Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

Dynamic Resilient Graph Games for State-Dependent Jamming Attacks Analysis on Multi-Agent Systems

Yurid Nugraha * **Ahmet Cetinkaya** ** **Tomohisa Hayakawa** *
Hideaki Ishii *** **Quanyan Zhu** ****

* *Dept. of Systems and Control Engineering, Tokyo Institute of Technology, Tokyo 152-8552, Japan. (yurid@dsl.sc.e.titech.ac.jp, hayakawa@sc.e.titech.ac.jp)*
** *Information Systems Architecture Science Research Division, National Institute of Informatics, Tokyo 101-8430, Japan. (cetinkaya@nii.ac.jp)*
*** *Dept. of Computer Science, Tokyo Insitute of Technology, Yokohama 226-8502, Japan. (ishii@c.titech.ac.jp)*
**** *Dept. of Electrical and Computer Engineering, New York University, Brooklyn, NY 11201, USA. (quanyan.zhu@nyu.edu)*

Abstract: A cybersecurity problem for a multi-agent consensus problem is investigated through a dynamic game formulation. Specifically, we consider a game repeatedly played between a jamming attacker and a defender. The attacker attempts to jam the links between a number of agents to delay their consensus. On the other hand, the defender tries to maintain the connection between agents by attempting to recover some of the jammed links with the goal of achieving faster consensus. In each game, the players decide which links to attack/recover and for how long to continue doing so based on a Lyapunov-like function representing the largest difference between the states of the agents. We analyze the subgame perfect equilibrium of the game and obtain an upper bound of the consensus time that is influenced by the strategies of the players. The results are illustrated with a numerical example.

Keywords: Multi-agent systems, Consensus problem, Game theory, Cybersecurity

1. INTRODUCTION

Jamming attacks are one of the most common security threats in networked multi-agent systems, where the adversary from outside the system transmits interference signals that disrupt the communication process among the agents in a network. These attacks are potentially more dangerous if the adversary is intelligent and aware of the system parameters and the agent states, since the adversary can then decide how and when to attack in order to maximize the damage.

In response to the jamming attacks, a defense mechanism can be incorporated to coordinate the recovery process of the network. Similar to the attacks, the recovery process may be more efficient if the defense mechanism is aware of system parameters and states.

In this paper, we investigate the effects of state-dependent attack and defense strategies in a networked multi-agent system. In particular, we formulate a two-player game which will be repeatedly played by an attacker and a defender in the context of a consensus problem. The agents attempt to reach consensus over edges which may be attacked but then possibly recovered. The attacker is motivated to delay consensus by attacking links connecting agents, whereas the defender, in response to the attacks, attempts to recover some of the attacked links to maintain communication among agents and therefore reduces the consensus delay. The players spend energy by attacking and recovering, and therefore the attack and recovery durations are limited.

We provide an optimal network design in the face of cyber-attacks as in Chen et al. (2020a,b); Nugraha et al. (2019); Kordonis and Papavassilopoulos (2017). To characterize the game, we follow our recent work (Nugraha et al., 2019), which considers links connecting agents and attack or recovery intervals as decision variables. The strategies of the players are constrained by their available energies. For this, we follow the model studied in Feng and Tesi (2017); Cetinkaya et al. (2017, 2020). Differently from the abovementioned works, here we focus on the state dependent attack/recovery strategies. To identify the tight relation of such strategies with the consensus problem, we utilize a Lyapunov-like function of the agent states in characterizing the utilities in the game.

Consensus problems of multi-agent systems with self-triggered communication protocol in the presence of jamming attacks are discussed in Senejohnny et al. (2018).

⋆ This work was supported in the part by the JST CREST (Grant No. JPMJCR15K3) and by JST ERATO HASUO Metamathematics for Systems Design Project (Grant No. JPMJER1603).

Moreover, game-theoretic approaches have also been utilized for the analysis of false data injection attacks (see, e.g., Pirani et al. (2019) and the references therein). In the related studies on resilient consensus, some agents may be attacked by an adversary, making them update their state values in a faulty and even malicious manner. Distributed algorithms to mitigate such effects on the consensus process have been proposed in, e.g., Wang and Ishii (2020).

The main contribution of this work is to formulate a game problem in a multi-agent consensus setting, where the players' strategies depend on the state values of the agents and on how close to consensus they may be. This aspect is novel in comparison to the conventional security works for networked systems including our own (Nugraha et al., 2019). We find explicit conditions characterizing the players' optimal strategies and then investigate the implication of the conditions by studying simple cases, leading us to some conditions on the players' utilities that determine the players' strategies.

2. PROBLEM FORMULATION AND UTILITY FUNCTION DESIGN

We explore a cybersecurity problem for a multi-agent system of n agents. The network topology in this system is described by an *undirected* graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ that consists of the set $\mathcal{V}$ of vertices with $|\mathcal{V}| = n$ and the set $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ of edges. The agents are described by the vertices, while the communication links between the agents correspond to the edges. We use $\mathcal{N}_i(t)$ to denote the set of agents that are able to communicate with agent i at time t. Note that the set $\mathcal{N}_i(t)$ may be different at different times due to jamming attacks. We assume that agent i has the scalar state x_i whose dynamics are defined as

$$\dot{x}_i(t) = \sum_{j \in \mathcal{N}_i(t)} (x_j(t) - x_i(t)), \quad x(0) = x_0, \quad t \geq 0. \quad (1)$$

Under the dynamics (1), all agents are expected to converge towards the same state as time progresses. We assume that the underlying, attack-free communication topology $\mathcal{G}$ is connected.

A game between two players, the attacker and the defender, is considered in terms of the communication among the agents. The attacker is an entity capable to block the communication by jamming some targeted links and therefore delay the consensus process, whereas the defender tries to recover some or all of the attacked links. The actions of both players are subject to constraints due to limited energy resources for attack/recovery.

