This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2021.3106866, IEEE Transactions on Automatic Control

A Game-Theoretic Framework for the 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 leader-follower networked control system for improving its security against cyber-physical attacks. In a zero-sum game, the attacker selects f nodes of the network to attack and the detector places f sensors to detect the presence of the attack signals. In our formulation, the attacker's objective is to have a large impact on a target node in the network while being as little visible as possible to the detector. The detector, however, seeks to maximize the visibility of the attack signals. The effects of the attack signals on both the target node and the detector nodes are captured via the system L_2 gain from the attack signals to the target node and deployed sensors' outputs, respectively. The equilibrium strategy of the game determines the optimal locations of the sensors. The existence of Nash equilibrium for the case of single-attack-single-sensor is studied when the underlying connectivity graph is a directed or an undirected tree. We show that, under the optimal sensor placement strategy, an undirected topology provides a higher security level for a networked control system compared to its corresponding directed topology. For the case of multiple-attacks-multiple-sensors case, we show that the game does not necessarily admit a Nash equilibrium and introduce a Stackelberg game approach where the detector acts as the leader. Finally, these results are used to study the sensor placement problem in a vehicle platooning application in the presence of bias injection attacks.**

I. Introduction

The vulnerability of distributed control systems to attacks has triggered the research on their resilience and security in recent years [1]. Several detection methods and defense mechanisms have been proposed based on the system specifications and the attack strategy [2]–[5]. One of these approaches is to define a game between the attacker and the defender to mitigate the effect of the attack as much as possible. The game-theoretic approach can be also used to increase the visibility of the attacker's actions.

Game-theoretic approaches to the security and resilience of control systems have been studied in the literature [6]. 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 the earlier approaches, at each layer (physical and cyber) a particular game is defined. This introduces the concept of *games-in-games* that reflects two interconnected games, one in the physical layer and the other in the cyber layer. The payoff of each game affects the result of the other one [7]. In the latter approach (games based on the type of malicious action), depending on the type of the adversarial behaviour (active or passive) appropriate game strategy, e.g., Nash or Stackelberg, was discussed [8]–[10]. In addition to these approaches, the evolution of some network control systems are modeled as cooperative games [11] and the resilience of these cooperative games to the actions of adversarial agents or communication failures are studied [12], [13]. Recent works have discussed attack detection using game-theoretic approaches [14], [15].

In this paper, which is an extended version of the conference paper [16], we propose a game-theoretic approach to security-aware sensor placement in leader-follower dynamical systems which have diverse applications ranging from multi-agent formation control and vehicle platooning [17] to opinion dynamics in social networks [18]. In our model, the strategic interaction between the attacker and the detector is captured using a non-cooperative game. More specifically, the contributions of the paper are:

- We derive graph-theoretic interpretations of the system L_2 gain which allow us to study the existence of Nash equilibrium (NE) and the game values for both directed and undirected topologies.
- For the single-attack-single-sensor case, we study the existence of NE strategy for the attacker-detector game and characterize its equilibrium strategies.
- We show that the attacker-detector game with the multiple-attacks-multiple-sensors case does not admit an NE in general. The Stackelberg equilibrium of the game is studied, in this case, with the detector as the game leader. For path graphs, it is shown that, at the Stackelberg equilibrium of the game, the detector places the sensors at the last f nodes in the graph. Moreover, the equilibrium strategy of the attacker can be computed efficiently for path graphs.
- We study the optimal sensor placement problem in a platoon of vehicles operating based on a cooperative cruise control algorithm.

In this paper, we consider undirected and directed tree topologies. This is inspired by a class of large-scale systems that follow acyclic graph structures, such as vehicle platoons (as discussed in this paper) or power distribution networks [19], [20].

A. 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

M. Pirani is with the Department of Electrical and Computer Engineering, University of Toronto. E-mail: mohammad.pirani@utoronto.ca. E. Nekouei is with the Department of Electrical Engineering, City University of Hong Kong. E-mail: enekouei@cityu.edu.hk. H. Sandberg and K. H. Johansson are with Division of Decision and Control Systems, School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, and they are also affiliated with Digital Futures. E-mail: {hsan,kallej}@kth.se. The work is supported by Knut Alice Wallenberg foundation. The work of the second author was partially supported by CityU 21208921 and the High-Speed Communications and Control System project.

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 directed edge from v_i to v_j in $\mathcal{G}_d$, then there is no directed edge from v_j to v_i.[1] 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 networks) for node v_i as $d_i = \sum_{j:v_j\in\mathcal{N}_i} A_{ij}$. A cut vertex in a connected graph is a node such that if it is removed (along with its incident edges) the graph becomes disconnected. The Laplacian matrix of a graph is denoted by $L = D - A$, where $D = \text{diag}(d_1, d_2, ..., d_n)$. A *tree* is a connected acyclic graph. A directed tree is a digraph whose undirected counterpart is a tree. A *leaf* is a node in a tree with degree (or in-degree) one. We use $\mathbf{e}_i$ to indicate the i-th vector of the canonical basis.

II. Problem Statement

Consider a connected directed or undirected network $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ comprised of a leader (or reference) agent, denoted by v_ℓ, and rest of the agents are called followers. The state of follower agent j at time t is $x_j(t) \in \mathbb{R}$ evolves based on the interactions with its neighbors according to

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

The state of the leader is a constant exogenous reference signal, *i.e.,* $x_\ell(t) = u(t)$, which should be tracked by the followers. If the graph is connected, the states of the follower agents will track the reference signal [21]. We assume without loss of generality that the leader is placed last in the ordering of the agents. The update rule of each follower agent is prone to an intrusion (or attack). More specifically, there exists an attacker which chooses a set of attack nodes, called $\mathcal{F}$ consisting of f nodes in the network, to inject the attack signals. In practice, the number of attacked nodes is unknown; thus f represents an upper bound on the number of attack nodes. The leader is not affected by the attack signals as its state evolves according to the exogenous input $u(t)$. If the follower agent v_j is influenced by the attacker, its the dynamics is written in the following form

$$\dot{x}_j(t) = \sum_{v_i\in\mathcal{N}_j} (x_i(t) - x_j(t)) + w_j(t) \quad \text{if} \quad v_j \in \mathcal{F}, \tag{2}$$

