Dynamic Resilient Network Games with Applications to Multi-Agent Consensus

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

Abstract—A cyber security problem in a networked system formulated as a resilient graph problem based on a game-theoretic approach is considered. 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. For this two-stage game, we 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 a multi-agent consensus problem, where the game is played repeatedly over time. We study how the attacks and the recovery on the edges affect the consensus process. Finally, we also provide numerical simulation to illustrate the results.

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 [4]. 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.

Noncooperative game theory approaches are widely used for addressing security problems including jamming attacks [5], [6]. Jamming attacks on networked systems were previously analyzed through game-theoretic approaches. The works [7]–[9] model the activity of jamming and transmitting signals as zero-sum games where the payoff structure of the players is balanced. In [10], [11], the authors consider a Stackelberg game approach, in which the players decide their actions sequentially by following a certain hierarchy.

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 is with the Information Systems Architecture Science Research Division, National Institute of Informatics, Tokyo 101-8430, Japan. cetinkaya@nii.ac.jp

Hideaki Ishii is with the Department of Computer Science, Tokyo Insitute of Technology, Yokohama 226-8502, Japan. 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

Multi-agent consensus problems in the presence of such jamming attacks have been studied in [12], [13]. The work [14] introduces a stochastic communication protocol so that the attackers do not know the exact transmission times of the agents in advance. Jamming attack models with energy constraints were introduced in [14]–[17] in the context of networked control. These models have been generalized to further take account of probabilistic packet losses in [17]. 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; the resilience and robustness in such problems have been discussed in [18]–[20]. Also, nonmalicious packet losses that can interrupt the communication among agents have been studied in [21], [22].

However, in the abovementioned works, optimal strategies for the attackers have not been well addressed. In addition, in those works there is also no defense mechanism to mitigate the attacks and restore the communication so as not to simply wait for the attacks to end. On the other hand, there are a limited number of works employing game-theoretic approaches. The work [23] applies game theory to study jamming attacks on the communication links between a team of uncrewed aerial vehicles. A two-player game over networks is discussed in [24], where the players influence the communication signals to maximize/minimize the effect of their actions through a formulation using $\mathcal{H}_2$ norms.

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 [25], where the decision variables are limited to the links in the graphs for both players. In our problem setting, more dynamics are present as the time intervals for attacking and recovering are to be decided as well.

More specifically, in regards to our formulation of resilient graphs, a two-stage game is played by the attacker and the defender with energy constraints. In this game, the attacker decides the links and the durations for the attacks. The attacker's utility depends on the number of connected components of the graph after the attack as well as the energy cost of the attacker. In response to the attacks, the defender attempts to recover some of the links that are important for maintaining the connectivity of the graph. Once the attacker ends attacking, the defender also ends recovering since there are no attacks anymore. Our study is based on the analysis of the subgame perfect equilibria of the games, and we use backward induction to obtain optimal strategies for both players, as in [25].

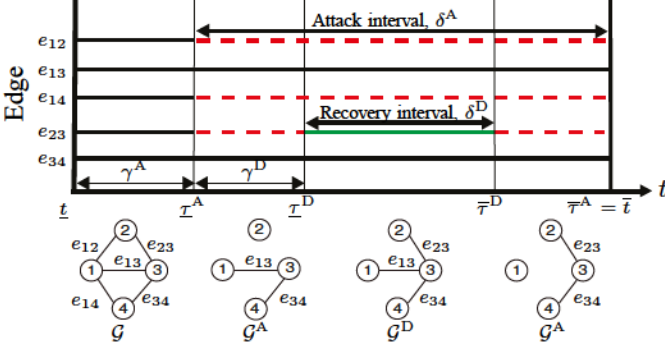We emphasize that our contribution is the introduction

Fig. 1. Illustration of graph transition. At time interval $[\underline{t}, \bar{t}]$, the defender recovers one edge e_{23} at $\underline{\tau}^D$ and stops recovering at $\bar{\tau}^D$. Note that the solid lines indicate that the edges are connected, and dashed lines indicate that the edges are disconnected.

of a game-theoretic framework to jamming attack problems. We follow the attack models dealt with in [14]–[17], where the energy for communication by the players is under time-varying constraints. Moreover, the defender can overcome the attacker's jamming by sending signals with increased signal-to-interference-plus-noise ratio (SINR); such models are employed in [10], [11]. Though the setting is centralized in the sense that both players have control over the networked system, our approach addresses the question on how to design the underlying networks having structures resilient to cyber attacks. As an application of the game problem, we further consider a consensus problem and analyze how the time for reaching consensus is affected by the strategies of the players when the two-stage game is played repeatedly over time.

The paper is organized as follows. In Section II, we introduce the framework for the resilient graph game. In Section III, we analyze the subgame perfect equilibria and characterize the optimal strategies for the players. In Section IV, we apply the obtained results to a consensus problem for multi-agent systems in a repeated game setting. We then provide numerical examples in Section V and conclude the paper in Section VI. Finally, all the proofs for our main results are given in the Appendix. A preliminary version of this paper appeared as [26]; the scenarios considered there are more restricted as the attacker stops attacking only when running out of energy.

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 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 are represented by the edges. We assume that the underlying, attack-free communication topology $\mathcal{G}$ is connected, i.e., there exists a path connecting every pair of vertices in $\mathcal{V}$.

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.

Our problem setting is centralized in that the attacker and the defender know the conditions of the communication networks at each time and have control over the links individually.

That is, the attacker can strategically decide the links to attack while the defender may ask the chosen agents to increase their transmission level to recover their links. As we mentioned in the Introduction, even in such a centralized setting, game-theoretic studies on resilient graphs are very limited. Our game formulation provides insights into networks having resilient structures against adversaries even under a powerful defender having the full knowledge of the system.

The game is played in the time interval $[\underline{t}, \bar{t}]$, which is determined by the players' actions with $\underline{t} < \bar{t}$. We denote the start time of the game as $\underline{t}$, instead of 0, to further generalize the notation for the sequence of games in Section IV below. Initially, at the start time $\underline{t}$, 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 whether to recover some of the attacked links or not. The durations and the links for the attack and the recovery are the action variables. The end time $\bar{t}$ is when the attacker and hence the defender stop their actions. The game may also end after a fixed time duration when no attack occurs.

In the time interval $[\underline{t}, \bar{t}]$, the attacker (resp., the defender) can start and end attacking (resp., recovering) at most once. At the start time $\underline{t}$, the active communication links are prescribed by the original edge set $\mathcal{E}$. We assume that the attacker fully knows the edge set $\mathcal{E}$. More specifically, the attacker attacks $\mathcal{G}$ by deleting some of the existing edges $\mathcal{E}^A \subseteq \mathcal{E}$ from time $\underline{\tau}^A$ until $\bar{\tau}^A$, where $\underline{t} < \underline{\tau}^A \leq \bar{\tau}^A \leq \bar{t}$. Consequently, $\mathcal{G}$ is changed to $\mathcal{G}^A := (\mathcal{V}, \mathcal{E} \setminus \mathcal{E}^A)$ at $\underline{\tau}^A$. For transmitting jamming signals, the attacker spends some 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 interval as $[\underline{\tau}^A, \bar{\tau}^A]$, where the values of $\bar{\tau}^A$ are related to the attacker's energy, as discussed later. If there is no attack, it is understood that $\underline{\tau}^A = \bar{\tau}^A$.

On the other hand, the defender aims to maintain the connectivity of the graph by recovering some of the edges blocked by the attacker. The defender recovers the edges $\mathcal{E}^D$ from time $\underline{\tau}^D$ until $\bar{\tau}^D$, with $\mathcal{E}^D \subseteq \mathcal{E}^A$ and $\underline{t} < \underline{\tau}^A < \underline{\tau}^D \leq \bar{\tau}^D \leq \bar{\tau}^A \leq \bar{t}$. As soon as the defender starts the recovery action at $\underline{\tau}^D$, the graph $\mathcal{G}^A$ is changed to $\mathcal{G}^D := (\mathcal{V}, (\mathcal{E} \setminus \mathcal{E}^A) \cup \mathcal{E}^D))$. 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 $\underline{\tau}^D = \bar{\tau}^D$. We define the recovery interval as $[\underline{\tau}^D, \bar{\tau}^D]$, where values of $\bar{\tau}^D$ are related to the energy of the defender, as discussed later. Once the attacker stops attacking, the attacked edges come back to normal and the graph becomes $\mathcal{G}$ again, which ends the game.

In this formulation, we assume that there is a constant dwell time $\gamma^A > 0$ between the beginning of the game $\underline{t}$ and the beginning of the attack time $\underline{\tau}^A$. For the defender, there is also a constant dwell time $\gamma^D > 0$ between the beginning of attack time $\underline{\tau}^A$ and the beginning of recovery time $\underline{\tau}^D$ unless the attacker ends attacking earlier, i.e., $\bar{\tau}^A < \underline{\tau}^D$. Thus, let

$$\underline{\tau}^A := \underline{t} + \gamma^A, \quad \underline{\tau}^D := \min\{\bar{\tau}^A, \underline{\tau}^A + \gamma^D\}. \quad (1)$$

The lengths of the attack and the recovery intervals are denoted by δ^A and δ^D, respectively, with

$$\delta^A := \bar{\tau}^A - \underline{\tau}^A, \quad \delta^D := \bar{\tau}^D - \underline{\tau}^D. \quad (2)$$

The timeline of the attack and the recovery sequences is

illustrated in Fig. 1.

In the game, both players attempt to choose the best strategies to maximize their own utility functions defined as how much the agents are connected or disconnected over the time interval $[\underline{t}, \overline{t}]$. To characterize how much the agents are connected or disconnected in a unified way, we introduce the generalized edge connectivity $\widehat{\lambda}(\mathcal{G}')$ as an extension of the notion of edge connectivity for the graph $\mathcal{G}'$. It is defined as

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

where $\lambda(\mathcal{G}')$ denotes the edge connectivity of the graph $\mathcal{G}'$, i.e., the minimum number of edges required to be removed to make the connected graph $\mathcal{G}'$ disconnected. On the other hand, $\widetilde{\lambda}(\mathcal{G}')$ denotes the minimum number of edges required to make the disconnected graph $\mathcal{G}'$ connected; in this case, there are $\widetilde{\lambda}(\mathcal{G}') + 1$ connected components in the disconnected graph $\mathcal{G}'$, since one edge is needed to connect two connected components. Note that a larger positive value of $\widehat{\lambda}$ implies that the graph $\mathcal{G}$ has more links to be removed by the attacker, and a smaller negative value of $\widehat{\lambda}$ indicates that the graph $\mathcal{G}$ requires more links to be recovered by the defender. Since $\mathcal{G}^A \subseteq \mathcal{G}^D \subseteq \mathcal{G}$, note that $\widehat{\lambda}(\mathcal{G}^A) \leq \widehat{\lambda}(\mathcal{G}^D) \leq \widehat{\lambda}(\mathcal{G})$.

The attacker chooses the optimal edges to attack based on the generalized edge connectivity $\widehat{\lambda}(\mathcal{G})$ of the graph $\mathcal{G}$, and the defender chooses the optimal edges to recover based on the generalized edge connectivity of the graph $\mathcal{G}^A$. The attacker should strategically choose the edges to jam to reduce $\widehat{\lambda}(\mathcal{G}^A)$ (making $\mathcal{G}^A$ more disconnected), and the defender also should choose the edges to efficiently increase $\widehat{\lambda}(\mathcal{G}^D)$ (making $\mathcal{G}^D$ more connected).