The attacker attacks the networked system by sending jamming signals. We define the attack action by the attacker as the removal of edges in graph $\mathcal{G}$. In response to the attacks, the defender demands the agents to send stronger communication signals to overcome jamming signals in some of the attacked communication links, which is represented by rebuilding some of the removed edges. We define this as the recovery action. From this sequence of attacks and recoveries in a single game, we observe that the graphs are *resilient*, i.e., the group of agents are able to recover from the damages caused by the attacker.

In this paper we consider games played repeatedly between the players. The kth game is played in the time interval $[\underline{t}_k, \bar{t}_k]$, with $k \in \mathbb{N}$ and $\bar{t}_k > \underline{t}_k = \bar{t}_{k-1}$. At time $\underline{t}_k$, the communication topology of the system is represented by the original graph $\mathcal{G}$. Then, the players may start attacking and recovering certain links in two stages, with the attacker acting first before the defender. The attack/recovery durations and the links for the attack/recovery actions are the action variables to be decided by the players. We assume that the players can make their actions at most once in $[\underline{t}_k, \bar{t}_k]$. Once the attacker stops the attacks (and therefore also ending all recovery attempts), the kth game ends at $\bar{t}_k$. If there is no attack, the kth game ends after a fixed time duration. The players play the next $(k+1)$th game immediately after the kth game ends, that is, $\underline{t}_{k+1} = \bar{t}_k$.

The attacker attacks $\mathcal{G}$ by deleting $\mathcal{E}_k^{\mathrm{A}} \subseteq \mathcal{E}$ from time $\underline{\tau}_k^{\mathrm{A}}$ until $\overline{\tau}_k^{\mathrm{A}}$ for $\delta_k^{\mathrm{A}} := \overline{\tau}_k^{\mathrm{A}} - \underline{\tau}_k^{\mathrm{A}}$ duration, whereas the defender recovers $\mathcal{E}_k^{\mathrm{D}} \subseteq \mathcal{E}_k^{\mathrm{A}}$ from time $\underline{\tau}_k^{\mathrm{D}}$ until $\overline{\tau}_k^{\mathrm{D}}$ for $\delta_k^{\mathrm{D}} := \overline{\tau}_k^{\mathrm{D}} - \underline{\tau}_k^{\mathrm{D}}$ duration, with $\underline{t}_k < \underline{\tau}_k^{\mathrm{A}} \leq \underline{\tau}_k^{\mathrm{D}} \leq \overline{\tau}_k^{\mathrm{D}} \leq \overline{\tau}_k^{\mathrm{A}} \leq \bar{t}_k$. Because of the presence of the attacks, $\mathcal{G}$ is changed to $\mathcal{G}_k^{\mathrm{A}} := (\mathcal{V}, \mathcal{E} \setminus \mathcal{E}_k^{\mathrm{A}})$ at $\underline{\tau}_k^{\mathrm{A}}$, and $\mathcal{G}_k^{\mathrm{A}}$ is further changed to $\mathcal{G}_k^{\mathrm{D}} := (\mathcal{V}, (\mathcal{E} \setminus \mathcal{E}_k^{\mathrm{A}}) \cup \mathcal{E}_k^{\mathrm{D}})$ at $\underline{\tau}_k^{\mathrm{D}}$ until $\overline{\tau}_k^{\mathrm{D}}$ because of the recovery action by the defender. The graph becomes $\mathcal{G}$ again when the attacker stops jamming, and immediately a new $(k+1)$th game begins. For attacking/recovering links, both players spend some energy in proportion to the attack/recovery duration. Fig. 1 illustrates the sequences of the attack and recovery actions in a single game.

In the kth game, both players attempt to choose the best strategy to maximize their own utility functions that are defined over the time interval $[\underline{t}_k, \bar{t}_k]$, as discussed later. The attacker's and the defender's strategies are determined in terms of $(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}})$ and $(\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}})$, respectively.

It is assumed that there is a constant waiting time $\gamma^{\mathrm{A}} > 0$ (resp., $\gamma^{\mathrm{D}} > 0$) between the start of the interval $\underline{t}_k$ and the start of attack time $\underline{\tau}_k^{\mathrm{A}}$ (resp., between $\underline{\tau}_k^{\mathrm{A}}$ and $\underline{\tau}_k^{\mathrm{D}}$ unless the attacker ends attacking earlier), given by

$$\underline{\tau}_k^{\mathrm{A}} := \underline{t}_k + \gamma^{\mathrm{A}}, \quad \underline{\tau}_k^{\mathrm{D}} := \min\{\overline{\tau}_k^{\mathrm{A}}, \underline{\tau}_k^{\mathrm{A}} + \gamma^{\mathrm{D}}\}.$$

We also assume that the end time $\bar{t}_k$ of the kth game is given by

$$\bar{t}_k := \begin{cases} \overline{\tau}_k^{\mathrm{A}}, & \text{if } \mathcal{E}_k^{\mathrm{A}} \neq \emptyset, \\ \underline{t}_k + \gamma^{\mathrm{A}} + \gamma^{\mathrm{D}}, & \text{otherwise.} \end{cases} \quad (2)$$

The players cannot keep sending signals for very long durations due to energy constraints. We follow the approach in Cetinkaya et al. (2020) to model such energy constraints. The total energy used for player $p \in \{\mathrm{A}, \mathrm{D}\}$ must satisfy

$$\sum_{m=1}^{k-1} \beta^p |\mathcal{E}_m^p| \delta_m^p + \beta^p |\mathcal{E}_k^p| (t - \underline{\tau}_k^p) \leq \kappa^p + \rho^p t, \quad (3)$$

for any time $t \in [\underline{\tau}_k^p, \underline{\tau}_{k+1}^p]$, with $\kappa^p > 0$, $\beta^p > \rho^p > 0$, and $k \in \mathbb{N}$. Note that κ^p and ρ^p denote the initial energy at $t = 0$ and the recharge rate of energy for player p, respectively. Also, β^p denotes player p's cost to attack/recover one edge per one time unit. The inequality (3) implies that total energy spent by a player cannot exceed the available energy characterized by the initial energy κ^p and the supplied energy $\rho^p t$ by time t.

