A Graph-Theoretic Equilibrium Analysis of Attacker-Defender Game on Consensus Dynamics Under $\mathcal{H}_2$ Performance Metric

Mohammad Pirani, Ehsan Nekouei, Henrik Sandberg, and Karl Henrik Johansson, *Fellow, IEEE*

***Abstract*—In this paper, we propose a game-theoretic framework for improving the resilience of the consensus algorithm, under the $\mathcal{H}_2$ performance metric, in the presence of a strategic attacker. In this game, an attacker selects a subset of nodes in the network to inject attack signals. Its objective is to maximize the $\mathcal{H}_2$ norm of the system from the attack signal to the output of the system. The defender improves the resilience of the system by adding self-feedback loops to certain nodes of the network to minimize the system's norm. We investigate the interplay between the equilibrium strategies of the game and the underlying connectivity graph, using the $\mathcal{H}_2$ performance metric as the game pay-off. The equilibrium of the (zero-sum) attacker-defender game determines the optimal location of the defense nodes in the network. The existence of a Nash equilibrium for consensus dynamics is studied under undirected and directed network topologies. For the cases where the attacker-defender game does not admit a Nash equilibrium, the Stackelberg equilibrium of the game is studied with the defender as the game leader. Our results indicate that the equilibrium strategies of the game are characterized by graph-theoretic notions such as network centrality metrics. In particular, we show that the *effective center* of the graph, a new network centrality measure, captures the optimal location of defense nodes in undirected networks. In directed networks, however, the optimal locations of defenders are those nodes with small in-degrees. The theoretical results are applied to the design of a resilient formation of vehicle platoons.**

***Index Terms*—Security of Networked Systems, Game Theory, $\mathcal{H}_2$ Performance, Network Centrality.**

I. Introduction

A. Motivation

NETWORKED Control Systems are control systems wherein the control loops are closed through a communication network. The communication network can be in the sensing, control, or actuation part of the control loop. By increasing the scale and the complexity of interactions in network control systems, they become more prone to adversarial actions [1]–[4]. A suitable framework to model the battle between a cyber-attack and the defense mechanism is the game theory [5]–[8]. In this paper, we study a game between an attacker and a defender on consensus dynamics in which the attacker tries to maximize its impact on the system while the defender tries to minimize it.

B. Related Work

Game-theoretic approaches to the security of networked systems have been investigated in the past decade [5], [6]. Various approaches have been adopted, either based on the structure of the cyber-physical system or the type of malicious actions. According to the nature of adversarial actions, appropriate game strategies, e.g., Nash or Stackelberg, have been studied [6], [9], [10]. When games are defined on large-scale systems, the strategies of the players, and consequently their equilibrium strategies, depend on the structure of the underlying network. Thus, the game equilibria have to be interpreted in terms of graph-theoretic notions. In attacker-defender game on networked systems, the attacker can target a subset of links in a network to disrupt, e.g., in the form of jamming attacks [11]–[13] or hijack a subset of nodes and change their updating rules. In those problems, the objective of the defender is to mitigate the impact of the attacker or maximize the energy that the attacker needs to disrupt the system [14], [15]. In similar problems, the attacker may target a subset of nodes to inject stealthy and undetectable attacks. The defender, thus, counteracts the attacker by deploying sensors on some nodes to detect the attacks. These problems, known as network monitoring games, have been investigated for both static and randomized (mixed) strategies [7], [16], [17]. Although game-theoretic approaches have been widely used in the security of networked systems, their applications to the resilience of consensus dynamics and its variations, e.g., formation control problems, have not been well studied.

Resilient consensus has attracted attention in recent years. Several studies have been done to enhance the resilience of consensus algorithms against attacks. In [18], an attack detection technique is proposed to detect and isolate the attacked nodes in parallel to the averaging task. Another approach is to calculate the true initial states of the agents, in the presence of a limited number of adversaries, and then do the averaging [19]. In those methods, the averaging has to be performed after

Manuscript received May 11, 2020; revised October 30, 2020; accepted November 2, 2020. Date of publication November 6, 2020; date of current version September 16, 2021. This work was supported by the Knut and Alice Wallenberg Foundation, the Swedish Foundation for Strategic Research and the Swedish Research Council. Recommended for acceptance by Hideaki Ishii. *(Corresponding author: Mohammad Pirani.)*

Mohammad Pirani is with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario M2K0E4, Canada (e-mail: mpirani@uwaterloo.ca).

Ehsan Nekouei is with the Department of Electrical Engineering, City University of Hong Kong, Kowloon, Hong Kong (e-mail: enekouei@cityu.edu.hk).

Henrik Sandberg and Karl Henrik Johansson are with the Division of Decision and Control Systems, KTH Royal Institute of Technology, 11428 Stockholm, Sweden (e-mail: hsan@kth.se; kallej@kth.se).

Digital Object Identifier 10.1109/TNSE.2020.3035964

gathering the true initial conditions of the agents. In [20]–[23], an online resilient consensus method is proposed by filtering the values of malicious agents, i.e., extreme values, while performing the averaging. The former methods reach the exact average of the initial conditions; however, demand extensive computation. The latter requires much less computational cost, while, it only guarantees that the final value will be in a convex hull of initial conditions (and not necessarily the average). These methods, however, require that the underlying network is well-connected. In most applications, the underlying topology is given and can be sparse. In this case, alternative approaches to counteract the adversarial actions have to be proposed.

In a parallel research direction, the effect of the network structure to mitigate or propagate communication disturbances has been studied, usually referred to as *network coherence* [24]. Given networks with arbitrary connectivity levels, the objective is to identify the most effective nodes for placing controllers to maximize the robustness of the network control system [25]–[27]. In our paper, we use this framework to place defense nodes to increase the resilience of consensus algorithms against adversarial actions. We provide graph-theoretic interpretations for the optimal locations of the defense nodes which appear in the form of equilibrium strategies of a zero-sum game between the attacker and the defender.

C. Contributions

In this paper, we introduce the attacker-defender zero-sum game, for multi-agent consensus systems, wherein an attacker selects a set of nodes to inject attack signals. In our set-up, to reduce the impact of attack signals, the defender adds self-feedback loops to the dynamics of certain nodes. We investigate the interplay between the equilibrium strategies of the attacker-defender game and the underlying inter-agent connectivity graph when the game pay-off is characterized by the system $\mathcal{H}_2$ performance metric. More specifically, the contributions of the paper are:

- We introduce a zero-sum game between an attacker and a defender in consensus dynamics. The game payoff is the system $\mathcal{H}_2$ norm from the attack input to the states of the agents. The equilibrium of the game determines the optimal places of the defense nodes in the network.
- For the case where the underlying network is undirected, we show that the game does not admit a Nash equilibrium (NE). Hence, we discuss the Stackelberg game when the defender is the game leader. We show that the equilibrium strategy of the defender is determined by a new network centrality metric, called *effective center* of the graph. This centrality reduces to the well-known notion of graph's center when the underlying graph is a tree. We also discuss the extension of the result to a second-order consensus on undirected graphs.
- For directed graphs, via using an approximation, we characterize necessary and sufficient conditions for the existence of an NE and discuss the Stackelberg game for the cases where there is no NE. We show that the optimal location of the defenders belongs to nodes with the smallest in-degrees.
- We apply the theoretical results to the design of a resilient formation control algorithm for κ-nearest neighbor vehicle platoons.