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

$$y_i(t) = x_i(t) \quad \text{if} \quad v_i \in \mathcal{D}, \tag{3}$$

where $y_i(t)$ is the output of the sensor (detector) deployed at follower v_i. We refer to these sensors as *detector sensors* as they are dedicated for attack detection and they are not used for feedback control purposes. Aggregating the states of all followers into a vector $\boldsymbol{x}(t) \in \mathbb{R}^{n-1}$, and aggregating the attack signals to $\boldsymbol{w}(t)$, equations (2) and (3) yield the following dynamics

$$\begin{aligned} \dot{\boldsymbol{x}}(t) &= -L_g\boldsymbol{x}(t) + \bar{L}u + B\boldsymbol{w}(t), \\ \boldsymbol{y}(t) &= C\boldsymbol{x}(t). \end{aligned} \tag{4}$$

where L_g is called the grounded Laplacian matrix (formed by removing the row and the column corresponding to the leader from the Laplacian matrix) and the vector $\bar{L}$ captures the influence of the leader on its neighbors. Considering $\mathcal{F} = \{v_{i_1}, v_{i_2}, ..., v_{i_f}\}$ and $\mathcal{D} = \{v_{j_1}, v_{j_2}, ..., v_{j_f}\}$ as the set of attacker and detector nodes, respectively, matrices $B_{n\times f} = [\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, ..., \mathbf{e}_{i_f}]$, and $C_{f\times n} = [\mathbf{e}_{j_1}^T; \mathbf{e}_{j_2}^T; ...; \mathbf{e}_{j_f}^T]$ specify the decisions of the attacker and the detector, respectively. In particular, there is a single 1 in the i-th row (column) of matrix B (C) if the i-th node is under attack (has a sensor). We assume that there exists at least one attacker node in 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 [22].

By defining the error state $\tilde{\boldsymbol{x}}(t)$, $\boldsymbol{x}(t) - L_g^{-1}\bar{L}u(t)$ and writing the dynamics of $\tilde{\boldsymbol{x}}(t)$, the term $\bar{L}u(t)$ will be removed from (4). The following theorem characterizes the system L_2 gain from the attack signals to the output measurement of the error dynamics of (4).

Theorem 1 ([23]): Let $G(s) = C(sI - A)^{-1}B$ be the transfer function of the error dynamics of (4). The L_2 gain from the attack signals to the output measurement of (4) is given by

$$\sup_{\|\boldsymbol{w}\|_2\neq 0} \frac{\|\boldsymbol{y}\|_2}{\|\boldsymbol{w}\|_2} = \sigma_{\max}(G(0)) = \sigma_{\max}(CL_g^{-1}B) \tag{5}$$

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

III. Attacker-Detector Game

In this subsection, we formally define a game between the attacker and detector.

1) Decisions of Players: The attacker's objective is to select a set of nodes to inject the attack signals such that the attack has a large impact on a target node $v_j \in \mathcal{V}$,[2] while the L_2 gain from attack signals to the output measurements $\boldsymbol{y}(t)$, defined in (5), is relatively small. On the other hand, the detector deploys a set of sensors on specific nodes in the network to maximize the L_2 gain from the attack signals to the measurements, *i.e.,* the effect of attacks becomes more apparent in output $\boldsymbol{y}(t)$.

2) Game Payoff: The game payoff for the attacker and the detector is (for some $\lambda \geq 0$):

$$J(\mathcal{F}, \mathcal{D}) = \sigma_{\max}(C^T L_g^{-1}B) - \lambda\, \sigma_{\max}(\mathbf{e}_j^T L_g^{-1}B). \tag{6}$$

Matrices B and C are determined by the set of the attacked nodes $\mathcal{F}$ and the set of the detector nodes $\mathcal{D}$, respectively.

[1]The main motivation behind this assumption is its application in predecessor-following platoons which will be discussed in Section VI.

[2]This target node can be the most expensive part of the network or be a node which performs specific tasks.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2021.3106866, IEEE Transactions on Automatic Control

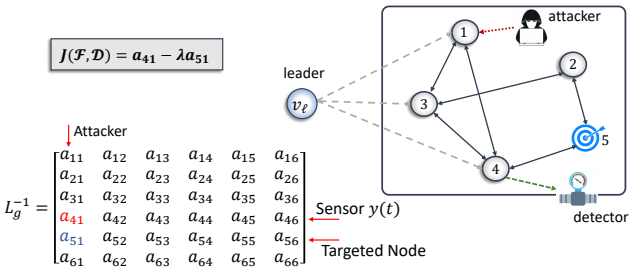

Fig. 1: An example of an attacker-detector game with $f = 1$.

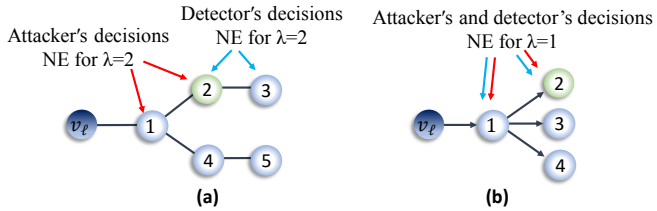

Fig. 2: Examples of an undirected tree, (a), and a directed tree, (b). NE strategies for $f = 2$ for specific values of λ for the target node specified in green color.

The attacker aims at minimizing the objective function in (6) whereas the detector tries to maximize it. Parameter λ determines the level of the priority of the impact versus visibility for the attacker. Note that the action of the attacker is only determined by matrix B and the value of the attack signal $\boldsymbol{w}(t)$, *i.e.,* its magnitude and frequency content, is not a decision variable. In practice, it is difficult for an attacker to precisely predict the impact of the injected attack signal on the detector output, due to different omnipresent sources of disturbance in networked control systems. Hence, the attacker considers the worst impact of the attack signal on the detector output, *i.e.,* the system L_2 gain, as its visibility metric. From the attacker point of view, it is desirable to minimize this visibility measure whereas the detector prefers to maximize it.