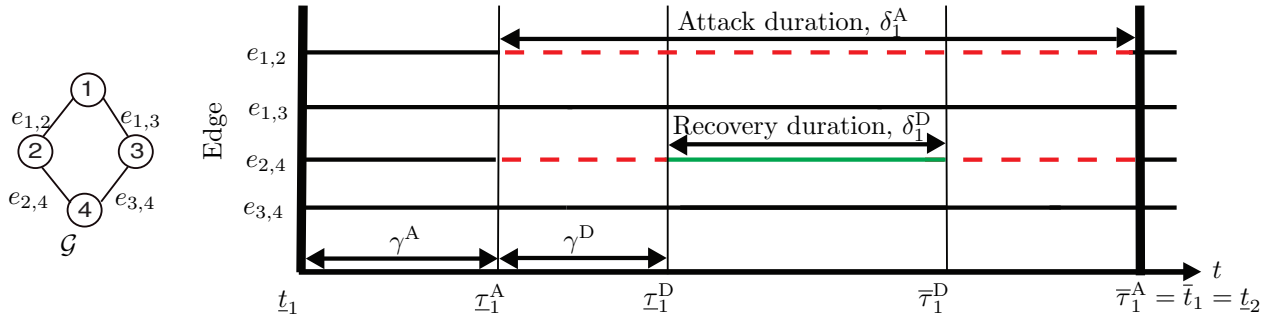

Fig. 1. Illustration of graph transitions for the first game, with the underlying graph $\mathcal{G}$ shown in the left side. At time interval $[\underline{t}_1, \overline{t}_1]$, the attacker attacks two edges $e_{1,2}$ and $e_{2,4}$, but the defender recovers one of them. Note that the solid lines in the right figure indicate that the edges are connected, i.e., the agents are able to communicate through these edges, and the dashed lines indicate that the edges are disconnected.

Under this problem formulation, if the player attacks or recovers $\mathcal{E}_k^p$, then from (3), we obtain an explicit expression for the maximum interval Δ_k^p on the time duration δ_k^p when player p completes the attack/recovery actions as

$$\Delta_k^p := \frac{\kappa^p + \rho^p \underline{\tau}_k^p - \sum_{m=1}^{k-1} \beta^p |\mathcal{E}_m^p| \delta_m^p}{\beta^p |\mathcal{E}_k^p| - \rho^p}.$$

For simplicity, we assume that there are finite numbers of possible attack and recovery durations, since the optimal durations can be found easier from finite numbers of choices. In particular, the choices of durations δ_k^{A} and δ_k^{D} are determined by parameters $\alpha^{\mathrm{A}}, \alpha^{\mathrm{D}} \in \mathbb{N}$ as

$$\delta_k^{\mathrm{A}} \in \left\{0, \frac{\Delta_k^{\mathrm{A}}}{\alpha^{\mathrm{A}}}, \frac{2\Delta_k^{\mathrm{A}}}{\alpha^{\mathrm{A}}}, \ldots, \frac{(\alpha^{\mathrm{A}}-1)\Delta_k^{\mathrm{A}}}{\alpha^{\mathrm{A}}}, \Delta_k^{\mathrm{A}}\right\},$$

$$\delta_k^{\mathrm{D}} \in \left\{0, \min\left\{\delta_k^{\mathrm{A}} - (\underline{\tau}_k^{\mathrm{D}} - \underline{\tau}_k^{\mathrm{A}}), \frac{\Delta_k^{\mathrm{D}}}{\alpha^{\mathrm{D}}}\right\}, \ldots, \min\left\{\delta_k^{\mathrm{A}} - (\underline{\tau}_k^{\mathrm{D}} - \underline{\tau}_k^{\mathrm{A}}), \Delta_k^{\mathrm{D}}\right\}\right\}.$$

Note that the choices of recovery durations of the defender are also limited by the attack durations of the attacker, since the recovering action immediately ends when the attack ends. In this paper, we assume that all parameters associated with the system are known by both players.

In this game, both players maximize their own utilities which are affected by the states of the agents. The agent states are in turn influenced by the actions taken by the players in the form of attacked/recovered edges $\mathcal{E}_k^p$ and attack/recovery durations δ_k^p.

We first define the max-min nonnegative-definite function $V(x)$ representing the difference among the agent state values as

$$V(x) := \max_{i \in \mathcal{V}} x_i - \min_{i \in \mathcal{V}} x_i. \tag{4}$$

Then we define $z_k((\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}), (\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}}))$ as

$$z_k((\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}), (\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}})) := V(x(\overline{t}_k))\delta_k^{\mathrm{A}}, \tag{5}$$

for the kth game. The function z_k represents the reward for the attacker, which is larger if the attacks are longer and are able to keep $V(\cdot)$ from decreasing too fast over the attack duration δ_k^{A}, since $V(\cdot)$ is multiplied by δ_k^{A}.

We define the utility function of the players for the kth game of time interval $[\underline{t}_k, \overline{t}_k]$ as

$$U_k^{\mathrm{A}}((\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}), (\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}})) := z_k - \beta^{\mathrm{A}} |\mathcal{E}_k^{\mathrm{A}}| \delta_k^{\mathrm{A}}, \tag{6}$$

$$U_k^{\mathrm{D}}((\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}), (\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}})) := -z_k - \beta^{\mathrm{D}} |\mathcal{E}_k^{\mathrm{D}}| \delta_k^{\mathrm{D}}. \tag{7}$$

Note that the utility function (6) represents the reward of the attacker and the cost for jamming $\mathcal{E}_k^{\mathrm{A}}$. Similarly, (7) represents the attacker's reward (with the negative sign) and the cost for recovering $\mathcal{E}_k^{\mathrm{D}}$. For simplicity, we formulate that β^{A} (resp., β^{D}) is uniform for every attacked edge (resp., recovered edge), regardless of the position of the edge in the topology.