D. Notations and Definitions

A weighted undirected graph is denoted by $\mathcal{G}_u = \{\mathcal{V}, \mathcal{E}\}$, where $\mathcal{V}$ is the set of vertices (or nodes) and $\mathcal{E}$ is the set of undirected edges. In particular, $(v_i, v_j) \in \mathcal{E}$ 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 weighted directed graph (digraph). Let $|\mathcal{V}| = n$ and define the adjacency matrix for $\mathcal{G}$, denoted by $A \in \mathbb{R}^{n\times n}$, to be a matrix where $A_{ij} = w_{ij}$ if and only if there is an edge with weight w_{ij} between v_j and v_i in $\mathcal{G}_u$ (or there is an edge with weight w_{ij} from v_j to v_i in $\mathcal{G}_d$). The *neighbors* of vertex $v_i \in \mathcal{V}$ in the graph $\mathcal{G}_u$ are denoted by the set $\mathcal{N}_i = \{v_j \in \mathcal{V} \mid \{v_j, v_i\} \in \mathcal{E}\}$ and in $\mathcal{G}_d$ are denoted by the set $\mathcal{N}_i^{in} = \{v_j \in \mathcal{V} \mid (v_j, v_i) \in \mathcal{E}\}$. We define the degree for node v_i as $\Delta_i = \sum_{v_j \in \mathcal{N}_i} A_{ij}$. Respectively, the in-degree for node v_i in $\mathcal{G}_d$ as $\Delta_i = \sum_{v_j \in \mathcal{N}_i^{\text{in}}} A_{ij}$. The Laplacian matrix of an undirected graph is denoted by $L = D - A$, where $D = \text{diag}(\Delta_1, \Delta_2, \ldots, \Delta_n)$. We use $\mathbf{e}_i$ to indicate the i-th vector of the canonical basis. The distance between a pair of nodes v_i and v_j is the weighted length of the shortest path between v_i and v_j. The eccentricity $\epsilon(v)$ of a vertex v in a connected undirected graph $\mathcal{G}_u$ is the maximum graph (weighted) distance between v and any other vertex $u \in \mathcal{V}$. The center of a graph is a set of vertices with minimum (weighted) eccentricity. The f-eccentricity of a vertex v in a connected weighted graph $\mathcal{G}_u$ is the maximum sum of graph weighted distances between v and any subset of f vertices $u_1, u_2, \ldots, u_f \in \mathcal{V}$. The f-center of a graph is a set of vertices with minimum (weighted) f-eccentricity. The *effective resistance*, R_{ij}, between two vertices v_i and v_j in a graph is the equivalent resistance between these two vertices when we treat the resistance of each edge e as $\frac{1}{w_e}$, where w_e is its weight. The effective eccentricity $\epsilon_f(v)$ of node v in a connected graph $\mathcal{G}$ is the maximum graph effective resistance between v and any other vertex u of $\mathcal{G}$. The *effective center* of a graph is a set of vertices with minimum effective eccentricity.

II. Problem Formulation

Consider a network of interconnected agents, represented by a connected undirected graph $\mathcal{G}_u = \{\mathcal{V}, \mathcal{E}\}$.[1] Each agent $v_i \in \mathcal{V}$ has a scalar state $x_i(t)$ which evolves as

$$\dot{x}_i(t) = \sum_{j \in \mathcal{N}_i} w_{ij} \big(x_j(t) - x_i(t)\big), \tag{1}$$

where $w_{ij} > 0$ represents the positive communication strength. There is a subset of agents, denoted by $\mathfrak{D}$, which use an additional feedback from their own initial state and evolve as [2]

[1] The model is the same for digraphs as will be discussed in Section IV.

[2] This type of state evolution where agents used their initial states as feedbacks is used in opinion dynamics literature [28].

$$\dot{x}_i(t) = \sum_{j \in \mathcal{N}_i} w_{ij}\big(x_j(t) - x_i(t)\big) + u_i(t), \quad v_i \in \mathfrak{D}, \tag{2}$$

where $u_i(t) = -k(x_i(t) - x_i(0))$ with $k > 0$ as the gain of the self-feedback. The gain value k is constant and the same for all agents who use this self-feedback loop. These pure state feedback terms are added to some agents' dynamics to increase the resilience of the consensus to attacks. Dynamics (2) in a matrix form become

$$\dot{\boldsymbol{x}}(t) = -\bar{L}\boldsymbol{x}(t) + K\boldsymbol{x}(0), \tag{3}$$

where $\bar{L} = L + K$, $K = kD_z$, and $D_z = \mathrm{diag}(z)$ in which $z = [z_1, z_2, ..., z_n]^T$ is a binary vector. We have $z_i = 1$ if node i has a self feedback and $z_i = 0$ otherwise. We refer to the nodes with the self feedback loops as the *defense nodes*. When there is no self-feedback loop, dynamics (3) converges to the average of the initial conditions [29]. If there exists at least a single node with a feedback, then dynamics (3) converges to some convex combination of agents' initial conditions [25], [30].

A. Attack Model

There is an attacker which injects attack signals to a subset of nodes in the graph. Let $\mathfrak{F} = \{v_{i_1}, v_{i_2}, ..., v_{i_{f_a}}\}$ denote the set of f_a nodes under attack. Since the exact number of attacked nodes is unknown to the defender, f_a is considered as a *known* upper bound on the number of attacked nodes. The dynamic of an attacked node is

$$\dot{x}_i(t) = \sum_{j \in \mathcal{N}_i} w_{ij}\big(x_j(t) - x_i(t)\big) + \zeta_i(t), \quad v_i \in \mathfrak{F} \tag{4}$$

where $\zeta_i(t)$ represents the attack signal on node v_i. Dynamics (3) with additive attack signal becomes

$$\dot{\boldsymbol{x}}(t) = -\bar{L}\boldsymbol{x}(t) + K\boldsymbol{x}(0) + B\boldsymbol{\zeta}(t), \tag{5}$$

where the matrix $B_{n \times f_a} = [\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, ..., \mathbf{e}_{i_{f_a}}]$ specifies the nodes selected by the attacker. We consider full state measurement in (5). Note that the attacker only selects matrix B and the attack signal $\boldsymbol{\zeta}(t)$ is not a decision variable.

Based on the above problem formulation, we define the attacker-defender game.

B. Attacker-Defender Game

We now pose the decision-making problem between the attacker and the defender as a zero-sum game. Let $\bar{\boldsymbol{x}}(t) = \boldsymbol{x}(t) - \bar{L}^{-1}K\boldsymbol{x}(0)$ be the error state and write the error dynamics of (5). The resulting error dynamics becomes

$$\dot{\bar{\boldsymbol{x}}}(t) = -\bar{L}\bar{\boldsymbol{x}}(t) + B\boldsymbol{\zeta}(t). \tag{6}$$

We use the system $\mathcal{H}_2$ norm of the transfer function $G(s) = (sI + \bar{L})^{-1}$ from $\boldsymbol{\zeta}(t)$ to $\bar{\boldsymbol{x}}(t)$ defined as

$$||G||_2 \triangleq \left(\frac{1}{2\pi}\mathrm{tr}\int_0^\infty G^*(j\omega)G(j\omega)d\omega\right)^{\frac{1}{2}}. \tag{7}$$

The above $\mathcal{H}_2$ norm for state-space model (6) can be calculated by $||G||_2 = \mathrm{tr}(B^TWB)$, where W is the observability Gramian obtained from the the Lyapunov equation

$$\bar{L}^TW + W\bar{L} = I. \tag{8}$$

When the network is undirected ($\bar{L}$ is symmetric) the solution of (8) is easily obtained as $W = \frac{1}{2}\bar{L}^{-1}$. We drop factor $\frac{1}{2}$ for simplicity. Such a closed form solution for general directed network does not exist. Based on the above discussion, the attacker-defender game is defined. **Attacker-Defender Game:** The attacker injects the vector of attack signals $\boldsymbol{\zeta}(t)$ to the set $\mathfrak{F}$ of f_a nodes in the network to maximize the system $\mathcal{H}_2$ norm from $\boldsymbol{\zeta}(t)$ to $\bar{\boldsymbol{x}}(t)$, while the defender places self feedback loops on the set $\mathfrak{D}$ of f_d nodes to minimize this system norm. Thus the game payoff becomes

$$J(B, D_z) = \mathrm{tr}\big(B^TWB\big) = \sum_{i \in \mathfrak{F}} w_{ii}. \tag{9}$$

The attacker's decision determines matrix B to maximize $J(B, D_z)$ and the defender's decision affects matrix D_z, and consequently $\bar{L}$ and W, to minimize $J(B, D_z)$.

Remark 1: In our setting, the defender does not have any information about the frequency content of the attack signal $\zeta(t)$. With this in mind, one of the main reasons for considering the $\mathcal{H}_2$ norm is that this system norm is calculated based on all frequencies, i.e., (7).

The number of all possible combinations of f_a attacked nodes and f_d defense nodes in a network of n nodes is $\binom{n}{f_a} \times \binom{n}{f_d}$. As a result, the game matrix will have $\binom{n}{f_d}$ rows, one for each combination of defence nodes, and $\binom{n}{f_a}$ columns, one for each combination of attack nodes. Let $\{\mathfrak{F}_1, \mathfrak{F}_2, ..., \mathfrak{F}_{\binom{n}{f_a}}\}$ and $\{\mathfrak{D}_1, \mathfrak{D}_2, ..., \mathfrak{D}_{\binom{n}{f_d}}\}$ denote the sets of all possible subsets of $\mathcal{V}$ with f_a and f_d elements, respectively. Matrix $\mathcal{A}$, with size $\binom{n}{f_a} \times \binom{n}{f_d}$, is defined as the payoff matrix of the attacker-defender game where $\mathcal{A}_{ij} = J(\mathfrak{F}_j, \mathfrak{D}_i)$ is the system $\mathcal{H}_2$ norm when the attacked nodes are in $\mathfrak{F}_j$ and the defense nodes are in $\mathfrak{D}_i$.[3] The attacker, i.e., the maximizer, is the column player and the defender, i.e., the minimizer, is the row player. Fig. 1 is an example of the attacker and defender decisions. Based on this figure, nodes 1 and 3 are under attack, i.e., $\mathfrak{F} = \{1, 3\}$, and the defender chooses nodes 1 and 2, i.e., $\mathfrak{D} = \{1, 2\}$. The game matrix is shown in Fig. 1 whose rows determine the defender's strategies and columns determine the attacker's strategies. In this example, based on the attacker and defender's decisions and (9), the game value is $\mathcal{A}_{12} = w_{11} + w_{33}$, i.e., the summation of the first and the third diagonal elements of the observability Gramian. If the graph is undirected it becomes $\mathcal{A}_{12} = \bar{L}^{-1}_{11} + \bar{L}^{-1}_{33}$.