Fig. 1 shows an example of this game in a network of five agents where the attacker chooses node 1, the detector chooses node 4, and node 5 is the attacker's target node. The attacker seeks to maximize its impact on node 5 while, at the same time, tends to be covered as much as possible to the detector.

Remark 1: **(Trade-off Between Impact and Visibility)** There are several works in the literature on quantifying the trade-off between the attack impact and its visibility [24]. Our approach to introducing the game objective follows this line of research. In the way we presented the payoff, the game equilibria are sensitive to the parameter λ, i.e., the attacker's strategy varies by changing λ. This can be interpreted as the level of risk aversion of the attacker to perform an attack. When λ is small, the attacker's concern is more on being stealthy. A special case is when $\lambda = 0$ which was analyzed in [16]. There, the attacker's objective is visibility and it does not target a specific node. This extreme case can be viewed as the *pre-attack* phase, i.e., when the attacker only tries to learn the system (without being detected) before performing the attack. The high regime of λ corresponds to the case where the detectability is not of importance for the attacker and it focuses on having large impact on the target node. □

In this paper, we investigate the effect of parameter λ on the game equilibrium when the underlying network is an undirected or a directed tree. For directed trees, we impose the following assumption throughout the paper.

Assumption 1: In directed tree $\mathcal{G}_d$, each follower v_i can be reached through a directed path from the leader. [3]

[3]Digraphs which satisfy Assumption 1 and do not have a directed cycle are called *rooted-out-branching* in the literature [25].

For the analyses in this paper, we need to have a graph-theoretic sense of the elements of matrix L_g^{-1}, which is discussed in the following lemma.

Lemma 1: Suppose that $\mathcal{G}_u$ is an undirected tree and let $\mathcal{P}_{i\ell}$ be the set of edges involved in the (unique) path from the leader node v_ℓ to v_i. Then, we have

$$[L_g^{-1}]_{ij} = |\mathcal{P}_{i\ell} \cap \mathcal{P}_{j\ell}|. \tag{7}$$

□

Proof: See Appendix A. ■

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, in Fig. 2 (a), we have $[L_g^{-1}]_{35} = |\mathcal{P}_{3\ell} \cap \mathcal{P}_{5\ell}| = 1$ and $[L_g^{-1}]_{32} = |\mathcal{P}_{3\ell} \cap \mathcal{P}_{2\ell}| = 2$.

The following lemma characterizes the elements of L_g^{-1} for directed trees.

Lemma 2: Suppose that $\mathcal{G}_d$ is a directed tree with the leader node v_ℓ satisfying Assumption 1. Then, we have

$$[L_g^{-1}]_{ij} = \begin{cases} 1 & \text{if there is a directed path from } j \text{ to } i, \\ 0 & \text{if there is no directed path from } j \text{ to } i. \end{cases} \tag{8}$$

□

Proof: See Appendix B. ■

For the directed tree shown in Fig. 2 (b), we have $[L_g^{-1}]_{12} = 0$ and $[L_g^{-1}]_{21} = 1$, since there is a directed path from node 2 to node 1.

IV. Equilibrium Analysis of the Game: Single-Attack-Single-Sensor Case

We characterize the equilibrium of the attacker-detector game with a single attacked node and a single detector node, *i.e.,* $f = 1$ on directed and undirected trees for different values of λ. In this case, the game payoff reduces to

$$J(\mathcal{F},\mathcal{D}) = \mathbf{e}_k^T L_g^{-1} \mathbf{e}_i - \lambda \mathbf{e}_j^T L_g^{-1} \mathbf{e}_i, \tag{9}$$

where v_i, v_k, and v_j are the attacked node, the detector node, and the target node, respectively. In the rest of the paper, *target node* or node v_j are used interchangeably.

In the following theorems, we use the term *leader-rooted path* in a tree, which is a path starting from the leader v_ℓ and ends at a node with degree 1 (the leaf). If v_ℓ is not a cut vertex in a tree, it has a single neighbor which is the starting node of all leader rooted paths. We label the nodes in a leader rooted path of length m containing the target node

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2021.3106866, IEEE Transactions on Automatic Control

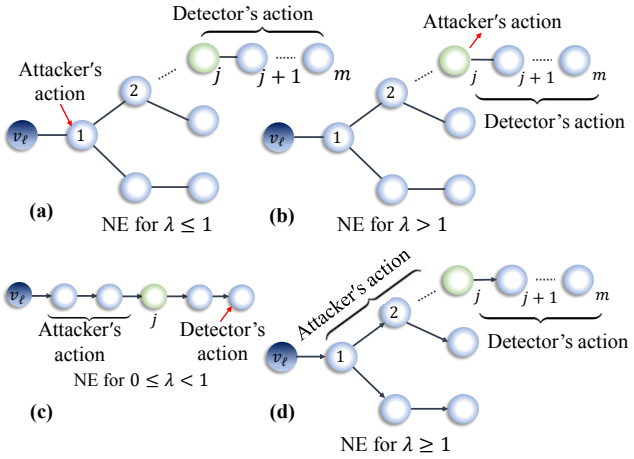

Fig. 3: NE strategies of the attacker-detector game for directed and undirected networks. The green node is the target node.

v_j as $v_\ell, v_1, ..., v_j, ...v_m$ as shown in Fig. 3 (a). The following theorem discusses the existence of NE for the attacker-detector game when $0 \leq \lambda \leq 1$. This case models scenarios in which visibility dominates the impact from the attacker's perspective.

Theorem 2: **(Undirected Tree with $0 \leq \lambda \leq 1$):** Let $\mathcal{G}_u$ be an undirected tree and $f = 1$.