We formulate the game as a two-stage game where the attacker first attacks and then the defender makes recoveries. This will be played repeatedly over k. It should be noted that each game is played independently at time $\underline{t}_k$. The strategies of the players will depend on the consensus level that the agents have reached and also their energy level at that point. It is however noted that there is another stage, which will be implicit in our formulation; this stage is related to the design of the network structure of the underlying graph $\mathcal{G}$. The graph is assumed to be given here, but clearly affects the game as it is the default network at the start of each game. Our formulation will thus be useful in finding resilient networks under hostile environments.

Here, we seek the equilibrium of this game, which will be a *subgame perfect equilibrium* as in the works by Chen et al. (2020a,b); Nugraha et al. (2019). The defender's game is formulated in the subgame of the attacker's game, since the defender decides its action after the attacker. To obtain the optimal strategies, a *backward induction* approach is used for each kth game.

The optimal edges and durations are specified as follows. For the kth game in $[\underline{t}_k, \overline{t}_k]$, given the attacker's strategy $(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}})$, the optimal strategy for the defender is given by

$$(\mathcal{E}_k^{\mathrm{D}*}(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}), \delta_k^{\mathrm{D}*}(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}})) \in \arg\max_{(\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}})} U_k^{\mathrm{D}}((\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}), (\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}})),$$

with $\mathcal{E}_k^{\mathrm{D}}$ and δ_k^{D} depending on $\mathcal{E}_k^{\mathrm{A}}$ and δ_k^{A}. Likewise, given $\mathcal{E}$, the attacker decides the strategy as

$$(\mathcal{E}_k^{\mathrm{A}*}, \delta_k^{\mathrm{A}*}) \in \arg\max_{(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}})} U_k^{\mathrm{A}}((\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}), (\mathcal{E}_k^{\mathrm{D}*}(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}), \delta_k^{\mathrm{D}*}(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}))).$$

In this research, we analyze the strategy profile of the players in terms of the pairs $(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}})$ and $(\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}})$. Therefore, we seek pairs $(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}})$ and $(\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}})$ such that $(\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}})$ is the best response to $(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}})$. We call the strategy profile $((\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}), (\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}}))$ that follow the subgame perfect equilibrium principle as the *optimal combined strategy*.

3. GAME AND CONSENSUS ANALYSIS

3.1 Optimal Strategies

To derive optimal strategies of the players, we consider three cases based on the presence of attack and recovery. We analyze the game case-by-case.

Case 1 (No Attack, therefore no recovery): Since both players do not attack/recover, their utilities in (6) and (7) become

$$U_k^{\mathrm{A}}((\emptyset,0),(\emptyset,0)) = 0, \quad U_k^{\mathrm{D}}((\emptyset,0),(\emptyset,0)) = 0.$$

We classify these strategies for the players as Combined Strategy 1:={Strategy A1, Strategy D1}.

Case 2 (Attack without Recovery): In this case, the attacker attacks while the defender chooses not to recover. From (6), since z_k depends only on the maximum and minimum states of agents, an option for the attacker is to isolate them from the rest of the network. This should be done by removing as few edges as possible. Such agents can be found by $\bar{i}_k \in \arg\min_i\{d(i) : x_i(\underline{\tau}_k^{\mathrm{A}}) = \max_j x_j(\underline{\tau}_k^{\mathrm{A}}),\ i,j \in \mathcal{V}\}$ and $\underline{i}_k \in \arg\min_i\{d(i) : x_i(\underline{\tau}_k^{\mathrm{A}}) = \min_j x_j(\underline{\tau}_k^{\mathrm{A}}),\ i,j \in \mathcal{V}\}$, with $d(i)$ being the degree of agent i. By isolating agents $\bar{i}_k$ and $\underline{i}_k$, the attacker obtains maximum $V(x(\bar{t}_k))$. We divide the discussion of the attacker's strategy into two parts based on whether the attacker isolates state-wise farthest agents $\bar{i}_k$ and $\underline{i}_k$ or not.

(i) Combined Strategy 2a (The farthest agents are isolated): If the attacker isolates agents $\bar{i}_k$ and $\underline{i}_k$, then $V(x)$ does not change, and therefore the optimal duration for the attacker is $\delta_k^{\mathrm{A}} = \Delta_k^{\mathrm{A}}$. Hence, (6) becomes $U_k^{\mathrm{A}}((\mathcal{E}_k^{\mathrm{A}}, \Delta_k^{\mathrm{A}}),(\emptyset,0)) = (x_{\bar{i}_k}(\underline{\tau}_k^{\mathrm{A}}) - x_{\underline{i}_k}(\underline{\tau}_k^{\mathrm{A}}) - \beta^{\mathrm{A}}|\mathcal{E}_k^{\mathrm{A}}|)\Delta_k^{\mathrm{A}} =: \hat{U}_k^{\mathrm{A2a}}(\mathcal{E}_k^{\mathrm{A}})$.

The edges needed to isolate agents $\bar{i}_k$ and $\underline{i}_k$ are given by

$$\mathcal{E}_k^{\mathrm{iso}} = \{e_{\bar{i}_k,j}, \forall j \in \mathcal{N}_{\bar{i}_k}\} \cup \{e_{\underline{i}_k,j}, \forall j \in \mathcal{N}_{\underline{i}_k}\},$$

and the number of edges $|\mathcal{E}_k^{\mathrm{iso}}|$ can also be expressed as

$$|\mathcal{E}_k^{\mathrm{iso}}| = \sum_{j=1}^{n} A(\mathcal{G})_{\bar{i}_k,j} + \sum_{j=1}^{n} A(\mathcal{G})_{\underline{i}_k,j} - A(\mathcal{G})_{\bar{i}_k,\underline{i}_k},$$

with $A(\mathcal{G})$ denoting the adjacency matrix of $\mathcal{G}$.

