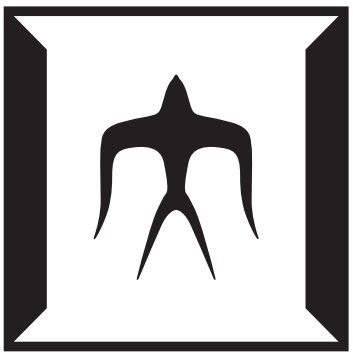
論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	Consensus and Clustering of Dynamic Resilient Multiagent Systems under Repeated Games
著者(和文)	NUGRAHA Yurid Eka
Author(English)	Yurid Eka Nugraha
出典(和文)	学位:博士(学術), 学位授与機関:東京工業大学, 報告番号:甲第12295号, 授与年月日:2022年12月31日, 学位の種別:課程博士, 審査員:早川 朋久,中尾 裕也,畑中 健志,石﨑 孝幸,石井 秀明
Citation(English)	Degree:Doctor (Academic), Conferring organization: Tokyo Institute of Technology, Report number:甲第12295号, Conferred date:2022/12/31, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Type(English)	Doctoral Thesis

Consensus and Clustering of Dynamic Resilient Multiagent Systems under Repeated Games



Yurid Eka Nugraha

Supervised by

Assoc. Prof. Tomohisa Hayakawa

This dissertation is submitted for the degree of

Doctor of Philosophy

Department of Systems and Control Engineering
School of Engineering
Tokyo Institute of Technology

October 2022

Abstract

Multiagent systems are used to model interaction between agents in a communication network. Due to the distributed nature of the agents in the network, they are prone to cyber attacks initiated by malicious adversaries. This thesis provides a line of work on game-theoretical approaches between a centralized attacker and a centralized defender that attempt to respectively block and recover the communication among agents in the network with consensus dynamics. The game is played repeatedly over time where the attacker is motivated to delay or prevent the consensus whereas the defender wants to maintain the communication among the agents.

In one game, the players decide their actions sequentially based on payoff functions characterizing the network design and the states of the agents following the consensus protocol. We investigate the equilibrium of the game and obtain the optimal strategies for the players in terms of edges and action durations. We examine how these optimal strategies affect agents' dynamics at infinite time.

In the first part of the thesis, we focus on the continuous time setting where players' strategies are decided every certain interval. There, we discuss how the players' strategies following subgame perfect equilibrium solution affect the consensus among agents. The upper time bound of the consensus is also obtained, which depends on several parameters characterizing the network design and the players' capability to attack or recover. In the second part of the thesis, we consider a discrete time setting where players have different computational abilities represented by a moving horizon approach with non-uniform horizon lengths and game periods, resulting in an asynchronous decision making process for the players. We show that player with better horizon parameters is able to perform better than the opponent in the context of agent consensus and obtained utilities over time.

Contents

Chapter 1

Introduction

1.1 Jamming attacks on multiagent systems

A network is defined as a group of interconnected computing devices, which agree on a set of common communication protocols. There exists a great variety of networks in terms of their scale, connection methods, and functions. Networks continue to evolve and diversify as time goes. The devices, or nodes, on the network can also be heterogeneous and may vary from small sensors to smartphones, laptops, desktops, and servers [1, 2].

Applications of large-scale networked systems have rapidly grown in various areas of critical infrastructures including power grid and transportation systems. Multiagent systems provide a framework for studying distributed decision-making problems as a number of agents make local decisions by interacting with other agents over networks [3–5]. Due to the rise in the use of wireless communication channels connecting physically-separated agents for such systems, cybersecurity has become a major critical issue on networked multiagent systems [6–8], including transportation networks [9] and infrastructure networks [10].

Due to its decentralized nature, networks are prone to the outside threats. These threats may damage the connection among components in the networks, which in turn make the network lose its function. Several types of threats in the context of network security have been studied, namely jamming attacks [11], eavesdropping and injection attacks [12, 13], and others.

One of the most common threats is jamming attacks [11, 14], where the adversary from outside the system transmits interference signals on the communication channels that disrupt the communication process among the agents in a network. These attacks

are also studied in the context of multiagent systems where each agent/component in the network admits certain dynamics. Such attacks may make the agents update their state values in a faulty and even malicious manner. Multiagent consensus problems in the presence of such jamming attacks have been studied in, e.g., [15, 16]. Also, [17] considers a multiagent system under jamming, where a stochastic communication protocol is introduced so that the attackers do not know the exact transmission times in advance. Event-triggered approach in consensus dynamics under attacks is discussed in [18, 19]. The resilience and robustness in consensus problems under attacks have been discussed in [20–22]. Distributed algorithms on the consensus process in the face of attacks have been proposed in, e.g., [23].