(i) If v_ℓ is not a cut vertex and $\lambda < 1$, there exists at least one NE in which the attacker chooses the leader's neighbor and the detector chooses any node between the target node and the leaf in the leader rooted path containing v_j. In this case, the game value will be $J^* = 1 - \lambda$.

(ii) If v_ℓ is a cut vertex and $\lambda < 1$, the game does not admit an NE.

(iii) For $\lambda = 1$, the game has an NE with value zero whether v_ℓ is a cut vertex or not. The NE strategy is similar to (i).

(iv) For $\lambda = 0$, if v_ℓ is not a cut vertex, NE belongs to the case where the attacker chooses the leader's neighbor (regardless of the detector's decision). If v_ℓ is a cut vertex, there is no NE.

□

Proof: See Appendix C. ■

The NE strategies of the attacker and detector are schematically shown in Fig. 3 (a). Here, as the visibility dominates the impact from the attacker's perspective, it acts in a conservative manner and does not attack directly the target node.

For the case where $\lambda > 1$, the NE strategies are different, as discussed in the following theorem. The structure of the proof of the following theorem is similar to that of Theorem 2.

Theorem 3: **(Undirected Trees with $\lambda > 1$):** Let $\mathcal{G}_u$ be an undirected tree and v_ℓ be the leader node and $\lambda > 1$. Then, there exists at least one NE when the detector chooses any node between v_j and the leaf in a leader rooted path containing v_j, and the attacker chooses the target node, *i.e.,* $v_i = v_j$. In this case, the game value will be $J^* = \ell_j(1 - \lambda)$, where ℓ_j is the path length between v_j and the leader. □

Unlike Theorem 2, Theorem 3 holds regardless of the fact that v_ℓ is a cut vertex or not. Fig. 3 (b) shows possible NE strategies discussed in Theorem 3. Physically speaking, for $\lambda > 1$ where the impact dominates the visibility, the attacker chooses the target node without considering the visibility effects. For undirected trees, when $\lambda > 1$, the position of the target node v_j plays a critical role on the game value. In this case, the closer v_j is to the leader, *i.e.,* smaller ℓ_j, results in a larger game value.

Theorem 4: **(Directed Trees with $0 \leq \lambda \leq 1$):** Let $\mathcal{G}_d$ be a directed tree with the leader node v_ℓ satisfying Assumption 1, and $f = 1$.

(i) For $\lambda = 1$: An NE exists in which the attacker chooses any node between the leader and v_j and detector chooses any node between v_j and the leaf in the leader rooted path containing v_j. The game value in this case will be $J^* = 0$.

(ii) For $\lambda < 1$: There is no NE except when $\mathcal{G}_d$ is a directed path in which the detector chooses the leaf node and the attacker chooses any node between the leader and v_j. The game value will be $J^* = 1 - \lambda$.

□

Proof: See Appendix D. ■

The NE strategy discussed in Theorem 4 for $\lambda < 1$ is shown in Fig. 3 (c). Note that in this case the unique topology which admits an NE is a directed path. The proof of the following theorem follows the same procedure as Theorem 4.

Theorem 5: **(Directed Trees with $\lambda > 1$):** Let $\mathcal{G}_d$ be a directed tree and $\lambda > 1$. Then, there exists an NE is when the attacker chooses any node between the leader and v_j and the detector chooses any node between v_j and the leaf in the leader rooted path which includes v_j. The game value in this case is $J^* = 1 - \lambda$. □

The NE strategies for the attacker and detector discussed in Theorem 5 are shown in Fig. 3 (d). Note that there exists sudden emergence of an equilibrium for the game on directed trees when $\lambda \geq 1$. For $\lambda < 1$, according to Theorem 4, there is no NE for digraphs other than directed paths. However, when λ passes 1, an NE appears. Table I summarizes the results of Theorems 2 to 5.

Graph	$\lambda \leq 1$	$\lambda > 1$
Undirected Tree	NE exists	NE exists
Game Value	$J^* = 1 - \lambda$	$J^* = \ell_j(1 - \lambda)$
Directed Tree	$\lambda < 1$, no NE except for path $\lambda = 1$, NE exists	NE exists
Game Value	$J^* = 1 - \lambda$	$J^* = 1 - \lambda$

TABLE I: Summarizing the results of Theorems 2 to 5.

The following corollary compares the value of the attacker-detector game when the underlying networks are directed and undirected trees. The proof is straightforward based on the game values mentioned in Theorems 2 to 5.

Corollary 1: 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 J_d and J_u denote the values of the attacker-detector games corresponding to the graphs $\mathcal{G}_d$ and $\mathcal{G}_u$, respectively. Then we have $J_d \leq J_u$.

Based on the above corollary, for $f = 1$, the undirected network is more secure compared to the directed network for any regime of λ.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2021.3106866, IEEE Transactions on Automatic Control

V. Equilibrium Analysis of the Game: Multiple-Attacks-Multiple-Sensors Case

In this section, we investigate the case where the number of attacked nodes and detection sensors is more than one.

A. General Topology with $f > 1$

As shown in the following examples, the attacker-detector game does not necessarily admit an NE in general undirected or directed topologies.

