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

Subgame Perfect Equilibrium Analysis for Jamming Attacks on Resilient Graphs

Yurid Nugraha, Ahmet Cetinkaya, Tomohisa Hayakawa, Hideaki Ishii, and Quanyan Zhu

***Abstract*— A cyber security problem is considered in a networked system formulated as a resilient graph problem based on a game theoretic approach. The connectivity of the underlying graph of the network system is reduced by an attacker who removes some of the edges whereas the defender attempts to recover them. Both players are subject to energy constraints so that their actions are restricted and cannot be performed continuously. We provide a subgame perfect equilibrium analysis and fully characterize the optimal strategies for the attacker and the defender in terms of edge connectivity and the number of connected components of the graph. The resilient graph game is then applied to the multi-agent consensus problem. We study how the attacks and the recovery on the edges affect the consensus process.**

I. Introduction

Multi-agent systems provide a framework for studying distributed decision-making problems as a number of agents make local decisions by interacting with each other over networks [1]–[3]. Due to the rise in the use of general purpose networks and wireless communication channels for such systems, cyber security has become a major critical issue. Each agent in the network can be vulnerable to various threats initiated by malicious adversaries.

One of the common security threats in networked systems is jamming attacks. The adversary can simply transmit interference signals to interrupt communication among agents. While jamming attacks against multi-agent systems can be harmful as it does not require any knowledge of the systems, the danger level may further increase if the attacker is more aware of system parameters.

In this paper, we model the interaction between an attacker and a defender in a two-player game setting. The attacker is motivated to disrupt the communication by attacking individual links while the defender attempts to recover some or all of them whenever possible. Both players are constrained in terms of their available energy for the actions of attacks and recovery. We extend the problem formulation of [4], where the decision variables are limited to the links in the graphs for both players. In our problem setting, more dynamics are present; the time intervals for attacking and recovering are to be decided subject to energy constraints.

Noncooperative game theory approaches are widely used in security problems where multiple players are involved [5]. Jamming attacks on networked systems were previously analyzed through game-theoretic approaches in, e.g., [6]–[8]. We follow the jamming attack model with energy constraints introduced in [9], [10] in the context of networked control. This model has been generalized to further take account of probabilistic packet losses in [11]. Multi-agent consensus problems in the presence of such jamming attacks have been studied in [12]. Also, [13] considers multi-agents under jamming, where a stochastic communication protocol is introduced so that the attackers do not know the exact transmission times in advance.

More specifically, in our formulation of resilient graphs, a sequence of games is played by the attacker and the defender. In each attack interval, the attacker decides the links and the duration for the attacks. His utility depends on the number of connected components of the graph after the attack as well as his remaining energy. On the other hand, the defender recovers some of the links that are important for maintaining the connectivity of the graph. Our study is based on the analysis of the subgame perfect equilibria of the problem, and we use backward induction to obtain optimal strategies for both players.

To describe the relation between jamming and recovering on a two-player game, we follow the modelling approach of [14]. The defender can overcome the attacker's jamming by sending signals that have a greater signal to interference plus noise ratio (SINR). Furthermore, our study is motivated by [13] for formulating the maximum duration energy constraints of the players, which are time varying. In the current paper, we apply the game to a consensus problem and analyze how the time for reaching consensus is affected by the strategies of the attacker and the defender.

The paper is organized as follows. In Section II, we introduce the problem for the resilient graph game. In Section III, we characterize the optimal strategies for the players. In Section IV, we apply the obtained results to a consensus problem for multi-agent systems. We conclude the paper in Section V. Note that for space reasons, the proofs of the main results are omitted.

II. Problem Formulation

We consider a multi-agent system of n agents with a communication topology described by the undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. It 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

Yurid Nugraha and Tomohisa Hayakawa are with the Department 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

Ahmet Cetinkaya and Hideaki Ishii are with the Department of Computer Science, Tokyo Insitute of Technology, Yokohama, 226-8502, Japan. ahmet@sc.dis.titech.ac.jp, ishii@c.titech.ac.jp

Quanyan Zhu is with the Department of Electrical and Computer Engineering, New York University, Brooklyn NY, 11201, USA. quanyan.zhu@nyu.edu

This work was supported in the part by the JST CREST Grant No. JPMJCR15K3.

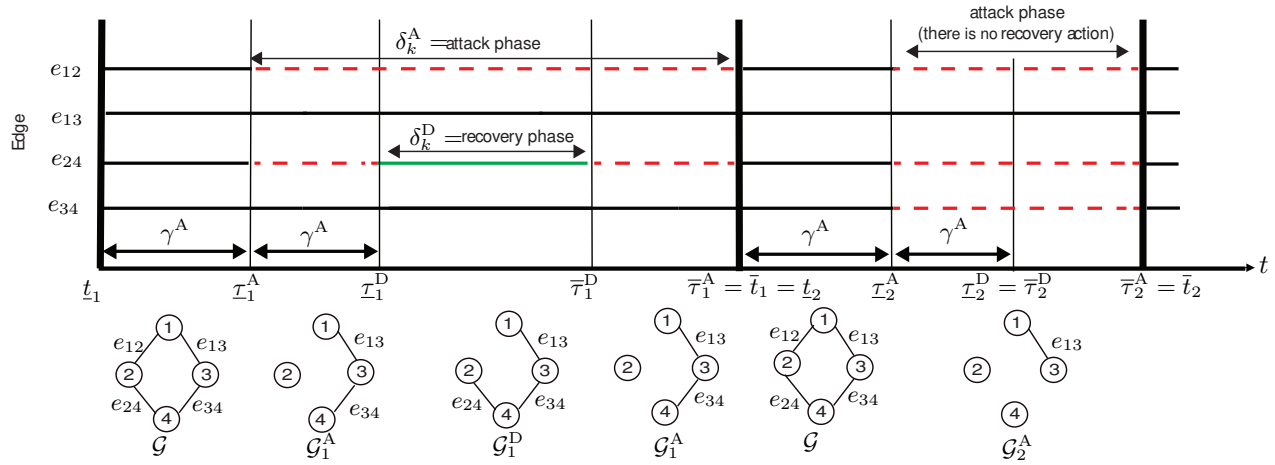

Fig. 1. Illustration of graph transitions: Changes in connectivity of the four edges over time are shown. Solid lines indicate that the corresponding edges are connected while dashed lines show that they are disconnected by attacks. At time interval $[\underline{t}_1, \bar{t}_1]$, two edges e_{12} and e_{24} are attacked at time $\underline{\tau}_1^{\mathrm{A}}$, but the defender recovers e_{24} from $\underline{\tau}_1^{\mathrm{D}}$ until $\overline{\tau}_1^{\mathrm{D}}$. At time interval $[\underline{t}_2, \bar{t}_2]$, the attacker removes three edges, which are not recovered by the defender. The corresponding graphs are shown under the time intervals.

agents are represented by the edges of the graph. Every agent is able to communicate with its neighbor agents via the communication links. We assume that the underlying, attack-free communication topology $\mathcal{G}$ is connected.