In discussing jamming attacks, it is reasonable to assume that attacker is constrained so that it could not attack the network at all time. Jamming attack models with energy constraints of the outside attacker were introduced in [17, 24–26] in the context of networked control. These models have been generalized to further take account of probabilistic packet losses in [27]. Also, nonmalicious packet losses that can interrupt the communication among agents have been studied for consensus in [28, 29].

In response to jamming attacks, in resilient systems there exists a defense mechanism that can be incorporated to coordinate the recovery process of the network [30]. In practice, this defense mechanism can be represented by, for example, system administrators and firewall. Similar to the attacks, the recovery process may be more efficient if the defense mechanism is aware of system parameters and states. The relation between jamming and recovering of the networks where the defense mechanism can overcome the attacker's jamming by sending signals that increase signal-to-interference-plus-noise ratio (SINR) is employed in [31, 32].

In this thesis, we focus on analyzing jamming attacks and defenses in networked multiagent systems where the attacker and the defender are intelligent and aware of system parameters and the agent states. The jamming attacks are represented by the removal of edges/links of the graph which model the network, whereas the defenses are represented by the rebuilding of some of the attacked edges.

1.2 Game-theoretical approaches of cyber-attacks and networks

As mentioned above, the attacks on the networked systems are more dangerous if the attacker decides optimally how and when to attack. The way the attacker decides the attack strategy may be different time to time, depending on the situations in the systems.

On the other hand, the defense mechanism in the resilient networked systems also needs to take optimal measures dynamically to lessen the attacks. Hence, it is natural to formulate the relation between the attacker and the defense mechanism with game-theoretic approach. This game-theoretical approach has an advantage over optimization of only one party (attacker or defender), since the actions of other parties are also captured in this approach.

A game can be defined with four components: players, action spaces, payoffs, and information structures [33]. These components need to be formulated precisely in order to get appropriate models of the networked multiagent systems. It is common to formulate the game regarding cyber-attacks as a *noncooperative game*, since the players have different objectives, often opposite to others [1, 7]. It is also intuitive to analyze the *equilibrium* of the game, which is a set of actions where the players cannot obtain higher payoff by changing only their own actions.

The works [34–36] models the relation between the activity of jamming and transmitting as zero-sum games, where the payoff structure of the players is balanced. *Stackelberg game* approach is considered for two-player games in [31, 32], in which the players decide their strategies sequentially by following a certain hierarchy. Game-theoretic approaches to model the interaction between attackers and other players protecting the network have also been utilized for the analysis of jamming attacks [37] and false data injection attacks on networks [38–40]. Games on jamming attacks with *imperfect knowledge* of the players are considered in [41], where the players do not exactly know the systems environment. *Subgame perfect equilibrium* between the attacker and the defense mechanism on the networked systems is studied in [42]. The optimal design of networks in face of the attacks is discussed in [42, 43].

Other types of games in the context of network include mean-field games [44, 45], aggregative games [46], potential games [47], and Markov games [48]. The setting where players do not have a complete information is studying as signalling and screening games in [49, 50]. Instead of noncooperative setting, some works as [51] consider cooperation among agents in the networks in achieving their goals. To reach equilibrium, players may employ certain learning methods, such as no-regret learning, which is discussed in [52] in the context of multiagent system.

In addition, this game-theoretical approach can be used to design an effective system where rational players in the system act optimally. This optimal network design is called *mechanism design*, as studied in [53–55].

Repeated games refer to a game setting when the players apply the actions repeatedly over time [33], where players have to choose between long-term or short-term preferences,

often by considering *discount factor* over different steps of the game [56]. Some related works in repeated games include [57]. In the context of games over networks, the fact that players apply their actions repeatedly will affect the dynamics of the agents. This is discussed in [58] in the context of consensus dynamics. Model predictive control under game theoretical setting is discussed in [58, 59].

In this thesis, we focus on analyzing game-theoretical approach on the interaction between an attacker and a defender in networked multiagent systems setting. Specifically, we consider sequential games following *Stackelberg* model played repeatedly over time, where the attacker decides its action first by deciding which edges to attack and for how long. In response to that attack, the defender then determines which edges are to be recovered. We examine how the difference of abilities between the attacker and the defender represented by the *energy parameters* and *horizon parameters* affect equilibrium and agents' dynamics in the long term.

1.3 Overview of the thesis

In this thesis, we formulate a two-player game problem where players follow certain attack-defense sequence, repeated over time, in a multiagent consensus setting. We investigate the effects of state-dependent and graph-dependent attack and defense strategies in a consensus process in networked multiagent system. We specifically consider two formulations: first is where the players' strategies depend on graph parameters, and second is where the players' strategies depend on state of the agents and on how close to consensus they may be. The players are supposed to spend their limited resources by attacking and recovering, and therefore the attack and recovery edges and times/durations are limited.

In the first part of the thesis, we find explicit conditions characterizing the players' optimal strategies. Then, we investigate the implication of the conditions by studying simple cases, leading us to some conditions on the players' utilities that determine the players' strategies.