We discuss the equilibrium of the above game for the cases of single attacked-single defense nodes (*SA-SD*) and multiple

[3] Since sets $\mathfrak{F}$ and $\mathfrak{D}$ correspond to matrices B and D_z, respectively, in this paper we use $J(\mathfrak{F}, \mathfrak{D})$ and $J(B, D_z)$ interchangeably.

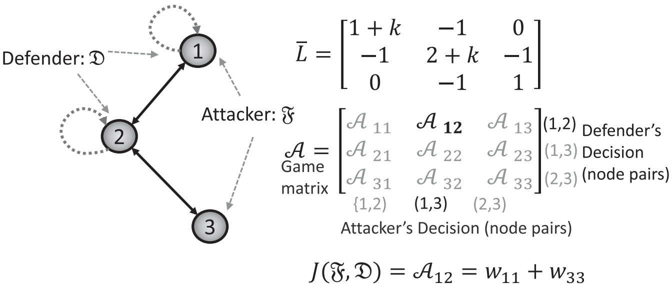

Defender: $\mathfrak{D}$
Attacker: $\mathfrak{F}$
1
2
3
$\bar{L} = \begin{bmatrix} 1+k & -1 & 0 \\ -1 & 2+k & -1 \\ 0 & -1 & 1 \end{bmatrix}$
$\mathcal{A} = \begin{bmatrix} \mathcal{A}_{11} & \mathcal{A}_{12} & \mathcal{A}_{13} \\ \mathcal{A}_{21} & \mathcal{A}_{22} & \mathcal{A}_{23} \\ \mathcal{A}_{31} & \mathcal{A}_{32} & \mathcal{A}_{33} \end{bmatrix}$
Game matrix
(1,2) (1,3) (2,3)
Defender's Decision (node pairs)
{1,2} (1,3) (2,3)
Attacker's Decision (node pairs)
$J(\mathfrak{F}, \mathfrak{D}) = \mathcal{A}_{12} = w_{11} + w_{33}$

Fig. 1. Example of a game between the attacker and the defender and its game payoff.

attacked-multiple defense nodes (*MA-MD*). Before that, we define NE for game

Definition 1: The game (9) admits an NE if there exists attacker and defender decisions $\mathfrak{F}^*$ and $\mathfrak{D}^*$ such that

$$J(\mathfrak{F}, \mathfrak{D}^*) \leq J(\mathfrak{F}^*, \mathfrak{D}^*) \leq J(\mathfrak{F}^*, \mathfrak{D}), \tag{10}$$

for all attacker and defender's decisions $\mathfrak{F} \neq \mathfrak{F}^*$ and $\mathfrak{D} \neq \mathfrak{D}^*$.

III. Equilibrium Analysis for Undirected Graphs

In this section, we study the equilibrium of the attacker-defender game on undirected graphs. We start by considering trees (connected acyclic graphs) as they provide insights about the optimal placement of defense nodes in the graph.

A. Undirected Trees: Single Attacked-Single Defense Nodes

Recalling that for undirected graphs, the observability Gramian is $W = \frac{1}{2}(L + kD_z)^{-1}$, for the *SA-SD* case, the game payoff simply becomes

$$J(B, D_z) = [(L + k\mathbf{e}_j\mathbf{e}_j^T)^{-1}]_{ii}, \tag{11}$$

where i is the index of the node under attack and j is the index of the defense node.

Proposition 1: The *SA-SD* game on undirected trees does not admit a pure Nash equilibrium.

Proof: First, we need to find a graph-theoretic expression for each diagonal element of $\bar{L}^{-1}$. We have

$$[\bar{L}^{-1}]_{ii} = \frac{1}{k} + \sum_{h \in \mathcal{P}_{ij}} \frac{1}{w_h}, \tag{12}$$

where $\mathcal{P}_{ij}$ is the set of edges in the unique path from v_i to v_j and w_h is the weight of the edge h. The proof of (12) is straightforward as it is a special case of Lemma 1 which will be discussed later in Section III-C. To prove the proposition we use contradiction. Based on (12) we have

$$\mathcal{A}_{ii} = \frac{1}{k} < \mathcal{A}_{ij} = \frac{1}{k} + \sum_{h \in \mathcal{P}_{ij}} \frac{1}{w_h}, \quad i \neq j.$$

Suppose there exists an NE for the game, denoted by (i^*, j^*). This must satisfy

$$[\mathcal{A}]_{i^*j} \leq [\mathcal{A}]_{i^*j^*} \leq [\mathcal{A}]_{ij^*} \tag{13}$$

for all $i \neq i^*$ and $j \neq j^*$. If $i^* = j^*$, then the left inequality is violated and if $i^* \neq j^*$, the right inequality is violated. ■

When the game does not admit a Nash equilibrium, an alternative approach is to define a Stackelberg game between the attacker and defender. In a Stackelberg game with two players, the player who announces his strategy first is called the *leader* and the other player who reacts to the leader's decision is called the *follower*.

Remark 2 (Stackelberg vs. Nash Equilibrium): The interaction between an active attacker, e.g., a jammer, and a passive defender can be reasonably captured by a Stackelberg game in that the jammer is an active player who sends signals at an intended level to interfere communication channels while the legitimate user rationally defends itself from such an attack. In the case where the defending behaves actively or either side has information advantage, the Nash equilibrium becomes a reasonable solution concept [6].

In security problems, the defender acts as the game leader of the Stackelberg game formulation. In particular, the defender solves the following optimization problem

$$J^*(D_z) = \min_{D_z} \operatorname{tr}\Big(B^{*^T}(D_z)\bar{L}^{-1}B^*(D_z)\Big). \tag{14}$$

where D_z is chosen over all f_d defense nodes in $\mathcal{V}$ (here $f_d = 1$) and $B^*(D_z)$ is the optimal response of the attacker when the strategy of the defender is D_z, i.e., $B^*(D_z)$ is the solution of

$$B^*(D_z) \in \arg\max_{B} \operatorname{tr}\big(B^T\bar{L}^{-1}B\big), \tag{15}$$

where B is chosen over all f_a attacked nodes (here $f_a = 1$) in $\mathcal{V}$. The following theorem discusses the solution of the Stackelberg game on undirected trees.

Theorem 1: For the *SA-SD* Stackelberg game on the connected undirected tree $\mathcal{G}_u$, a solution belongs to the case where the defender chooses the graph's center. The attacker's best response is to choose the farthest node from the center.

Proof: We have $\mathcal{A}_{ij} = \frac{1}{k} + \sum_{h \in \mathcal{P}_{ij}} \frac{1}{w_h}$. The defender minimizes the maximum element of each row, over all rows of $\mathcal{A}$. The defender's optimal strategy is then $v^* = \arg\min_i \max_j \sum_{h \in \mathcal{P}_{ij}} \frac{1}{w_h}$ and this is the graph's center. Since the graph's center may not be unique, the strategies of the defender and attacker may not be unique. However, the game value is unique. The attacker's best response in this case is the maximum element on the row which belongs to node v^* and that is a node with maximum weighted distance from v^*. ■

One can interpret the system $\mathcal{H}_2$ norm as the ability of the networked system to propagate the attack signal throughout the network. This property is denoted by network incoherence in the literature [24]. From a graph-theoretic perspective, the longer the path between the attacked node and the defense node results in a larger propagation of the attack signal throughout the network. From this view, the result of Theorem 1 is intuitive as it indicates that the optimal decision of the defender is to choose a node in the graph whose largest distance from the nodes in the graph is minimum.

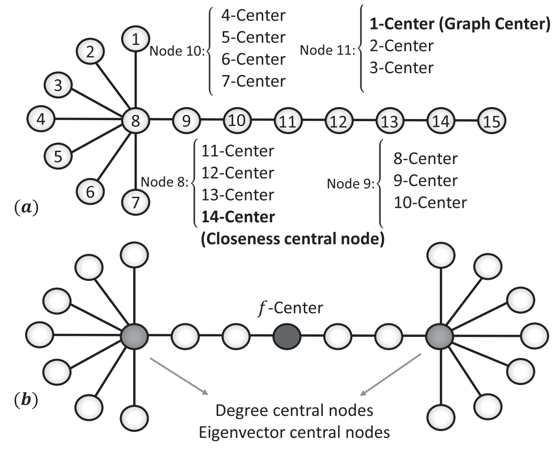


Fig. 2. (a) A graph in which the location of f-center changes with f. (b) Deviation of f-centrality from degree-based centralities in a graph.