In this paper, we consider a game between two players, the attacker and the defender, in terms of the communication among the agents. The attacker is an entity capable to block the communication by jamming some targeted links, whereas the defender tries to recover some or all of the attacked links. However, the actions of both players are constrained by the limited energy resources they have.

The attacker wants to attack the communication activities between the agents by sending jamming signals that are stronger than the communication signals. This action by the attacker is represented as a deletion of edges in the graph. We call this an attack action. When the communication links are jammed, the defender asks the agents to send even stronger signals in certain communication links in order to maintain the connectivity over the entire set of agents. We call this a recovery action.

The kth game with $k \in \mathbb{N}$ is played in the time interval $[\underline{t}_k, \bar{t}_k]$, which is determined by the players' actions with $\bar{t}_k > \underline{t}_k = \bar{t}_{k-1}$. Initially, at the start time $\underline{t}_k$, there is no attack or recovery, and the underlying graph is $\mathcal{G}$. Then, the attacker may start an attack on certain links, at which point the defender will decide his actions whether to recover some links or not. The durations and the links for the attack and the recovery are the action variables. The end time $\bar{t}_k$ is when the attacker and hence the defender stop their actions. The kth game may also end after a fixed time duration when no attack occurs. The $(k+1)$th game starts immediately after the kth game, that is, $\underline{t}_{k+1} = \bar{t}_k$.

The attacker can start and end attacking, and the defender can start and end recovering at most once in each time interval $[\underline{t}_k, \bar{t}_k]$. The end of the kth time interval $\bar{t}_k$ is specified more concretely later in this section. At the start time $\underline{t}_k$, we assume that the active communication links are prescribed by the original edge set $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ for all $k \in \mathbb{N}$.

More specifically, the attacker attacks $\mathcal{G}$ by deleting some of the existing edges $\mathcal{E}_k^{\mathrm{A}} \subseteq \mathcal{E}$ from time $\underline{\tau}_k^{\mathrm{A}}$ until $\overline{\tau}_k^{\mathrm{A}}$, where $\underline{t}_k < \underline{\tau}_k^{\mathrm{A}} \leq \overline{\tau}_k^{\mathrm{A}} \leq \bar{t}_k$. Consequently, $\mathcal{G}$ is changed to $\mathcal{G}_k^{\mathrm{A}} := (\mathcal{V}, \mathcal{E} \setminus \mathcal{E}_k^{\mathrm{A}})$ at $\underline{\tau}_k^{\mathrm{A}}$. For transmitting jamming signals, the attacker spends some amount of energy in proportion to the attack duration. For the attacker, it is also an option not to make an attack action considering its utility defined later. We define the attack phase as $[\underline{\tau}_k^{\mathrm{A}}, \overline{\tau}_k^{\mathrm{A}}]$ for every $k \in \mathbb{N}$, where the values of $\overline{\tau}_k^{\mathrm{A}}$ are related to the energy of the attacker, as discussed later. If there is no attack in the kth time interval, it is understood that $\underline{\tau}_k^{\mathrm{A}} = \overline{\tau}_k^{\mathrm{A}}$.

On the other hand, the defender aims to maintain the connectivity of the graph by recovering some of the edges that are blocked by the attacker. The defender recovers the edges $\mathcal{E}_k^{\mathrm{D}}$ from time $\underline{\tau}_k^{\mathrm{D}}$ until $\overline{\tau}_k^{\mathrm{D}}$, with $\mathcal{E}_k^{\mathrm{D}} \subseteq \mathcal{E}_k^{\mathrm{A}}$ and $\underline{t}_k < \underline{\tau}_k^{\mathrm{A}} < \underline{\tau}_k^{\mathrm{D}} \leq \overline{\tau}_k^{\mathrm{D}} \leq \bar{t}_k$. As soon as the defender starts the recovery action at $\underline{\tau}_k^{\mathrm{D}}$, the graph $\mathcal{G}_k^{\mathrm{A}}$ is changed to $\mathcal{G}_k^{\mathrm{D}} := (\mathcal{V}, (\mathcal{E} \setminus \mathcal{E}_k^{\mathrm{A}}) \cup \mathcal{E}_k^{\mathrm{D}})$. By recovering the edges, the defender spends some amount of energy similarly to the attacker. If there is no recovery action due to the absence of the attack action or the decision by the defender, we set $\underline{\tau}_k^{\mathrm{D}} = \overline{\tau}_k^{\mathrm{D}}$. We define the recovery phase as $[\underline{\tau}_k^{\mathrm{D}}, \overline{\tau}_k^{\mathrm{D}}]$ for every $k \in \mathbb{N}$, where values of $\overline{\tau}_k^{\mathrm{D}}$ are related to the energy of the defender, as discussed later. Once the attacker stops attacking, the graph becomes $\mathcal{G}$ again, and a new game ($(k+1)$th game) begins. The timeline of the attack and the recovery sequences is illustrated in Fig. 1.

In this formulation, we assume that there is a constant dwell time γ^{A} between the beginning of the kth game $\underline{t}_k$ and the beginning of the attack time $\underline{\tau}_k^{\mathrm{A}}$. For the defender, we assume that there is also a constant dwell time γ^{D} between the beginning of attack time $\underline{\tau}_k^{\mathrm{A}}$ and the beginning of recovery time $\underline{\tau}_k^{\mathrm{D}}$ unless the attacker ends attacking earlier, i.e., $\overline{\tau}_k^{\mathrm{A}} < \underline{\tau}_k^{\mathrm{D}}$. Thus, $\underline{\tau}_k^{\mathrm{A}}$ and $\underline{\tau}_k^{\mathrm{D}}$ are given by

$$\underline{\tau}_k^{\mathrm{A}} = \underline{t}_k + \gamma^{\mathrm{A}}, \quad \underline{\tau}_k^{\mathrm{D}} = \min(\overline{\tau}_k^{\mathrm{A}}, \underline{\tau}_k^{\mathrm{A}} + \gamma^{\mathrm{D}}). \tag{1}$$

The length of the attack and the recovery intervals are denoted by δ_k^{A} and δ_k^{D}, respectively. Note that

$$\delta_k^{\mathrm{A}} := \overline{\tau}_k^{\mathrm{A}} - \underline{\tau}_k^{\mathrm{A}}, \quad \delta_k^{\mathrm{D}} := \overline{\tau}_k^{\mathrm{D}} - \underline{\tau}_k^{\mathrm{D}}. \tag{2}$$

In the kth game, both of the players attempt to choose the best strategy to maximize their own utility functions that

are defined over the time interval $[\underline{t}_k,\bar{t}_k]$ without foreseeing the future activities. The attacker's strategy is determined in terms of $(\mathcal{E}_k^{\mathrm{A}},\delta_k^{\mathrm{A}})$, and the defender's strategy is determined in terms of $(\mathcal{E}_k^{\mathrm{D}},\delta_k^{\mathrm{D}})$.

