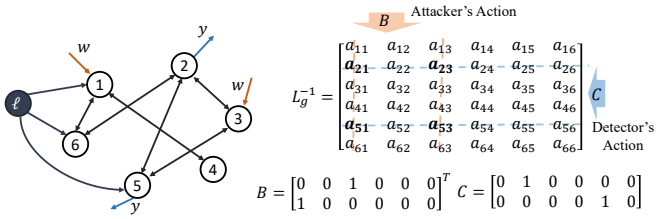

Fig. 1: An Example of an attacker-detector game with $f = 2$.

attack (has a sensor).[4] We assume that there exists at least one attack to the system, i.e., $f \geq 1$. When the graph $\mathcal{G}$ is connected, L_g is nonsingular and L_g^{-1} is nonnegative elementwise [21]. An example of the dynamics in (5) is shown in Fig. 1. In this example, a 2×2 submatrix is chosen by the attacker and the detector from L_g^{-1} which is shown in bold. Based on (5), the dynamics of the follower agents are given by

$$\begin{aligned} \dot{\boldsymbol{x}}_F(t) &= -L_g \boldsymbol{x}_F(t) + L_{12} u(t) + B\boldsymbol{w}(t), \\ \boldsymbol{y}(t) &= C\boldsymbol{x}_F(t). \end{aligned} \tag{6}$$

The following theorem characterizes the system L_2 gain from the attack signal to the output measurement of (6).

Theorem 1 ([20]): The system L_2 gain from the attack signal to the output measurement of (6) is given by

$$\sup_{||\boldsymbol{w}||_2 \neq 0} \frac{||\boldsymbol{y}||_2}{||\boldsymbol{w}||_2} = \sigma_{\max}(G(0)) = \sigma_{\max}(CL_g^{-1}B) \tag{7}$$

where $\sigma_{\max}$ is the maximum singular value of matrix $G(0)$ and the L_2 norm of signal $\boldsymbol{u}$ is $||\boldsymbol{u}||_2^2 \triangleq \int_0^\infty \boldsymbol{u}^T \boldsymbol{u} dt$. □

Based on Theorem 1, the attacker-detector game is defined as follows:

> **Attacker-Detector Game:** We model the interaction between the attacker and the detector as a zero-sum security game. In this game, the attacker's decision is the location of each attack signal, i.e., the matrix B and the detector's decision is the location of sensors, i.e., matrix C. The attacker's objective is to reduce the visibility of the attack signal at the output by minimizing the system L_2 gain (7) whereas the detector's objective is to increase the visibility of the attack signal at the output by maximizing the L_2 gain.

Based on the definition above, the attacker-detector game is a matrix game. For the case $f = 1$, the well-known matrix game is formed with the payoff matrix equal to $[L_g^{-1}]_{ij} \geq 0$. When $f > 1$, the payoff will be the largest singular value of the nonnegative matrix $CL_g^{-1}B$.

Remark 2: The reason of choosing L_2 gain (7) as the game payoff is that the attacker desires to be as stealthy as possible by minimizing the largest system norm (worst case gain from its perspective) over all frequencies. Having this attitude from the attacker, the detector tries to maximize this payoff. □

Next lemma states a property of the non-negative matrices which is helpful in the equilibrium analysis of the attacker-detector game.

Lemma 1 ([22]): The largest singular value of a nonnegative matrix M is a non-decreasing function of its entries. Moreover, if M is irreducible, its singular value is strictly increasing with its entries.

III. Equilibrium Analysis of the Attacker-Detector Game: Undirected Trees

In this section, we analyze the equilibrium of the attacker-detector game on undirected trees. We first provide an explicit characterization of L_g^{-1}, for undirected trees, in terms of the properties of its underlying connectivity graph. This result is helpful in our equilibrium analysis and allows us to investigate the game value. The proof of this result is presented in Appendix A.

Lemma 2: Suppose that $\mathcal{G}_u$ is an undirected tree and let $\mathcal{P}_{i\ell}$ be the set of nodes involved in the (unique) path from the leader node v_ℓ to v_i (including v_i). Then we have

$$[L_g^{-1}]_{ij} = |\mathcal{P}_{i\ell} \cap \mathcal{P}_{j\ell}|. \tag{8}$$

According to this lemma, the (i,j)th element of L_g^{-1} is equal to the number of common edges between the path from the leader to the node v_i and the path from the leader to the node v_j. As an example, $|\mathcal{P}_{3\ell} \cap \mathcal{P}_{6\ell}| = 1$ for nodes 3 and 6 and $|\mathcal{P}_{3\ell} \cap \mathcal{P}_{4\ell}| = 2$ for nodes 3 and 4 in Fig. 2 (a).