Note that for the same number of edges to attack/recover, there may be multiple optimal choices of edges to attack/recover that yield the same values of $\widehat{\lambda}(\mathcal{G}^A)$ or $\widehat{\lambda}(\mathcal{G}^D)$. Since we focus on the connectivity of the agents to characterize the utility functions below without specifying particular edges to attack/recover, we define $\widehat{\lambda}_{\mathcal{G}}(m^A, m^D)$ to represent the generalized edge connectivity of the underlying graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with $m^A = |\mathcal{E}^A|$ edges attacked and $m^D = |\mathcal{E}^D|$ edges recovered, given by

$$\widehat{\lambda}_{\mathcal{G}}(m^A, m^D) := \min_{\mathcal{E}^A : |\mathcal{E}^A| = m^A} \max_{\mathcal{E}^D : |\mathcal{E}^D| = m^D} \widehat{\lambda}((\mathcal{V}, (\mathcal{E} \backslash \mathcal{E}^A) \cup \mathcal{E}^D)). \quad (4)$$

For the simple case of $m^D = 0$, calculating the right-hand side in (4) reduces to the min-cut problem for undirected and unweighted graph $\mathcal{G}$, for which efficient randomized algorithms are available [27]. More in general, we can apply the so-called k-cut algorithms [28] by increasing the number k of the connected components. Thus, in principle, the players can obtain the full solution *offline* prior to playing the game.

This $\widehat{\lambda}_{\mathcal{G}}$ can be presented as a lower triangular matrix $\widehat{\lambda}_{\mathcal{G}} \in \mathbb{R}^{(|\mathcal{E}|+1) \times (|\mathcal{E}|+1)}$, where $\widehat{\lambda}_{\mathcal{G}}(m^A, m^D)$ represents the $(m^A + 1, m^D + 1)$ entry of the matrix. For example, the matrix $\widehat{\lambda}_{\mathcal{G}}$ for the graph $\mathcal{G}$ in Fig. 1 is given by

$$\widehat{\lambda}_{\mathcal{G}} = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 \\ -1 & 1 & 2 & 0 & 0 & 0 \\ -1 & 1 & 1 & 2 & 0 & 0 \\ -2 & -1 & 1 & 1 & 2 & 0 \\ -3 & -2 & -1 & 1 & 1 & 2 \end{bmatrix}.$$

In general, the matrix $\widehat{\lambda}_{\mathcal{G}}$ is not Toeplitz, i.e., the values of the (i, j) entries with the same $i - j$ may be different. We also note that the values for the same row/column do not change linearly and that attacking/recovering more number of edges does not necessarily change the graph connectivity.

The strategies of the attacker and the defender are in terms of (m^A, δ^A) and (m^D, δ^D), respectively. For the game of the time interval $[\underline{t}, \overline{t}]$, we define the utility function U^A of the attacker as

$$U^A((m^A, \delta^A), (m^D, \delta^D))$$
$$:= -\widehat{\lambda}_{\mathcal{G}}(m^A, 0)(\delta^A - \delta^D) - \widehat{\lambda}_{\mathcal{G}}(m^A, m^D)\delta^D - \beta^A m^A \delta^A, \quad (5)$$

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

$$U^D((m^A, \delta^A), (m^D, \delta^D))$$
$$:= \widehat{\lambda}_{\mathcal{G}}(m^A, 0)(\delta^A - \delta^D) + \widehat{\lambda}_{\mathcal{G}}(m^A, m^D)\delta^D - \beta^D m^D \delta^D, \quad (6)$$

where $\beta^D > 0$ is the defender's cost to recover one edge per time unit. Note that the utility function (5) represents the total generalized edge connectivity (with the negative sign) for the attacker over the game horizon $[\underline{\tau}^A, \overline{t}]$ plus the cost for jamming m^A number of communication links. Similarly, (6) represents the total generalized edge connectivity for the defender over the game horizon $[\underline{\tau}^A, \overline{t}]$ plus the cost for recovering m^D number of communication links. We assume that each player knows all parameters of the other player.

If the attacker decides to attack at least one edge, then the game ends at $\overline{\tau}^A$. Otherwise, the game ends at $\underline{t} + \gamma^A + \gamma^D$. In other words, the end time $\overline{t}$ of the game is

$$\overline{t} := \begin{cases} \overline{\tau}^A, & \text{if } m^A > 0, \\ \underline{t} + \gamma^A + \gamma^D, & \text{otherwise.} \end{cases} \quad (7)$$

According to the utility functions (5) and (6), there is a case where the defender stops recovering m^D number of links before the game ends while the attacker keeps sending jamming signals to m^A number of links. In this case, the graph changes back to $\mathcal{G}^A$ at $\overline{\tau}^D$, with generalized edge connectivity $\widehat{\lambda}_{\mathcal{G}}(m^A, 0)$. Therefore, in $[\overline{\tau}^D, \overline{t}]$, the utilities of both players in (5) and (6) are computed based on $\widehat{\lambda}_{\mathcal{G}}(m^A, 0)$.

The players cannot keep sending signals for very long durations due to energy constraints. We assume that if player $p \in \{A, D\}$ keeps sending jamming/recovering signals starting at time $\underline{\tau}^p$, it will run out of energy after attacking/recovering for $\Delta^p(m^p) > 0$ duration, i.e., $\delta^p \in [0, \Delta^p(m^p)]$, $m^p > 0$. It is assumed that $\Delta^p(m^p)$ is given throughout the discussion in Sections II and III.

We formulate the game as a two-stage game where the attacker first attacks and then the defender makes recoveries. It is, however, noted that there would be a preceding stage, which is implicit in our formulation; this stage is related to the design of the network structure of the underlying graph $\mathcal{G}$. The underlying graph is assumed to be given in this paper, but clearly affects the game as it is the default network at the start of the game. In this respect, our formulation will be useful in finding resilient networks under hostile environments.

We seek the subgame perfect equilibrium of the game as in [25]. To this end, one needs to divide the game into

some subgames. The equilibrium must be optimal in every subgame. The defender's game is formulated as a subgame of the attacker's game. Therefore, the attacker also maximizes the defender's utility function to obtain the defender's best strategy given the attacker's strategy, and uses the defender's best strategy to formulate the best strategy for the attacker. To obtain the optimal strategy for each player, *backward induction* is used in the game consisting of two-stage decision-making levels corresponding to the attack and recovery sequences.

In the time interval $[\underline{t}, \overline{t}]$, given the attacker's strategy $(m^{\mathrm{A}}, \delta^{\mathrm{A}})$, the defender decides the strategy as

$$
\begin{aligned}
(m^{\mathrm{D}*}&(m^{\mathrm{A}}, \delta^{\mathrm{A}}), \delta^{\mathrm{D}*}(m^{\mathrm{A}}, \delta^{\mathrm{A}})) \\
&\in \arg \max_{(m^{\mathrm{D}}, \delta^{\mathrm{D}})} U^{\mathrm{D}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}}, \delta^{\mathrm{D}})),
\end{aligned} \quad (8)
$$

with m^{D} and δ^{D} depending on m^{A} and δ^{A}. Likewise, given the initial graph $\mathcal{G}$, the attacker decides the strategy as

$$
\begin{aligned}
(m^{\mathrm{A}*}&, \delta^{\mathrm{A}*}) \\
&\in \arg \max_{(m^{\mathrm{A}}, \delta^{\mathrm{A}})} U^{\mathrm{A}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}*}(m^{\mathrm{A}}, \delta^{\mathrm{A}}), \delta^{\mathrm{D}*}(m^{\mathrm{A}}, \delta^{\mathrm{A}}))).
\end{aligned}
$$
$$(9)$$

We study the subgame perfect equilibrium and seek pairs $(m^{\mathrm{A}}, \delta^{\mathrm{A}})$ and $(m^{\mathrm{D}}, \delta^{\mathrm{D}})$ such that $(m^{\mathrm{D}}, \delta^{\mathrm{D}})$ is the best response to $(m^{\mathrm{A}}, \delta^{\mathrm{A}})$. The combination of strategies $((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}}, \delta^{\mathrm{D}}))$ that follows the subgame perfect equilibrium principle is called the *optimal combined strategy*. A tie-break condition happens if the players have multiple options for the 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.

III. GAME ANALYSIS

In this section, we discuss the subgame perfect equilibrium formulation and the strategies of the players on the time interval $[\underline{t}, \overline{t}]$. Here, for simplicity of notation, we omit the variable m^{A} (resp., m^{D}) for the presentation of Δ^{A} (resp., Δ^{D}).

A. Brief Summary of the Results

We first provide a summary of the results. To characterize the optimal strategies, from the sequence of actions by the attacker and the defender described in the previous section, we categorize the possible combinations of generalized edge connectivities $\widehat{\lambda}(\mathcal{G})$, $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)$, and $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}})$ into three cases shown in Table I. Note that these cases cover all the possible combinations of the actions by both players. Since $m^{\mathrm{D}} \leq m^{\mathrm{A}}$, it is impossible to have $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0) = \widehat{\lambda}(\mathcal{G})$ and $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) > \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)$. Also, note that since by definition $m^{\mathrm{D}} \geq 0$, condition $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) < \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)$ cannot be fulfilled. Furthermore, even if the attacker attacks some edges of $\mathcal{E}$, there is a possibility that the edge connectivity does not change, as in Case 1. The same remark applies to the recovery action. As a result, there are four possible optimal combined strategies that are derived from the three cases in Table I. A summary of the results of the optimal strategies is shown in Table II. Note that it may be optimal for the attacker to continue attacking even after the recovery finishes, since the attacker gets higher utility in $[\overline{\tau}^{\mathrm{D}}, \overline{\tau}^{\mathrm{A}}]$.

TABLE I
POSSIBLE CASES OF ATTACK AND RECOVERY ACTIONS

Case	$\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)$	$\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}})$
1	$\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0) = \widehat{\lambda}(\mathcal{G})$	$\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) = \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)$
2	$\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0) < \widehat{\lambda}(\mathcal{G})$	$\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) = \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)$
3	$\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0) < \widehat{\lambda}(\mathcal{G})$	$\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) > \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)$

TABLE II
OPTIMAL COMBINED STRATEGY CANDIDATES

Comb. Str.	Action
1	Attacker: No attack Defender: No need to recover
2a	Attacker: Attacks the optimal edges for Δ^{A} duration Defender: No recovery
2b	Attacker: Attacks the optimal edges until $\underline{\tau}^{\mathrm{D}}$ Defender: No chance to recover
3	Attacker: Attacks the optimal edges for Δ^{A} duration Defender: Recovers the optimal edges for $\min\{\Delta^{\mathrm{D}}, \Delta^{\mathrm{A}} + \underline{\tau}^{\mathrm{A}} - \underline{\tau}^{\mathrm{D}}\}$ duration

B. Subgame Perfect Equilibrium Analysis

In this subsection, 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 $\widehat{\lambda}(\mathcal{G}) \geq \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) \geq \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)$, we obtain three cases based on the combinations of $\widehat{\lambda}(\mathcal{G})$, $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)$, and $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}})$, as shown in Table I. We analyze the subgame perfect equilibrium for the time interval $[\underline{t}, \overline{t}]$ in each case. The results in terms of links and durations of the optimal combined strategy candidates are summarized in Table III.

Case 1: In this case, we show that the optimal strategy for the players are not to recover any edge, i.e., $m^{\mathrm{A}*}, m^{\mathrm{D}*} = 0$. By Table I, the utility function in (6) of the defender becomes

$$
U^{\mathrm{D}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}}, \delta^{\mathrm{D}})) = \widehat{\lambda}(\mathcal{G})\delta^{\mathrm{A}} - \beta^{\mathrm{D}} m^{\mathrm{D}} \delta^{\mathrm{D}}. \quad (10)
$$

Furthermore, because the defender receives no reward by recovering any link, the optimal strategy for the defender is $m^{\mathrm{D}*} = 0$ and $\delta^{\mathrm{D}*} = 0$, resulting in

$$
U^{\mathrm{D}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*})) = \widehat{\lambda}(\mathcal{G})\delta^{\mathrm{A}}. \quad (11)
$$

This strategy $m^{\mathrm{D}*} = 0$ and $\delta^{\mathrm{D}*} = 0$ for the defender is named **Strategy D1** (see Table III).