Then, in the later part of the thesis, we further examine the effect of the optimal strategies of game on the network in the long term. Under the repeated games formulation, we consider a rolling/receding horizon setting of the players, where different horizon parameters are used to characterized players' various abilities. The consensus process of agents are affected by the resource/energy parameters as well as the horizon parameters of the players.

This thesis is organized as follows. We discuss the general problem formulation in the

Chapter 2. We then explain the problem formulation in more detail and its corresponding results in each subsequent chapter.

In Chapter 3, we formulate that the players decide their strategies based on the graph parameters such as edge connectivity and pairwise connectivity in continuous time. There, we obtain the optimal strategies for the players in terms of edges and attack/recovery durations.

In Chapter 4 we suppose that the players play a multiple-step game by considering the future time interval as well as the current time interval. There, we also consider a more powerful attack setting that enables the attacker to entirely prevent consensus among agents.

The discrete-time version of the formulation is first discussed in Chapter 5. In this setting, the players determine their strategies for several discrete time-step ahead. A moving horizon setting is then adopted for this setting, where the players are able to revise their strategies that were previously obtained.

We continue this moving horizon approach in Chapter 6, where we examine how the players perform under non-uniform values of horizon parameters. The expected utility is used to measure players' performance. Furthermore, in Chapter 6 we discuss how the consensus of agents may be impacted by this non-uniform horizon setting. The proofs for the theoretical results are located in the appendix section in the end of each chapter.

1.4 Mathematical notations

We use a fairly standard notation in the thesis. Specifically, we write $\mathbb{R}$ for the set of real numbers, $\mathbb{N}_0$ for the set of nonnegative integers, and $\mathbb{N}$ for the set of positive integers. We denote $|\cdot|$ as cardinality of a set, $\lfloor x \rfloor$ as a floor function of x, and $\lceil x \rceil$ as a ceiling function of x.

Throughout this thesis, we consider an underlying undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, with $\mathcal{V}$ representing the set of agents and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ representing the set of links/edges connecting agents $\mathcal{V}$. The graph $\mathcal{G}$ consists of $n = |\mathcal{V}|$ number of agents. We denote the Laplacian matrix of a complete graph with n agents (not to be confused with graph $\mathcal{G}$) as L_{c}.

As we consider a repeated game setting in this thesis, several variables will have superscripts and subscripts. In this thesis, the superscripts are denoting the player of the game (A for attacker, D for defender), whereas the subscripts denote the time index of the game. Other notations are explained independently later in each chapter.

Chapter 2

Sequential Two-player Game Formulation

In this chapter we discuss the general problem formulation of the attack and recovery sequences in networked systems. The results of the thesis, which are shown in Chapter 3–6, are based on this general formulation. We later specify the more detailed formulation in each subsequent chapter. This chapter also explains briefly about general theoretical background and methods used to obtain the results.

The chapter is organized as follows. We first described briefly about the consensus dynamics on time-varying multiagent systems in Section 2.1. In Section 2.2, we first discuss the game where the players play sequentially, i.e., they do not decide their actions simultaneously. We then discuss one of the solution concept for the aforementioned game, called subgame perfect equilibrium, in Section 2.3. We describe the general problem formulation used in this thesis in Section 2.4 and the energy constraints of the players in Section 2.5.

2.1 Consensus process on time-varying multiagent systems

In the analysis of networked multiagent systems, it is common to model the system using graph, which is a collection of *vertices* (also referred as *agents*) and *edges* (also referred as *links*). Specifically, the graph $\mathcal{G}$ is defined as $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, with $\mathcal{V}$ representing set of agents and $\mathcal{E}$ representing set of links. it is then assumed that each agent possesses a state which is influenced by the states of other agents, characterized by the graph topology, i.e., set of links between agents [4, 5].

Consensus (or also commonly referred as averaging) is one of the most common dynamics considered when studying multiagent systems [4, 5]. In the consensus process, each agent is expected to converge in states at infinite time. We assume throughout this thesis that agent $i \in \mathcal{V}$ of the graph $\mathcal{G}$ has a scalar state, whose dynamics are defined as

$$\dot{x}_i(t) = \sum_{j \in \mathcal{N}_i} (x_j(t) - x_i(t)), \quad x(0) = x_0, \quad t \geq 0. \tag{2.1}$$

The speed of the consensus is influenced by how connected the graph is [4, 5]. The more connected graphs enable the agents to communicate with more neighbors $\mathcal{N}_i$, which implies that $\dot{x}_i(t)$ changes more drastically. On the other hand, if the underlying graph becomes disconnected, the consensus is achieved slower, or even not achieved at all if the graph is disconnected (there are pair of vertices without path between them) for infinite time.