A. Equilibrium Analysis: $f = 1$

In the single attacker-detector case, i.e., $B = \mathbf{e}_j$ and $C = \mathbf{e}_i^T$ for some $1 \leq i, j \leq n$, the system L_2 gain will become

$$\mathbf{e}_i^T L_g^{-1} \mathbf{e}_j = [L_g^{-1}]_{ij}, \tag{9}$$

where $[L_g^{-1}]_{ij}$ is the ij-th element of L_g^{-1}.

The following theorem establishes the existence of NE for the attacker-detector game with $f = 1$.

Theorem 2: Let $\mathcal{G}_u$ be an undirected tree and v_ℓ be the leader node. Then, for $f = 1$,

(i) The attacker-detector game admits at least one NE if v_ℓ is not a cut vertex and the game value is 1 for all NE in this case.

(ii) The game does not admit any NE if v_ℓ is a cut vertex.

□

Proof: For part (i), the NE belongs to the case where the attacker (the minimizer) chooses the column corresponding to the leader's neighbor. According to Lemma 2 since all elements of this column are all 1, then, regardless of the actions of the detector, the game payoff will be 1. Moreover, if the attacker chooses a node other than the leader's neighbor, the payoff will be at least 1. Hence, not the attacker, nor the detector have an incentive to change their strategy. For part (ii), if the leader is removed, the graph will be splitted into two parts and the resulting grounded Laplacian matrix, and consequently L_g^{-1}, become block diagonalized. Assume that

[4]Note that the action of the attacker is to choose matrix B and the value of the attack signal $\boldsymbol{w}(t)$ is not a decision variable.

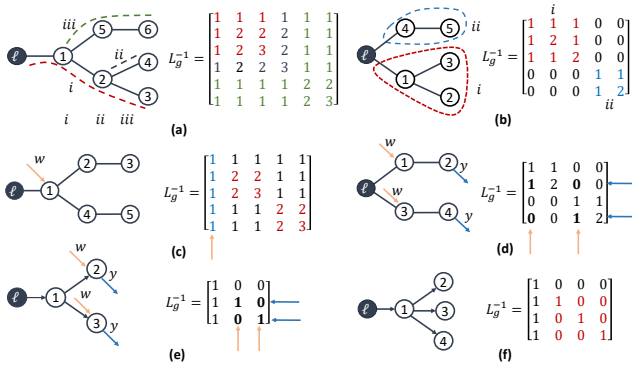

Fig. 2: (a) An undirected tree with its three paths to leader v_ℓ, (b) An undirected tree where v_ℓ is a cut vertex, (c) An undirected tree which does not admit NE for $f = 2$, (d) n undirected tree with a NE for $f = 2$, (e) A directed tree with NE for $f = 2$, (f) A directed tree which does not admit NE for $f = 2$.

a NE exists in this case and let (i^*, j^*) denote the equilibrium strategies of the attacker and detector. Thus, we should have

$$[L_g^{-1}]_{ij^*} \leq [L_g^{-1}]_{i^*j^*} \leq [L_g^{-1}]_{i^*j} \tag{10}$$

for all $i \neq i^*$ and $j \neq j^*$. If element $[L_g^{-1}]_{i^*j^*}$ is in one of the zero blocks, as shown in Fig. 2 (b), then the left inequality will be violated and if it is in one of the nonzero blocks, the right inequality will be violated. ■

B. Equilibrium Analysis: $f > 1$

For $f > 1$, the attacker-detector game deos not admit a Nash equilibrium in general as shown in the following example.