Example 1 (Undirected Topology): Consider the attacker-detector game in Fig. 2 (a) with $f = 2$. By direct computation, it can be verified that the game does not admit an NE for $\lambda = 1$. However, for $\lambda = 2$ an NE strategy emerges as shown in that figure. □

Example 2 (Directed Topology): Consider the attacker-detector game in Fig. 2 (b). In this case, there is no NE for $\lambda = 0$ but it admits an NE for $\lambda = 1$. □

For the case where there is no NE, we study the Stackelberg game between the attacker and the detector. For the Stackelberg game, we assume that the detector acts as the game leader as it reflects its willingness to consider the worst case attack. In this formulation, the leader solves

$$J^*(C) = \max_{C} \sigma_{\max}(CL_g^{-1}B^*(C)) - \lambda\sigma_{\max}(\mathbf{e}_j^T L_g^{-1}B^*(C)), \tag{10}$$

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

$$B^*(C) = \arg\min_{B} \sigma_{\max}(CL_g^{-1}B) - \lambda\sigma_{\max}(\mathbf{e}_j^T L_g^{-1}B). \tag{11}$$

In particular, for a given strategy of the detector, *i.e.,* matrix C, the attacker finds its best response strategy to the detector's decision, which is given by (11). 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 computational complexity of solving (10) is $O\left(\binom{n}{f}^2\right)$. That is, we have to solve (11) from the attacker's perspective for all possible choices of f attacked nodes. Then, the detector selects the sensor placement strategy which maximizes (11). Unlike the case of $\lambda = 0$ discussed in [16], for $\lambda > 0$ due to the trade-off between visibility and impact from the attacker's perspective, both attacker and detector have to perform more computations.

B. Path Graphs with $f > 1$

Specific network topologies can also help decreasing the computational cost of (10). Here, we discuss Stackelberg game equilibrium strategies when the underlying graph is a directed or undirected path. Solving the Stackelberg game for path graphs can shed light on solving more complicated graph structures using the notion of a graph's path covering [26]. The canonical structures of L_g for undirected and directed path graph, according to Lemmas 1 and 2, are shown in Fig. 4.

Proposition 1: let $\mathcal{G}_u$ and $\mathcal{G}_d$ be an undirected and directed path graphs, respectively, with the leader v_ℓ being a leaf. We label the nodes starting from the leader, by $v_\ell, v_1, v_2, ..., v_n$.

$$L_g^{-1} = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2 & 2 & \cdots & 2 \\ 1 & 2 & 3 & 3 & \cdots & 3 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & 3 & 4 & \cdots & n-1 \end{bmatrix} \quad L_g^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \cdots & 1 \end{bmatrix}$$

Non-decreasing (↓) Non-decreasing (→)

(a) (b)

Fig. 4: Matrix canonical structure for the undirected (a) and directed (b) path graphs.

At the equilibrium of the Stackelberg game with the detector as the game leader, the detector places sensors on $v_{n-f}, v_{n-f+1}, ..., v_n$, regardless of the value of λ, for both directed and undirected path graphs. Furthermore, the equilibrium strategy of the attacker can be computed with a cost that is independent of the network size.

Proof: See Appendix E. ■

Remark 2: **(Computational Complexity)** As shown in Theorems 2 to 5, in the cases where a NE exists, the optimal locations of the sensor nodes can be computed instantaneously and independent of the network size. Procedures to determine the NE strategies for both attacker and detector are described in those theorems. When the game does not admit an NE, finding the equilibria of the Stackelberg game is a combinatorial problem. However, for specific graph structures, one can find efficient algorithms to find the equilibria, e.g., the example of a path graph discussed in Proposition 1. There, as shown in the proof, the detector finds its optimal decision instantaneously and the attacker calculates the best response independent of the network size. □

VI. Case Study: Bias Injection Attacks in Vehicle Platoons

In this section, we study the attacker-detector game on a vehicle platoon. In this setting, the objective for each follower vehicle is to track a reference velocity while remains in a safe distance from its neighboring vehicles. Two widely used inter-vehicular communications for platooning are *bidirectional* communication and *predecessor-following* communication [17], as shown in Fig. 5.

Consider a connected network of n vehicles. The position and longitudinal velocity of each vehicle v_i at time t is denoted by scalars $p_i(t)$ and $u_i(t)$, respectively. Each vehicle v_i is able to communicate its kinematic parameters, e.g., velocity, to its neighbor vehicles, specified by the communication graph. The desired vehicle formation will be determined by specific constant inter-vehicular distances. Let Δ_{ij} denote the desired distance between vehicles v_i and v_j. The desired vehicle formation and velocity tracking are schematically shown in Fig. 5 (a) and (b). Considering the fact that each vehicle v_i has access to its own position, the positions of its neighboring vehicles, and the desired inter-vehicular distances Δ_{ij}, the dynamics of vehicle v_i can be expressed as [17]

$$\ddot{p}_i(t) = \sum_{j\in\mathcal{N}_i} k_p\big(p_j(t) - p_i(t) + \Delta_{ij}\big) + k_u\big(u_j(t) - u_i(t)\big) + w_i(t), \tag{12}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2021.3106866, IEEE Transactions on Automatic Control

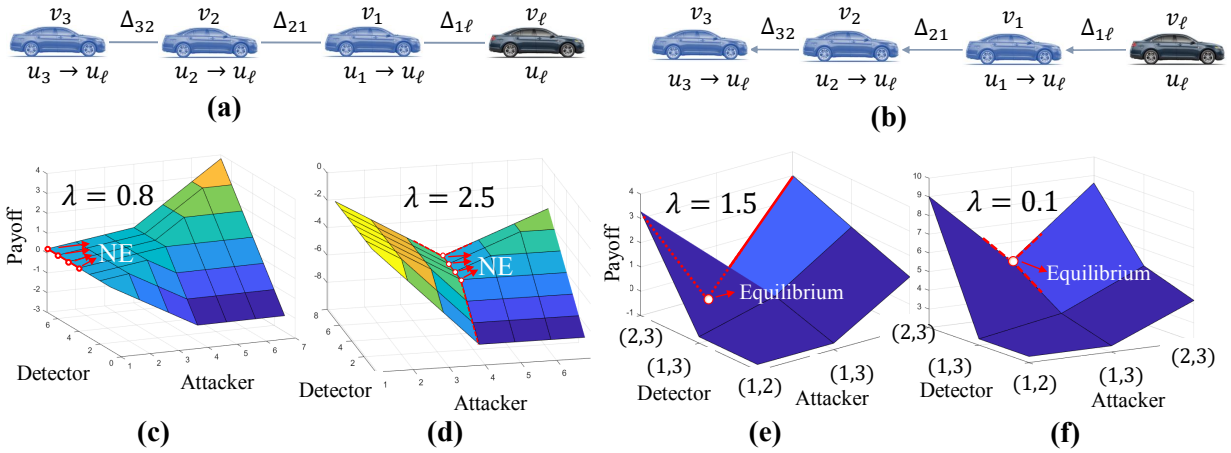

Fig. 5: Desired inter-vehicular distances Δ_{ij} and velocity u_ℓ in (a) a vehicle platoon with bidirectional communication, and (b) a predecessor-following communication. Game payoff and equilibrium strategies of the attacker-detector game for (c) $\lambda = 0.8$, $f = 1$ and (d) $\lambda = 2.5$, $f = 1$ (e) $\lambda = 1.5$, $f = 2$ and (f) $\lambda = 0.1$, $f = 2$. Vehicles are labeled as in (a).