In this work, we investigate how the consensus in a time-varying graph as in [3], i.e., the topology of the graph changes by time, is characterized. In that case, the neighbors of agent i also change by time, and the dynamics in (2.1) can be slightly modified to

$$\dot{x}_i(t) = \sum_{j \in \mathcal{N}_i(t)} (x_j(t) - x_i(t)), \quad x(0) = x_0, \quad t \geq 0. \tag{2.2}$$

We consider this continuous-time setting in Chapters 3 and 4. For Chapters 5 and 6, we consider agents consensus dynamics in discrete time k as

$$x_i[k+1] = x_i[k] + u_i[k], \quad x[0] = x_0, \tag{2.3}$$

where $u_i[k]$ denotes the control input applied to agent i. We assume that $u_i[k]$ is constructed as the weighted sum of the state differences between agent i and its neighbor agents, commonly used in, e.g., [60], which is given by

$$u_i[k] = \sum_{j \in \mathcal{N}_i[k]} a_{ij}(x_j[k] - x_i[k]), \tag{2.4}$$

where $\mathcal{N}_i[k]$ denotes the set of agents that can communicate with agent i at time k, and $a_{ij} > 0$ represents the weight of edge $(i, j) \in \mathcal{E}$ such that $\Sigma_{j=1, j \neq i}^{n} a_{ij} < 1$, $i \in \mathcal{V}$ to ensure that the agents achieve consensus without any attack [4, 5]. Note that $\mathcal{N}_i[k]$ may also change due to the attacks.

2.2 Attack-recovery sequence and extensive-form game

In this thesis, we consider that the attack and recovery processes of the networked systems do not happen simultaneously. Naturally, the defense mechanism (also referred as the defender) is able to recover the communications among agents by reacting in response to the attacks.

The defender first needs to acknowledge the attacks before it can make the recoveries. In practice, we suppose that the agents recognize the attacks affecting the communication links and consequently report the abnormality to the centralized defender. The defender then asks some agents to send stonger communication signals on some communication links.

The sequence in general is formulated as

$$\text{No attack} \longrightarrow \text{Attack} \longrightarrow \text{Recover} \longrightarrow \text{No attack} \longrightarrow \text{Attack} \longrightarrow \text{Recover} \longrightarrow \dots$$

The game where the players do not decide their actions in the same time is better expressed with the extensive-form game (as opposed to payoff matrix, which is normally used on simultaneous two-player game). The utilities of the players' action in the extension-form game are shown in a tree-like structure. In the extensive form game, each decision-making node is called *subgame*. The player associated with the node then makes its decision for its corresponding subgame(s), by selecting the action that arises from the abovementioned node [33].

The example of the extensive-form game is shown in Figure 2.1. There are 2 players in this game: Player 1 and Player 2 (represented by the number inside the circle in each branch), and each player has two actions (U and D for Player 1, and U' and D' for Player 2). The payoff of the actions are shown in the numbers inside the bracket, with the first number representing the payoff of Player 1 and the second number representing the payoff of Player 2. The subgame here is each decision-making point of Player 1 and Player 2.

2.3 Subgame perfect equilibrium and backward induction

Throughout this thesis, we utilize a solution concept of the extensive-form game called *subgame perfect equilibrium*, modeled by Stackelberg sequential model [2, 33]. To find the equilibrium of the extensive-form game, we use *backward induction* method.

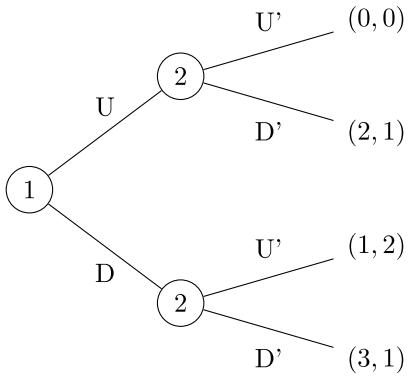


Figure 2.1 Example 1 of extensive-form game.

In this thesis, we focus on a subgame perfect equilibrium analysis of a two-player game. The players' strategies/policies belong to certain *strategy space* are $s_1 \in S_1$ and $s_2 \in S_2$ for player 1 and 2, respectively. In general, the set of strategies/policies of the two players (s_1^*, s_2^*), with player 1 as a *leader* and player 2 as a *follower* are said to follow the subgame perfect equilibrium if

$$u_1(s_1^*, s_2^*(s_1^*)) \geq u_1(s_1, s_2^*(s_1)), \tag{2.5}$$

where $(s_2^*(s_1))$ satisfy

$$u_2(s_1, s_2^*) \geq u_2(s_1, s_2), \tag{2.6}$$

with u_1 and u_2 being the utility of player 1 and 2, respectively.

This method is easier to explain with the example as in Figure 2.1. In the tree, with the backward induction method the players choose the strategies that maximizes its payoff, beginning from the smallest subgame. In Figure 2.1, Player 2 chooses D' given that Player 1 chooses U, and Player 2 chooses U' given that Player 1 chooses D. We can remove other strategies that are not selected from the equilibrium candidates.