Example 1: In Fig. 2 (c) for the case of $f = 2$, it is clear, according to Lemma 1, that one of the choices of the attacker is node 1. Then for the second choice, both attacker and detector should choose from the blocks of all 1 or the red blocks. Thus, similar to the proof of part (ii) of Theorem 2, there would be no NE for the game. In Fig. 2 (d) there exists a NE for $f = 2$. □

C. Stackelberg Game Approach $f > 1$

According to the Example 1, a NE may not exist for general trees. More formally, the following equality does not hold in general

$$\min_B \max_C \sigma_{\max}(CL_g^{-1}B) = \max_C \min_B \sigma_{\max}(CL_g^{-1}B).$$

In this case, we study the Stackelberg equilibrium strategy of the attacker-detector game when the detector acts as the game leader and the attacker acts as the follower. In the Stackelberg game formulation, the leader solves the following optimization problem

$$J^*(C) = \max_C \sigma_{\max}\left(CL_g^{-1}B^*(C)\right). \tag{11}$$

where $B^*(C)$ is the best response of the attacker when the strategy of the detector is C, i.e., $B^*(C)$ is the solution of the following optimization problem

$$B^*(C) = \arg\min_B \sigma_{\max}\left(CL_g^{-1}B\right). \tag{12}$$

In particular, for a given strategy of the detector, i.e., C, the attacker finds its best response strategy to the detector's decision, which is given by $\min_B CL_g^{-1}B$. Then, the detector optimizes its decision based on all possible best response strategies of the attacker. Unlike the NE, a Stackelberg game always admits an equilibrium strategy.

In general, the computation complexity of solving (11) is $O\left(\binom{n}{f}^2\right)$. That is, the attacker needs to solve (12) for all possible choice of f victim nodes. Then, the detector selects the sensor placement strategy which maximizes (12). However, based on properties of the grounded Laplacian matrix, we propose an algorithm for finding the Stackelberg equilibrium with much less computational cost. This algorithm, in a nutshell, is that both attacker and detector identify all m leader-rooted paths[5] in $\mathcal{G}$. Then for each partition of f into m nonnegative values $f_1, f_2, ..., f_m$, the detector (attacker) places f_i sensors (attacks) to f_i farthest (closest) nodes to the leader in the i-th leader rooted path (i.e., there is no computational cost for the placement of attacks and detectors for a given partitioning). The proposed algorithm for solving the Stackelberg game is shown in Algorithm 1. As it will be shown in Theorem 3, the complexity of this algorithm does not scale with the network size.

Algorithm 1 Stackelberg Attacker-Detector Game on Undirected Trees.

```
// Inputs: G(V,E), f
  J* ← 0_{S_{f,m}}, where S_{f,m} is the number of solutions of (13).
  for i = 1 : S_{f,m} do
    for j = 1 : S_{f,m} do
      B*(C_i) = arg min_{B_j} σ_max(C_i L_g^{-1} B_j)
    end for
      J*_i = σ_max(C_i L_g^{-1} B*(C_i))
  end for
      // Output: C* = arg max_{C_i} J*_i
```

Theorem 3: Consider the Stackelberg attacker-detector game, with the detector as the game leader, over the connected tree $\mathcal{G}_u$ with leader node v_ℓ and m leader rooted paths. Then, Algorithm 1 finds the Stackelberg equilibrium of the game. Moreover, its computational complexity is $O\left(\mathcal{S}_{f,m}^2\right)$, where $\mathcal{S}_{f,m}$ is the number of constrained partitions of f into m nonnegative integers, i.e., the integer solutions of

$$f = \sum_{i=1}^{m} f_i, \quad 0 \leq f_i \leq \ell_i, \tag{13}$$

where ℓ_i is the length of the i-th leader rooted path. □

Proof: Without loss of generality, we label the nodes in a tree in the following form. We start labeling the nodes a

[5]A leader-rooted path in a tree is a unique path starting from the leader and ends at a node with degree 1.

leader rooted path from the leader neighbor, node 1, to a leaf, called ℓ_1. Then we continue from another leader rooted path which has maximum sharing nodes with the previous leader rooted path can label that from $\ell_1 + 1$ to the leaf called ℓ_2. We continue labeling until all nodes are labeled and the leaf of the last leader rooted path is called ℓ_m. For the proof, it is sufficient to show that f_i attackers (f_i detectors) have to be placed in the first (last) f_i columns (f_i rows) of partition i. We prove this by contradiction for placing the attack signals and the detector case it follows the same discussion. Let's denote C_i to be the set of columns from $\ell_i + 1$ to ℓ_{i+1}. By contradiction, suppose there exists at least one column C_i^j of C_i where $j < f_i$ which is not chosen by an attacker. Since in this case there exists another column C_i^h, $h > j$ which is chosen by an attacker and, as a consequence of Lemma 2, each elements of C_i^j is smaller than or equal to C_i^h, this contradicts the optimal strategy of the attacker and the proof is complete. ■

IV. Equilibrium Analysis of the Attacker-Detector Game: Directed Trees

In this section, we investigate the existence of equilibrium for the attacker-detector game, when the underlying network is a directed tree. We present the following assumption.