B. Undirected Trees: Multiple Attacked-Single Defense Nodes

Now, we analyze the case where there are multiple attacked nodes and a single defense node. As mentioned before, we assume that the defender knows an upper bound on the number of attacks, f_a. Thus, the optimal strategy of the defender depends on the number of (assumed) attack nodes f_a. The following proposition discusses this fact more formally. The proof follows a similar procedure to that of Theorem 2 with the exception that instead of weighted distances between pairs on nodes, the game payoff is a function of effective resistances. The notion of graph's f-center was defined in Section I-D.

Proposition 2: Consider the Stackelberg game with a single defence node and f_a attack nodes over connected undirected tree $\mathcal{G}_u$. Then, a defender's equilibrium strategy is to choose the f_a-center of the graph. The attacker's best response is to choose the farthest f_a nodes from the f_a-center.

In graph theory and network analysis, indicators of centrality identify the most important vertices within a graph. There are various network centrality metrics, such as degree centrality, closeness centrality, and eigenvector centrality [31]. Here, we interpret the graph's f-center as a new centrality measure and compare it with other centrality metrics via examples. The graph's closeness center node (a node which has the minimum summation of distances to all other nodes in the graph) is the $(n-1)$-center node. The location of graph's f-center in the network is a function of f.

Example 1: Consider a tree formed by a star of size m attached to a path of length m, as shown in Fig. $2(a)$ for $m = 7$. In this graph, the closeness center node remains in the center of the star by changing m; however, the graph's f-center moves to left through the path as m increases.

Example 1 shows that when the exact number of the attacks is unknown to the defender, choosing an f-center of the graph for some f results in a sub-optimal solution. In particular, with a single defense node and (potentially) multiple attacked nodes, if the known upper bound f_a is considerably different from the actual attacked nodes, it will have a large impact on the defender's decision. As an example, suppose that only one node is attacked while $f_a = 11$. In this case, the defender chooses the center of the star (node 8) whereas the true decision is to choose node 11, i.e., the center of the graph. By increasing the scale of the tree in Fig. 2 (a), i.e., adding nodes to the star and increasing the length of the tail simultaneously, the gap between the defender's decision with and without the knowledge of the actual attacked nodes become larger. However, distance-based centralities, e.g., graph's f-central nodes, are still among the appropriate choices for the defender. In other words, degree-based centralities, e.g., the degree center or the eigenvector center of the graph [31], can lead to decisions which are arbitrarily far from the optimal one. This observation is discussed in the following example.

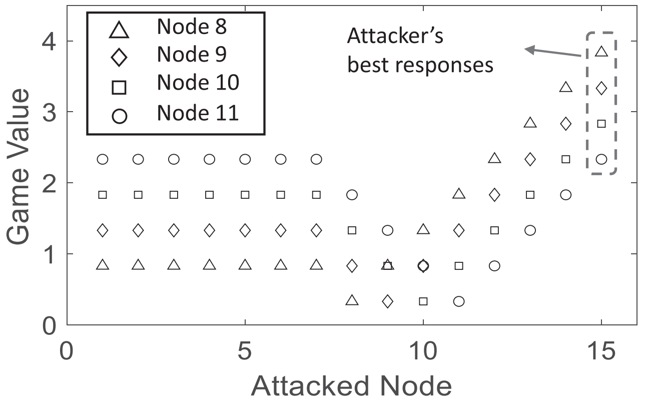


Fig. 3. The effect of choosing the center of the graph as the defender for graph in Fig. 2 (a).

Example 2: The degree center and eigenvector center nodes in Fig. 2 (b) are located at the center of the stars; however, the f-central node, for any $f \leq n-1$, is in the middle of the path. As the length of the path increases, the f-center becomes arbitrarily far from the degree center and the eigenvector center.

The following example shows the attacker and defender's equilibrium strategies and confirms the result of in Proposition 2.

Example 3: The game values for four sample defense nodes (nodes 8, 9, 10, and 11 in Fig. 2) and for all possible choices of the attacked nodes are shown in Fig. 3. The horizontal axis shows the attacker's decision.According to this figure, the best response of the attacker to any defender's decision is to select the node in the end of the line (node 15). Thus, the optimal value from the defender's perspective is to choose node 11, i.e., the graph's center. The attacker's best response to the defender's decisions is node 15.

C. General Undirected Graphs

Here, we discuss the *MA-MD* game on general undirected graphs. Note that adding feedback loops to a set of nodes is equivalent to connecting them to a virtual node ℓ, as shown in Fig. 4.Matrix $\bar{L}$ is a submatrix of the Laplacian matrix $L_{(n+1)\times(n+1)}$ of an extended graph (including node ℓ) in which the row and the column corresponding to ℓ are removed. $\bar{L}$ is called the grounded Laplacian matrix in the literature [25]. The following lemma interprets the diagonal elements of $\bar{L}^{-1}$ via graph-theoretic notions.

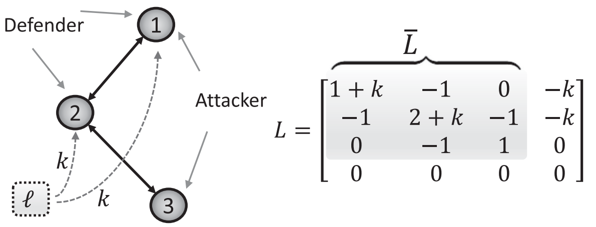

Defender
1
2
3
Attacker
k
k
ℓ
$\bar{L}$
$L = \begin{bmatrix} 1+k & -1 & 0 & -k \\ -1 & 2+k & -1 & -k \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

Fig. 4. Extended graph and the virtual agent.

Lemma 1 ([32]): For an extended graph $\mathcal{G}_u$ we have $\bar{L}_{ii}^{-1} = R_{i\ell}$, where $R_{i\ell}$ is the effective resistance between v_i and the virtual node ℓ.

For trees, the effective resistance between two nodes reduces to their physical distance. As an example of Lemma 1, consider nodes 1 and 2 in Fig. 4 as defenders while 1 and 3 are the attacked nodes. We have $J(B, D_z) = \sum_{i\in B} \bar{L}_{ii}^{-1} = R_{1\ell} + R_{3\ell}$.

Theorem 2: For the *SA-SD* Stackelberg game over the connected undirected graph $\mathcal{G}_u$, a solution belongs to the case where the defender chooses the effective center of the graph (defined in Section I-D), i.e., $v^* \in \arg\min_{v\in\mathcal{V}} \epsilon_f(v)$, and the attacker chooses the node with the largest effective resistance from v^*.

Proof: Element $\mathcal{A}_{ij}$ in the game matrix is equal to $R_{j\ell}$ which is the effective resistance from the attacked node v_j to the virtual agent connected to the defense node v_i. Since the virtual node ℓ is only connected to the defense node v_i, we have $R_{j\ell} = R_{ij} + R_{i\ell} = R_{ij} + \frac{1}{k}$. Thus, the term $\frac{1}{k}$ is shared over all elements of $\mathcal{A}$. The rest of the proof follows the similar procedure as that of Theorem 1, except that the physical distance is replaced with the effective resistance. ■

The following theorem generalizes Theorem 2 to the *MA-MD* case.

Theorem 3 (MA-MD): Consider the *MA-MD* Stackelberg game with f_d defense nodes and f_a attack nodes, $f_a, f_d \geq 1$ over the connected undirected graph $\mathcal{G}_u$. The virtual agent corresponding to the set of defense nodes $\mathfrak{D}$ is denoted by $\ell_{\mathfrak{D}}$. Then, a solution of the game is when the defender chooses $\mathfrak{D}^* \in \arg\min_{\mathfrak{D}\subseteq\mathcal{V}} \max_{\mathfrak{F}\subseteq\mathcal{V}} \sum_{j\in\mathfrak{F}} R_{\ell_{\mathfrak{D}}j}$. The attacker's best response is $\mathfrak{F}^*(\mathfrak{D}^*) \in \arg\max_{\mathfrak{F}\subseteq\mathcal{V}} \sum_{j\in\mathfrak{F}} R_{\ell_{\mathfrak{D}^*}j}$.

Remark 3 (Effect of Increasing Connectivity and Adding Defense Nodes): The effective resistance between each pair of nodes is a decreasing function of edge weights [32]. Thus, increasing the weight of edges or adding edges to the network decreases the diagonal elements of $\bar{L}^{-1}$ which results in decreasing $\mathcal{H}_2$ norm. Hence, increasing the network connectivity improves the resilience of the system to cyber-attacks. Furthermore, adding a defense node v_i, i.e., a self-feedback loop to node v_i, is equivalent to adding an edge between v_i and ℓ. Hence, similar to the above discussion, adding defense nodes results in decreasing the game value, i.e., increases the security of the system.