We then select the optimal strategies for Player 1 from the remaining possibilities. Knowing that Player 2 responds optimally, Player 1 chooses U, with the strategy profile {U,D'} being the subgame perfect equilibrium. This is called subgame perfect equilibrium since it represents the Nash equilibrium in every subgame [33].

We can also look at one more example shown in Figure 2.2. In this example, the strategy {Attack, Recover} is the subgame perfect equilibrium. The defender chooses to recover rather than not, and the attacker also decides to attack given that the defender will choose to recover.

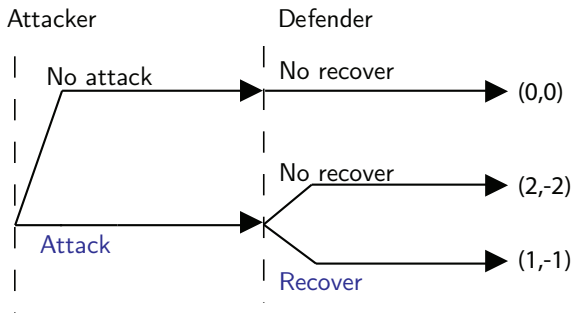


Figure 2.2 Example 2 of extensive-form game.

2.4 General sequence and problem formulation

The networked system is represented by a connected and undirected graph $\mathcal{G}$. 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 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, i.e., there exists a path connecting every pair of vertices in $\mathcal{V}$.

In this thesis, we consider a game between two players, the attacker and the defender, in terms of the communication among the agents. The attacker is defined as 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's objective is to attack the communication activities between the agents. We assume that the attacker sends jamming signals from outside the network that interfere with the communication signals. The presence of the jamming signals worsen the quality of the communication signals, and therefore making communications among the agents impossible. 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 agents send abnormality reports consisting of which links are jammed and the start jamming time to the defender. The defender then decides which links to be recovered and subsequently 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. From this sequence of attacks and recoveries in a single game, we observe that the graphs are *resilient*, i.e., the group of agents are able to recover from the damages caused by the attacker.

We seek the subgame perfect equilibrium of this game as in [42, 61]. To this end,

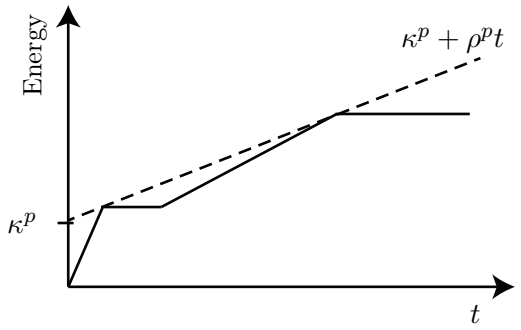


Figure 2.3 Energy constraint of player p considered in the formulation.

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, a *backward induction* approach is used. The more detailed explanation on the game is explained in each chapter.

2.5 Energy constraints

In a jamming attack formulation, it is natural to consider that the jammer/the attacker has an energy constraint such that, if it is not connected to energy sources, it is impossible to attack all communication links of the network at all times [17, 27]. In the context of game-theoretical approaches, this constraint becomes important to characterize the strategic behaviors of the players [34].

In this work, we suppose that the players consume energy by doing their actions, i.e., by attacking or recovering. A player $p \in \{\mathrm{A}, \mathrm{D}\}$, with A denoting the attacker and D denoting the defender, consumes more energy if it does its action longer or in more links. We formulate that the energy consumed by the players cannot exceed certain value. Specifically, throughout this thesis it is assumed that the energy consumed by the players cannot exceed the total supplied energy which increases linearly in time. This constraint in turn will limit the actions of the players.

We follow the approach in [14, 17] to model such energy constraints. In general, in the continuous-time setting, the total energy used for player $p \in \{\mathrm{A}, \mathrm{D}\}$ at any time t must satisfy

$$\text{Total energy used by player } p \leq \kappa^p + \rho^p t, \tag{2.7}$$

with $\kappa^p, \rho^p > 0$, and $k \in \mathbb{N}$. The parameters κ^p and ρ^p denote the initial energy at $t = 0$ and the recharge rate of energy for player p, respectively. The inequality (2.7) implies

that total energy spent by a player cannot exceed the available energy characterized by the initial energy κ^p and the supplied energy $\rho^p t$ by time t. In practice, this implies that the players may be assumed to be able to supply energy wirelessly to devices that obstruct/retain communication signals between the agents so that the energy supply rates to these devices are limited by the parameters κ^p and ρ^p. Figure 2.3 shows the energy constraint of player p, with the dashed line being the available energy and the solid line being total energy spent. This general constraint becomes the basis of the formulation of energy constraints in Chapters 3 and 4.