Then, we obtain the optimal edges as $\mathcal{E}_k^{\mathrm{A2a}*} = \mathcal{E}_k^{\mathrm{iso}}$. With this strategy, the utility of the defender becomes

$$\begin{aligned} &U_k^{\mathrm{D}}((\mathcal{E}_k^{\mathrm{A2a}*}, \Delta_k^{\mathrm{A}}),(\emptyset,0)) \\ &\quad = (x_{\bar{i}_k}(\underline{\tau}_k^{\mathrm{A}}) - x_{\underline{i}_k}(\underline{\tau}_k^{\mathrm{A}}))\Delta_k^{\mathrm{A}} =: \hat{U}_k^{\mathrm{D2a}}, \end{aligned} \tag{8}$$

The combination of the optimal strategies in the case where the farthest agents are isolated is classified as Combined Strategy 2a:={Strategy A2a, Strategy D1}.

As a remark, attacking $\mathcal{E}_k^{\mathrm{A}}$ such that $|\mathcal{E}_k^{\mathrm{A}}| \geq |\mathcal{E}_k^{\mathrm{A2a}*}|$ is not optimal for the attacker, because the attacker suffers from higher cost while getting no additional payoff from $V(\bar{t}_k)$.

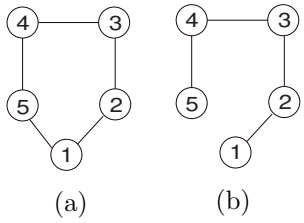

Fig. 2. Two different graph topologies resulting in different optimal strategies for the attacker. The parameters used are $x(0) = [1\ 0\ 0\ 0\ -1]$, $\rho^{\mathrm{A}} = 0.01$, $\beta^{\mathrm{A}} = 0.2$, $\kappa^{\mathrm{A}} = 3$, $\alpha^{\mathrm{A}} = 1$. Assume that there is no recovery.

(ii) Combined Strategy 2b (The farthest agents are not isolated): The attacker may obtain better payoff by attacking fewer edges, depending on the agents' states and graph topology. Here, the attacker simply attacks $\mathcal{E}_k^{\mathrm{A}}$ with $|\mathcal{E}_k^{\mathrm{A}}| < |\mathcal{E}_k^{\mathrm{iso}}|$, implying that agents $\bar{i}_k$ and $\underline{i}_k$ are not isolated. In this strategy, we cannot easily determine the optimal attack duration. Hence, the optimal edges and durations of the attacker are given by

$$\begin{aligned} &(\mathcal{E}_k^{\mathrm{A2b}*}, \delta_k^{\mathrm{A2b}*}) \in \arg\max_{\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}} \hat{U}_k^{\mathrm{A2}}(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}), \\ &\text{s.t.} \quad 0 < |\mathcal{E}_k^{\mathrm{A}}| < |\mathcal{E}_k^{\mathrm{iso}}|, \end{aligned}$$

with $\hat{U}_k^{\mathrm{A2}}(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}) := U_k^{\mathrm{A}}((\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}),(\emptyset,0))$. However, note that this strategy is not available for $n = 2$, since $\mathcal{E} = \mathcal{E}_k^{\mathrm{iso}}$. In that case, only Combined Strategy 2a is considered in formulating the optimal strategy in Case 2. The combination of the optimal strategies in the case where the farthest agents are not isolated is classified as Combined Strategy 2b:={Strategy A2b, Strategy D1}, with the utility of the defender $\hat{U}_k^{\mathrm{D2b}} := U_k^{\mathrm{D}}((\mathcal{E}_k^{\mathrm{A2b}*}, \delta_k^{\mathrm{A2b}*}),(\emptyset,0))$.

In Fig. 2, we provide an example showing the Strategy 2a and 2b on different graph topologies. In topology (a), the attacker isolates agents 1 and 5 by attacking 3 edges $e_{1,2}$, $e_{1,5}$, and $e_{4,5}$ in the first game ($k = 1$), whereas in the topology (b), the attacker only attacks the edge connecting agent 1, i.e., $e_{1,2}$, in $k = 1$. In (b), the attacker obtains relatively high payoff by attacking only $e_{1,2}$, because δ_k^{A} becomes longer (attacking fewer edges) and $V(x(t))$, $t \geq 0$ is relatively high since agent $\bar{i}_k$ is isolated. However, since the attacker needs to attack two edges to isolate only $\bar{i}_k$ in (a), it is better for the attacker to isolate both agents $\bar{i}_k$ and $\underline{i}_k$ with only attacking one more edge.

Case 3 (Attack and Recovery): Unlike in the previous case, in this case attacking more edges such that $|\mathcal{E}_k^{\mathrm{A}}| > |\mathcal{E}_k^{\mathrm{iso}}|$ may be optimal for the attacker, since it forces the defender to recover for a shorter duration. Thus, the players simply calculate the utilities among all possibilities of nonzero $\mathcal{E}_k^{\mathrm{A}}$, δ_k^{A}, $\mathcal{E}_k^{\mathrm{D}}$, and δ_k^{D}.

The optimal edges and durations are given by

$$\begin{aligned} &(\mathcal{E}_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A}} \neq \emptyset, \delta_k^{\mathrm{A}} > 0), \delta_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A}} \neq \emptyset, \delta_k^{\mathrm{A}} > 0)) \\ &\qquad \in \arg\max_{\mathcal{E}_k^{\mathrm{D}} \neq \emptyset, \delta_k^{\mathrm{D}} > 0} U_k^{\mathrm{D}}((\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}),(\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}})), \end{aligned}$$

and

$$(\mathcal{E}_k^{\mathrm{A3}*}, \delta_k^{\mathrm{A3}*}) \in \arg\max_{\mathcal{E}_k^{\mathrm{A}} \neq \emptyset, \delta_k^{\mathrm{A}} > 0} U_k^{\mathrm{A}}((\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}),(\mathcal{E}_k^{\mathrm{D3}*}, \delta_k^{\mathrm{D3}*})).$$

The combination of the optimal strategies in Case 3 is called Combined Strategy 3:={Strategy A3, Strategy D3}.

In this case, the utility of the attacker is denoted by $\hat{U}_k^{\mathrm{A3}*} := U_k^{\mathrm{A}}((\mathcal{E}_k^{\mathrm{A3}*}, \delta_k^{\mathrm{A3}*}), (\mathcal{E}_k^{\mathrm{D3}*}, \delta_k^{\mathrm{D3}*}))$.