D. Discussion on the Second-Order Consensus

In this subsection, we extend the results to the second order consensus. The state of a node under attack evolves as

$$\begin{aligned} \dot{x}_i(t) &= v_i(t), \\ \dot{v}_i(t) &= u_i(t) + \zeta_i(t), \quad i \in \mathfrak{F}, \end{aligned} \tag{16}$$

where $\zeta_i(t)$ is the attack signal as mentioned before. We use a variation of the control law which is widely used in formation control problems [33], [34]

$$\begin{aligned} u_i(t) = &- \sum_{j\in\mathcal{N}_i} a_{ij}\big(x_i(t) - x_j(t)\big) - \sum_{j\in\mathcal{N}_i} b_{ij}\big(v_i(t) - v_j(t)\big) \\ &- k(x_i(t) - x_i(0)) - kv_i(t), \quad k > 0. \end{aligned} \tag{17}$$

In (17), we consider the same feedback gain value k for both x_i and v_i to reach to a closed form expression for $\mathcal{H}_2$ norm. Here a_{ij} and b_{ij} are communication weights and k is the additional control gain applied by the defender. Dynamics (16) in vector form becomes

$$\begin{bmatrix} \dot{\boldsymbol{x}} \\ \ddot{\boldsymbol{x}} \end{bmatrix} = \underbrace{\begin{bmatrix} \mathbf{0}_n & I_n \\ -\bar{L} & -\bar{L} \end{bmatrix}}_{A} \begin{bmatrix} \boldsymbol{x} \\ \dot{\boldsymbol{x}} \end{bmatrix} + \begin{bmatrix} \mathbf{0} \\ \boldsymbol{K} \end{bmatrix} \boldsymbol{x}(0) + \begin{bmatrix} \mathbf{0} \\ B \end{bmatrix} \boldsymbol{\zeta}(t), \tag{18}$$

where B, $\bar{L}$, and $\boldsymbol{K}$ are the same before. A conventional output of interest is $\dot{\boldsymbol{x}}$. Note that in the steady state (in the absence of attacks) we have $\dot{\boldsymbol{x}}(0) = \ddot{\boldsymbol{x}}(0) = \mathbf{0}$. Substituting these values into (18), assuming $\boldsymbol{\zeta}(t) = 0$, we get $-\bar{L}\boldsymbol{x} + \boldsymbol{K}\boldsymbol{x}(0) = \mathbf{0}$ which is exactly the same as the first order model (5) reaching the steady state. Hence, in the absence of attack, the state of each node converge to some convex combination of the initial states.

Proposition 3: The $\mathcal{H}_2$ norm of (18) from $\boldsymbol{\zeta}(t)$ to $\boldsymbol{y} = \dot{\boldsymbol{x}}$ is

$$||G_2||_2^2 = \frac{1}{2} \sum_{i\in\mathfrak{F}} \bar{L}_{ii}^{-1}. \tag{19}$$

Proof: We have to first calculate the observability Gramian W for (18) with output $\boldsymbol{y} = \dot{\boldsymbol{x}}$. We have

$$\begin{bmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{bmatrix} A + A^{\mathsf{T}} \begin{bmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{bmatrix} = \begin{bmatrix} \mathbf{0}_n & \mathbf{0}_n \\ \mathbf{0}_n & -I_n \end{bmatrix}. \tag{20}$$

By solving (20) we get $w_{11} = \frac{1}{2}I$, $w_{22} = \frac{1}{2}\bar{L}^{-1}$ and $w_{12} = w_{21} = \mathbf{0}$. Hence we have $||G||_2^2 = \mathrm{tr}(B^{\mathsf{T}} w_{22} B) = \frac{1}{2}\mathrm{tr}(B^{\mathsf{T}} \bar{L}^{-1} B)$ which yields the result. ■

The above proposition bridges the results of Sections III-A, III-B, and III-C to the second order consensus and Theorems 2 and 3 can be readily applied to the game on dynamics (16).

IV. Equilibrium Analysis for Directed Graphs

In this section, we discuss the game when the underlying graph has directed edges. The main challenge for digraphs is that the observability Gramian (and consequently the $\mathcal{H}_2$ norm) can not be derived in closed-form. Thus, we use an approximation by considering that each diagonal element of the Gramian follows the behaviour of the in-degree of the corresponding node. In Section V, we show that for specific topologies, this approximation yields the equilibrium strategies which are compatible with those of the exact $\mathcal{H}_2$ norm of the system.

Due to some topological necessities for reaching a consensus, we assume that the graph contains a directed spanning tree. Based on the Lyapunov equation (8), the $\mathcal{H}_2$ norm is the summation of some of the diagonal elements of W chosen by the attacker. Solving the Lyapunov equation for a diagonal element w_{ii} of matrix W yields

$$w_{ii} = \frac{1}{\Delta_i}\left(\sum_{k\in\mathcal{N}_i^{\text{out}}} w_{ik} + \frac{1}{2}\right), \tag{21}$$

where Δ_i is the in-degree of node i and $\mathcal{N}_i^{\text{out}} = \{v_j \in \mathcal{V} \mid (v_i, v_j) \in \mathcal{E}\}$ are the out-neighbors of node v_i. Unlike undirected graphs, the relation between w_{ii} and the structure of the underlying digraph is not clear. Thus, we make an approximation by assuming that w_{ii} follows the behaviour of the coefficient $\frac{1}{\Delta_i}$ in (21), i.e., $w_{ii} \leq w_{jj}$ if $\Delta_i \geq \Delta_j$. We will show the applicability of this assumption later via examples. By introducing matrix X whose i-th diagonal element is $\frac{1}{\Delta_i}$, we define the game payoff for directed graphs as

$$J(B, D_z) = \text{tr}\big(B^T X B\big) = \sum_{i\in\mathfrak{F}\setminus\mathfrak{D}} \frac{1}{\Delta_i} + \sum_{i\in\mathfrak{F}\cap\mathfrak{D}} \frac{1}{\Delta_i + k}. \tag{22}$$

A. Directed Graphs: Single Attacked-Single Defense Nodes

The following theorem characterizes the NE for *SA-SD* game on digraphs.

Proposition 4: The *SA-SD* game on digraph $\mathcal{G}_d$ has an NE if and only if $k \leq \Delta_{n-1} - \Delta_n$ where Δ_n and Δ_{n-1} are smallest and second smallest in-degrees in the graph. An NE strategy for both attacker and defender is to choose $v \in \arg\min_i \Delta_i$, i.e., a node with the smallest in-degree.

Proof: Based on (22), the game matrix $\mathcal{A}$ is of the following form

$$\mathcal{A}_{ij} = cases\frac{1}{\Delta_j + k} \quad i = j, \frac{1}{\Delta_j} \quad i \neq j.cases \tag{23}$$

First, we prove the necessary condition. Suppose that the players decisions, i.e., the node with the smallest degree, yield an NE. Then, we must have $\frac{1}{\Delta_n+k} \geq \frac{1}{\Delta_j}$ for all $j = 1, 2, ..., n$ which results in having $k \leq \Delta_{n-1} - \Delta_n$. Now, if $k \leq \Delta_{n-1} - \Delta_n$, then by changing the attacker's strategy (unilaterally) from the node with the minimum in-degree to some node v_i, according to (23), the game value becomes $J = \frac{1}{\Delta_i} \leq \frac{1}{\Delta_n+k}$. Moreover, if the defender changes its decision to another node v_i, according to (23) as the minimum component of each column is its diagonal element, it will get $J = \frac{1}{\Delta_n} \geq \frac{1}{\Delta_n+k}$. Thus, none of the players tend to change their decisions unilaterally. ■

Remark 4: For the cases where the node with the smallest degree is not unique, there is no NE for any $k > 0$, because $\Delta_{n-1} - \Delta_n = 0$. An example of such graphs is Fig. 5(a) where nodes 1 and 2 both have the smallest in-degree $\Delta_n = 1$.

Similar to undirected graphs, for the cases where there is no NE, the Stackelberg game approach with the defender as the game leader is considered.

Theorem 4: For the *SA-SD* Stackelberg game on digraph $\mathcal{G}_d$ with $k > \Delta_{n-1} - \Delta_n$, an optimal decision of the defender is $v \in \arg\min_i \Delta_i$, i.e., a node with the smallest in-degree. In this case, the attacker's best response is the node with the second smallest degree, i.e., $v \in \arg\min_{v_i \neq v} \Delta_i$.