Assumption 1: In directed tree $\mathcal{G}_d$ each follower v_i can be reached through a directed path from leader v_ℓ.

Similar to Lemma 2, we derive a closed-from expression for the inverse of grounded Laplacian matrix L_g^{-1} for the directed case. This result is presented in the next lemma and its proof is presented in Appendix B.

Lemma 3: Suppose that $\mathcal{G}_d$ is a directed tree with the leader node v_ℓ satisfying Assumption 1. Then, the entries of the matrix L_g^{-1} are given by

$$[L_g^{-1}]_{ij} = \begin{cases} 1 & \text{if there is a directed path from } j \text{ to } i, \\ 0 & \text{if there is no directed path from } j \text{ to } i. \end{cases} \tag{14}$$

A. Equilibrium Analysis: $f = 1$

The following theorem discusses the existence of NE for the attacker-detector game with dynamics (6) on directed trees when f is equal to 1.

Theorem 4: Suppose that $\mathcal{G}_d$ is a directed tree with the leader node v_ℓ satisfying Assumption 1. Then, the attacker-detector game does not accept a NE $f = 1$ except when $\mathcal{G}_d$ is a directed path. □

Proof: We know that L_g^{-1} is a lower triangular matrix with diagonal elements equal to 1, due to the fact that the diagonal elements of L_g^{-1} in this case are the inverses of the in-degrees of the nodes and the in-degree of each node is 1. Thus, there exists at least one element 1 in each row and column of L_g^{-1}. Moreover, based on Lemma 3, L_g^{-1} is a binary matrix. A NE state should satisfy (10). If $[L_g^{-1}]_{i^*j^*} = 0$ then the left inequality in (10) will be violated and if $[L_g^{-1}]_{i^*j^*} = 1$ the right inequality is violated unless the elements in the i^*-th row are all 1. This means, based on Lemma 3, that there must be a directed path from any node to node v_{j^*} and this means that v_{j^*} is at the end of a directed path graph which yields the result. ■

B. Equilibrium Analysis: $f > 1$

Similar to the case of undirected trees, for directed trees when $f > 1$ we may or may not have NE in general, as shown in the following example.

Example 2: It can be easily checked that the attacker-detector game over the directed tree with $f = 2$ shown in Fig. 2 (e) has a NE, whereas it does not admit a NE over the graph in Fig. 2 (f). It is because of the fact that the attackers chooses its target nodes from nodes $2, 3, 4$, since the first column of L_g^{-1} is all 1 and choosing it will result in a larger payoff (Lemma 1). As the detector tries to maximize the payoff, it will also choose from these three nodes. Thus the corresponding block in L_g^{-1} is an identity matrix which does not admit a NE. □

C. Stackelberg Game Approach $f > 1$

Although for many directed trees there is no NE, similar to the case of undirected trees, we can show that performing the Stackelberg max-min game does not cost much computational effort.

Theorem 5: Let $\mathcal{G}_d$ be a directed tree with leader node v_ℓ and m leader rooted paths satisfying Assumption 1. Then the objective function (12) can be solved within $\mathcal{S}_{f,m}^2$ iterations, where $\mathcal{S}_{f,m}$ is the number of constrained partitions of f into m nonnegative integers, i.e., the integer solutions of (13). □

Proof: The procedure of the proof is similar to that of Theorem 3. However, in this case the attackers or detectors selected for each partition i, called f_i, are placed in the end of the partition. ■

The following theorem compares the value of the attacker-detector game when the underlying networks are directed and undirected trees. The proof is straightforward based on Lemmas 2 and 3 as well as the monotonicity of the largest singular value, mentioned in Lemma 1.