To characterize how much the nodes are connected or disconnected in a unified way, we introduce the generalized edge connectivity $\hat{\lambda}$ as an extension of the notion of edge connectivity. Specifically, for any undirected graph $\mathcal{G}'$, define

$$\hat{\lambda}(\mathcal{G}') := \begin{cases} \lambda(\mathcal{G}'), & \text{if } \mathcal{G}' \text{ is connected,} \\ -\tilde{\lambda}(\mathcal{G}'), & \text{otherwise,} \end{cases} \tag{3}$$

where $\lambda(\mathcal{G}')$ denotes the edge connectivity, i.e., the minimum number of edges required to be removed in order to make the connected graph $\mathcal{G}'$ disconnected, and $\tilde{\lambda}(\mathcal{G}')$ denotes the minimum number of edges required to make the disconnected graph $\mathcal{G}'$ connected. Note that a larger positive value of $\hat{\lambda}$ implies that the graph $\mathcal{G}'$ has more links to be removed by the attacker, and a smaller negative value of $\hat{\lambda}$ indicates that the graph $\mathcal{G}'$ requires more links to be recovered by the defender. Since $\mathcal{G}_k^{\mathrm{A}} \subseteq \mathcal{G}_k^{\mathrm{D}} \subseteq \mathcal{G}$, note that $\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}}) \leq \hat{\lambda}(\mathcal{G}_k^{\mathrm{D}}) \leq \hat{\lambda}(\mathcal{G})$.

The attacker chooses the edges to attack based on the generalized edge connectivity of the graph $\mathcal{G}$, and the defender chooses the edges to recover based on the generalized edge connectivity of the graph $\mathcal{G}_k^{\mathrm{A}}$. The attacker should strategically choose the edges to destroy in order to reduce $\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})$ (and make $\mathcal{G}_k^{\mathrm{A}}$ more disconnected), and the defender also should strategically choose the edges to efficiently increase $\hat{\lambda}(\mathcal{G}_k^{\mathrm{D}})$ (and make $\mathcal{G}_k^{\mathrm{D}}$ more connected).

For the game of the kth time interval $[\underline{t}_k,\bar{t}_k]$, we define the utility function U^{A} of the attacker as

$$\begin{aligned} U^{\mathrm{A}}(\mathcal{E}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{D}},\delta_k^{\mathrm{A}},\delta_k^{\mathrm{D}}) := &-\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})(\delta_k^{\mathrm{A}}-\delta_k^{\mathrm{D}}) - \hat{\lambda}(\mathcal{G}_k^{\mathrm{D}})\delta_k^{\mathrm{D}} \\ &- \beta^{\mathrm{A}}|\mathcal{E}_k^{\mathrm{A}}|\delta_k^{\mathrm{A}}, \end{aligned} \tag{4}$$

where $\beta^{\mathrm{A}} > 0$ is the attacker's cost to destroy one edge per one time unit. Similarly, we define the utility function U^{D} of the defender as

$$\begin{aligned} U^{\mathrm{D}}(\mathcal{E}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{D}},\delta_k^{\mathrm{A}},\delta_k^{\mathrm{D}}) := &\ \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})(\delta_k^{\mathrm{A}}-\delta_k^{\mathrm{D}}) + \hat{\lambda}(\mathcal{G}_k^{\mathrm{D}})\delta_k^{\mathrm{D}} \\ &- \beta^{\mathrm{D}}|\mathcal{E}_k^{\mathrm{D}}|\delta_k^{\mathrm{D}}, \end{aligned} \tag{5}$$

where $\beta^{\mathrm{D}} > 0$ is the defender's cost to recover one edge per one time unit. Note that the utility function (4) represents the total generalized edge connectivity (with the negative sign) for the attacker over the game horizon $[\underline{\tau}_k^{\mathrm{A}},\bar{t}_k]$ plus the cost for jamming $\mathcal{E}_k^{\mathrm{A}}$. Similarly, (5) represents the total generalized edge connectivity for the defender over the game horizon $[\underline{\tau}_k^{\mathrm{A}},\bar{t}_k]$ plus the cost for recovering $\mathcal{E}_k^{\mathrm{D}}$.

If the attacker decides to attack at least one edge or the defender decides not to recover, the attacker can end the game at $\overline{\tau}_k^{\mathrm{A}}$. Otherwise, the game ends at $\underline{t}_k + \gamma^{\mathrm{A}} + \gamma^{\mathrm{D}}$. Hence, the end time $\bar{t}_k$ of the kth game is

$$\bar{t}_k := \begin{cases} \overline{\tau}_k^{\mathrm{A}}, & \text{if } \mathcal{E}_k^{\mathrm{A}} \neq \emptyset, \\ \underline{t}_k + \gamma^{\mathrm{A}} + \gamma^{\mathrm{D}}, & \text{otherwise.} \end{cases} \tag{6}$$

From (6), it is understood that if the defender stops recovering $\mathcal{E}_k^{\mathrm{D}}$ before the game ends while the attacker keeps sending jamming signals at $\mathcal{E}_k^{\mathrm{A}}$, the graph is changed back to $\mathcal{G}_k^{\mathrm{A}}$ at $\overline{\tau}_k^{\mathrm{D}}$, with generalized edge connectivity $\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})$. Therefore, in $[\overline{\tau}_k^{\mathrm{D}},\bar{t}_k]$, the utilities of both players in (4) and (5) are computed based on $\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})$.

The players cannot keep sending signals for very long durations due to energy resource constraints. We follow the approach in [13] to model such energy constraints. The total energy used for the attacker must satisfy

$$\sum_{m=1}^{k-1} \beta^{\mathrm{A}}|\mathcal{E}_m^{\mathrm{A}}|\delta_m^{\mathrm{A}} + \beta^{\mathrm{A}}|\mathcal{E}_k^{\mathrm{A}}|(t-\underline{\tau}_k^{\mathrm{A}}) \leq \kappa^{\mathrm{A}} + \rho^{\mathrm{A}}t, \tag{7}$$

for any time $t \in [\underline{\tau}_k^{\mathrm{A}},\underline{\tau}_{k+1}^{\mathrm{A}}]$, with $\kappa^{\mathrm{A}} > 0$, $\rho^{\mathrm{A}} \in (0,1)$, $\beta^{\mathrm{A}} > \rho^{\mathrm{A}}$, and $k \in \mathbb{N}$. For the defender, the total energy used must satisfy

$$\sum_{m=1}^{k-1} \beta^{\mathrm{D}}|\mathcal{E}_m^{\mathrm{D}}|\delta_m^{\mathrm{D}} + \beta^{\mathrm{D}}|\mathcal{E}_k^{\mathrm{D}}|(t-\underline{\tau}_k^{\mathrm{D}}) \leq \kappa^{\mathrm{D}} + \rho^{\mathrm{D}}t, \tag{8}$$

for any time $t \in [\underline{\tau}_k^{\mathrm{D}},\underline{\tau}_{k+1}^{\mathrm{D}}]$, with $\kappa^{\mathrm{D}} > 0$, $\rho^{\mathrm{D}} \in (0,1)$, $\beta^{\mathrm{D}} > \rho^{\mathrm{D}}$, and $k \in \mathbb{N}$. Note that κ^{A} and κ^{D} denote the initial energy that the attacker and the defender have, respectively. Moreover, ρ^{A} and ρ^{D} denote the recharge rate of energy for the attacker and the defender, respectively. In this paper, we assume that each player knows all parameters of the other player, including $\rho^{\mathrm{A}},\rho^{\mathrm{D}},\kappa^{\mathrm{A}}$, and κ^{D}.