Likewise, for the attacker, the utility function in (5) becomes

$$
U^{\mathrm{A}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*})) = (-\widehat{\lambda}(\mathcal{G}) - \beta^{\mathrm{A}} m^{\mathrm{A}})\delta^{\mathrm{A}}. \quad (12)
$$

It is then clear that the optimal strategy for the attacker is $m^{\mathrm{A}*} = 0$ and $\delta^{\mathrm{A}*} = 0$. As a result, the utility functions in Case 1 are given by

$$
U^{\mathrm{A}}((m^{\mathrm{A}*}, \delta^{\mathrm{A}*}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*})) = 0 =: \hat{U}^{\mathrm{A}1}, \quad (13)
$$
$$
U^{\mathrm{D}}((m^{\mathrm{A}*}, \delta^{\mathrm{A}*}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*})) = 0 =: \hat{U}^{\mathrm{D}1}. \quad (14)
$$

From (7), because $m^{\mathrm{A}} = m^{\mathrm{D}} = 0$, it follows that the game ends at $\overline{t} = \underline{t} + \gamma^{\mathrm{A}} + \gamma^{\mathrm{D}}$. This optimal strategy candidate $m^{\mathrm{A}}, \delta^{\mathrm{A}} = 0$ for the attacker is classified as **Strategy A1**. In this case, the optimal combined strategy corresponding

TABLE III
LINKS AND DURATIONS OF THE OPTIMAL COMBINED STRATEGY CANDIDATES

Comb. Str.	Att. Str.	$m^{\mathrm{A}*}$	$\delta^{\mathrm{A}*}$	Def. Str.	$m^{\mathrm{D}*}$	$\delta^{\mathrm{D}*}$
1	A1	0	0	D1	0	0
2a	A2a	$m^{\mathrm{A2a}*}$	$\Delta^{\mathrm{A}}(m^{\mathrm{A2a}*})$			
2b	A2b	$m^{\mathrm{A2b}*}$	$\underline{\tau}^{\mathrm{D}} - \underline{\tau}^{\mathrm{A}}$			
3	A3	$m^{\mathrm{A3}*}$	$\Delta^{\mathrm{A}}(m^{\mathrm{A3}*})$	D3	$m^{\mathrm{D3}*}(m^{\mathrm{A3}*})$	ξ

to $((m^{\mathrm{A}*}, \delta^{\mathrm{A}*}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*}))$ is then labelled as **Combined Strategy 1 := (Strategy A1, Strategy D1)**.

Case 2: In this case, we show that the attacker's optimal strategy is to attack until running out of energy, whereas the optimal strategy for the defender is not to recover any edge.

Similarly with the analysis in Case 1, because $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) = \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)$, the utility function of the defender with $m^{\mathrm{D}*}, \delta^{\mathrm{D}*} = 0$ as in (11) is given by

$$U^{\mathrm{D}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*})) = \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)\delta^{\mathrm{A}}. \quad (15)$$

For the attacker, from (5) with $\delta^{\mathrm{D}} = 0$, we have

$$U^{\mathrm{A}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*})) = (-\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0) - \beta^{\mathrm{A}}m^{\mathrm{A}})\delta^{\mathrm{A}}. \quad (16)$$

If $-\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0) - \beta^{\mathrm{A}}m^{\mathrm{A}} > 0$, the attacker maximizes δ^{A}, by attacking as long as possible. Hence, $\delta^{\mathrm{A}} = \Delta^{\mathrm{A}}$, and

$$U^{\mathrm{A}}((m^{\mathrm{A}}, \delta^{\mathrm{A}*}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*}))$$
$$= (-\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0) - \beta^{\mathrm{A}}m^{\mathrm{A}})\Delta^{\mathrm{A}} =: \hat{U}^{\mathrm{A2a}}(m^{\mathrm{A}}). \quad (17)$$

Now we only need to choose m^{A}, as δ^{A} is already determined. Specifically, we search for $m^{\mathrm{A2a}*}$, which denotes the optimal m^{A}. This is done by maximizing the simplified utility $\hat{U}^{\mathrm{A2a}}(m^{\mathrm{A}})$ in (17), resulting in

$$m^{\mathrm{A2a}*} \in \arg\max_{m^{\mathrm{A}}>0} \hat{U}^{\mathrm{A2a}}(m^{\mathrm{A}}). \quad (18)$$

Note that with this strategy, (15) becomes

$$U^{\mathrm{D}}((m^{\mathrm{A}*}, \delta^{\mathrm{A}*}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*})) = \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A2a}*}, 0)\Delta^{\mathrm{A}} =: \hat{U}^{\mathrm{D2a}}. \quad (19)$$

The attacker's strategy in this case is specified as **Strategy A2a**, which is $m^{\mathrm{A}} = m^{\mathrm{A2a}*}$ and $\delta^{\mathrm{A}} = \Delta^{\mathrm{A}}$. This combination of strategies of $((m^{\mathrm{A}*}, \delta^{\mathrm{A}*}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*}))$ is labelled as **Combined Strategy 2a := (Strategy A2a, Strategy D1)**.

Case 3: In this case, we show that the optimal strategy for the attacker is to attack the optimal edges until running out of energy or to attack until the defender starts to recover, whereas the optimal strategy for the defender is to recover the optimal edges until the defender runs out of energy or the attacker ends attacking. In this case, by Table I, the generalized edge connectivities satisfy $\widehat{\lambda}(\mathcal{G}) \geq \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) > \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)$.

From (6), the defender's utility function can be written as

$$U^{\mathrm{D}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}}, \delta^{\mathrm{D}})) = \phi\delta^{\mathrm{D}} + \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)\delta^{\mathrm{A}}, \quad (20)$$

with $\phi := (\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) - \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0) - \beta^{\mathrm{D}}m^{\mathrm{D}})$ for simplicity. Since $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0) < \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}})$, in order to maximize the term $\phi\delta^{\mathrm{D}}$, the defender recovers m^{D} links as long as possible if $\phi \geq 0$, so that $\overline{\tau}^{\mathrm{D}} = \min\{\Delta^{\mathrm{D}} + \underline{\tau}^{\mathrm{D}}, \overline{\tau}^{\mathrm{A}}\}$. Alternatively, if $\phi < 0$, then the defender should not recover. It follows that

the utility function of the defender becomes

$$U^{\mathrm{D}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}}, \min\{\Delta^{\mathrm{D}}, \overline{\tau}^{\mathrm{A}} - \underline{\tau}^{\mathrm{D}}\}))$$
$$= \phi(\min\{\Delta^{\mathrm{D}}, \overline{\tau}^{\mathrm{A}} - \underline{\tau}^{\mathrm{D}}\}) + \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)\delta^{\mathrm{A}}. \quad (21)$$

Since the attacker is able to attack for Δ^{A}, we divide the analysis for this case into two parts: (i) the attacker ends attacking before $\Delta^{\mathrm{D}} + \underline{\tau}^{\mathrm{D}}$, and (ii) the attacker ends attacking after $\Delta^{\mathrm{D}} + \underline{\tau}^{\mathrm{D}}$.

(i) In this case, the attacker ends the game before the defender finishes the recovery attempt that would have lasted for Δ^{D} units of time. However, since the attacker ends the game earlier, the recovery duration is only $\overline{\tau}^{\mathrm{A}} - \underline{\tau}^{\mathrm{D}}$ units of time. Thus, we have $\overline{\tau}^{\mathrm{D}} = \overline{\tau}^{\mathrm{A}} = \overline{t}$, and the attacker's utility function in (5) can be stated as

$$U^{\mathrm{A}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}}, (\overline{\tau}^{\mathrm{A}} - \underline{\tau}^{\mathrm{D}})))$$
$$= (-\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0) - \beta^{\mathrm{A}}m^{\mathrm{A}})(\underline{\tau}^{\mathrm{D}} - \underline{\tau}^{\mathrm{A}})$$
$$+ (-\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) - \beta^{\mathrm{A}}m^{\mathrm{A}})(\overline{\tau}^{\mathrm{A}} - \underline{\tau}^{\mathrm{D}}). \quad (22)$$

(ii) In this case, the attacker ends the game after the defender finishes the recovery attempt. Hence, $\overline{\tau}^{\mathrm{D}} = \Delta^{\mathrm{D}} + \underline{\tau}^{\mathrm{D}}$, where the utility function for the attacker keeps the form as in (5).

Combined Strategy 3: From (i) and (ii) above, one of the obvious choices for the attacker is to attack for Δ^{A} duration. Depending on the value of Δ^{A}, the attacker can end attacking before or after $\Delta^{\mathrm{D}} + \underline{\tau}^{\mathrm{D}}$. If the attacker ends attacking before $\Delta^{\mathrm{D}} + \underline{\tau}^{\mathrm{D}}$, then $\overline{t} = \overline{\tau}^{\mathrm{D}} = \Delta^{\mathrm{A}} + \underline{\tau}^{\mathrm{A}}$. Otherwise, the defender recovers for Δ^{D}, and $\Delta^{\mathrm{D}} + \underline{\tau}^{\mathrm{D}} < \overline{t} = \Delta^{\mathrm{A}} + \underline{\tau}^{\mathrm{A}}$. Hence, we can rewrite (21) as

$$U^{\mathrm{D}}((m^{\mathrm{A}}, \Delta^{\mathrm{A}}), (m^{\mathrm{D}}, \xi)) = \phi\xi + \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)\delta^{\mathrm{A}}$$
$$=: \hat{U}^{\mathrm{D3}}(m^{\mathrm{A}}, m^{\mathrm{D}}), \quad (23)$$

with

$$\xi := \min\{\Delta^{\mathrm{D}}, \Delta^{\mathrm{A}} + \underline{\tau}^{\mathrm{A}} - \underline{\tau}^{\mathrm{D}}\}. \quad (24)$$

Then the optimal number of edges to be recovered for given m^{A} is obtained by

$$m^{\mathrm{D3}*}(m^{\mathrm{A}}) \in \arg\max_{m^{\mathrm{D}}>0} \hat{U}^{\mathrm{D3}}(m^{\mathrm{A}}, m^{\mathrm{D}}). \quad (25)$$

The utility function of the attacker can be rewritten as

$$U^{\mathrm{A}}((m^{\mathrm{A}}, \delta^{\mathrm{A}*}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*}))$$
$$= -\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)(\Delta^{\mathrm{A}} - \xi) - \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D3}*})\xi - \beta^{\mathrm{A}}m^{\mathrm{A}}\Delta^{\mathrm{A}}$$
$$=: \hat{U}^{\mathrm{A3}}(m^{\mathrm{A}}). \quad (26)$$

The attacker looks for the optimal number of edges $m^{\mathrm{A3}*}$ by maximizing the simplified utility function $\hat{U}^{\mathrm{A3}}(m^{\mathrm{A}})$. Specifically,

$$m^{\mathrm{A3}*} \in \arg\max_{m^{\mathrm{A}}>0} \hat{U}^{\mathrm{A3}}(m^{\mathrm{A}}). \quad (27)$$

Note that to obtain $m^{\mathrm{A3}*}$, the attacker needs to obtain $m^{\mathrm{D3}*}$ first. Hence, the attacker solves the maximization problem in (25) beforehand to obtain $m^{\mathrm{D3}*}(m^{\mathrm{A}})$. This strategy for the attacker is named as **Strategy A3**.

Finally, after the attacker obtains $m^{\mathrm{A3}*}$, the defender searches for $m^{\mathrm{D3}*}$, based on $\hat{U}^{\mathrm{D3}}(m^{\mathrm{A3}*}, m^{\mathrm{D}})$ in (23), as

$$m^{\mathrm{D3}*}(m^{\mathrm{A3}*}) \in \arg\max_{m^{\mathrm{D}}>0} \hat{U}^{\mathrm{D3}}(m^{\mathrm{A3}*}, m^{\mathrm{D}}). \quad (28)$$

This strategy $m^{\mathrm{D}} = m^{\mathrm{D3}*}(m^{\mathrm{A3}*})$, $\delta^{\mathrm{D}} = \xi$ for the defender

is labelled as **Strategy D3.** We call this combined strategy as **Combined Strategy 3 := (Strategy A3, Strategy D3)**.