For discrete-time setting, we consider the similar constraint that has to be satisfied at any time $k \in \mathbb{N}_0$

$$\text{Total energy used by player } p \leq \kappa^p + \rho^p k, \tag{2.8}$$

with $\kappa^p, \rho^p > 0$. This general constraint becomes the basis of the formulation of energy constraints in discrete-time setting formulation in Chapters 5 and 6.

Chapter 3

Dynamic Resilient Network Games with Applications to Multiagent Consensus

3.1 Introduction

Noncooperative game theory approaches are widely used for addressing security problems including jamming attacks [1, 7]. Jamming attacks on networked systems were previously analyzed through game-theoretic approaches. The works [34–36] model the activity of jamming and transmitting signals as zero-sum games where the payoff structure of the players is balanced. In [31, 32], the authors consider a Stackelberg game approach, in which the players decide their actions sequentially by following a certain hierarchy. Stackelberg equilibrium computation is discussed in [62]. Other works that use Stackelberg setting in the context of cyber security include [63, 64]. *Actor-critic* method has also been used under two-player Stackelberg setting in [65].

Multiagent consensus problems in the presence of such jamming attacks have been studied in [11, 14]. The work [17] 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 [17, 24–26] in the context of networked control. These models have been generalized to further take account of probabilistic packet losses in [26]. 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 [20–22]. Also, nonmalicious packet losses that can interrupt the communication among agents have been studied in [28, 29].

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 [66] 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 [38], 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 chapter, 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 [61], 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 [61].

We emphasize that our contribution is the introduction of a game-theoretic framework to jamming attack problems. We follow the attack models dealt with in [17, 24–26], 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 [31, 32]. 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

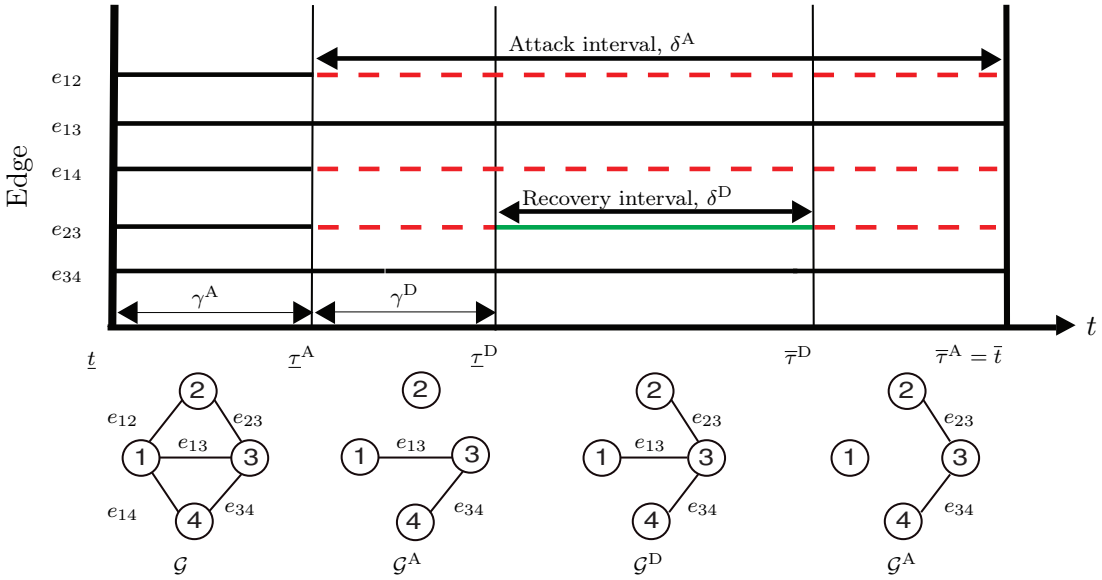


Figure 3.1 Illustration of graph transition. At time interval $[\underline{t}, \overline{t}]$, the defender recovers one edge e_{23} at $\underline{\tau}^{\mathrm{D}}$ and stops recovering at $\overline{\tau}^{\mathrm{D}}$. Note that the solid lines indicate that the edges are connected, and dashed lines indicate that the edges are disconnected.

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.

To compute the equilibrium, we use combinatiorial optimization of all edges. The related algorithms and works on combinatiorial optimization can be found in [67]. In a more sophisticated approachh, neural network is used to solve combinatorial optimization in [68].

In this chapter, we introduce the framework for the resilient graph game in Section 3.2. In Section 3.3, we examine the equilibria of the game in a single interval. We provide an analysis of consensus among agents as well as the optimal strategies of the players considering the energy constraints in Section 3.4. We then present simulations on the dynamic graph games and the resulting states evolutions in Section 3.5. Finally, we conclude the chapter in Section 3.6. The content in this chapter is published in conference proceedings [C1,C3,O1] and in a journal article [J1].