Under this problem formulation, if the attacker keeps sending signals from $\underline{\tau}_k^{\mathrm{A}}$ until he runs out of energy, then from (7) we obtain an explicit expression for the maximum time interval δ_k^{A} when the attacker completes the attack as

$$\Delta_k^{\mathrm{A}} := \frac{\kappa^{\mathrm{A}} + \beta^{\mathrm{A}}|\mathcal{E}_k^{\mathrm{A}}|\underline{\tau}_k^{\mathrm{A}} - \sum_{m=1}^{k-1}\beta^{\mathrm{A}}|\mathcal{E}_m^{\mathrm{A}}|\delta_m^{\mathrm{A}}}{\beta^{\mathrm{A}}|\mathcal{E}_k^{\mathrm{A}}| - \rho^{\mathrm{A}}} - \underline{\tau}_k^{\mathrm{A}}. \tag{9}$$

Similarly, from (8), we obtain an explicit form for the time δ_k^{D} when the defender completes the recovery as

$$\Delta_k^{\mathrm{D}} := \frac{\kappa^{\mathrm{D}} + \beta^{\mathrm{D}}|\mathcal{E}_k^{\mathrm{D}}|\underline{\tau}_k^{\mathrm{D}} - \sum_{m=1}^{k-1}\beta^{\mathrm{D}}|\mathcal{E}_m^{\mathrm{D}}|\delta_m^{\mathrm{D}}}{\beta^{\mathrm{D}}|\mathcal{E}_k^{\mathrm{D}}| - \rho^{\mathrm{D}}} - \underline{\tau}_k^{\mathrm{D}}. \tag{10}$$

For simplicity of presentation, in this paper we first consider the scenarios where $\delta_k^{\mathrm{A}} \in \{0,\Delta_k^{\mathrm{A}}\}$. In other words, for each game the attacker either does not attack or attacks until running out of energy.

We seek the subgame perfect equilibrium of this game as in [4]. To this end, one needs to divide the game into some subgames. The equilibrium must be optimal in every subgame. To obtain the optimal strategy for every player, a *backward induction* approach is used.

In the time interval $[\underline{t}_k,\bar{t}_k]$, given the attacker's strategy $(\mathcal{E}_k^{\mathrm{A}},\delta_k^{\mathrm{A}})$, the defender chooses his strategy as

$$\begin{aligned} &(\mathcal{E}_k^{\mathrm{D}*}(\mathcal{E}_k^{\mathrm{A}},\delta_k^{\mathrm{A}}),\delta_k^{\mathrm{D}*}(\mathcal{E}_k^{\mathrm{A}},\delta_k^{\mathrm{A}})) \\ &\qquad \in \arg\max_{(\mathcal{E}_k^{\mathrm{D}},\delta_k^{\mathrm{D}})} U^{\mathrm{D}}(\mathcal{E}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{D}},\delta_k^{\mathrm{A}},\delta_k^{\mathrm{D}}), \end{aligned} \tag{11}$$

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

$$\begin{aligned} &(\mathcal{E}_k^{\mathrm{A}*},\delta_k^{\mathrm{A}*}) \\ &\in \arg\max_{(\mathcal{E}_k^{\mathrm{A}},\delta_k^{\mathrm{A}})} U^{\mathrm{A}}(\mathcal{E}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{D}*}(\mathcal{E}_k^{\mathrm{A}},\delta_k^{\mathrm{A}}),\delta_k^{\mathrm{A}},\delta_k^{\mathrm{D}*}(\mathcal{E}_k^{\mathrm{A}},\delta_k^{\mathrm{A}})). \end{aligned} \tag{12}$$

We assume that the players are strategic. In this research,

TABLE I

POSSIBLE CASES OF ATTACK AND RECOVERY ACTIONS

Case	$\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})$	$\hat{\lambda}(\mathcal{G}_k^{\mathrm{D}})$
1	$\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}}) = \hat{\lambda}(\mathcal{G})$	$\hat{\lambda}(\mathcal{G}_k^{\mathrm{D}}) = \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})$
2	$\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}}) < \hat{\lambda}(\mathcal{G})$	$\hat{\lambda}(\mathcal{G}_k^{\mathrm{D}}) = \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})$
3	$\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}}) < \hat{\lambda}(\mathcal{G})$	$\hat{\lambda}(\mathcal{G}_k^{\mathrm{D}}) > \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})$

we study the subgame perfect equilibrium and analyze the strategies 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 $(\mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}})$.

A tie-break condition happens if the players have multiple options for the choices on which edges to attack or recover, and those edges yield the same values of the utility functions. In this case, we suppose that the players choose more edges to attack or recover. As we see later in the context of consensus, if the utility is the same for different graphs, then the players choose the edges to attack or recover according to certain principles as explained in Section IV below.

III. GAME ANALYSIS

In this section, we analyze the subgame perfect equilibrium of the system. From the sequence of actions, we obtain several cases that might happen and seek the equilibrium in each case, i.e., the candidate optimal strategies of the system. Then, we seek the optimal strategy among the candidate strategies by using backward induction.

1) Subgame Perfect Equilibrium Analysis in Each Case: From the problem formulation, since $\hat{\lambda}(\mathcal{G}) \geq \hat{\lambda}(\mathcal{G}_k^{\mathrm{D}}) \geq \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})$, we can divide all possible sequences into three cases based on the combinations of $\hat{\lambda}(\mathcal{G})$, $\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})$, and $\hat{\lambda}(\mathcal{G}_k^{\mathrm{D}})$, as shown in Table I. We analyze the subgame perfect equilibrium for the time interval $[\underline{t}_k, \overline{t}_k]$ in each case.