Combined Strategy 2b: Another choice of the attacker is to end attacking at $\underline{\tau}^{\mathrm{D}}$, which is preferred if $-\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) - \beta^{\mathrm{A}} m^{\mathrm{A}} < 0$ (from the second term of (22)), i.e., the cost of attacking is too high at interval $[\underline{\tau}^{\mathrm{D}}, \overline{\tau}^{\mathrm{A}}]$. Since the attacker ends attacking at $\underline{\tau}^{\mathrm{D}}$, the defender cannot recover any edge (Strategy D1), i.e., $m^{\mathrm{D}} = 0$ and $\delta^{\mathrm{D}} = 0$. Consequently, the attacker's utility function becomes

$$U^{\mathrm{A}}((m^{\mathrm{A}}, \delta^{\mathrm{A}*}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*}))$$
$$= (-\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0) - \beta^{\mathrm{A}} m^{\mathrm{A}})(\underline{\tau}^{\mathrm{D}} - \underline{\tau}^{\mathrm{A}}) =: \hat{U}^{\mathrm{A2b}}(m^{\mathrm{A}}). \quad (29)$$

As in the previous strategy, the attacker looks for the optimal number of edges $m^{\mathrm{A2b}*}$ by maximizing the simplified utility function $\hat{U}^{\mathrm{A2b}}(m^{\mathrm{A}})$. Specifically,

$$m^{\mathrm{A2b}*} \in \arg \max_{m^{\mathrm{A}} > 0} \hat{U}^{\mathrm{A2b}}(m^{\mathrm{A}}). \quad (30)$$

Strategy $m^{\mathrm{A}} = m^{\mathrm{A2b}*}$ and $\delta^{\mathrm{A}} = \underline{\tau}^{\mathrm{D}} - \underline{\tau}^{\mathrm{A}}$ for the attacker is specified as **Strategy A2b**. Note that with this strategy, utility function in (20) becomes

$$U^{\mathrm{D}}((m^{\mathrm{A}*}, \delta^{\mathrm{A}*}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*})) = \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A2b}*}, 0)\Delta^{\mathrm{A}} =: \hat{U}^{\mathrm{D2b}}. \quad (31)$$

As $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0) < \widehat{\lambda}(\mathcal{G})$ and $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) = \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)$, this optimal strategy of $((m^{\mathrm{A}*}, \delta^{\mathrm{A}*}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*}))$ is named as **Combined Strategy 2b := (Strategy A2b, Strategy D1)**.

2) Subgame Perfect Equilibrium Analysis of All Cases: Here, we discuss the subgame perfect equilibrium analysis of the system among all cases. Specifically, we find the strategy that yields the maximum utility out of the four possible combined strategies described in Section III.B.1, in accordance with the subgame perfect equilibrium principle. This is done by applying the backward induction method to the maximum values of the simplified utility functions $\hat{U}^{\mathrm{A1}}$, $\hat{U}^{\mathrm{A2a}*} := \hat{U}^{\mathrm{A2a}}(m^{\mathrm{A2a}*})$, $\hat{U}^{\mathrm{A2b}*} = \hat{U}^{\mathrm{A2b}}(m^{\mathrm{A2b}*})$, $\hat{U}^{\mathrm{A3}*} := \hat{U}^{\mathrm{A3}}(m^{\mathrm{A3}*})$, $\hat{U}^{\mathrm{D1}}$, $\hat{U}^{\mathrm{D2a}}$, $\hat{U}^{\mathrm{D2b}}$, and $\hat{U}^{\mathrm{D3}*} := \hat{U}^{\mathrm{D3}}(m^{\mathrm{A3}*}, m^{\mathrm{D3}*}(m^{\mathrm{A3}*}))$.

We first state properties of utility functions in some strategies. In Lemma 3.1, we state that the attacker's utility without recovery is always higher than the one with recovery by the defender, for the same m^{A} and δ^{A}. Lemmas 3.2 and 3.3 characterize the properties of $\hat{U}^{\mathrm{A2a}*}$, $\hat{U}^{\mathrm{A2b}*}$, and $\hat{U}^{\mathrm{A3}*}$ in terms of their values relative to others.

Lemma 3.1: For all possible combinations of m^{D} and δ^{D}, it holds $U^{\mathrm{A}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (0, 0)) \geq U^{\mathrm{A}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}}, \delta^{\mathrm{D}}))$.

Lemma 3.2: For any possible $m^{\mathrm{A2a}*}$ and $m^{\mathrm{A3}*}$, it follows that $\hat{U}^{\mathrm{A2a}*} \geq \hat{U}^{\mathrm{A3}*}$.

Lemma 3.3: $\hat{U}^{\mathrm{A2a}*}$ has the same sign with $\hat{U}^{\mathrm{A2b}*}$. Also, $\hat{U}^{\mathrm{A2a}*} \geq \hat{U}^{\mathrm{A2b}*}$ if $\hat{U}^{\mathrm{A2a}*} > 0$.

We are now ready to state the main result of this paper. Since $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}})$ is a nonlinear function of m^{A} and m^{D} and its particular form depends on the underlying graph $\mathcal{G}$, the utility functions cannot be represented as simple functions of the action and energy variables except for certain cases. For this reason, we present our general result in terms of the
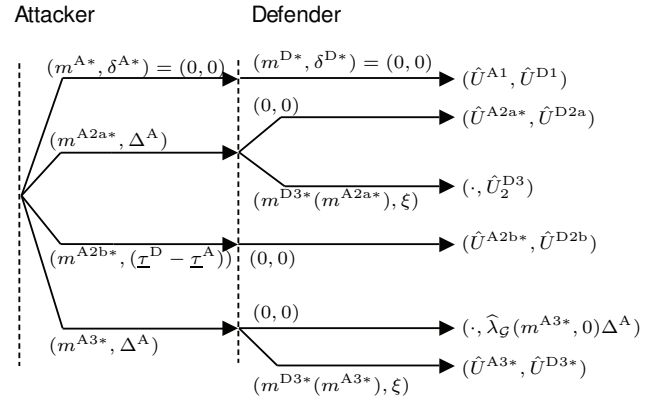

Fig. 2. Illustration of possible optimal strategies. Arrows that represent possible actions of the attacker and the defender lead to pairs of utilities obtained under those actions. The dot in the attacker's utilities in $(\cdot, \hat{U}_2^{\mathrm{D3}})$ and $(\cdot, \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A3}*}, 0)\Delta^{\mathrm{A}})$ means that those utilities are not considered to find the optimal strategy.

functions $\hat{U}^{*}$. In particular, we use $\hat{U}_0^{\mathrm{A3}}$ and $\underline{m}^{\mathrm{A}*}$ defined by

$$\hat{U}_0^{\mathrm{A3}} := \max_{m^{\mathrm{A}} \in \mathcal{M}} \hat{U}^{\mathrm{A2a}}(m^{\mathrm{A}}), \quad (32)$$

$$\underline{m}^{\mathrm{A}*} \in \arg \max_{m^{\mathrm{A}} \in \mathcal{M}} \hat{U}^{\mathrm{A2a}}(m^{\mathrm{A}}), \quad (33)$$

where $\mathcal{M} := \{\underline{m}^{\mathrm{A}} \in \{0, |\mathcal{E}|\} : \widehat{\lambda}_{\mathcal{G}}(\underline{m}^{\mathrm{A}}, m^{\mathrm{D3}*}) - \widehat{\lambda}_{\mathcal{G}}(\underline{m}^{\mathrm{A}}, 0) - \beta^{\mathrm{D}} m^{\mathrm{D3}*} < 0\}$. Furthermore, we let $\hat{U}_2^{\mathrm{D3}} := \hat{U}^{\mathrm{D3}}(m^{\mathrm{A2a}*}, m^{\mathrm{D3}*}(m^{\mathrm{A2a}*}))$.

Theorem 3.4: The subgame perfect equilibrium of the game in the time interval $[\underline{t}, \overline{t}]$ satisfies the following:

1) Combined Strategy 1 is optimal if $\hat{U}^{\mathrm{A2a}*} < 0$.
2) Combined Strategy 2a is optimal if $\hat{U}^{\mathrm{A2a}*} \geq 0$ and
   a) $\hat{U}_2^{\mathrm{D3}} < \hat{U}^{\mathrm{D2a}}$, or
   b) $\hat{U}_2^{\mathrm{D3}} \geq \hat{U}^{\mathrm{D2a}}$ and
      I) $\hat{U}^{\mathrm{A3}*} < \hat{U}^{\mathrm{A2b}*}$ and $\hat{U}_0^{\mathrm{A3}} > \hat{U}^{\mathrm{A2b}*}$, or
      II) $\hat{U}^{\mathrm{A3}*} \geq \hat{U}^{\mathrm{A2b}*}$ and $\hat{U}_0^{\mathrm{A3}} > \hat{U}^{\mathrm{A3}*}$.
   In these cases (a) and (b) above, the optimal number of edges $m^{\mathrm{A}*}$ for the attacker to attack are $m^{\mathrm{A2a}*}$ and $\underline{m}^{\mathrm{A}*}$, respectively .
3) Combined Strategy 2b is optimal if $\hat{U}^{\mathrm{A2a}*} \geq 0$, $\hat{U}_2^{\mathrm{D3}} \geq \hat{U}^{\mathrm{D2a}}$, $\hat{U}^{\mathrm{A2b}*} > \hat{U}^{\mathrm{A3}*}$, and $\hat{U}^{\mathrm{A2b}*} > \hat{U}_0^{\mathrm{A3}}$.
4) Combined Strategy 3 is optimal if $\hat{U}^{\mathrm{A3}*} \geq \hat{U}^{\mathrm{A2b}*} \geq 0$, $\hat{U}_2^{\mathrm{D3}} \geq \hat{U}^{\mathrm{D2a}}$, and $\hat{U}_0^{\mathrm{A3}} \leq \hat{U}^{\mathrm{A3}*}$.

The combined strategies above cover all possible cases.

Possible optimal strategies for both players are illustrated in Fig. 2. Moreover, combinations of the conditions of the possible optimal strategies in all cases are shown in Table IV. We also note that even if the unit costs β^{A} and β^{D} for attacking/recovering one edge per time depend on edges, the procedure to find the optimal combined strategies as in Theorem 3.4 does not change.

From the optimal strategies in Theorem 3.4, we can state some corollaries about the effects of the uniform cost β^{A} and β^{D} to the optimal strategy as follows. It is interesting to note that the critical values of β^{A} and β^{D} are different.

Corollary 3.5: The optimal strategy for the defender is not to recover if $\beta^{\mathrm{D}} > 2$.

Corollary 3.6: The optimal strategy for the attacker is not to attack if $\beta^{\mathrm{A}} > 1$. Also, under the optimal strategy, if the attacker attacks (i.e., $m^{\mathrm{A}}, \delta^{\mathrm{A}} > 0$), then $\mathcal{G}^{\mathrm{A}}$ always becomes disconnected.

TABLE IV
CHARACTERIZATION OF THE OPTIMAL STRATEGY OF ALL CASES

Conditions				$\hat{U}_2^{\mathrm{D3}} < \hat{U}^{\mathrm{D2a}}$	$\hat{U}_2^{\mathrm{D3}} \geq \hat{U}^{\mathrm{D2a}}$
$\hat{U}^{\mathrm{A2a*}} \geq 0$	$\hat{U}^{\mathrm{A3*}} < \hat{U}^{\mathrm{A2b*}}$	$\hat{U}_0^{\mathrm{A3}} \geq \hat{U}^{\mathrm{A2b*}}$		Comb. Str. 2a	Comb. Str. 2a
		$\hat{U}_0^{\mathrm{A3}} < \hat{U}^{\mathrm{A2b*}}$			Comb. Str. 2b
	$\hat{U}^{\mathrm{A3*}} \geq \hat{U}^{\mathrm{A2b*}}$	$\hat{U}_0^{\mathrm{A3}} > \hat{U}^{\mathrm{A3*}}$			Comb. Str. 2a
		$\hat{U}_0^{\mathrm{A3}} \leq \hat{U}^{\mathrm{A3*}}$			Comb. Str. 3
$\hat{U}^{\mathrm{A2a*}} < 0$				Comb. Str. 1	

Fig. 3. Optimal strategies of all cases for $n = 2$

Remark 1: If $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0) < 0$ (i.e., $\mathcal{G}^{\mathrm{A}}$ is disconnected), then in order to make $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}})$ larger, the defender can reduce the number of connected components by adding links until the graph becomes connected ($\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) > 0$). The minimum number of edges to add in order to achieve certain $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}})$ in a disconnected $\mathcal{G}^{\mathrm{A}}$ is given by

$$m^{\mathrm{D}} = \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) - \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0),$$
$$\text{for } \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) < 0, \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0) < 0. \quad (34)$$

To provide a more explicit relation between optimal strategies and attack/recovery parameters, we present a result for a simple case. It allows us to determine the equilibrium based on the cost and action durations. To this end, we consider a graph with $n = 2$ and $|\mathcal{E}| = 1$. In this setup, both players can only attack/recover one edge. Based on the results in Theorem 3.4, the optimal combined strategy can be stated as follows.