3.2 Problem formulation

We consider a multiagent system of n agents with a communication topology described by the undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. 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 chapter, 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 3.4 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 $\mathcal{E}^{\mathrm{A}} \subseteq \mathcal{E}$ from time $\underline{\tau}^{\mathrm{A}}$ until $\overline{\tau}^{\mathrm{A}}$, where $\underline{t} < \underline{\tau}^{\mathrm{A}} \leq \overline{\tau}^{\mathrm{A}} \leq \bar{t}$. Consequently, $\mathcal{G}$ is changed to $\mathcal{G}^{\mathrm{A}} := (\mathcal{V}, \mathcal{E} \setminus \mathcal{E}^{\mathrm{A}})$ at $\underline{\tau}^{\mathrm{A}}$. 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 $[\underline{\tau}^{\mathrm{A}}, \overline{\tau}^{\mathrm{A}}]$, where the values of $\overline{\tau}^{\mathrm{A}}$ are related to the attacker's energy, as discussed later. If there is no attack, it is understood that $\underline{\tau}^{\mathrm{A}} = \overline{\tau}^{\mathrm{A}}$.

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 $\mathcal{E}^{\mathrm{D}}$ from time $\underline{\tau}^{\mathrm{D}}$ until $\overline{\tau}^{\mathrm{D}}$, with $\mathcal{E}^{\mathrm{D}} \subseteq \mathcal{E}^{\mathrm{A}}$ and $\underline{t} < \underline{\tau}^{\mathrm{A}} < \underline{\tau}^{\mathrm{D}} \leq \overline{\tau}^{\mathrm{D}} \leq \overline{\tau}^{\mathrm{A}} \leq \bar{t}$. As soon as the defender starts the recovery action at $\underline{\tau}^{\mathrm{D}}$, the graph $\mathcal{G}^{\mathrm{A}}$ is changed to

$\mathcal{G}^{\mathrm{D}} := (\mathcal{V}, (\mathcal{E} \setminus \mathcal{E}^{\mathrm{A}}) \cup \mathcal{E}^{\mathrm{D}}))$. 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 $\underline{\tau}^{\mathrm{D}} = \overline{\tau}^{\mathrm{D}}$. We define the recovery interval as $[\underline{\tau}^{\mathrm{D}}, \overline{\tau}^{\mathrm{D}}]$, where values of $\overline{\tau}^{\mathrm{D}}$ 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 $\gamma^{\mathrm{A}} > 0$ between the beginning of the game $\underline{t}$ and the beginning of the attack time $\underline{\tau}^{\mathrm{A}}$. For the defender, there is also a constant dwell time $\gamma^{\mathrm{D}} > 0$ between the beginning of attack time $\underline{\tau}^{\mathrm{A}}$ and the beginning of recovery time $\underline{\tau}^{\mathrm{D}}$ unless the attacker ends attacking earlier, i.e., $\overline{\tau}^{\mathrm{A}} < \underline{\tau}^{\mathrm{D}}$. Thus, let

$$\underline{\tau}^{\mathrm{A}} := \underline{t} + \gamma^{\mathrm{A}}, \quad \underline{\tau}^{\mathrm{D}} := \min\{\overline{\tau}^{\mathrm{A}}, \underline{\tau}^{\mathrm{A}} + \gamma^{\mathrm{D}}\}. \tag{3.1}$$

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

$$\delta^{\mathrm{A}} := \overline{\tau}^{\mathrm{A}} - \underline{\tau}^{\mathrm{A}}, \quad \delta^{\mathrm{D}} := \overline{\tau}^{\mathrm{D}} - \underline{\tau}^{\mathrm{D}}. \tag{3.2}$$

The timeline of the attack and the recovery sequences is illustrated in Figure 3.1.

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

$$\widehat{\lambda}(\mathcal{G}') := \begin{cases} \lambda(\mathcal{G}'), & \text{if } \mathcal{G}' \text{ is connected,} \\ -\widetilde{\lambda}(\mathcal{G}'), & \text{otherwise,} \end{cases} \tag{3.3}$$

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 $\mathcal{G}^{\mathrm{A}} \subseteq \mathcal{G}^{\mathrm{D}} \subseteq \mathcal{G}$, note that $\widehat{\lambda}(\mathcal{G}^{\mathrm{A}}) \leq \widehat{\lambda}(\mathcal{G}^{\mathrm{D}}) \leq \hat{\lambda}(\mathcal{G})$.