From (8), the defender recovers for $\mathcal{E}_k^{\mathrm{A}} \neq \emptyset$ if

$$\beta^{\mathrm{D}} < \frac{z_k((\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}), (\emptyset, 0)) - z_k((\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}), (\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}}))}{|\mathcal{E}_k^{\mathrm{D}}|\delta_k^{\mathrm{D}}}, \quad (9)$$

which means that the defender recovers if the cost of recovering one edge is less than the decaying speed of $V(x(t))$ per recovered edge. Since z_k varies for different attacked edges, the defender's decision whether to recover or not may be different for different attacked edges. Note that though the defender recovers, the attacker is still able to obtain relatively high utility since the defender may end recovering earlier or the attacker can attack for a short time to minimize the recovery duration.

From the three cases discussed above, we are now ready to state the main result of this paper. We apply the backward induction method to the simplified utility functions in the form of $\hat{U}_k^{\mathrm{A2a}*} := \hat{U}_k^{\mathrm{A2}}(\mathcal{E}_k^{\mathrm{A2a}*})$, $\hat{U}_k^{\mathrm{A2b}*} := \hat{U}_k^{\mathrm{A2}}(\mathcal{E}_k^{\mathrm{A2b}*}, \delta_k^{\mathrm{A2b}*})$, and $\hat{U}_k^{\mathrm{A3}*}$ for the attacker, and $\hat{U}_k^{\mathrm{D3}*} := U_k^{\mathrm{D}}(\ (\mathcal{E}_k^{\mathrm{A3}*}, \delta_k^{\mathrm{A3}*}),\ (\mathcal{E}_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A3}*},\ \delta_k^{\mathrm{A3}*}), \delta_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A3}*}, \delta_k^{\mathrm{A3}*}))\ )$, $\hat{U}_k^{\text{D3-2a}} := U_k^{\mathrm{D}}(\ (\mathcal{E}_k^{\mathrm{A2a}*}, \Delta_k^{\mathrm{A}}), (\mathcal{E}_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A2a}*}, \Delta_k^{\mathrm{A}}), \delta_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A2a}*}, \Delta_k^{\mathrm{A}}))\ )$, $\hat{U}_k^{\text{D3-2b}} := U_k^{\mathrm{D}}\ (\ (\mathcal{E}_k^{\mathrm{A2b}*}, \delta_k^{\mathrm{A2b}*}), (\mathcal{E}_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A2b}*}, \delta_k^{\mathrm{A2b}*}), \delta_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A2b}*}, \delta_k^{\mathrm{A2b}*}))\ )$ for the defender.

Since the defender's strategy depends on the attacked edges, we also use $\hat{U}_k^{\text{A3-0}} := \max_{\mathcal{E}_k^{\mathrm{A}} \in E_k, \delta_k^{\mathrm{A}}} \hat{U}_k^{\mathrm{A2}}(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}})$ and $(\underline{\mathcal{E}}_k^{\mathrm{A}*}, \underline{\delta}_k^{\mathrm{A}*}) \in \arg\max_{\mathcal{E}_k^{\mathrm{A}} \in E_k, \delta_k^{\mathrm{A}}} \hat{U}_k^{\mathrm{A2}}(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}})$, where E_k is the set of edge sets $\underline{\mathcal{E}}_k^{\mathrm{A}}$ such that for the pair $\{\underline{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D3}*}(\underline{\mathcal{E}}_k^{\mathrm{A}})\}$, inequality (9) is not satisfied.

Theorem 1. With the utility functions (6), (7) and $n > 2$, the optimal combined strategy of the players is given by

(1) Combined Strategy 1 if $\max\{\hat{U}_k^{\mathrm{A2a}*}, \hat{U}_k^{\mathrm{A2b}*}\} \leq 0$,
(2) Combined Strategy 2a if $\hat{U}_k^{\mathrm{A2a}*} > 0$, $\hat{U}_k^{\mathrm{A2a}*} \geq \hat{U}_k^{\mathrm{A2b}*}$, and $\hat{U}_k^{\text{D3-2a}} \leq \hat{U}_k^{\mathrm{D2a}}$,
(3) Combined Strategy 2b if $\hat{U}_k^{\mathrm{A2b}*} > 0$, $\hat{U}_k^{\mathrm{A2b}*} > \hat{U}_k^{\mathrm{A2a}*}$, and $\hat{U}_k^{\text{D3-2b}} \leq \hat{U}_k^{\mathrm{D2b}}$,
(4) Combined Strategy 3 if $\hat{U}_k^{\mathrm{A3}*} > 0$ and $\hat{U}_k^{\mathrm{A3}*} > \hat{U}_k^{\text{A3-0}}$.

Theorem 1 presents a characterization of the optimal strategies of the players under different conditions. This characterization is general and applies to all graph topologies. To provide more explicit relation between optimal strategies and attack/recovery parameters, we present a result for a specific case which allows us to determine the equilibrium based on the cost, agent states (represented by $V(\cdot)$), and action durations.

To this end, we consider a graph with $n = 2$ and $|\mathcal{E}| = 1$ with $\alpha^{\mathrm{A}} = \alpha^{\mathrm{D}} = 1$. In this setup, both players can only attack/recover one edge. First, note that the dynamics in (1) can also be stated as $x(t) = e^{-t(L(\mathcal{G}'))}x(0)$, with $\mathcal{G}'$ being the graph representing communication topology (either $\mathcal{G}$, $\mathcal{G}_k^{\mathrm{A}}$, or $\mathcal{G}_k^{\mathrm{D}}$, depending on time) and $L(\mathcal{G}')$ being the Laplacian matrix of $\mathcal{G}'$. Then we define P_2 representing matrix exponential if the defender recovers by

$$P_2 := e^{(-(\min\{\Delta_k^{\mathrm{A}} - (\underline{\tau}_k^{\mathrm{D}} - \underline{\tau}_k^{\mathrm{A}}), \Delta_k^{\mathrm{D}}\})[1\ -1; -1\ 1])}.$$