Proposition 3.7: The optimal combined strategy of the players with $n = 2$ is given by

1) Combined Strategy 1 if $\beta^{\mathrm{A}} > 1$;
2) Combined Strategy 2a if $\beta^{\mathrm{A}} \leq 1$ and $\beta^{\mathrm{D}} > 2$;
3) Combined Strategy 2b if $1 - \frac{2\xi}{\Delta^{\mathrm{A}} - \underline{\tau}^{\mathrm{D}} + \underline{\tau}^{\mathrm{A}}} < \beta^{\mathrm{A}} \leq 1$ and $\beta^{\mathrm{D}} \leq 2$;
4) Combined Strategy 3 if $\beta^{\mathrm{A}} \leq 1 - \frac{2\xi}{\Delta^{\mathrm{A}} - \underline{\tau}^{\mathrm{D}} + \underline{\tau}^{\mathrm{A}}}$ and $\beta^{\mathrm{D}} \leq 2$.

Proposition 3.7 characterizes the players' strategies in terms of the unit costs β^{A} and β^{D} as well as energy levels that influence Δ^{A} and Δ^{D}. This result can be summarized in the $(\beta^{\mathrm{A}}, \beta^{\mathrm{D}})$ plane as shown in Fig. 3. We will see later in a numerical example that the relation expressed in this plot holds for networks with more agents. In general, the player decides to attack (resp., to recover) if the unit cost β^{A} (resp., β^{D}) is not too expensive. The attacker decides to attack for longer duration (Combined Strategy 3) if the attacker has large enough energy so that it is able to continue the attack for longer after the defender ends its recovery at $\overline{\tau}^{\mathrm{D}}$.

C. Discussion on the Usage of Generalized Edge Connectivity

In our formulation, the generalized edge connectivity $\widehat{\lambda}$ is used in the utilities of both players. This $\widehat{\lambda}$ captures the idea that some edges are weaker than others in connected graphs (and thus the attacker should attack the weakest edges while minimizing its energy usage). Moreover, some of the attacked edges are more crucial for the agents' communication than others (and thus the defender should recover the most important edges for the agents' communication). Among the different connectivity measures, the generalized edge connectivity is useful to characterize the resilience of the multi-agent systems represented by both connected and disconnected graphs.
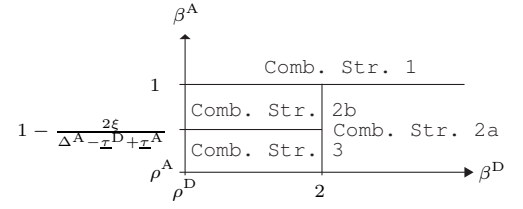
IV. APPLICATION TO CONSENSUS PROBLEM

In this section, a consensus problem of a multi-agent system [1]–[3] in the face of jamming attacks is investigated. We apply our game approach to this problem in a repeated manner.

A. Extension to Multiple Intervals with Energy Constraints

We first extend the problem formulation to multiple game intervals. Specifically, we suppose that the kth game with $k \in \mathbb{N}$ is played in the time interval $[\underline{t}_k, \overline{t}_k]$, which is determined by the players' actions with $\underline{t}_k = \underline{t}_{k-1} < \overline{t}_k$ and $\underline{t}_1 = 0$. Initially, at the start time $\underline{t}_k$, there is no attack or recovery, and the underlying graph is $\mathcal{G}$, as discussed in Section II. The $(k + 1)$th game starts immediately after the kth game, that is, $\underline{t}_{k+1} = \overline{t}_k$, with the graph becoming $\mathcal{G}$ again at $\underline{t}_{k+1}$. The rest of the formulation follows the one discussed in Section II, with subscript k added to all variables, e.g., m_k^{A}, m_k^{D}, to indicate the game index.

In the kth game, the players cannot keep sending signals for very long durations due to their energy constraints. We follow the approach in [14] to model such energy constraints. Specifically, the total energy used by player $p \in \{A, D\}$ must satisfy

$$\sum_{l=1}^{k-1} \beta^p m_l^p \delta_l^p + \beta^p m_k^p (t - \underline{\tau}_k^p) \leq \kappa^p + \rho^p t, \quad (35)$$

for any time $t \in [\underline{\tau}_k^p, \underline{\tau}_{k+1}^p]$, with $\kappa^p > 0$, $\rho^p \in (0, 1)$, $\beta^p > \rho^p$, and $k \in \mathbb{N}$. Note that κ^p denotes the initial energy that player p has, and ρ^p denotes the recharge rate of energy for player p. The left-hand side of (35) represents the energy consumed by player p up to time t and is affected by the number of attacked/recovered edges and the attack/recovery durations from the first game until the kth game. The right-hand side represents the total available energy, dictated by the parameters κ^p and ρ^p. We assume that each player knows all parameters of the other player, including κ^p and ρ^p.

Under this problem formulation, if player p keeps sending jamming/recovering signals starting at time $\underline{\tau}_k^p$ until running out of energy, then from (35) 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 as

$$\Delta_k^p(m_k^p) := \frac{\kappa^p + \rho^p \underline{\tau}_k^p - \sum_{l=1}^{k-1} \beta^p m_l^p \delta_l^p}{\beta^p m_k^p - \rho^p}. \quad (36)$$

Each game is played independently at time $\underline{t}_k$ and the strategies of the players will depend on their energy levels at that point, represented by the maximum interval $\Delta_k^p(m_k^p)$.

B. Approximate Consensus Time Bound

We assume that the graph $\mathcal{G}$ is connected and the agents communicate with neighbors continuously in time. Let $\mathcal{N}_i(t)$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2020.3016839, IEEE Transactions on Control of Network Systems

8

be the set of neighbors of agent i, i.e., the agents sharing edges with agent i at time t. Every agent i has the scalar state x_i whose dynamics are defined as

$$\dot{x}_i(t) = \sum_{j \in \mathcal{N}_i(t)} (x_j(t) - x_i(t)), \quad x(0) = x_0, \quad t \geq 0, \quad (37)$$

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

We now introduce the notion of approximate consensus. Specifically, 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

$$V(x) := \max_{i \in \mathcal{V}} x_i - \min_{i \in \mathcal{V}} x_i, \quad x \in \mathbb{R}^n. \quad (38)$$

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

$$T_*(x_0) := \inf\{t \geq 0 : x(t) \in \mathcal{D}_\epsilon\}. \quad (39)$$

In our analysis, we also use the Laplacian matrix $L \in \mathbb{R}^{n \times n}$ associated with graph $\mathcal{G}$. Moreover, let $P := e^{-\gamma^A L}$ and $\underline{p} := \max_{j \in \{1,\dots,n\}} \min_{i \in \{1,\dots,n\}} P_{i,j}$, where $P_{i,j}$ denotes the (i,j)th entry of the matrix P. Notice that since $\mathcal{G}$ is connected and $\gamma^A > 0$, we have $P_{i,j} \in (0,1)$, and hence, $\underline{p} \in (0,1)$.

The next proposition gives an upper bound for the approximate consensus time of agents under jamming attacks. Here, we define $\lceil x \rceil$ as the ceiling function of x.

Proposition 4.1: Consider the multi-agent system (37) with the initial condition $x_0 \in \mathbb{R}^n \setminus \mathcal{D}_\epsilon$. Under the optimal attack and defense strategies for the resilient graph game in Section III, the approximate consensus time satisfies

$$T_*(x_0) \leq \frac{\beta^A(\gamma^A + \gamma^D)\left\lceil \frac{\ln \epsilon - \ln V(x_0)}{\ln(1-\underline{p})} \right\rceil + \kappa^A}{\beta^A - \rho^A}. \quad (40)$$

Proposition 4.1 provides an upper bound related directly to the scalars β^A, κ^A, ρ^A that characterize the attacker's energy constraint, and 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. It is interesting to note that the attacker's energy parameters influence the bound more than the defender's energy parameters. In scenarios where there is no jamming attack (and hence no defense), from (40), an upper bound of the approximate consensus time can be obtained as $T_*(x_0) \leq (\gamma^A + \gamma^D)\left\lceil (\ln \epsilon - \ln V(x_0))/(\ln(1-\underline{p})) \right\rceil$. This bound for the attack-free case is clearly smaller than that in (40) when the attacker has positive energy resources ($\kappa^A, \rho^A > 0$) and the defender has a nonzero initial waiting duration ($\gamma^D > 0$). Note that with larger values of κ^A and ρ^A, the bound (40) becomes even larger, indicating the possibility of slower consensus due to more damaging attacks.

V. NUMERICAL EXAMPLES

We demonstrate the efficacy of the approach in the approximate consensus problem through numerical examples. We first compare the actual approximate consensus time for different energy parameters. We use the graph shown in Fig. 1 with $n = 4$, and parameters $\beta^A = 0.4$, $\beta^D = 0.6$, $\kappa^D = 1$, $\rho^D = 0.1$, $\gamma^A = 0.1$, and $\gamma^D = 0.3$.
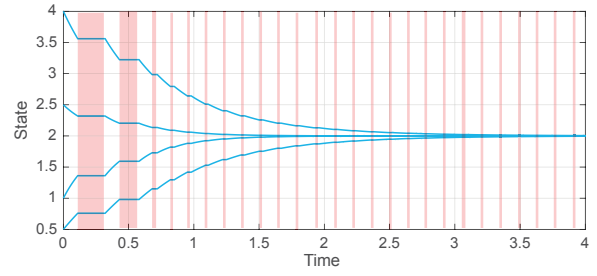

Fig. 4. State trajectories with $\kappa^A = 0.5$ and $\rho^A = 0.3$. The red areas indicate the intervals where the attacker attacks.
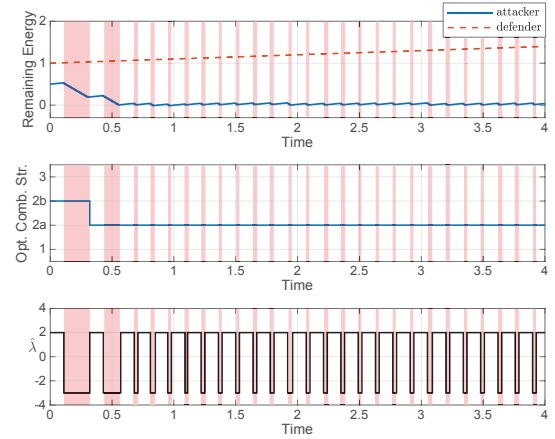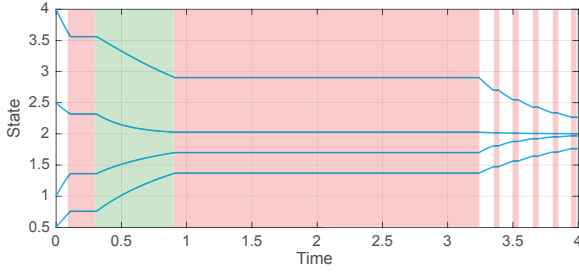

Fig. 5. Remaining energy and optimal combined strategy for the two players, and the resulting $\hat{\lambda}$ with $\kappa^A = 0.5$ and $\rho^A = 0.3$. Note that the defender does not recover any edge, and hence the available energy for the defender accumulates continuously.