where $k_p, k_u > 0$ are control gains and $w_i(t)$ models an attack signal. Dynamics (12) in matrix form can be written as

$$\dot{\boldsymbol{x}}(t) = \underbrace{\begin{bmatrix} \mathbf{0}_n & I_n \\ -k_p L_g & -k_u L_g \end{bmatrix}}_{A} \boldsymbol{x}(t) + \underbrace{\begin{bmatrix} \mathbf{0}_{n\times 1} \\ k_p \boldsymbol{\Delta} \end{bmatrix}}_{\bar{B}} + \underbrace{\begin{bmatrix} \mathbf{0}_n \\ B \end{bmatrix}}_{F} \mathbf{w}(t),$$
$$\boldsymbol{y}(t) = [C \quad \mathbf{0}_n]\boldsymbol{x}(t) \tag{13}$$

where $\boldsymbol{x} = [p_1, p_2, ..., p_n, \dot{p}_1, \dot{p}_2, ..., \dot{p}_n]^\mathsf{T}$, $\boldsymbol{\Delta} = [\Delta_1, \Delta_2, ..., \Delta_n]^\mathsf{T}$ in which $\Delta_i = \sum_{j\in\mathcal{N}_i} \Delta_{ij}$. Here $\mathbf{w}(t)$ is the vector of attacks and $\boldsymbol{y}(t)$ is the vector of sensor measurements. Since L_g is non-singular, matrix A becomes non-singular as well [17]. By defining new variable $\tilde{\boldsymbol{x}} = \boldsymbol{x} + A^{-1}\bar{B}$, where $\bar{B}$ is defined in (13), the dynamics of $\tilde{\boldsymbol{x}}$ will not include term $\bar{B}$. We take Laplace transform from its dynamics, assuming zero initial condition, to get

$$s^2\tilde{X}(s) = -k_p L_g \tilde{X}(s) - s k_u L_g \tilde{X}(s) + BW(s), \tag{14}$$

where $\tilde{X}(s)$ and $W(s)$ are Laplace transforms of $\tilde{\boldsymbol{x}}(t)$ and $\boldsymbol{w}(t)$, respectively. This results in

$$Y(s) = C\tilde{X}(s) = C\big(\underbrace{s^2 I + (sk_u + k_p)L_g}_{\bar{A}(s)}\big)^{-1} BW(s). \tag{15}$$

Note that the system (13) is no longer positive and its L_2 gain generally happens at some nonzero frequency. In order to make it compatible with the original game formulation (6) and facilitate the application of the theoretical results, we assume that the attack happens at zero frequency, i.e., $s = 0$. This type of attack is called *the bias injection attack* in the literature [27]. Under this assumption, we study the attacker-detector game for (13) when the attacker's objective is to minimize the DC gain of the transfer function, whereas the detector's objective is to maximize this quantity. The DC gain of (15), from W to Y, can be written as

$$G(0) = \sigma_{\max}(C\bar{A}(0)^{-1}B) = \frac{1}{k_p}\sigma_{\max}(CL_g^{-1}B). \tag{16}$$

Based on (16) and (6), the game payoff is a scaled version of the game payoff discussed so far. Hence, we can readily use the results in Proposition 1 for calculating the equilibria of the Stackelberg game.

A. A Numerical Example

The equilibrium strategies for the single-attack-single-sensor game, and its game payoff, on a platoon of seven vehicles with undirected topology are shown in Fig. 5 (c) and (d) for two values of λ. Here, vehicle 4 is the target node. According to Fig. 5 (c), the attacker selects the node 1 when λ is equal to 0.8 since the visibility dominates the attack impact. However, when λ is equal to 2.5 the attacker selects the node 4 (the target node) as the impact of attack dominates its visibility in this case. Moreover, the equilibrium strategies of the attacker and detector follow the results in Theorems 2 and 3.

Fig. 5 (e) and (f) present the Stackelberg equilibrium and the game payoff of the attacker-detector game on a platoon of three vehicles with undirected topology and $f = 2$. Here, the second vehicle is the target node. As shown in the figure, the solution of the Stackelberg game belongs to the case where the detector chooses the last two vehicles, *i.e.,* nodes 2 and 3.

VII. Conclusions

In this paper, we studied a sensor placement problem in a leader-follower dynamical system. The sensor placement was formulated as a non-cooperative game between an attacker and a detector. Equilibrium strategies of the attacker-detector game were studied for this game under both directed and undirected topologies. An avenue for further study is to find alternative ways to quantify the impact-visibility trade-off, other than the one proposed in (6). For instance, one can formulate the attacker problem as optimizing the attack impact subject to a visibility constraint. Moreover, extending the results to general graph structures (with time varying topologies) as well as general linear systems, including non-positive systems, is another future research direction.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2021.3106866, IEEE Transactions on Automatic Control

APPENDIX

A. Proof of Lemma 1

Before proving Lemma 1 we need some preliminary definitions.

Definition 1 ([28]): 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 1.