Case 1: In this case, we show that the optimal strategy for the attacker is not to attack, and the optimal strategy for the defender is not to recover any edge. Here, the generalized edge connectivities satisfy $\hat{\lambda}(\mathcal{G}) = \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}}) = \hat{\lambda}(\mathcal{G}_k^{\mathrm{D}})$. Thus, the utility function in (5) of the defender becomes

$$U^{\mathrm{D}}(\mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{A}}, \delta_k^{\mathrm{D}}) = \hat{\lambda}(\mathcal{G})\delta_k^{\mathrm{A}} - \beta^{\mathrm{D}}|\mathcal{E}_k^{\mathrm{D}}|\delta_k^{\mathrm{D}}. \tag{13}$$

Furthermore, because the defender gets no reward by recovering any link, the optimal strategy for the defender is $\mathcal{E}_k^{\mathrm{D}*} = \emptyset$ and $\delta_k^{\mathrm{D}*} = 0$, resulting in

$$U^{\mathrm{D}}(\mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}*}, \delta_k^{\mathrm{A}}, \delta_k^{\mathrm{D}*}) = \hat{\lambda}(\mathcal{G})\delta_k^{\mathrm{A}}. \tag{14}$$

Likewise, for the attacker, the utility function in (4) becomes

$$U^{\mathrm{A}}(\mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}*}, \delta_k^{\mathrm{A}}, \delta_k^{\mathrm{D}*}) = (-\hat{\lambda}(\mathcal{G}) - \beta^{\mathrm{A}}|\mathcal{E}_k^{\mathrm{A}}|)\delta_k^{\mathrm{A}}. \tag{15}$$

Since $\hat{\lambda}(\mathcal{G})$ is constant, the attacker gets no reward by attacking any link. Thus, the optimal strategy for the attacker is $\mathcal{E}_k^{\mathrm{A}*} = \emptyset$ and $\delta_k^{\mathrm{A}*} = 0$. As a result, the utility functions in Case 1 are given by

$$U^{\mathrm{A}}(\mathcal{E}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{D}*}, \delta_k^{\mathrm{A}*}, \delta_k^{\mathrm{D}*}) = 0 =: \hat{U}^{\mathrm{A}1}, \tag{16}$$

$$U^{\mathrm{D}}(\mathcal{E}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{D}*}, \delta_k^{\mathrm{A}*}, \delta_k^{\mathrm{D}*}) = 0 =: \hat{U}^{\mathrm{D}1}. \tag{17}$$

From (6), because $\mathcal{E}_k^{\mathrm{A}} = \mathcal{E}_k^{\mathrm{D}} = \emptyset$, it follows that the game ends at $\overline{t}_k = \underline{t}_k + \gamma^{\mathrm{A}} + \gamma^{\mathrm{D}}$. This optimal strategy corresponding to $\mathcal{E}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{D}*}, \delta_k^{\mathrm{A}*}, \delta_k^{\mathrm{D}*}$ is then labelled as **Strategy 1** (see Table II).

Case 2: In this case, we show that the optimal strategy for the attacker is to attack optimal edges until running out of energy, and the optimal strategy for the defender is not to recover any edge. Note that in this case, the generalized edge connectivities satisfy $\hat{\lambda}(\mathcal{G}) > \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})$ and $\hat{\lambda}(\mathcal{G}_k^{\mathrm{D}}) = \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})$ by Table I. Similarly with the analysis in Case 1, because $\hat{\lambda}(\mathcal{G}_k^{\mathrm{D}}) = \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})$, the utility function of the defender with $\mathcal{E}_k^{\mathrm{D}*} = \emptyset$ and $\delta_k^{\mathrm{D}*} = 0$ as in (14) is given by

$$U^{\mathrm{D}}(\mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}*}, \delta_k^{\mathrm{A}}, \delta_k^{\mathrm{D}*}) = \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})\delta_k^{\mathrm{A}}. \tag{18}$$

For the attacker, from (4) with $\delta_k^{\mathrm{D}} = 0$, we have

$$U^{\mathrm{A}}(\mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}*}, \delta_k^{\mathrm{A}}, \delta_k^{\mathrm{D}*}) = (-\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}}) - \beta^{\mathrm{A}}|\mathcal{E}_k^{\mathrm{A}}|)\delta_k^{\mathrm{A}}. \tag{19}$$

Since $\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}}) < \hat{\lambda}(\mathcal{G})$, it follows that $\mathcal{E}_k^{\mathrm{A}} \neq \emptyset$, which means that the attacker attacks for Δ_k^{A}. Hence, $\delta_k^{\mathrm{A}} = \Delta_k^{\mathrm{A}}$, and

$$\begin{aligned} &U^{\mathrm{A}}(\mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}*}, \delta_k^{\mathrm{A}*}, \delta_k^{\mathrm{D}*}) \\ &\quad = (-\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}}) - \beta^{\mathrm{A}}|\mathcal{E}_k^{\mathrm{A}}|)\Delta_k^{\mathrm{A}} =: \hat{U}^{\mathrm{A}2}(\mathcal{E}_k^{\mathrm{A}}). \end{aligned} \tag{20}$$

Now we only need to choose $\mathcal{E}_k^{\mathrm{A}}$, as δ_k^{A} is already determined. Specifically, we search for $\mathcal{E}_k^{\mathrm{A}2*}$, which is the optimal $\mathcal{E}_k^{\mathrm{A}}$. This is done by maximizing the simplified utility function $\hat{U}^{\mathrm{A}2}(\mathcal{E}_k^{\mathrm{A}})$ in (20), resulting in

$$\mathcal{E}_k^{\mathrm{A}2*} \in \arg\max_{\mathcal{E}_k^{\mathrm{A}} \neq \emptyset} \hat{U}^{\mathrm{A}2}(\mathcal{E}_k^{\mathrm{A}}). \tag{21}$$

Note that with this strategy, (18) becomes

$$U^{\mathrm{D}}(\mathcal{E}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{D}*}, \delta_k^{\mathrm{A}*}, \delta_k^{\mathrm{D}*}) = \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}2*})\Delta_k^{\mathrm{A}} =: \hat{U}^{\mathrm{D}2}. \tag{22}$$

This optimal strategy of $\mathcal{E}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{D}*}, \delta_k^{\mathrm{A}*}, \delta_k^{\mathrm{D}*}$ is labelled as **Strategy 2**.