First, we use the parameters $\kappa^A = 0.5$ and $\rho^A = 0.3$. Figs. 4 and 5 show the states of the agents and properties of the players of the first simulation, with the agents eventually achieving approximate consensus at $t \approx 1.54$ with $\epsilon = 0.5$. For comparison, when there is no jamming, it takes $t \approx 1.04$ to achieve the same level of approximate consensus. In the second simulation, we use the parameters $\kappa^A = 5$ and $\rho^A = 0.39$. We present the results of this simulation in Figs. 6 and 7. It takes $t \approx 4$ with $\epsilon = 0.5$ to achieve approximate consensus, which is longer than the first simulation because the attacker is given more energy. In these examples, the attacker decides to attack all edges, since by attacking more edges the defender has to recover more to increase the connectivity of the graph, which makes the recovery interval shorter.

Next, we compare the strategies of the players under different graph structures. Specifically, we run simulations on the path graph and the complete graph consisting of four nodes, while all other parameters are set to be the same across these two simulations. Fig. 8 shows the state trajectory and Figs. 9 shows the remaining energy, the optimal combined strategy, and the generalized edge connectivity versus time in the path graph. The corresponding results for the complete graph are shown in Figs. 10 and 11. We note that for the complete graph the attacker chooses to attack for shorter duration (Combined Strategy 2b) due to the high connectivity of the graph structure. Specifically, the attacker needs to attack more edges (and hence takes more energy) to make the graph disconnected, and therefore the maximum attack interval becomes shorter compared to the attacks in the path graph. This shorter maximum attack duration results in a situation where the attacks on $[\overline{\tau}_k^D, \overline{\tau}_k^A]$ interval are not able to

Fig. 6. State trajectories with $\kappa^{\mathrm{A}} = 5$ and $\rho^{\mathrm{A}} = 0.39$. The green areas indicate the intervals where the defender recovers.
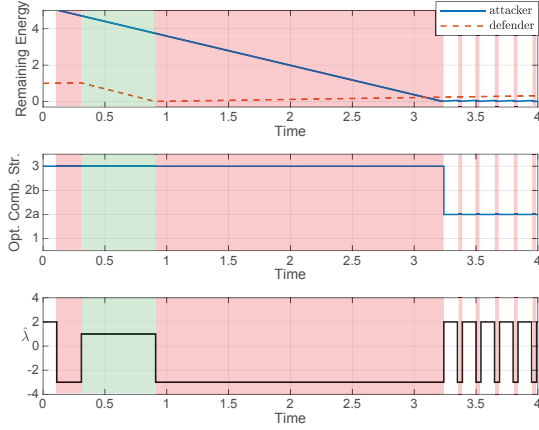

Fig. 7. Remaining energy and optimal combined strategy for the two players, and the resulting $\widehat{\lambda}$. In this case, the attacker attacks all edges to achieve $\widehat{\lambda}(\mathcal{G}_k^{\mathrm{A}}) = -3$, where the defender recovers briefly in the first game to make the graph connected again.
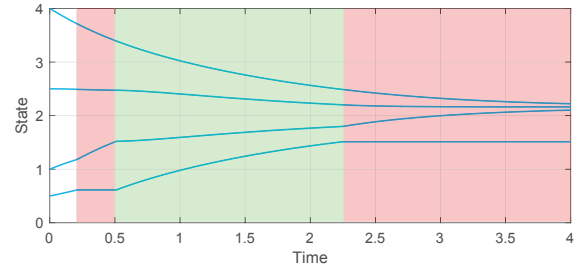

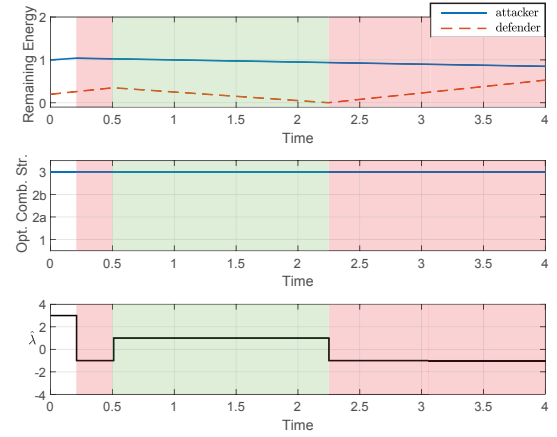Fig. 8. State trajectories in the system with the path graph $\mathcal{G}$.

Fig. 9. Remaining energy and optimal combined strategy for the two players, and the resulting generalized edge connectivity with the path graph $\mathcal{G}$.

compensate the negative payoff that the attacker receives on the $[\overline{\tau}_k^{\mathrm{D}}, \overline{\tau}_k^{\mathrm{A}}]$ interval, causing the attacker to attack for only γ^{D} duration instead. Consequently, consensus is achieved faster in the complete graph than in the path graph. We can infer that graph structures influence the attack and recovery actions of the players, and graphs that have higher generalized edge connectivity are more resilient to attacks.

We also provide an example of how the energy, which affects the maximum attack/recovery durations, influences the equilibrium. We consider the graph in Fig. 1 with selected values of $\Delta_k^{\mathrm{A}}(m_k^{\mathrm{A}})$ and $\Delta_k^{\mathrm{D}}(m_k^{\mathrm{D}})$ in (36) by changing the total consumed energy up to game $(k-1)$ represented as $\sum_{l=1}^{k-1} \beta^{\mathrm{A}} m_l^{\mathrm{A}} \delta_l^{\mathrm{A}}$ and $\sum_{l=1}^{k-1} \beta^{\mathrm{D}} m_l^{\mathrm{D}} \delta_l^{\mathrm{D}}$. The result is shown in Fig. 12 for $m_k^{\mathrm{A}} = m_k^{\mathrm{D}} = 1$. In the figure, the yellow circles indicate that Combined Strategy 2b is optimal with attacking five edges for given Δ_k^{A} and Δ_k^{D}, whereas the green squares indicate that Combined Strategy 3 is optimal with attacking five edges. The optimal strategy for the defender is to recover one edge and three edges (to make the graph connected again, e.g., $\{e_{12}, e_{13}, e_{34}\}$) in the areas with light green and dark green squares, respectively. The attacker attacks for longer durations if it possesses high amount of energy relative to the defender's energy. On the other hand, the defender with more energy will attempt to make the graph connected by recovering more edges. Fig. 12 can also be useful to estimate the equilibrium based on the past actions and energy parameters.

The optimal combined strategies for varying β^{A} and β^{D} are shown in Fig. 13. We note that Fig. 13 is similar to Fig. 3 in terms of characterizing the influence of the unit costs β^{A} and β^{D} to the equilibrium, where the players tend not to attack or recover if the costs become higher. However, the

critical values of β^{A} and β^{D} separating the optimal combined strategies in this set of simulations are lower than those found in Corollaries 3.5 and 3.6. These critical values of β^{A} and β^{D} in the simulations are affected by generalized edge connectivity of $\mathcal{G}$ in Fig. 1.

VI. Conclusion

In this paper, we have considered resilient network problem in the context of multi-agent systems, formulated as a two-player game between the attacker and defender. Their utilities are determined by the communication among the agents. We fully characterized the optimal strategies of the players in terms of the edges and durations of action intervals. Several cases are possible to happen depending on the available energy of the players. For the consensus problem, we have shown that the time for the agents to reach approximate consensus will be delayed due to attacks by deriving an upper bound.

Note that in this paper, we have considered the generalized edge connectivity as one specific way to measure the network connectivity. It is also worth investigating other connectivity notions and non-uniform unit costs for practical applications. In [29], we have considered a problem formulation where not only the available energy but also the agents' states affect the results of the optimal strategies; this provides a more direct relation between the game and agents' dynamics. Extending the game setting into multiple intervals (rather than considering game played repeatedly in one interval $[\underline{t}_k, \overline{t}_k]$) may also be one of the possible future research directions.

Appendix A: Proof of Lemma 3.1

The utility function in (5) can be rewritten as $U^{\mathrm{A}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}}, \delta^{\mathrm{D}})) = -\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0)\delta^{\mathrm{A}} - (\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) - \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, 0))\delta^{\mathrm{D}} - \beta^{\mathrm{A}} m^{\mathrm{A}} \delta^{\mathrm{A}}$. If there is
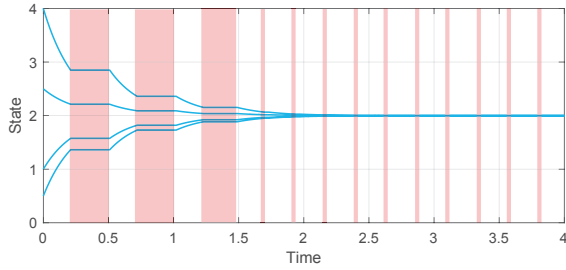
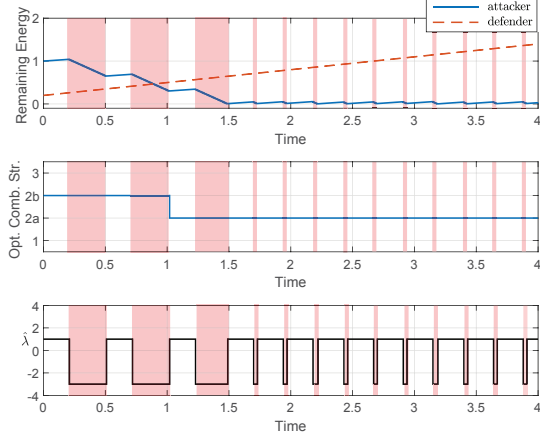Fig. 10. State trajectories in the system with the complete graph $\mathcal{G}$.

Fig. 11. Remaining energy and optimal combined strategy for the two players, and the resulting generalized edge connectivity in the system with the complete graph $\mathcal{G}$.
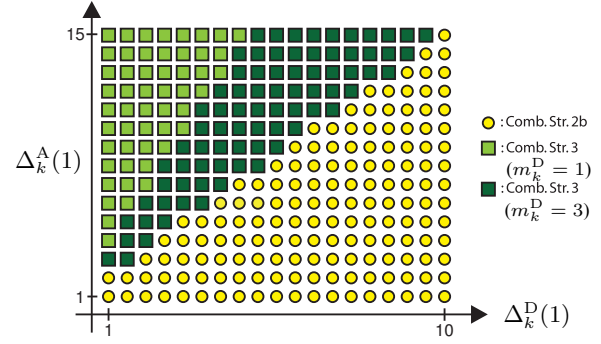

Fig. 12. Optimal combined strategies for different $\Delta_k^A(m_k^A = 1)$ and $\Delta_k^D(m_k^D = 1)$.
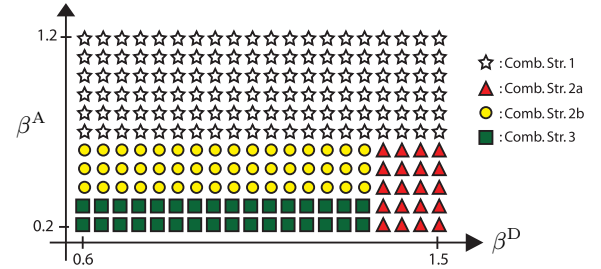

Fig. 13. Optimal combined strategies for different β^A and β^D. The optimal numbers of edges are $m_k^A = 5$, $m_k^D = 3$ if the players attack or recover.

recovery, i.e., $m^D, \delta^D > 0$, then $\widehat{\lambda}_{\mathcal{G}}(m^A, m^D) > \widehat{\lambda}_{\mathcal{G}}(m^A, 0)$ according to the optimal strategy candidates. This implies that $-(\widehat{\lambda}_{\mathcal{G}}(m^A, m^D) - \widehat{\lambda}_{\mathcal{G}}(m^A, 0))\delta^D < -\widehat{\lambda}_{\mathcal{G}}(m^A, 0)\delta^D$ holds.