Proof: From [28], Lemma 2, 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 [28], Lemma 3, we know that the second order cofactor $\text{cof}(L)_{ij,\ell,\ell}$ 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 $[L_g^{-1}]_{ij} = \frac{\text{cof}(L)_{ij,\ell,\ell}}{\det(L_g)}$. and since $\mathcal{G}$ is a tree (with one spanning tree) we have $\det(L_g) = 1$ which yields $[L_g^{-1}]_{ij} = \text{cof}(L)_{ij,\ell,\ell}$. 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 2

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 [29]) which results in $L_{g_d}^{-1} L_{g_d}^{-T} = L_{g_u}^{-1}$. Based on Lemma 1, we have $[L_{g_u}^{-1}]_{ij} = |\mathcal{P}_{i\ell} \cap \mathcal{P}_{j\ell}|$ which gives

$$[L_{g_u}^{-1}]_{ij} = |\mathcal{P}_{i\ell} \cap \mathcal{P}_{j\ell}| = [L_{g_d}^{-1}]_i [L_{g_d}^{-1}]_j^T \tag{17}$$

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 (17) will be satisfied and this should hold for all $i, j = 1, 2, ..., n-1$. The uniqueness of this solution comes from the fact that the rows of L_{g_d} are all diagonally dominant with at least one strictly diagonally dominant row (corresponds to the leader's neighbor). Thus, L_{g_d} is positive definite and invertible with a unique inverse $L_{g_d}^{-1}$. Since the inverse is unique, the above solution for (17) is unique. ■

C. Proof of Theorem 2

Proof: (i) To show that the mentioned strategy is NE, we have to show that any unilateral deviation from it does not provide an incentive for each player. According to Lemma 1, since all elements of the first column of L_g^{-1} are 1, then, regardless of the actions of the detector, the game payoff will be $J = 1 - \lambda$. Thus, changing the detector's decision does not have an incentive for him. Now consider that the attacker tends to change its strategy provided that the detector's decision is a node between v_j and the leaf node in the leader rooted path containing v_j. If the attacker chooses a node other than the leader's neighbor, say the i-th column ($i \neq 1$), then the payoff will be $x(1-\lambda) \geq 1 - \lambda$, where $x \geq 1$ is the ji-th element of L_g^{-1}. Hence, not the attacker, nor the detector get an incentive in changing their strategies.

(ii) For the case when v_ℓ is a cut vertex, after removing v_ℓ the graph becomes disconnected and the resulting grounded Laplacian matrix, and consequently L_g^{-1}, becomes block diagonalized. Assume that a NE exists in this case and let (i^*, k^*) denote the equilibrium strategies of the attacker and detector. Thus, we should have

$$\begin{aligned}[L_g^{-1}]_{ki^*} - \lambda[L_g^{-1}]_{ji^*} &\leq [L_g^{-1}]_{k^*i^*} - \lambda[L_g^{-1}]_{ji^*} \\ &\leq [L_g^{-1}]_{k^*i} - \lambda[L_g^{-1}]_{ji},\end{aligned} \tag{18}$$

for all $i \neq i^*$ and $j \neq j^*$. Since v_ℓ is the cut vertex, L_g^{-1} is a block diagonal matrix. If (i^*, k^*) is in a zero block, the game payoff becomes $0 - [L_g^{-1}]_{ji^*}$ or 0. In either case, the detector can increase the payoff by choosing a node in another subgraph and that violates the left inequality in (18). If (i^*, k^*) is in a nonzero block, by appropriate choice of the detected node, k^*, the game payoff can be positive. Hence, the attacker can make it at most zero by choosing a node from the other subgraph and this violates the right inequality in (18).

(iii) The proof is similar to that of (i). Here, since $\lambda = 1$, the game payoff is $J^* = 1 - \lambda = 0$ and choosing zero or nonzero block does not affect the game value. Hence, it is independent of the v_ℓ being a cut vertex or not. The proof of (iv) is presented in [16]. ■

D. Proof of Theorem 4

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 2, L_g^{-1} is a binary matrix. We prove using contradiction. If a NE exists, it should satisfy (18) for all $i \neq i^*$ and $j \neq j^*$. Four different cases can occur. (i) $[L_g^{-1}]_{k^*i^*} = 0, [L_g^{-1}]_{ji^*} = 0$. In this case, the detector can choose a node v_k to make $[L_g^{-1}]_{ki^*} = 1$ (based on Assumption 1, such a node exists) which violates the left inequality in (18). (ii) $[L_g^{-1}]_{k^*i^*} = 1, [L_g^{-1}]_{ji^*} = 0$. In this case, the attacker can choose a node v_i to get $[L_g^{-1}]_{k^*i} = 0$ since L_g^{-1} is triangular, hence, the right inequality is violated. (iii) $[L_g^{-1}]_{k^*i^*} = 0, [L_g^{-1}]_{ji^*} = 1$. Then, similar to case (i), the detector can choose a node v_k to make $[L_g^{-1}]_{ki^*} = 1$. (iv) $[L_g^{-1}]_{k^*i^*} = 1, [L_g^{-1}]_{ji^*} = 1$. In this case, the payoff is $J = 1 - \lambda$. Clearly, the attacker can change its decision to another leader-rooted path and reduce the payoff to $J = 0 < 1 - \lambda$, i.e., violates the right inequality in (18). The only case where we have an NE is when there is a single leader-rooted path, i.e., a directed path graph. ■

E. Proof of Proposition 1

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

Lemma 3 ([30]): If M is a nonegative matrix and C is a matrix in which each element obeys $|c_{ij}| \leq M_{ij}$, then every eigenvalue $\lambda(C)$ of C satisfies $\lambda(C) \leq \lambda_{\max}(M)$. □

Based on the above result, the largest eigenvalue of a non-negative matrix M is non-decreasing with any entry of M. This result can be easily extended to the largest singular value as $\sigma_{\max}(M) = \lambda^{\frac{1}{2}}_{\max}(M^T M)$. If one element of M increases, then at least one element of $M^T M$ will increase (and no element decreases). Now, we prove Proposition 1.