Theorem 6: Let $\mathcal{G}_d$ be a directed tree with leader node v_ℓ and $\mathcal{G}_u$ be its corresponding undirected graph (by removing directions from the edges). Let the value of the Stackelberg game between f attackers and detectors on $\mathcal{G}_d$ and $\mathcal{G}_u$ be J_d and J_u, respectively. Then we have $J_d \leq J_u$. □

V. Conclusion

An attacker-detector game on a leader-follower network control system was studied, in which the attacker tries to minimize its visibility and the detector aims to maximize it. The game payoff was the system L_2 gain from the attack signal to the measurable outputs. Several conditions for the existence and the value of Nash equilibrium on both directed and undirected trees were studied. Moreover, the problem was studied under the Stackelberg game framework and it was shown that this game can be solved with low computational cost for large scale networks. Our results show that, under the optimal sensor placement strategy, an undirected topology provides a higher security level (in terms of attack detection) for a networked control system compared

with its corresponding directed topology. A rich avenue for further studies is to extend these results from trees to more general topologies and heterogeneous communication weights. Extensions of these results to non-positive systems is another direction for future works.

APPENDIX

A. Proof of Lemma 2

Before proving Lemma 2 we need some preliminary definitions.

A extension of the above theorem was presented in [23]. Before that, we have the following definition.

Definition 1: A spanning subgraph of a graph $\mathcal{G}$ is called a 2-tree of $\mathcal{G}$, if and only if, it has two components each of which is a tree. In other words, a 2-tree of $\mathcal{G}$ consists of two trees with disjoint vertices which together span $\mathcal{G}$. One (or both) of the components may consist of an isolated node. We refer to $t_{ab,cd}$ as a 2-tree where vertices a and b are in one component of the 2-tree, and vertices c and d in the other. □

Based on the above definition, we prove Lemma 2.

Proof: From [24] we know that any first order cofactor (principal minor) of the Laplacian matrix L is equal to the number of different spanning trees of the connected graph $\mathcal{G}$. Moreover, from [23] we know that the second order cofactor $\mathrm{cof}(L)_{ij,\ell,\ell}$ of the Laplacian matrix L is the number of different 2-trees $t_{ij,\ell\ell}$ in the connected graph $\mathcal{G}$. We know that $[L_g^{-1}]_{ij} = \frac{\mathrm{cof}(L)_{ij,\ell,\ell}}{\det(L_g)}$. and since $\mathcal{G}$ is a tree (with one spanning tree) we have $\det(L_g) = 1$ which yields $[L_g^{-1}]_{ij} = \mathrm{cof}(L)_{ij,\ell,\ell}$. Moreover, in $\mathcal{G}$ as a tree, the number of 2-trees $t_{ij,\ell\ell}$ is equal to the number of trees which contain v_i and v_j and do not contain v_ℓ and that is equal to $|\mathcal{P}_{i\ell} \cap \mathcal{P}_{j\ell}|$ which proves the claim. ■

B. Proof of Lemma 3

Proof: Let L_{g_d} and L_{g_u} be grounded Laplacian matrices of a directed tree and its undirected counterpart, respectively. The proof is based on the fact that for a directed tree with one leader node v_ℓ we have $L_{g_d}^T L_{g_d} = L_{g_u}$ (proved in [25]) which results in $L_{g_d}^{-1} L_{g_d}^{-T} = L_{g_u}^{-1}$. Based on Lemma 2, we have $[L_{g_u}^{-1}]_{ij} = |\mathcal{P}_{i\ell} \cap \mathcal{P}_{j\ell}|$ which gives

$$[L_{g_u}^{-1}]_{ij} = |\mathcal{P}_{i\ell} \cap \mathcal{P}_{j\ell}| = [L_{g_d}^{-1}]_i [L_{g_d}^{-1}]_j^T \tag{15}$$

where $[L_{g_d}^{-1}]_i$ is the i-th row of $L_{g_d}^{-1}$. Now consider another node v_k in $\mathcal{G}$. If there is a directed path from v_k to v_i for some $v_k \in \mathcal{V}$, we set the k-th element of $[L_{g_d}^{-1}]_i$ equal to 1 and zero otherwise and doing the same work for row $[L_{g_d}^{-1}]_j$. If $v_k \in \mathcal{P}_{i\ell} \cap \mathcal{P}_{j\ell}$ in the undirected graph, then the k-th elements of both $[L_{g_d}^{-1}]_i$ and $[L_{g_d}^{-1}]_j$ are 1 and likewise if we consider all elements of $\mathcal{P}_{i\ell} \cap \mathcal{P}_{j\ell}$, then equality (15) will be satisfied and since it should hold for all $i, j = 1, 2, ..., n-1$, this solution will be unique. ■

ACKNOWLEDGMENT

The first author would like to thank Bahman Gharesifard for the valuable discussions.