APPENDIX B: PROOF OF LEMMA 3.2

Substitute m^{A3*} of (27) into (26) to obtain $\hat{U}^{A3*} = (\widehat{\lambda}_{\mathcal{G}}(m^{A3*}, 0) - \widehat{\lambda}_{\mathcal{G}}(m^{A3*}, m^{D3*}))\xi + \hat{U}^{A2a}(m^{A3*})$. Since $\widehat{\lambda}_{\mathcal{G}}(m^{A3*}, m^{D3*}) > \widehat{\lambda}_{\mathcal{G}}(m^{A3*}, 0)$, it follows that $\hat{U}^{A3*} \leq \hat{U}^{A2a}(m^{A3*})$, and therefore $\hat{U}^{A3*} \leq \hat{U}^{A2a*}$.

APPENDIX C: PROOF OF LEMMA 3.3

First, we show that $\text{sgn}(\hat{U}^{A2a*}) = \text{sgn}(\hat{U}^{A2b*})$. We can state $\hat{U}^{A2a}(m^A)$ as $\hat{U}^{A2a}(m^A) = \hat{U}^{A2b}(m^A) + (-\widehat{\lambda}_{\mathcal{G}}(m^A, 0) - \beta^A m^A)(\Delta^A + \underline{\tau}^A - \underline{\tau}^D)$. By (1), we have $\underline{\tau}^D \leq \overline{\tau}^A$. Consequently, since $\overline{\tau}^A \leq \underline{\tau}^A + \Delta^A$, we have $\Delta^A + \underline{\tau}^A \geq \underline{\tau}^D$ for any possible Δ^A. Therefore, if $-\widehat{\lambda}_{\mathcal{G}}(m^A, 0) - \beta^A m^A > 0$ is satisfied, then $\hat{U}^{A2a}(m^A) > 0$ and $\hat{U}^{A2b}(m^A) > 0$, and vice versa. Again, since $\Delta^A + \underline{\tau}^A \geq \underline{\tau}^D > \underline{\tau}^A$, it follows that $\hat{U}^{A2b*} > 0$ if and only if $\hat{U}^{A2a*} > 0$, since the attacker can always choose edges to make $\hat{U}^{A2a*}$ and $\hat{U}^{A2b*}$ positive. By a similar argument, $\hat{U}^{A2b*} < 0$ if and only if $\hat{U}^{A2a*} < 0$. Thus, $\text{sgn}(\hat{U}^{A2a*}) = \text{sgn}(\hat{U}^{A2b*})$.

Now, since $(-\widehat{\lambda}_{\mathcal{G}}(m^{A2a*}, 0) - \beta^A m^{A2a*}) > 0$ and $\Delta^A + \underline{\tau}^A \geq \underline{\tau}^D$, it then follows that $\hat{U}^{A2a*} \geq \hat{U}^{A2b*}$ if $\hat{U}^{A2a*} > 0$.

APPENDIX D: PROOF OF THEOREM 3.4

We prove this result using the backward induction method. In Combined Strategy 1, recall that the attacker does not attack and the defender does not recover, so $\hat{U}^{A1} = \hat{U}^{D1} = 0$. Therefore, the attacker chooses the optimal $m^A > 0$ to achieve positive utility. If the attacker attacks m^{A*}, then the optimal strategy for the defender is to recover if and only

if $U^D((m^{A*}, \delta^{A*}), (m^{D*}, \delta^{D*} > 0)) > \widehat{\lambda}_{\mathcal{G}}(m^{A*})\Delta^A$. Recall that the utility of a player also depends on the other player's strategy. For example, if the defender's optimal strategy is to recover ($m^D > 0$) for given m^A, then the attacker's utility for given m^A is $U^A((m^A, \delta^A), (m^D, \delta^D > 0))$.

By backward induction, the six facts (i)–(vi) below hold:

(i) From Lemmas 3.2 and 3.3, since $\hat{U}^{A2a*} > \hat{U}^{A3*}$ and $\hat{U}^{A2a*}$ has the same sign with $\hat{U}^{A2b*}$, Combined Strategy 1 is optimal if $\hat{U}^{A2a*} < 0 = \hat{U}^{A1}$, regardless of the defender's utility. This fact proves point 1) in the theorem.

Since the case where $\hat{U}^{A2a*} < 0$ is covered, it is assumed that $\hat{U}^{A2a*} \geq 0$ holds in all subsequent analysis for (ii)–(vi).

(ii) Combined Strategy 2a with attacking m^{A2a*} is the optimal combined strategy if $\hat{U}_2^{D3} = U^D((m^{A2a*}, \Delta^A), (m^{D*}, \Delta^D > 0))$ is less than $\hat{U}^{D2a} = U^D((m^{A2a*}, \Delta^A), (0, 0))$, since the defender chooses not to recover ($m^{D*} = 0$) and $\hat{U}^{A2a*} = U^A((m^{A2a*}, \Delta^A), (0, 0))$ is the maximum possible utility for the attacker from Lemmas 3.2 and 3.3. This fact corresponds to point 2)a) in the theorem.

Since the case where $\hat{U}_2^{D3} < \hat{U}^{D2a}$ is covered, beginning from (iii) to (vi), it is further assumed that $\hat{U}_2^{D3} \geq \hat{U}^{D2a}$, i.e., the defender chooses to recover from m^{A2a*}. Since $m^{D*} > 0$ and $\hat{U}^{A2a*} = U^A((m^{A2a*}, \Delta^A), (0, 0))$, in the subsequent cases, the attacker's optimal number of edges are not m^{A2a*} (which corresponds to $\hat{U}^{A2a*}$). In (iii) and (iv), we analyze the case where $\hat{U}^{A3*} \geq \hat{U}^{A2b*}$, which means that Strategy A3 yields more or equal utility than Strategy A2b for the attacker.

(iii) Due to the possible jump between $\widehat{\lambda}_{\mathcal{G}}(m^A, m^D) = -1$ to $\widehat{\lambda}_{\mathcal{G}}(m^A, m^D) = 1$ by recovering only one edge, the defender may have different optimal strategies (whether to recover or not) given different attacked edges. From Lemma 3.1, since the attacker has better utility if the defender does not recover, here the attacker's optimal strategy is to attack $\underline{m}^{A*}$ if $\hat{U}_0^{A3} = U^A((\underline{m}^{A*}, \Delta^A), (0, 0))$ is greater than

$\hat{U}^{A3*} = U^A((m^{A3*}, \Delta^A), (m^D, \Delta^D > 0))$, with $\underline{m}^{A*}$ being the optimal number of edges among the edges that cannot be recovered if attacked, as in (33). Therefore, Strategies A1, A2b, and A3 are not optimal. This corresponds to point 2)b)II) in the theorem.

(iv) Otherwise, Combined Strategy 3 (point 4) in the theorem) is the optimal combined strategy if $\hat{U}_0^{A3} \leq \hat{U}^{A3*}$. Here, the defender's optimal strategy is to recover if the attacker attacks m^{A3*}. Since $\hat{U}^{A3*} \geq \max\{\hat{U}^{A2b*}, 0\}$, the attacker has better utility than in Strategies A1, A2a, and A2b.

In (v) and (vi), we analyze the case where $\hat{U}^{A2b*} > \hat{U}^{A3*}$.

(v) Similar as in (iii), Combined Strategy 2a is the optimal strategy if $\hat{U}_0^{A3} \geq \hat{U}^{A2b*}$. In this case, the attacker has better utility than in Strategies A1, A2b, and A3. However, since $\hat{U}_2^{D3} \geq \hat{U}^{D2a}$, the attacker does not attack m^{A2a*}. This fact corresponds to point 2)b)I) in the theorem.

(vi) If $\hat{U}_0^{A3} < \hat{U}^{A2b*}$, Strategy A2b is the optimal strategy for the attacker since $\hat{U}^{A2b*} > \max(\hat{U}^{A3*}, \hat{U}_0^{A3})$ and utility $\hat{U}^{A2a*}$ cannot be achieved because $\hat{U}_2^{D3} \geq \hat{U}^{D2a}$. This corresponds to point 3) in the theorem.

APPENDIX E: PROOF OF COROLLARY 3.5

In Strategy D3, since $\min\{\Delta^D, \Delta^A + \underline{\tau}^A - \underline{\tau}^D\} > 0$, the necessary condition for Strategy D3 to be the optimal strategy is $\beta^D < (\widehat{\lambda}_{\mathcal{G}}(m^{A3*}, m^{D3*}) - \widehat{\lambda}_{\mathcal{G}}(m^{A3*}, 0))/m^{D3*}$, i.e., the cost of recovering edges is not too large. If this condition is not satisfied, then it is better for the defender not to recover as in Strategy D1. By recovering one edge the defender is able to make $(\widehat{\lambda}_{\mathcal{G}}(m^A, m^D) - \widehat{\lambda}_{\mathcal{G}}(m^A, 0))/m^D = 2$ at most. Thus, if $\beta^D > 2$, then the defender does not recover any edge.

APPENDIX F: PROOF OF COROLLARY 3.6

From Theorem 3.4, the attacker decides to attack if $\hat{U}^{A2a}(m^{A2a*}) \geq 0$. Since $\Delta^A > 0$, Strategy A2a is the optimal strategy if $-\widehat{\lambda}_{\mathcal{G}}(m^{A2a*}, 0) - \beta^A m^{A2a*} \geq 0$, assuming that the defender cannot recover. By Lemma 3.1, $\hat{U}^{A2a}(m^{A2a*}) > \hat{U}^{A3}(m^{A3*})$, and thus Strategy A1 is the optimal strategy if $-\widehat{\lambda}_{\mathcal{G}}(m^{A2a*}, 0) - \beta^A m^{A2a*} < 0$.

Since $\beta^A m^{A2a*} > 0$, to make $-\widehat{\lambda}_{\mathcal{G}}(m^{A2a*}, 0) - \beta^A m^{A2a*} > 0$, it must hold that $\widehat{\lambda}_{\mathcal{G}}(m^{A2a*}, 0) < 0$. Therefore, the attacker must attack enough edges to make $\mathcal{G}^A$ disconnected. Because $-\widehat{\lambda}_{\mathcal{G}}(m^{A2a*}, 0)/m^{A2a*}$ cannot exceed 1, in order to obtain positive utility, $\beta^A \leq 1$ must be satisfied.

APPENDIX G: PROOF OF PROPOSITION 3.7

Since $|\mathcal{E}| = 1$, the following four facts corresponding to points 1) to 4) in Theorem 3.4 hold:

(i) Combined Strategy 1 is optimal if $\hat{U}^{A2a*} < 0$. Since $|\mathcal{E}| = 1$, $\widehat{\lambda}_{\mathcal{G}}(m^A, 0) = -1$ is always true if $m^A > 0$. From (17), it is clear that $\hat{U}^{A2a*} < 0$ if $\beta^A > 1$.

(ii) In order for Combined Strategy 2a to be optimal, a common condition is that $\hat{U}^{A2a*} \geq 0$, which holds if $\beta^A \leq 1$. The condition $\hat{U}_2^{D3} < \hat{U}^{D2a}$ then holds if $\beta^D > 2$. Note that $\mathcal{M}$ consists of $|\mathcal{E}| = 1$ if $\beta^D > 2$ and empty otherwise. Hence, $\hat{U}_0^{A3} = \hat{U}^{A2a*}$ holds if $\beta^D > 2$, otherwise $\hat{U}_0^{A3} = 0$ holds. Therefore, in point 2)b) in Theorem 3.4, condition $\hat{U}_2^{D3} \geq \hat{U}^{D2a}$ implies that $\hat{U}_0^{A3} = 0$ holds, which means that the conditions 2)b)I) and 2)b)II) cannot be satisfied (from Lemma 3.3).