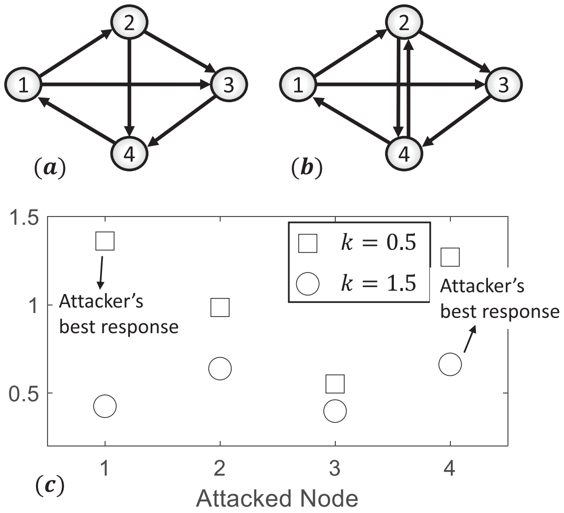


Fig. 5. A digraph with (a) non-unique Δ_n and (b) unique Δ_n. (c) The effect of the threshold value on the equilibrium strategies for digraph (b).

Proof: Since $k > \Delta_{n-1} - \Delta_n$, for each row of the game matrix $\mathcal{A}$, i.e., defender's action, the largest element is $\frac{1}{\Delta_n}$. The exception is the row of a node with the smallest degree for which the maximum element is $\frac{1}{\Delta_{n-1}}$. Thus, the defender's optimal decision is $v = \arg\min_{i\in\mathcal{V}} \Delta_i$ and the attacker's best response becomes $v = \arg\min_{v_i\neq v} \Delta_i$. In this case, if $\arg\min_i \Delta_i$ is unique, the attacker's best response is the node with the second-smallest in-degree and if it is not unique, the attacker's best response will be a node with the smallest degree, other than the one chosen by the defender. The game value is unique and given by $J^* = \frac{1}{\Delta+k}$ where $\Delta = \min_{v_i\neq v} \Delta_i$, although the optimal strategy of the players may be not unique. ■

Example 4: An example of the dependency of the equilibrium strategies on the value k is shown in Fig. 5 (b). In this graph, the smallest in-degree uniquely belongs to node 1. The threshold in Proposition 4 is $\Delta_{n-1} - \Delta_n = 1$. In Fig. 5 (c), the game values for all attacker's strategies when the defender chooses node 1 are shown for two values of k (one above and one bellow the threshold). Based on this plot, the attacker's best response changes from the node with smallest in-degree (node 1) for $k = 0.5$ to a node with the second smallest in-degree (node 4) for $k = 1.5$. This confirms the results of Proposition 4 and Theorem 4. Note that the game values are calculated from the observability Gramian W and not from the approximation (22).

B. Directed Graphs: Multiple Attacked-Multiple Defense Nodes

In this subsection, we study the Stackelberg game for *MA-MD* case.

Theorem 5: Consider a Stackelberg *MA-MD* game. If $f_a + f_d \leq n$ and $k \geq \Delta_1 - \Delta_n$, then an equilibrium decision of the defender is $\boldsymbol{v} \in \arg\max_{\mathfrak{D}\subseteq\mathcal{V}|\mathfrak{D}|=f_d} \sum_{v_i\in\mathfrak{D}} \frac{1}{\Delta_i}$, i.e., f_d nodes with the smallest in-degrees in the network. The best response of the attacker is $\bar{\boldsymbol{v}} \in \arg\max_{\mathfrak{F}\neq\boldsymbol{v}|\mathfrak{F}|=f_a} \sum_{v_i\in\mathfrak{F}} \frac{1}{\Delta_i}$.

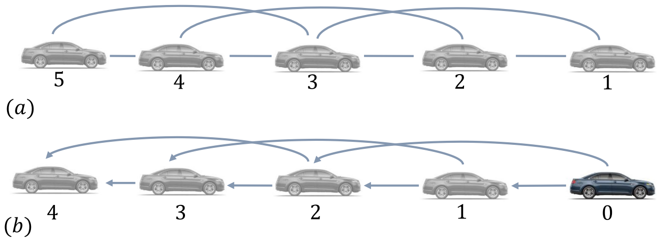


Fig. 6. (a) undirected 2-nearest neighbor platoon. (b) directed 2-nearest neighbor platoon.

Proof: The game matrix $\mathcal{A}$ is

$$\mathcal{A}_{ij} = \begin{cases} \sum_{h\in\mathfrak{F}_j} \frac{1}{\Delta_h + k} & i = j, \\ \sum_{h\in\mathfrak{F}_j\cap\mathfrak{D}_i} \frac{1}{\Delta_h+k} + \sum_{h\in\mathfrak{F}_j\setminus\mathfrak{D}_i} \frac{1}{\Delta_h} & i \neq j, \end{cases} \tag{24}$$

where $\mathfrak{D}_i$ and $\mathfrak{F}_j$ are defender and attacker's decisions, respectively. The defender chooses a row in $\mathcal{A}$ whose maximum element is minimum over all other rows. When $k \geq \Delta_1 - \Delta_n$, considering a fixed set $\mathfrak{D}$, for the row corresponding $\mathfrak{D}$, the maximum belongs to the set of attackers $\bar{\mathfrak{F}}$ for which $\bar{\mathfrak{F}} \cap \mathfrak{D} = \emptyset$. Thus, we must have $n \geq f_a + f_d$. In this case, based on the second term in (24), the maximum component in the row which belongs to $\mathfrak{D}$ is $\bar{\mathcal{M}} = \max_{\mathfrak{F}\subseteq\mathcal{V}\setminus\mathfrak{D}} \sum_{j\in\mathfrak{F}} \frac{1}{\Delta_j}$. Thus, the defender's optimal decision is $\bar{\mathfrak{D}} = \arg\max_{\mathfrak{D}\subseteq\mathcal{V}} \sum_{j\in\mathfrak{D}} \frac{1}{\Delta_j}$. ■

V. Applications to Secure Platooning

In this section, we study the optimal location of controllers on a directed and an undirected κ-nearest neighbor platoon of vehicles to mitigate the impact of cyber-attacks.

Definition 2 (κ-nearest neighbor platoons): For positive integers $n, \kappa \geq 1$ where $n > \kappa$, an undirected κ-nearest neighbor platoon, $\mathcal{P}(n, \kappa)$, is a network comprised of vehicles v_1, $v_2, \ldots, v_n$ in which v_i communicates with vehicles $v_{i-\kappa}, \ldots,$ $v_{i-1}, v_{i+1}, \ldots, v_{i+\kappa}$, for some $\kappa \in \mathbb{N}$. Directed κ-nearest neighbor platoon has the same definition, except that v_i only communicates with $v_{i+1}, \ldots, v_{i+\kappa}$.

An example of vehicle labeling in an undirected and a directed 2-nearest neighbor platoon of 5 vehicles, $\mathcal{P}(5, 2)$, is shown in Fig. 6 (a) and (b).

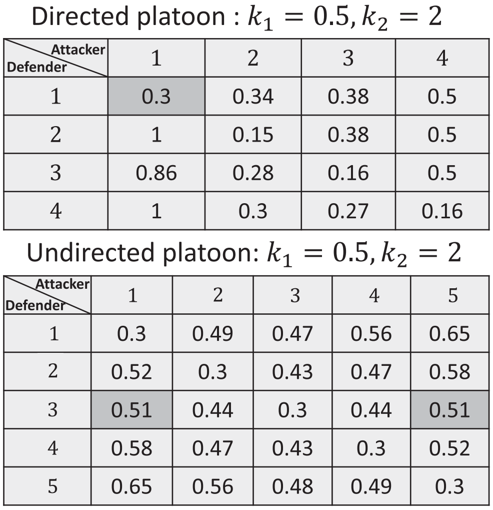
κ-nearest neighbor platoons can be considered as a generalization of well-known bidirectional and predecessor-following topologies [35].

Let p_i and $\dot{p}_i$ be the position and longitudinal velocity of vehicle v_i. Each vehicle's objective is to maintain specific distances from its neighbors. The desired constant distance between vehicles v_i and v_j is denoted by Δ_{ij}. The control law for v_i is [36]

$$\ddot{p}_i(t) = u_i(t) + w_i(t), \tag{25}$$

where $w_i(t)$ models communication disturbances and $u_i(t)$ is the control policy defined as

$$u_i(t) = \sum_{j\in\mathcal{N}_i} k_p\big(p_j(t) - p_i(t) + \Delta_{ij}\big) + k_u\big(\dot{p}_j(t) - \dot{p}_i(t)\big). \tag{26}$$



Directed platoon : $k_1 = 0.5, k_2 = 2$

Defender \ Attacker	1	2	3	4
1	0.3	0.34	0.38	0.5
2	1	0.15	0.38	0.5
3	0.86	0.28	0.16	0.5
4	1	0.3	0.27	0.16

Undirected platoon: $k_1 = 0.5, k_2 = 2$

Defender \ Attacker	1	2	3	4	5
1	0.3	0.49	0.47	0.56	0.65
2	0.52	0.3	0.43	0.47	0.58
3	0.51	0.44	0.3	0.44	0.51
4	0.58	0.47	0.43	0.3	0.52
5	0.65	0.56	0.48	0.49	0.3

Fig. 7. Game matrices for directed and undirected platoons. The game equilibria are shown in dark colors.