Case 3: In this case, we show that the optimal strategy for the attacker is to attack optimal edges until running out of energy, and the optimal strategy for the defender is to recover optimal edges until either he runs out of energy or the attacker runs out of energy. Note that in this case, by Table I, the generalized edge connectivities satisfy $\hat{\lambda}(\mathcal{G}) \geq \hat{\lambda}(\mathcal{G}_k^{\mathrm{D}}) > \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})$. From (5), the utility function of the defender can be written as

$$U^{\mathrm{D}}(\mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{A}}, \delta_k^{\mathrm{D}}) = \phi_k\delta_k^{\mathrm{D}} + \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})\delta_k^{\mathrm{A}}, \tag{23}$$

with $\phi_k := (\hat{\lambda}(\mathcal{G}_k^{\mathrm{D}}) - \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}}) - \beta^{\mathrm{D}}|\mathcal{E}_k^{\mathrm{D}}|)$ for simplicity. Since $\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}}) < \hat{\lambda}(\mathcal{G}_k^{\mathrm{D}})$, in order to maximize the term $\phi_k\delta_k^{\mathrm{D}}$, the defender recovers $\mathcal{E}_k^{\mathrm{D}}$ as long as possible if $\phi_k \geq 0$, so that $\overline{\tau}_k^{\mathrm{D}} = \min(\Delta_k^{\mathrm{D}} + \underline{\tau}_k^{\mathrm{D}}, \overline{\tau}_k^{\mathrm{A}})$. Alternatively, if $\phi_k < 0$, then the defender's utility is less than $\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})\Delta_k^{\mathrm{A}}$, which is the utility if the defender does not recover. Hence the defender should not recover at all.

From (23), it is clear that the defender should also maximize the term ϕ_k. Hence, the utility function of the defender is given by

$$\begin{aligned} &U^{\mathrm{D}}(\mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{A}}, \min(\Delta_k^{\mathrm{D}}, \overline{\tau}_k^{\mathrm{A}} - \underline{\tau}_k^{\mathrm{D}})) \\ &\quad = \phi_k(\min(\Delta_k^{\mathrm{D}}, \overline{\tau}_k^{\mathrm{A}} - \underline{\tau}_k^{\mathrm{D}})) + \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})\delta_k^{\mathrm{A}}. \end{aligned} \tag{24}$$

By assumption, $\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}}) < \hat{\lambda}(\mathcal{G})$, thus $\mathcal{E}_k^{\mathrm{A}} \neq \emptyset$. Hence the attacker attacks for Δ_k^{A} so that $\delta_k^{\mathrm{A}*} = \Delta_k^{\mathrm{A}}$.

If the attacker ends attacking before $\Delta_k^{\mathrm{D}} + \underline{\tau}_k^{\mathrm{D}}$, then $\overline{t}_k = \overline{\tau}_k^{\mathrm{D}} = \Delta_k^{\mathrm{A}} + \underline{\tau}_k^{\mathrm{A}}$. Otherwise, the defender recovers for Δ_k^{D},

TABLE II
POSSIBLE OPTIMAL STRATEGIES OF SUBGAME PERFECT EQUILIBRIUM

Strategy	$\mathcal{E}_k^{\mathrm{A}*}$	$\mathcal{E}_k^{\mathrm{D}*}$	$\delta_k^{\mathrm{D}*}$	$\delta_k^{\mathrm{A}*}$
1	$\emptyset$	$\emptyset$	0	0
2	$\mathcal{E}_k^{\mathrm{A2}*}$	$\emptyset$	0	Δ_k^{A}
3	$\mathcal{E}_k^{\mathrm{A3}*}$	$\mathcal{E}_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A3}*})$	ξ_k	Δ_k^{A}

and $\bar{t}_k = \Delta_k^{\mathrm{A}} + \underline{\tau}_k^{\mathrm{A}}$. Therefore, we can rewrite (24) as

$$\begin{aligned} U^{\mathrm{D}}(\mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{A}*}, \delta_k^{\mathrm{D}*}) &= \phi_k \xi_k + \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})\Delta_k^{\mathrm{A}} \\ &=: \hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}}), \end{aligned} \tag{25}$$

with $\xi_k := \min(\Delta_k^{\mathrm{D}}, \Delta_k^{\mathrm{A}} + \underline{\tau}_k^{\mathrm{A}} - \underline{\tau}_k^{\mathrm{D}})$. Then the optimal number of edges to be recovered for $\mathcal{E}_k^{\mathrm{A}}$ is obtained by

$$\mathcal{E}_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A}}) \in \arg\max_{\mathcal{E}_k^{\mathrm{D}} \neq \emptyset} \hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}}). \tag{26}$$

For the attacker, the utility function becomes

$$\begin{aligned} &U^{\mathrm{A}}(\mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}*}, \delta_k^{\mathrm{A}*}, \delta_k^{\mathrm{D}*}) \\ &\quad = -\hat{\lambda}(\mathcal{G}_k^{\mathrm{A}})(\Delta_k^{\mathrm{A}} - \xi_k) - \hat{\lambda}(\mathcal{G}_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A}}))\xi_k - \beta^{\mathrm{A}}|\mathcal{E}_k^{\mathrm{A}}|\Delta_k^{\mathrm{A}} \\ &\quad =: \hat{U}^{\mathrm{A3}}(\mathcal{E}_k^{\mathrm{A}}). \end{aligned} \tag{27}$$

The attacker looks for $\mathcal{E}_k^{\mathrm{A3}*}$ by maximizing the simplified utility function $\hat{U}^{\mathrm{A3}}(\mathcal{E}_k^{\mathrm{A}})$. Specifically,

$$\mathcal{E}_k^{\mathrm{A3}*} \in \arg\max_{\mathcal{E}_k^{\mathrm{A}} \neq \emptyset} \hat{U}^{\mathrm{A3}}(\mathcal{E}_k^{\mathrm{A}}). \tag{28}$$

Note that to obtain $\mathcal{E}_k^{\mathrm{A3}*}$, the attacker needs to obtain $\mathcal{E}_k^{\mathrm{D3}*}$. Hence, the attacker solves the maximization problem in (26) beforehand to obtain $\mathcal{E}_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A}})$.

Finally, after the attacker obtains $\mathcal{E}_k^{\mathrm{A3}*}$, the defender searches for $\mathcal{E}_k^{\mathrm{D3}*}$, based on $\hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A3}*}, \mathcal{E}_k^{\mathrm{D}})$ in (25), as

$$\mathcal{E}_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A3}*}) \in \arg\max_{\mathcal{E}_k^{\mathrm{D}} \neq \emptyset} \hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A3}*}, \mathcal{E}_k^{\mathrm{D}}). \tag{29}$$

We call this strategy as **Strategy 3**. The summary of the optimal strategy in each case is shown in Table II.

2) Subgame Perfect Equilibrium Analysis of All Cases: Here, we discuss the subgame perfect equilibrium analysis of the system among all cases. To do so, we must find the strategy that yields the maximum utility out of the three possible optimal strategies described in Section III.B.1, in accordance with the subgame perfect equilibrium principle. Specifically, we compare $\hat{U}^{\mathrm{A1}}$, $\hat{U}^{\mathrm{A2}}(\mathcal{E}_k^{\mathrm{A2}*})$, $\hat{U}^{\mathrm{A3}}(\mathcal{E}_k^{\mathrm{A3}*})$, $\hat{U}^{\mathrm{D1}}$, $\hat{U}^{\mathrm{D2}}$, and $\hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A3}*}, \mathcal{E}_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A3}*}))$.