Corollary 2. The optimal combined strategy of the players with $n = 2$, $\alpha^{\mathrm{A}} = 1$, and $\alpha^{\mathrm{D}} = 1$ is given by

(1) Combined Strategy 1 if $\beta^{\mathrm{A}} \geq V(x(\underline{\tau}_k^{\mathrm{A}}))$,
(2) Combined Strategy 2a if $\beta^{\mathrm{A}} < V(x(\underline{\tau}_k^{\mathrm{A}}))$ and

$$\beta^{\mathrm{D}} \geq \frac{(V(x(\underline{\tau}_k^{\mathrm{A}})) - V(P_2 x(\underline{\tau}_k^{\mathrm{A}})))\Delta_k^{\mathrm{A}}}{\min\{\Delta_k^{\mathrm{A}} - (\underline{\tau}_k^{\mathrm{D}} - \underline{\tau}_k^{\mathrm{A}}), \Delta_k^{\mathrm{D}}\}}, \quad (10)$$

(3) Combined Strategy 3 if $\beta^{\mathrm{A}} < V(P_2 x(\underline{\tau}_k^{\mathrm{A}}))$ holds and (10) is not satisfied.

From the corollary above, we note that the costs β^{A} and β^{D} need to be small enough in order for the players to attack/recover. The following lemmas, which hold for general graph topologies, provide sufficient conditions based on the energy levels and the agent states, under which no action will be made by the players.

Lemma 3. The optimal strategy for the attacker is not to attack, i.e., Combined Strategy 1 is optimal, if $\beta^{\mathrm{A}} \geq V(x(\underline{t}_k))$. Moreover, there is no attack for any k if $\beta^{\mathrm{A}} \geq V(x(0))$.

Lemma 4. The optimal strategy for the defender is not to recover if $\beta^{\mathrm{D}} \geq \frac{V(x(0))\Delta_k^{\mathrm{A}}}{\min\{\Delta_k^{\mathrm{A}} - (\underline{\tau}_k^{\mathrm{D}} - \underline{\tau}_k^{\mathrm{A}}), \frac{\Delta_k^{\mathrm{D}}}{\alpha^{\mathrm{D}}}\}}$.

3.2 Approximate Consensus Time Bound

Here we investigate the effects of state-dependent jamming attacks in terms of the time for the agents to reach approximate consensus. To this end we define an approximate consensus set $\mathcal{D}_\epsilon := \{x \in \mathbb{R}^n : V(x) \leq \epsilon\}$, with $\epsilon > 0$. For the initial state $x(0) = x_0 \in \mathbb{R}^n \setminus \mathcal{D}_\epsilon$, the *approximate consensus time* is given by $T_*(x_0) := \inf\{t \geq 0 : x(t) \in \mathcal{D}_\epsilon\}$. Let $P := [P_{i,j}] = e^{-\gamma^{\mathrm{A}} L(\mathcal{G})}$ and $\underline{p} := \max_{j\in\{1,\ldots,n\}} \min_{i\in\{1,\ldots,n\}} P_{i,j}$. Since $\gamma^{\mathrm{A}} > 0$ and $\mathcal{G}$ is connected, note that $P_{i,j} \in (0, 1)$ and therefore $\underline{p} \in (0, 1)$.

The next result gives an upper bound for the approximate consensus time of agents under jamming attacks. The bound here is smaller than the one in Nugraha et al. (2019), since the attacker's strategy relies on the agents' states, and the optimal strategy is not to attack when $V(\cdot)$ becomes sufficiently small (see Lemma 3). Here, it is assumed that $V(x(0)) > \beta^{\mathrm{A}}$, since there is no attack in any k otherwise. We denote the ceiling function by $\lceil\cdot\rceil$.

Proposition 5. Consider the multi-agent system (1) with the initial condition $x_0 \in \mathbb{R}^n \setminus \mathcal{D}_\epsilon$. Under the optimal attack and recovery strategies for games with utility functions (6), (7), the approximate consensus time satisfies

$$T_*(x_0) \leq \frac{\beta^{\mathrm{A}}(\gamma^{\mathrm{A}} + \gamma^{\mathrm{D}})k' + \kappa^{\mathrm{A}}}{\beta^{\mathrm{A}} - \rho^{\mathrm{A}}} + (\gamma^{\mathrm{A}} + \gamma^{\mathrm{D}})(k_* - k'), \quad (11)$$

with $k_* := \lceil(\ln\epsilon - \ln V(x_0))/\ln(1 - \underline{p})\rceil$ and $k' := \lceil(\ln(\max\{\beta^{\mathrm{A}}, \epsilon\}) - \ln V(x_0))/\ln(1 - \underline{p})\rceil$.

Note that if $\beta^{\mathrm{A}} > \epsilon$, then $k' < k_*$, and the bound in (11) is strictly smaller than the one obtained in Nugraha et al. (2019). Otherwise, we have $k' = k_*$, and the two bounds have the same value.

4. NUMERICAL EXAMPLES

In this section, we illustrate the results in the optimal combined strategy and upper bound of approximate consensus with a numerical example. The graph shown in Fig.

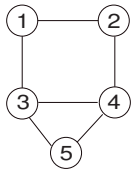

Fig. 3. $\mathcal{G}$ used in simulation.

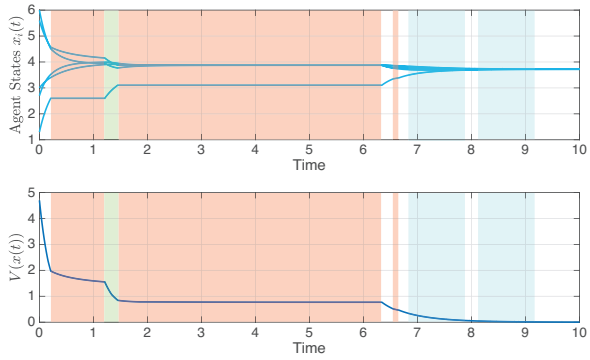

Fig. 4. States evolution of agents following communication protocol in (1) and $V(x(t))$ of the system represented by the initial graph as in Fig. 3.