Here, $k_p, k_u > 0$ are primary control gains used for the stability of the vehicle platoon formation. If node i is under attack or is chosen as the defender, (25) becomes

$$\ddot{p}_i(t) = \begin{cases} u_i(t) + \zeta_i(t) + w_i(t) & v_i \in \mathfrak{F}, \\ u_i(t) - k_1 p_i(t) - k_2 \dot{p}_i(t) + w_i(t) & v_i \in \mathfrak{D}, \end{cases} \tag{27}$$

where $k_1, k_2 > 0$ are secondary control gains used by the defense node and $\zeta_i(t)$ is the attack signal. Dynamics (27) in matrix form become

$$\dot{\boldsymbol{x}}(t) = \begin{bmatrix} \mathbf{0}_n & I_n \\ -k_p\bar{L}_1 & -k_u\bar{L}_2 \end{bmatrix}\boldsymbol{x}(t) + \begin{bmatrix} \mathbf{0}_{n\times 1} \\ k_p\boldsymbol{\Delta} \end{bmatrix} + \begin{bmatrix} \mathbf{0}_n \\ I_n \end{bmatrix}\boldsymbol{w}(t) + \begin{bmatrix} \mathbf{0}_n \\ [0.3em]B \end{bmatrix}\boldsymbol{\zeta}(t) \tag{28}$$

where $\boldsymbol{x} = [\mathbf{P}\ \ \dot{\mathbf{P}}]^\mathsf{T} = [p_1, p_2, \ldots, p_n, \dot{p}_1, \dot{p}_2, \ldots, \dot{p}_n]^\mathsf{T}$, $\boldsymbol{\Delta} = [\Delta_1, \Delta_2, \ldots, \Delta_n]^\mathsf{T}$ in which $\Delta_i = \sum_{j\in\mathcal{N}_i^{\text{in}}} \Delta_{ij}$ and $\boldsymbol{w}(t)$ is the vector of disturbances. Here $\bar{L}_1 = L + K_1$ and $\bar{L}_2 = L + K_2$ where $K = k_1 D_z$ and $K_2 = k_2 D_z$ in which $D_z = \operatorname{diag}(z)$ determines the location of defense nodes (vehicles). Matrix B determines the location of the attacked nodes. The game payoff is the system $\mathcal{H}_2$ norm of (28) from $\boldsymbol{\zeta}(t)$ to the velocity of vehicles $\dot{\boldsymbol{x}}(t)$.

Remark 5: As mentioned above, k_p and k_u are primary control gains and k_1 and k_2 are secondary control gains used to increase the resilience of the dynamics against attacks. The primary controller uses relative vehicle positions in the feedback whereas the secondary controller uses the pure position and velocity. The relative position between consecutive vehicles is easily measurable using low-cost sonar sensors. However, accurate localization of vehicles in real-time (to calculate their position) demands differential GPS which is costly and infeasible to be used in commercial vehicles. Thus, the measurement (or estimation) of vehicle longitudinal velocity is usually more reliable than its position. With this in mind, it

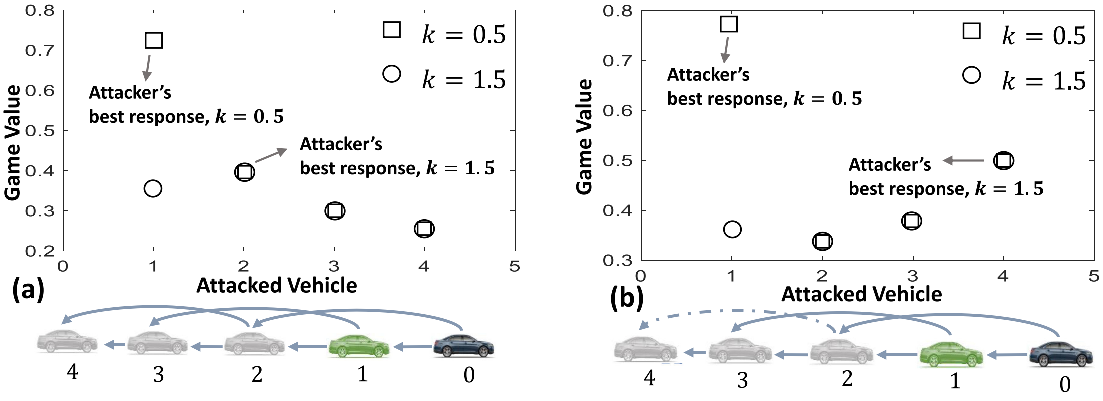


Fig. 8. Platoon topologies and game equilibrium strategies. The defender is shown in green color.

is realistic to assume that the velocity has a larger contribution to the secondary control policy, i.e., $k_2 > k_1$.

We calculate the game values for directed and undirected platoons based on the exact value of the system $\mathcal{H}_2$ norm. We will see that the equilibrium strategies follow those predicted by Proposition 4 which are based on the approximation (22).

The game matrix for a directed and an undirected 2-nearest neighbor platoons with position and velocity feedback gains $k_1 = 0.5$ and $k_2 = 2$ are shown in Fig. 7. Based on these game matrices, for a platoon with a directed topology, there is an NE when both attacker and defender choose vehicle 1 whose in-degree is minimum over all other nodes. This confirms the result of Proposition 4. For the undirected platoon, a solution of the Stackelberg game belongs to the case where vehicle 3, which is the effective center of the platoon, is chosen as the defender and the attacker chooses the farthest vehicles from vehicle 3, either vehicles 1 or 5. This confirm the theoretical result of Theorem 2.

For a 2-nearest neighbor platoon with a directed topology, we examine the threshold for the feedback parameter k mentioned in Proposition 4. For facilitate this comparison, we assume that $k_1 = k_2 = k$. The responses of the attacker are shown in Fig. 8 (a) when the defense vehicle is vehicle 1.

Based on this figure, for a value of k less than the threshold, i.e., $k < \Delta_{n-1} - \Delta_n = 1$, the attacker's best response is the vehicle with the minimum in-degree. For k bigger than the threshold, the attacker's best response is to choose a vehicle with the second smallest in-degree. Fig. 8 (b) belongs to the case where the communication between vehicles 2 and 4 drops. Thus, the in-degree of vehicles 2 and 4 are the same, i.e., Δ_n is not unique. In this case, the attacker's best response, for all positive values of k, is either of vehicles 1 or 4. Here, similar to the game matrices in (7), the game values and consequently equilibrium strategies are based on the exact $\mathcal{H}_2$ norm of (28) and not from the approximation (22).

VI. Conclusion

We discussed the resilience of consensus problems in the presence of adversarial actions, using a game-theoretic framework. It was shown that the optimal solutions of the game on undirected graphs follows a specific network centrality measure, called effective center of the graph. Moreover, for digraphs, the optimal nodes are those with the smallest in-degrees. The theoretical results are validated with simulations on a formation control of vehicle platoons. Further research can be done in the following directions:

- Studying graph-theoretic interpretations for the saddle-point of mixed strategy for the attacker-defender game.
- Analyzing the equilibrium strategies for large scale random networks with various degree distributions.
- Investigating a close form solution of the Lyapunov equation to obtain the observability Gramian for specific classes of digraphs. This helps to find the exact equilibrium strategies without using the approximation.
- Other measures, e.g., entropy and diversity, can be used to quantify the attack impact. Incorporating these measures in the game payoff is an avenue for future research.
- Incorporating the attack visibility, along with the impact, to capture a complete view of the attacker's objectives.

References

[1] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

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

[3] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proc. IEEE Conf. Decis. Control*, 2010, pp. 5991–5998.

[4] S. M. Dibaji, M. Pirani, D. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annu. Rev. Control*, vol. 47, pp. 394–411, Feb. 2015.

[5] 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," *IEEE Control Syst.*, vol. 35, no. 1, pp. 45–65, Feb. 2015.

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

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

[8] Y. Huang, J. Chen, L. Huang, and Q. Zhu, "Dynamic games for secure and resilient control system design," 2019, *arXiv:1910.07510*.

[9] A. Gupta, C. Langbort, and T. Basar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proc. 49th IEEE Conf. Decis. Control*, 2010, pp. 1096–1101.

[10] M. Felegyhazi and J.-P. Hubaux, "Game theory in wireless networks: A tutorial," *EPFL Lab. Comput. Commun. Appl.*, Lausanne, Switzerland, Tech. Rep. LCA-REPORT2006-002, 2006.