REFERENCES

[1] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, pp. 3–9, 2014.
[2] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, pp. 1454–1467, 2014.
[3] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. IEEE Int. Conf. Smart Grid Commun*, 2010, pp. 214–219.
[4] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *IEEE Conf. on Decision and Control*. IEEE, 2010, pp. 5991–5998.
[5] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," in *IEEE Trans. Autom. Control*, vol. 58, no. 11, 2013, pp. 2715–2729.
[6] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas, "Robustness of attack-resilient state estimators," in *ACM/IEEE 5th International Conference on Cyber-Physical Systems*, 2014, pp. 163–174.
[7] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *47th Annual Allerton Conf.*, 2009, pp. 91–918.
[8] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems," in *IEEE control systems*, vol. 35, no. 1, 2015, pp. 45–65.
[9] Z. Pan and T. Basar, "H-infinity control of large scale jump linear systems via averaging and aggregation," in *International Journal of Control*, vol. 72, no. 10, 1999, pp. 866–881.
[10] Q. Zhu and T. Basar, "robust and resilient control design for cyber-physical systems with an application to power systems," in *in Proc. 50th IEEE Conf. Decision Control European Control*, 2011, pp. 4066–4071.
[11] A. Gupta, C. Langbort, and T. Basar, "Optimal control in the presence of an intelligent jammer with limited actions," *49th IEEE Conference on Decision and Control*, pp. 1096–1101, 2010.
[12] J. P. H. M. Felegyhazi, *Game Theory in Wireless Networks: A Tutorial*. EPFL Technical report, 2006.
[13] M. Pirani, E. Nekouei, S. M. Dibaji, H. Sandberg, and K. H. Johansson, "Design of attack-resilient consensus dynamics: A game-theoretic approach," *Proceedings of European Control Conference*, 2019.
[14] J. Marden, G. Arslan, and J. S. Shamma, "Cooperative control and potential games," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 39, no. 6, pp. 1393–1407, 2009.
[15] P. N. Brown, H. Borowski, and J. R. Marden, *Security Against Impersonation Attacks in Distributed Systems*. arXiv preprint arXiv:1711.00609, 2017.
[16] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems," *Automatica*, pp. 186–192, 2013.
[17] S. M. Dibaji, M. Pirani, D. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Submitted for Journal Publication.*, 2019.
[18] H. Hao and P. Barooah, "Stability and robustness of large platoons of vehicles with double-integrator models and nearest neighbor interaction," *International Journal of Robust and Nonlinear Control*, vol. 23, no. 18, pp. 2097–2122, 2013.
[19] A. Clark, B. Alomair, L. Bushnell, and R. Poovendran, *Submodularity in Dynamics and Control of Networked Systems*. Springer, 2016.
[20] M. Pirani, E. M. Shahrivar, B. Fidan, and S. Sundaram, "Robustness of leader - follower networked dynamical systems," *IEEE Transactions on Control of Network Systems*, 2017.
[21] M. Pirani and S. Sundaram, "On the smallest eigenvalue of grounded Laplacian matrices," *IEEE Transactions on Automatic Control*, vol. 61, no. 2, pp. 509–514, 2016.
[22] P. V. Mieghem, *Graph spectra for complex networks*. Cambridge University Press, 2010.
[23] U. Miekkala, "Graph properties for splitting with grounded Laplacian matrices," *BIT Numerical Mathematics*, vol. 33, pp. 485–495, 1993.
[24] W. K. Chen, "Applied graph theory, graphs and electrical networks," *North-Holland*, 1976.
[25] M. Pirani, H. Sandberg, and K. H. Johansson, "A graph-theoretic approach to the $\mathcal{H}_\infty$ performance of dynamical systems on directed and undirected networks," *arXiv:1804.10483v1*, 2018.