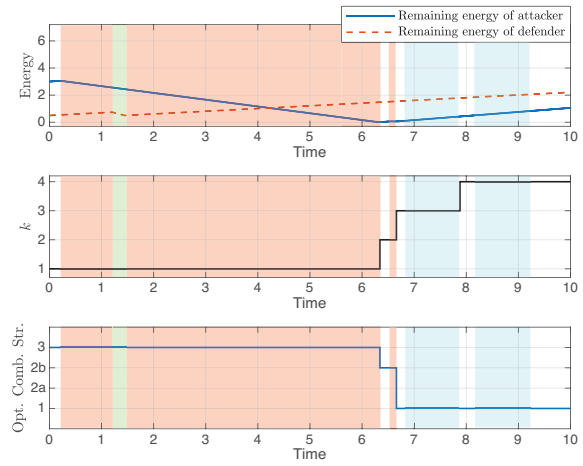

Fig. 5. Energy level, number of games, and optimal combined strategy of the simulation.

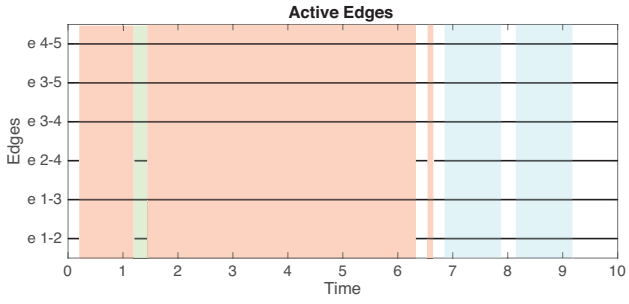

Fig. 6. Attacked and recovered edges during the games. The black lines indicate that the agents are able to communicate via the particular edges.

3 is considered, with parameters $\beta^{\mathrm{A}} = 0.4$, $\beta^{\mathrm{D}} = 0.5$, $\kappa^{\mathrm{A}} = 3$, $\kappa^{\mathrm{D}} = 0.5$, $\rho^{\mathrm{A}} = 0.3$, $\rho^{\mathrm{D}} = 0.2$, $\gamma^{\mathrm{A}} = 0.2$, $\gamma^{\mathrm{D}} = 1$, $\alpha^{\mathrm{A}} = 6$, $\alpha^{\mathrm{D}} = 3$, and $\epsilon = 0.3$. The initial states are $x(0) = [5.6\ 1.3\ 2.7\ 6.0\ 3.0]^{\mathrm{T}}$. Figs. 4 and 5 show the states of the agents, the max-min Lyapunov-like function $V(x)$, and some properties of the system with the utility functions (6), (7). In this simulation, the attacker attacks $e_{1,2}$ and $e_{2,4}$ to isolate agent 2 in the first game. In the second game, the attacker only attacks $e_{2,4}$ for a short duration because of the limitations in the available attack energy. The attacker does not attack from the third game onward, since $V(x(\underline{t}_3)) \leq \beta^{\mathrm{A}}$. The attacked and recovered edges over time are shown in Fig. 6. In the figures, the areas with red and green background denote time intervals where the attacker attacks and the defender recovers, respectively. Also, the areas in light blue denote time intervals with no attack due to $V(x(\underline{t}_k)) \leq \beta^{\mathrm{A}}$.

The approximate consensus is achieved at $T_*(x_0) \approx 7.52$, with the upper bound being $t \approx 482.77$ from Proposition 5 and $t \approx 522.82$ according to Nugraha et al. (2019).

5. CONCLUSION

We have provided the two-player subgame perfect equilibrium analysis of state-dependent attacks and recovery of the communication links in a multi-agent system. We have obtained the optimal strategies of the players in terms of edges and durations of action intervals by considering the effect of the attack or recovery actions to the states of the agents. In a consensus problem, we have explored how the time for the agents to reach approximate consensus is influenced by the value of the max-min function as well as the energies of the players and topology of the graph.

REFERENCES

Cetinkaya, A., Ishii, H., and Hayakawa, T. (2017). Networked control under random and malicious packet losses. *IEEE Trans. Autom. Contr.*, 62, 2434–2449.

Cetinkaya, A., Kikuchi, K., Hayakawa, T., and Ishii, H. (2020). Randomized transmission protocols for protection against jamming attacks in multi-agent consensus. *Automatica*, 117.

Chen, J., Touati, C., and Zhu, Q. (2020a). A dynamic game approach to strategic design of secure and resilient infrastructure network. *IEEE Trans. Inf. Forensics Security*, 15, 462–474.

Chen, J., Touati, C., and Zhu, Q. (2020b). Optimal secure two-layer IoT network design. *IEEE Trans. Control Netw. Syst.*, 7, 398–409.

Feng, S. and Tesi, P. (2017). Resilient control under denial-of-service: Robust design. *Automatica*, 79, 42–51.

Kordonis, I. and Papavassilopoulos, G. (2017). Network design in the presence of a link jammer: A zero-sum game formulation. In *IFAC PapersOnLine*, 9211–9217.

Nugraha, Y., Cetinkaya, A., Hayakawa, T., Ishii, H., and Zhu, Q. (2019). Subgame perfect equilibrium analysis for jamming attacks on resilient graphs. In *Proc. Amer. Contr. Conf.*, 2060–2065.

Pirani, M., Taylor, J., and Sinopoli, B. (2019). Attack resilient interconnected second order systems: A game-theoretic approach. In *Proc. IEEE Conf. Dec. Contr.*, 4391–4396.

Senejohnny, D., Tesi, P., and De Persis, C. (2018). A jamming resilient algorithm for self-triggered network coordination. *IEEE Trans. Control Netw. Syst.*, 5, 981–990.

Wang, Y. and Ishii, H. (2020). Resilient consensus through event-based communication. *IEEE Trans. Control Netw. Syst.*, 7, 471–482.