Proof: We prove for undirected path graph and the proof for the directed paths follows the same procedure. Without loss of generality, we start labeling the nodes from the leader neighbor, node 1, to the last node, which is node n and the target node is v_j. According to the structure of matrix L_g in Fig. 4 (a) together with Lemma 3, we know that the detector always chooses the last f nodes in the path. For the attacker, we consider two cases, when $j \leq n-f$ or $j > n-f$. If the attacker chooses its nodes from the first $n-f$ nodes, the payoff will be in the following form

$$J_i = \sigma_{\max}\left(\begin{bmatrix} a_1 & a_2 & \cdots & a_f \\ a_1 & a_2 & \cdots & a_f \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_f \end{bmatrix}\right) - \sigma_{\max}[a_1, a_2, ..., a_f]$$
$$= \left(a_1^2 + a_2^2 + ... + a_f^2\right)^{\frac{1}{2}} (\sqrt{f} - \lambda). \quad (19)$$

Based on this, the best response of the attacker and game payoff will be determined by (19) as follows: (i) if $\lambda \leq \sqrt{f}$ and $j \leq n-f$, then the game strategy of the attacker will be $B_1^* = \arg\min_{a_{1,2},...,a_f} \left(a_1^2 + a_2^2 + ... + a_f^2\right)^{\frac{1}{2}}$, i.e., the first f nodes due to monotonicity of the elements through columns. Otherwise, if $j > n-f$ then attacker has to check the last f columns and compare them with B_1^* to find the optimal strategy. (ii) if $\lambda > \sqrt{f}$ and $j \leq n-f$, then the game strategy of the attacker will be $B_2^* = \arg\max_{\substack{a_{1,2},...,a_f \\ f \leq j}} \left(a_1^2 + a_2^2 + ... + a_f^2\right)^{\frac{1}{2}}$, which are nodes $v_{j-f+1}, v_{j-f+2}, ..., v_j$. Otherwise, if $j > n-f$ then attacker should compare B_2^* with the last f columns as well.

We should note that the computational complexity for finding attcker's best response does not scale with n and exponentially grows with f, as it should compare the singular value of all combinations of last f columns with matrices B_1^* (or B_2^*). ■

REFERENCES

[1] S. M. Dibaji, M. Pirani, D. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annual Reviews in Control*, 2019.

[2] 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.

[3] 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.

[4] 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.

[5] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *47th Annual Allerton Conf.*, 2009, pp. 91–918.

[6] 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.

[7] 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.

[8] M. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J. P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys*, vol. 45, pp. 53–73, 2013.

[9] 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.

[10] J. P. H. M. Felegyhazi, *Game Theory in Wireless Networks: A Tutorial*. EPFL Technical report, 2006.

[11] J. Marden, G. Arslan, and J. S. Shamma, "Ieee transactions on systems, man, and cybernetics, part b (cybernetics)," *IEEE Trans. Smart Grid*, vol. 39, no. 6, pp. 1393–1407, 2009.

[12] P. N. Brown and H. B. N. J. R. Marden, *Security Against Impersonation Attacks in Distributed Systems*. arXiv preprint arXiv:1711.00609, 2017.

[13] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems," *Automatica*, pp. 186–192, 2013.

[14] M. Dahan, L. Sela, and S. Amin, "Network inspection for detecting strategic attacks," *arXiv:1705.00349v3*, 2018.

[15] J. Milosevic, M. Dahan, S. Amin, and H. Sandberg, "A network monitoring game with heterogeneous component criticality levels," *arXiv preprint arXiv:1903.07261*, 2019.

[16] M. Pirani, E. Nekouie, H. Sandberg, and K.H.Johansson, "A game-theoretic framework for security-aware sensor placement problem in networked control systems," *Proceedings of ACC, the 38th American Control Conference*, 2019.

[17] 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.

[18] A. Clark, B. Alomair, L. Bushnell, and R. Poovendran, *Submodularity in Dynamics and Control of Networked Systems*. Springer, 2016.

[19] B. R. Vellaboyana and J. A. Taylor, "Optimal decentralized control of DC-segmented power systems," *IEEE Transactions on Automatic Control*, vol. 63, pp. 3616–3622, 2018.

[20] H. Hao, P. Barooah, and J. J. P. Veerman, "Effect of network structure on the stability margin of large vehicle formation with distributed control," *IEEE Conference on Decision and Control*, pp. 4783–4788, 2010.

[21] M. Pirani, E. M. Shahrivar, B. Fidan, and S. Sundaram, "Robustness of leader - follower networked dynamical systems," *IEEE Transaction on Control of Network Systems*, vol. 5, no. 4, pp. 1752 – 1763, 2018.

[22] 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.

[23] L. Farina and S. Rinaldi, "Positive linear systems: theory and applications," *John Wiley & Sons*, 2000.

[24] C. Murguia, N. van der Wouw, and J. Ruths, "Reachable sets of hidden cps sensor attacks: Analysis and synthesis tools," in *20th World Congress The International Federation of Automatic Control*, 2017, pp. 2124–2130.

[25] S. G. Williamson, "Combinatorics for computer science," *Courier Dover Publications*, 1985.

[26] J. Bang-Jensen and G. Gutin, "Digraphs: Theory, algorithms and applications," in *Springer*, 2006, pp. 2124–2130.

[27] J. Milosevic, T. Tanaka, H. Sandberg, and K. H. Johansson, "Analysis and mitigation of bias injection attacks against a Kalman filter," *20th IFAC World Congress*, pp. 8393–8398, 2017.

[28] U. Miekkala, "Graph properties for splitting with grounded Laplacian matrices," *BIT Numerical Mathematics*, vol. 33, pp. 485–495, 1993.

[29] M. Pirani, H. Sandberg, and K. H. Johansson, "A graph-theoretic approach to the H_∞ performance of leader-follower consensus on directed networks," *IEEE Control Systems Letters*, vol. 3, pp. 954–959, 2019.

[30] P. V. Mieghem, *Graph spectra for complex networks*. Cambridge University Press, 2010.