For simplicity, we define $\hat{U}^{\mathrm{D3}*} := \hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A3}*}, \mathcal{E}_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A3}*}))$, $\hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A2}*}) := \hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A2}*}, \mathcal{E}_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A2}*}))$, $\hat{U}^{\mathrm{A2}*} := \hat{U}^{\mathrm{A2}}(\mathcal{E}_k^{\mathrm{A2}*})$, and $\hat{U}^{\mathrm{A3}*} := \hat{U}^{\mathrm{A3}}(\mathcal{E}_k^{\mathrm{A3}*})$.

Theorem 3.1: The subgame perfect equilibrium of the kth game in the time interval $[\underline{t}_k, \bar{t}_k]$ satisfies the following:

1) Strategy 1 is the optimal strategy if
   - $\hat{U}^{\mathrm{A2}*} < 0$, or
   - $\hat{U}^{\mathrm{A3}*} < 0$, $\hat{U}^{\mathrm{D3}*} \geq \hat{\lambda}(\mathcal{G}_k^{\mathrm{A3}*})\Delta_k^{\mathrm{A}}$, and $\hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A2}*}) \geq \hat{U}^{\mathrm{D2}}$.
2) Strategy 2 is the optimal strategy if $\hat{U}^{\mathrm{A2}*} \geq 0$ and
   - $\hat{U}^{\mathrm{D3}*} < \hat{\lambda}(\mathcal{G}_k^{\mathrm{A3}*})\Delta_k^{\mathrm{A}}$ or
   - $\hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A2}*}) < \hat{U}^{\mathrm{D2}}$.

   The optimal edges $\mathcal{E}_k^{\mathrm{A}*}$ for the attacker are given by
   - $\mathcal{E}_k^{\mathrm{A3}*}$ if $\hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A2}*}) \geq \hat{U}^{\mathrm{D2}}$,
   - $\mathcal{E}_k^{\mathrm{A2}*}$ otherwise.
3) Strategy 3 is the optimal strategy if $\hat{U}^{\mathrm{A3}*} \geq 0$, $\hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A2}*}) \geq \hat{U}^{\mathrm{D2}}$, and $\hat{U}^{\mathrm{D3}*} > \hat{\lambda}(\mathcal{G}_k^{\mathrm{A3}*})\Delta_k^{\mathrm{A}}$.

This theorem covers all possible cases of actions.

Combinations of the conditions of the possible optimal strategies in all cases are shown in Table III. Note that $\hat{U}^{\mathrm{A2}*} < 0$ and $\hat{U}^{\mathrm{A3}*} \geq 0$ cannot happen.

IV. APPLICATION TO CONSENSUS PROBLEM

In this section, a consensus problem of a multi-agent system in the face of jamming attacks is investigated. Specifically, we apply our game approach to the consensus problem and provide a numerical example.

Let $\mathcal{V} = \{1, 2, \ldots, n\}$ represent the set of agents and $\mathcal{E}$ the set of edges connecting the agents. Let $\mathcal{N}_i(t)$ be the set of neighbors of agent i, i.e., the agents sharing edges with agent i at time t. We assume that the agents communicate with their neighbors continuously in time. Every agent i has the scalar state x_i and the local control input u_i as

$$\dot{x}_i(t) = u_i(t), \quad t \geq 0, \quad x(0) = x_0. \tag{30}$$

If the attacker attacks some edges $\mathcal{E}_k^{\mathrm{A}}$ (resp., the defender recovers $\mathcal{E}_k^{\mathrm{D}}$), then the neighbors of each agent i may change. In this problem setting, it makes sense if the attacker attacks the edges connecting agents that take more different values in states, especially if the utility is the same for different strategies. The same argument applies to the defender's action.

Here we employ the control input $u_i(t)$ with

$$u_i(t) := \sum_{j \in \mathcal{N}_i(t)} (x_j(t) - x_i(t)), \tag{31}$$

so that the state of all agents $x = [x_1, x_2, \ldots, x_n]^{\mathrm{T}}$ is expected to converge to a consensus state x_*.

In this paper, we use the notion of approximate consensus. For a given $\epsilon > 0$, the approximate consensus set $\mathcal{D}_\epsilon \subset \mathbb{R}^n$ is given by $\mathcal{D}_\epsilon := \{x \in \mathbb{R}^n : V(x) \leq \epsilon\}$, where

$$V(x) := \max_{i \in \mathcal{V}} x_i - \min_{i \in \mathcal{V}} x_i, \quad x \in \mathbb{R}^n. \tag{32}$$

We characterize the effect of jamming attacks in terms of the time it takes the agents to reach the approximate consensus set $\mathcal{D}_\epsilon$. In particular, for the initial state $x(0) = x_0 \in \mathbb{R}^n \setminus \mathcal{D}_\epsilon$, the *approximate consensus time* $T_*(x_0)$ is given by

$$T_*(x_0) := \inf\{t \geq 0 : x(t) \in \mathcal{D}_\epsilon\}. \tag{33}$$

In our analysis, we also use the Laplacian matrix $L \in \mathbb{R}^{n \times n}$ associated with graph $\mathcal{G}$. Moreover, let $P := e^{-\gamma^{\mathrm{A}} L}$ and

$$\underline{p} := \max_{j \in \{1,\ldots,n\}} \min_{i \in \{1,\ldots,n\}} P_{i,j}, \tag{34}$$

where $P_{i,j}$ denotes the (i,j)th entry of the matrix P. Notice that since $\mathcal{G}$ is connected and $\gamma^{\mathrm{A}} > 0$, we have $P_{i,j} \in (0,1)$, and hence, $\underline{p} \in (0,1)$.

Proposition 4.1: Consider the multi-agent system (30) and (31) with initial condition $x_0 \in \mathbb{R}^n \setminus \mathcal{D}_\epsilon$. Under the optimal attack and defense strategies for the resilient graph game described in Section III, the approximate consensus

TABLE III

CONDITIONS OF THE OPTIMAL STRATEGY OF ALL CASES

Condition		$\hat{U}^{\mathrm{D3}*} < \hat{\lambda}(\mathcal{G}_k^{\mathrm{A3}*})\Delta_k^{\mathrm{A}}$		$\hat{U}^{\mathrm{D3}*} \geq \hat{\lambda}(\mathcal{G}_k^{\mathrm{A3}*})\Delta_k^{\mathrm{A}}$	
		$\hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A2}*}) < \hat{U}^{\mathrm{D2}}$	$\hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A2}*}) \geq \hat{U}^{\mathrm{D2}}$	$\hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A2}*}) < \hat{U}^{\mathrm{D2}}$	$\hat{U}^{\mathrm{D3}}(\mathcal{E}_k^{\mathrm{A2}*}) \geq \hat{U}^{\mathrm{D2}}$
$\hat{U}^{\mathrm{A2}*} \geq 0$	$\hat{U}^{\mathrm{A3}*} \geq 0$	Strategy 2			Strategy 3
$\hat{U}^{\mathrm{A2}*} \geq 0$	$\hat{U}^{\mathrm{A3}*} < 0$				Strategy 1
$\hat{U}^{\mathrm{A2}*} < 0$	$\hat{U}^{\mathrm{A3}*} < 0$	Strategy 1			

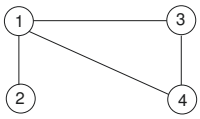

Fig. 2. $\mathcal{G}$ used in simulation.