[11] M. Dahan and S. Amin, “Network flow routing under strategic link disruptions,” in *Proc. 53rd Annu. Allerton Conf. Commun., Control, Comput.*, 2015, pp. 353–360.

[12] Y. Nugraha, T. Hayakawa, A. Cetinkaya, H. Ishii, and Q. Zhu, “Subgame perfect equilibrium analysis for jamming attacks on resilient graphs,” in *Proc. Amer. Control Conf.*, 2019, pp. 2060–2065.

[13] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, “Sinr-based dos attack on remote state estimation: A game-theoretic approach,” *IEEE Trans. Control Netw. Syst*, vol. 4, pp. 632–642, Sep. 2017.

[14] B. Gharesifard and T. Basar, “Resilience in consensus dynamics via competitive interconnections,” in *Proc. IFAC Volumes*, 2012, vol. 45, no 26, pp. 34–239.

[15] M. Pirani, E. Nekouei, S. M. Dibaji, H. Sandberg, and K. H. Johansson, “Design of attack-resilient consensus dynamics: A game-theoretic approach,” in *Proc. Eur. Control Conf.*, 2019, pp. 2227–2232.

[16] M. Pirani, E. Nekouei, H. Sandberg, and K. H. Johansson, “A game-theoretic framework for security-aware sensor placement problem in networked control systems,” in *Proc. Amer. Control Conf.*, 2019, pp. 114–119.

[17] A. Krause, A. Roper, and D. Golovin, “Randomized sensing in adversarial environments,” in *Proc. 22nd Int. Joint Conf. Artif. Intell.*, 2011, pp. 2133–2139.

[18] F. Pasqualetti, A. Bicchi, and F. Bullo, “Consensus computation in unreliable networks: A system theoretic approach,” *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 90–104, Jan. 2012.

[19] S. Sundaram and C. N. Hadjicostis, “Distributed function calculation via linear iterative strategies in the presence of malicious agents,” *IEEE Trans. Autom. Control*, vol. 56, no. 7, pp. 1495–1508, Jul. 2011.

[20] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, “Resilient asymptotic consensus in robust networks,” *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 766–781, Apr. 2013.

[21] S. M. Dibaji and H. Ishii, “Resilient consensus of second-order agent networks: Asynchronous update rules with delays,” *Automatica*, vol. 81, pp. 123–132, 2017.

[22] N. H. Vaidya, L. Tseng, and G. Liang, “Iterative approximate byzantine consensus in arbitrary directed graphs,” in *Proc. ACM Symp. Principles Distrib. Comput.*, 2012, vol. 4, pp. 365–374.

[23] A. Khanafer, B. Touri, and T. Basar, “Consensus in the presence of anadversary,” in *Proc. 3rd IFAC workshop Distrib. Estimation Control Netw. Syst.*, pp. 275–281, 2012.

[24] B. Bamieh, M. R. Jovanovic, P. Mitra, and S. Patterson, “Coherence in large-scale networks: Dimension-dependent limitations of local feedback,” *IEEE Trans. Autom. Control*, vol. 57, no. 9, pp. 2235–2249, Sep. 2012.

[25] M. Pirani, E. M. Shahrivar, B. Fidan, and S. Sundaram, “Robustness of leader – follower networked dynamical systems,” *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 4, pp. 1752–1763, Dec. 2018.

[26] K. E. Fitch and N. E. Leonard, “Joint centrality distinguishes optimal leaders in noisy networks,” *IEEE Trans. Control Netw. Syst.*, vol. 3, no. 4, pp. 366–378, Dec. 2016.

[27] N. Bof, G. Baggio, and S. Zampieri, “On the role of network centrality in the controllability of complex networks,” *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 3, pp. 643–653, Sep. 2017.

[28] J. Ghaderi and R. Srikant, “Opinion dynamics in social networks with stubborn agents: Equilibrium and convergence rate,” *Automatica*, vol. 50, pp. 3209–3215, 2014.

[29] R. Olfati-Saber, J. A. Fax, and R. M. Murray, “Consensus and cooperation in networked multi-agent systems,” *IEEE Trans. Autom. Control*, vol. 95, no. 1, pp. 215–233, Jan. 2007.

[30] M. Pirani and S. Sundaram, “On the smallest eigenvalue of grounded Laplacian matrices,” *IEEE Trans. Autom. Control*, vol. 61, no. 2, pp. 509–514, Feb. 2016.

[31] M. E. J. Newman, *Netw.: An Introduction*. Oxford University Press, 2010.

[32] A. Ghosh, S. Boyd, and A. Saberi, “Minimizing effective resistance of a graph,” *SIAM Rev.*, vol. 50, no. 1, pp. 37–66, 2008.

[33] W. Yu, G. Chen, and M. Cao, “Some necessary and sufficient conditions for second-order consensus in multi-agent dynamical systems,” *Automatica*, vol. 46, pp. 1089–1095, 2010.

[34] W. Ren, R. Beard, and E. Atkins, “Information consensus in multivehicle cooperative control,” *IEEE Control Syst. Mag.*, vol. 27, no. 2, pp. 71–82, Apr. 2007.

[35] M. Pirani, E. Hashemi, J. W. Simpson-Porco, B. Fidan, and A. Khajepour, “A graph theoretic approach to the robustness of k-nearest neighbor vehicle platoons,” *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 3218–3224, Nov. 2017.

[36] H. Hao and P. Barooah, “Stability and robustness of large platoons of vehicles with double-integrator models and nearest neighbor interaction,” *Int. J. Robust Nonlinear Control*, vol. 23, no. 18, pp. 2097–2122, 2013.

Mohammad Pirani received the B.Sc. degree in mechanical engineering from the Amirkabir University of Technology in 2011, the M.A.Sc. degree in electrical and computer engineering, and the Ph.D. degree in mechanical and mechatronics engineering, both from the University of Waterloo in 2014 and 2017, respectively. He is a Postdoctoral Researcher with the Department of Electrical and Computer Engineering, the University of Toronto. From 2018 to 2019, he was a Postdoctoral Researcher with the Department of Automatic Control, KTH Royal Institute of Technology, Sweden. His research interests include resilient and fault-tolerant control, networked control systems, and multi-agent systems.

Ehsan Nekouei received the B.S. degree from the Shahid Bahonar University of Kerman, Kerman, Iran, the M.S. degree from Tarbiat Modares University, Tehran, Iran, and the Ph.D. degree in electrical engineering from the University of Melbourne, Melbourne, VIC, Australia, in 2003, 2006, and 2013, respectively. He is an Assistant Professor with the Department of Electrical Engineering, the City University of Hong Kong. He was a Postdoctoral Researcher with the Department of Automatic Control, KTH Royal Institute of Technology, Sweden. Before that, he was a Research Fellow with the Department of Electrical and Electronic Engineering, University of Melbourne. His research interests include communications and information theories, mechanism design theory, and smart grid.

Henrik Sandberg received the M.Sc. degree in engineering physics and the Ph.D. degree in automatic control from Lund University, Lund, Sweden, in 1999 and 2004, respectively. He is Professor with the Department of Automatic Control, KTH Royal Institute of Technology, Stockholm, Sweden. From 2005 to 2007, he was a Postdoctoral Scholar with the California Institute of Technology, Pasadena, USA. In 2013, he was a Visiting Scholar with the Laboratory for Information and Decision Systems (LIDS), MIT, Cambridge, USA. He has also held visiting appointments with the Australian National University and the University of Melbourne, Australia. His current research interests include security of cyber-physical systems, power systems, model reduction, and fundamental limitations in control. He was a recipient of the Best Student Paper Award from the IEEE Conference on Decision and Control in 2004, an Ingvar Carlsson Award from the Swedish Foundation for Strategic Research in 2007, and Consolidator Grant from the Swedish Research Council in 2016. He was the Editorial Board for IEEE TRANSACTIONS ON AUTOMATIC CONTROL and is currently Associate Editor of the IFAC *Journal Automatica. information theories, mechanism design theory, and smart grid*.

Karl Henrik Johansson (Fellow, IEEE) received the M.Sc. and Ph.D. degrees from Lund University. He has held Visiting Positions with UC Berkeley, Caltech, NTU, HKUST Institute of Advanced Studies, and NTNU. He is Director of the Stockholm Strategic Research Area ICT The Next Generation and Professor with the School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology. His research interests are in networked control systems, cyber-physical systems, and applications in transportation, energy, and automation. He is a member of the IEEE Control Systems Society Board of Governors, the IFAC Executive Board, and the European Control Association Council. He has received several best paper awards and other distinctions. He has been awarded Distinguished Professor with the Swedish Research Council and Wallenberg Scholar. He has received the Future Research Leader Award from the Swedish Foundation for Strategic Research and the triennial Young Author Prize from IFAC. He is Fellow the Royal Swedish Academy of Engineering Sciences, and he is IEEE Distinguished Lecturer.