(iii) Combined Strategy 2b is optimal if $\hat{U}^{A2a*} \geq 0$, which holds if $\beta^A \leq 1$. The other condition is that $\hat{U}_2^{D3} \geq \hat{U}^{D2a}$,

which holds if $\beta^D \leq 2$. Conditions $\hat{U}^{A2b*} > \hat{U}_0^{A3}$ is always true (see point (ii) in this proof above). With $n = 2$, condition $\hat{U}^{A2b*} > \hat{U}^{A3*}$ is true if $\beta^A > 1 - \frac{2\xi}{\Delta^A - \underline{\tau}^D + \underline{\tau}^A}$ holds, with ξ defined in (24).

(iv) It then follows that Combined Strategy 3 is optimal if $\hat{U}^{A2a*} \geq 0$ (holds if $\beta^A \leq 1$), $\hat{U}_2^{D3} \geq \hat{U}^{D2a}$ (holds if $\beta^D \leq 2$), and $\hat{U}^{A2b*} \leq \hat{U}^{A3*}$ (holds if $\beta^A \leq 1 - \frac{2\xi}{\Delta^A - \underline{\tau}^D + \underline{\tau}^A}$), under which the condition $\hat{U}^{A3*} \geq \hat{U}_0^{A3}$ holds.

APPENDIX H: PROOF OF PROPOSITION 4.1

The agents do not face any attacks during the intervals $[\underline{t}_k, \underline{\tau}_k^A)$, $k \in \mathbb{N}$. Thus, from (37), $\dot{x}(t) = -Lx(t)$, $t \in [\underline{t}_k, \underline{\tau}_k^A)$, $k \in \mathbb{N}$. Noting that $\underline{\tau}_k^A = \underline{t}_k + \gamma^A$, we obtain $x(\underline{\tau}_k^A) = Px(\underline{t}_k)$, $k \in \mathbb{N}$. Now by using Lemma 12.8 of [3], it follows that

$$V(x(\underline{\tau}_k^A)) = V(Px(\underline{t}_k)) \leq (1 - \underline{p})V(x(\underline{t}_k)). \quad (41)$$

During the intervals $[\underline{\tau}_k^A, \underline{t}_{k+1})$, $k \in \mathbb{N}$, there may be attacks and the communication between certain agents may be jammed. It then follows from (37) that

$$V(x(\underline{t}_{k+1})) \leq V(x(\underline{\tau}_k^A)), \quad k \in \mathbb{N}. \quad (42)$$

By (41) and (42), $V(x(\underline{t}_{k+1})) \leq (1 - \underline{p})V(x(\underline{t}_k))$, and thus,

$$V(x(\underline{t}_{k+1})) \leq (1 - \underline{p})^k V(x(\underline{t}_1)) = (1 - \underline{p})^k V(x_0), k \in \mathbb{N}. \quad (43)$$

Let $k_* := \left\lceil (\ln \epsilon - \ln V(x_0))/\ln(1 - \underline{p}) \right\rceil$. By (43), it clearly holds $V(x(\underline{t}_{k_*+1})) \leq \epsilon$, and therefore,

$$x(t) \in \mathcal{D}_\epsilon, \quad t \geq \underline{t}_{k_*+1}. \quad (44)$$

Our next goal is to find an upper bound of $\underline{t}_{k_*+1}$. First, by the energy constraint for the attacker given in (35), $\beta^A \sum_{k=1}^{k_*} m_k^A \delta_k^A \leq \kappa^A + \rho^A \underline{t}_{k_*+1}$ holds. As indicated by the optimal strategies derived in Theorem 3.4, $m_k^A = 0$ implies that $\delta_k^A = 0$. Hence, we have $m_k^A \delta_k^A \geq \delta_k^A$, which implies

$$\sum_{k=1}^{k_*} \delta_k^A \leq \frac{1}{\beta^A} \beta^A \sum_{k=1}^{k_*} m_k^A \delta_k^A \leq \frac{\kappa^A}{\beta^A} + \frac{\rho^A}{\beta^A} \underline{t}_{k_*+1}. \quad (45)$$

Next, by (7), $\underline{t}_{k+1} = \overline{t}_k \leq \underline{t}_k + \gamma^A + \gamma^D + \delta_k^A$, $k \in \mathbb{N}$. It then follows from (45) that $\underline{t}_{k_*+1} = \sum_{k=1}^{k_*}(\underline{t}_{k+1} - \underline{t}_k) \leq (\gamma^A + \gamma^D)k_* + \frac{\kappa^A}{\beta^A} + \frac{\rho^A}{\beta^A}\underline{t}_{k_*+1}$, and hence,

$$\underline{t}_{k_*+1} \leq \frac{(\gamma^A + \gamma^D)\left\lceil \frac{\ln \epsilon - \ln V(x_0)}{\ln(1-\underline{p})} \right\rceil + \frac{\kappa^A}{\beta^A}}{1 - \frac{\rho^A}{\beta^A}}. \quad (46)$$

Finally, by (44) and (46), we obtain (40).

REFERENCES

[1] W. Ren and R. W. Beard, "Consensus seeking in multiagent systems under dynamically changing interaction topologies," *IEEE Trans. Autom. Control*, vol. 50, pp. 655–661, 2005.

[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. Kindle Direct Publishing, 2019.

[4] H. Sandberg, S. Amin, and K. H. Johansson, "Special issue on cyberphysical security in networked control systems," *IEEE Control Syst. Mag.*, vol. 35, pp. 20–23, 2015.

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2020.3016839, IEEE Transactions on Control of Network Systems

12

[6] S. R. Etesami and T. Basar, "Dynamic games in cyber-physical security: An overview," *Dynamic Games and Applications*, vol. 9, pp. 884–913, 2019.

[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. Control*, vol. 60, pp. 2831–2836, 2015.

[9] A. Gupta, A. Nayyar, C. Langbort, and T. Basar, "A dynamic transmitter-jammer game with asymmetric information," in *Proc. IEEE Conf. Dec. Contr.*, 2012, pp. 6477–6482.

[10] Y. Li, L. Xiao, J. Liu, and Y. Tang, "Power control Stackelberg game in cooperative anti-jamming communications," in *Proc. Int. Conf. Game Theory for Netw.*, 2014, pp. 1–6.

[11] D. Yang, G. Xue, J. Zhang, A. Richa, and X. Fang, "Coping with a smart jammer in wireless networks: A Stackelberg game approach," *IEEE Trans. Wireless Commun.*, vol. 12, pp. 4038–4047, 2013.

[12] A. Khanafer, B. Touri, and T. Basar, "Consensus in the presence of an adversary," in *Proc. IFAC NecSys*, 2012, pp. 276–281.

[13] 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.

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

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

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

[17] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Networked control under random and malicious packet losses," *IEEE Trans. Autom. Control*, vol. 62, pp. 2434–2449, 2017.

[18] 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, 2013.

[19] N. H. Vaidya, L. Tseng, and G. Liang, "Iterative approximate Byzantine consensus in arbitrary directed graphs," in *Proc. ACM Symposium on Principles of Distributed Computing*, 2012, pp. 365–374.

[20] L. Guerrero-Bonilla, A. Prorok, and V. Kumar, "Formations for resilient robot teams," *IEEE Robot. Autom. Lett.*, vol. 2, pp. 841–848, 2017.

[21] M. Huang, S. Dey, G. N. Nair, and J. H. Manton, "Stochastic consensus over noisy networks with Markovian and arbitrary switches," *Automatica*, vol. 46, pp. 1571–1583, 2010.

[22] R. Carli, G. Como, P. Frasca, and F. Garin, "Distributed averaging on digital erasure networks," *Automatica*, vol. 47, pp. 115–121, 2011.

[23] S. Bhattacharya, A. Gupta, and T. Başar, "Jamming in mobile networks: A game-theoretic approach," *J. Num. Algeb. Control Optim.*, vol. 3, pp. 1–30, 2013.

[24] M. Pirani, J. Taylor, and B. Sinopoli, "Attack resilient interconnected second order systems: A game-theoretic approach," in *Proc. IEEE Conf. Dec. Contr.*, 2019, pp. 4391–4396.

[25] J. Chen, C. Touati, and Q. Zhu, "A dynamic game approach to strategic design of secure and resilient infrastructure network," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 462–474, 2020.

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

[27] R. Motwani and P. Raghavan, *Randomized Algorithms*. Cambridge University Press, 1995.

[28] O. Goldschmidt and D. S. Hochbaum, "A polynomial algorithm for the k-cut problem for fixed k," *Mathematics of Operations Research*, vol. 19, pp. 24–37, 1994.

[29] Y. Nugraha, A. Cetinkaya, T. Hayakawa, H. Ishii, and Q. Zhu, "Dynamic resilient graph games for state-dependent jamming attacks analysis on multi-agent systems," in *Proc. IFAC World Congress*, 2020, to appear.

Ahmet Cetinkaya received his B.Eng. degrees from Control Engineering and Computer Engineering Departments of Istanbul Technical University, Turkey, both in 2007. He obtained M.Eng. and Ph.D. degrees in Mechanical and Environmental Informatics in 2011 and 2014 from Tokyo Institute of Technology, Japan, where he held postdoctoral research positions between 2014 and 2019 in the Departments of Mechanical and Environmental Informatics, Systems and Control Engineering, and Computer Science. Since 2019, he has been a researcher and project assistant professor at National Institute of Informatics, Japan. His research interests are in the areas of hybrid and stochastic dynamical systems, networked control, cybersecurity of control systems, as well as probability theory and its applications in physics, learning, and control.

Tomohisa Hayakawa received the B.Eng. degree in aeronautical engineering from Kyoto University, Kyoto, Japan, in 1997; the M.S. degree in aerospace engineering from The State University of New York, Buffalo, NY, USA, in 1999; and the M.S. degree in applied mathematics and the Ph.D. degree in aerospace engineering from Georgia Institute of Technology, Atlanta, GA, USA, in 2001 and 2003, respectively. He is currently appointed as an Associate Professor at the Department of Systems and Control Engineering, Tokyo Institute of Technology, Japan. His research interests include stability of nonlinear systems; nonnegative and compartmental systems; hybrid systems; nonlinear adaptive control; neural networks and intelligent control; stochastic dynamical systems; and applications to aerospace vehicles, formation control of multiagent systems, financial dynamics, and game theory and mechanism design.

Hideaki Ishii received the M.Eng. degree from Kyoto University, Kyoto, Japan, in 1998, and the Ph.D. degree from the University of Toronto, Toronto, ON, Canada, in 2002. He was a Postdoctoral Research Associate at the University of Illinois at Urbana-Champaign, Urbana, IL, USA, from 2001 to 2004, and a Research Associate at The University of Tokyo, Tokyo, Japan, from 2004 to 2007. Currently, he is an Associate Professor in the Department of Computer Science, Tokyo Institute of Technology, Yokohama, Japan. His research interests are in networked control systems, multi-agent systems, hybrid systems, cyber security of power systems, and probabilistic algorithms.

Dr. Ishii has served as an Associate Editor for the *IEEE Control Systems Letters*, and *Mathematics of Control, Signals, and Systems* and previously for *Automatica*, the *IEEE Transactions on Automatic Control*, and the *IEEE Transactions on Control of Network Systems*. He is the Chair of the IFAC Coordinating Committee on Systems and Signals since 2017. He received the IEEE Control Systems Magazine Outstanding Paper Award in 2015.

Quanyan Zhu received B. Eng. in Honors Electrical Engineering from McGill University in 2006, M. A. Sc. from the University of Toronto in 2008, and Ph.D. from the University of Illinois at Urbana-Champaign (UIUC) in 2013. He is currently an associate professor at the Department of Electrical and Computer Engineering, New York University (NYU). He is an affiliated faculty member of the Center of Cyber Security (CCS) and the Center for Urban Science and Progress (CUSP) at NYU. His current research interests include game and control theory, machine learning, cybersecurity and deception, network optimization and control, and cyber-physical systems.

Yurid Nugraha received his B.Eng. degree in electrical engineering from Sepuluh Nopember Institute of Technology, Indonesia, in 2016. He obtained his M. Eng. degree in systems and control engineering in 2020 from Tokyo Institute of Technology, Japan, where he is now a Ph.D. student. His research interests include game theory and its applications in networked control systems.