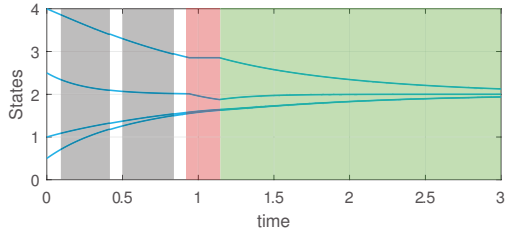

Fig. 3. Simulation result. The grey area indicates the interval where the attacker is able to attack but chooses to be silent. The red and green areas indicate the intervals where the attacker attacks and the defender recovers, respectively.

time satisfies

$$T_*(x_0) \leq \frac{\beta^{\mathrm{A}}(\gamma^{\mathrm{A}} + \gamma^{\mathrm{D}}) \left\lceil \frac{\ln \epsilon - \ln V(x_0)}{\ln(1-\underline{p})} \right\rceil + \kappa^{\mathrm{A}}}{\beta^{\mathrm{A}} - \rho^{\mathrm{A}}}. \quad (35)$$

Proposition 4.1 provides an upper bound of the approximate consensus time in terms of the scalars β^{A}, κ^{A}, ρ^{A} that characterize the attacker's energy constraints together with the scalars γ^{A} and γ^{D} that respectively represent the attacker's and the defender's waiting durations before taking actions in each game.

We demonstrate the efficacy of the presented results in the approximate consensus problem through a numerical example. We use the graph shown in Fig. 2 with $n = 4$, and parameters $\beta^{\mathrm{A}} = 0.4$, $\beta^{\mathrm{D}} = 0.6$, $\kappa^{\mathrm{A}} = 0.5$, $\kappa^{\mathrm{D}} = 1$, $\rho^{\mathrm{A}} = 0.3$, $\rho^{\mathrm{D}} = 0.1$, $\gamma^{\mathrm{A}} = 0.1$, and $\gamma^{\mathrm{D}} = 0.3$. Figs. 3 and 4 show the states of the agents and properties of the players, with the agents eventually achieving approximate consensus in $t \approx 2.1$ with $\epsilon = 0.5$. For comparison, when there is no jamming, it takes $t \approx 1.85$ to achieve the same level of approximate consensus. The boundary in this example is $T_*(x_0) \leq 41.8$.

V. CONCLUSION

We have provided the subgame perfect equilibrium analysis between two players, the attacker and the defender, in terms of communications among agents in a multi-agent system, by considering the generalized edge connectivity of communication graphs. Specifically, we have obtained the optimal strategies of the players in terms of the number of edges and duration of action intervals. For the consensus problem, we have seen that the time for the agents to reach approximate consensus will be delayed due to attacks and have derived an upper bound.

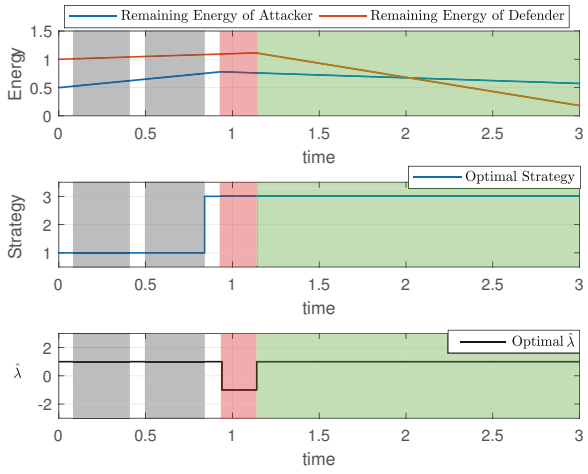

Fig. 4. Properties of the players and the system. In this case, the attacker attacks e_{12} in the 3rd game to make $\hat{\lambda}(\mathcal{G}_3^{\mathrm{A}}) = -1$.

REFERENCES

[1] A. Jadbabaie, J. Lin, and A. Morse, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," *IEEE Trans. Autom. Contr.*, vol. 48, pp. 988–1001, Jun. 2003.

[2] M. Mesbahi and M. Egerstedt, *Graph Theoretic Methods in Multiagent Networks*. Princeton University Press, 2010.

[3] F. Bullo, *Lectures on Network Systems*, 1st ed. CreateSpace, 2018.

[4] J. Chen, C. Touati, and Q. Zhu, "A dynamic game analysis and design of infrastructure network protection and recovery," *SIGMETRICS Perform. Eval. Rev.*, vol. 45, no. 2, p. 128, Oct. 2017.

[5] T. Alpcan and T. Basar, *Network Security: A Decision and Game-Theoretic Approach*. Cambridge University Press, 2010.

[6] A. Khanafer, B. Touri, and T. Basar, "Consensus in the presence of an adversary," in *Proc. of IFAC Workshop on Dist. Est. and Contr. in Netw. Sys.*, 2012, pp. 276–281.

[7] 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, 2017.

[8] Y. Li, L. Shi, P. Cheng, J. Chen, and D. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Trans. Autom. Contr.*, vol. 60, pp. 2831–2836, Oct. 2015.

[9] S. Feng and P. Tesi, "Resilient control under denial-of-service: Robust design," *Automatica*, vol. 79, pp. 42–51, 2017.

[10] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Contr.*, vol. 65, pp. 2930–2944, 2015.

[11] A. Cetinkaya, H. Ishii, and T. Hayakawa, "The effect of time-varying jamming interference of networked stabilization," *SIAM J. Control Optim.*, vol. 56, pp. 2398–2435, 2018.

[12] D. Senejohnny, P. Tesi, and C. De Persis, "A jamming resilient algorithm for self-triggered network coordination," *IEEE Trans. Control Netw. Syst.*, vol. 5, pp. 981–990, 2018.

[13] K. Kikuchi, A. Cetinkaya, T. Hayakawa, and H. Ishii, "Stochastic communication protocols for multi-agent consensus under jamming attacks," in *Proc. of IEEE Conf. on Dec. and Contr.*, Dec. 2017, pp. 1657–1662.

[14] Y. Li, L. Xiao, J. Liu, and Y. Tang, "Power control Stackelberg game in cooperative anti-jamming communications," in *Proc. of Int. Conference on Game Theory for Networks*, Nov. 2014.