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 $\mathcal{G}^{\mathrm{A}}$. The attacker should strategically choose the edges to jam to reduce $\widehat{\lambda}(\mathcal{G}^{\mathrm{A}})$ (making $\mathcal{G}^{\mathrm{A}}$ more disconnected), and the defender also should choose the edges to efficiently increase $\widehat{\lambda}(\mathcal{G}^{\mathrm{D}})$ (making $\mathcal{G}^{\mathrm{D}}$ 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 $\widehat{\lambda}(\mathcal{G}^{\mathrm{A}})$ or $\widehat{\lambda}(\mathcal{G}^{\mathrm{D}})$. Since we focus on the connectivity of the agents to characterize the utility functions below without specifying particular edges to attack/recover, we define $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}})$ to represent the generalized edge connectivity of the underlying graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with $m^{\mathrm{A}} = |\mathcal{E}^{\mathrm{A}}|$ edges attacked and $m^{\mathrm{D}} = |\mathcal{E}^{\mathrm{D}}|$ edges recovered, given by

$$\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}}) := \min_{\mathcal{E}^{\mathrm{A}}:|\mathcal{E}^{\mathrm{A}}|=m^{\mathrm{A}}} \max_{\mathcal{E}^{\mathrm{D}}:|\mathcal{E}^{\mathrm{D}}|=m^{\mathrm{D}}} \widehat{\lambda}((\mathcal{V}, (\mathcal{E} \setminus \mathcal{E}^{\mathrm{A}}) \cup \mathcal{E}^{\mathrm{D}})). \tag{3.4}$$

For the simple case of $m^{\mathrm{D}} = 0$, calculating the right-hand side in (3.4) reduces to the min-cut problem for undirected and unweighted graph $\mathcal{G}$, for which efficient randomized algorithms are available [69]. More in general, we can apply the so-called k-cut algorithms [70] 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 $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}}, m^{\mathrm{D}})$ represents the $(m^{\mathrm{A}}+1, m^{\mathrm{D}}+1)$ entry of the matrix. For example, the matrix $\widehat{\lambda}_{\mathcal{G}}$ for the graph $\mathcal{G}$ in Figure 3.1 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 $(m^{\mathrm{A}}, \delta^{\mathrm{A}})$ and $(m^{\mathrm{D}}, \delta^{\mathrm{D}})$, respectively. For the game of the time interval $[\underline{t}, \overline{t}]$, we define the utility function U^{A} of

the attacker as

$$U^{\mathrm{A}}((m^{\mathrm{A}},\delta^{\mathrm{A}}),(m^{\mathrm{D}},\delta^{\mathrm{D}})) := -\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}},0)(\delta^{\mathrm{A}}-\delta^{\mathrm{D}}) - \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}},m^{\mathrm{D}})\delta^{\mathrm{D}} - \beta^{\mathrm{A}}m^{\mathrm{A}}\delta^{\mathrm{A}}, \quad (3.5)$$

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

$$U^{\mathrm{D}}((m^{\mathrm{A}},\delta^{\mathrm{A}}),(m^{\mathrm{D}},\delta^{\mathrm{D}})) := \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}},0)(\delta^{\mathrm{A}}-\delta^{\mathrm{D}}) + \widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}},m^{\mathrm{D}})\delta^{\mathrm{D}} - \beta^{\mathrm{D}}m^{\mathrm{D}}\delta^{\mathrm{D}}, \quad (3.6)$$

where $\beta^{\mathrm{D}} > 0$ is the defender's cost to recover one edge per time unit. Note that the utility function (3.5) represents the total generalized edge connectivity (with the negative sign) for the attacker over the game horizon $[\underline{\tau}^{\mathrm{A}},\bar{t}]$ plus the cost for jamming m^{A} number of communication links. Similarly, (3.6) represents the total generalized edge connectivity for the defender over the game horizon $[\underline{\tau}^{\mathrm{A}},\bar{t}]$ 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 $\overline{\tau}^{\mathrm{A}}$. Otherwise, the game ends at $\underline{t} + \gamma^{\mathrm{A}} + \gamma^{\mathrm{D}}$. In other words, the end time $\bar{t}$ of the game is

$$\bar{t} := \begin{cases} \overline{\tau}^{\mathrm{A}}, & \text{if } m^{\mathrm{A}} > 0, \\ \underline{t} + \gamma^{\mathrm{A}} + \gamma^{\mathrm{D}}, & \text{otherwise.} \end{cases} \quad (3.7)$$

According to the utility functions (3.5) and (3.6), 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 $\mathcal{G}^{\mathrm{A}}$ at $\overline{\tau}^{\mathrm{D}}$, with generalized edge connectivity $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}},0)$. Therefore, in $[\overline{\tau}^{\mathrm{D}},\bar{t}]$, the utilities of both players in (3.5) and (3.6) are computed based on $\widehat{\lambda}_{\mathcal{G}}(m^{\mathrm{A}},0)$.

The players cannot keep sending signals for very long durations due to energy constraints. We assume that if player $p \in \{\mathrm{A},\mathrm{D}\}$ 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 the next two sections.

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 thesis, 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 [61]. 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

$$(m^{\mathrm{D}*}(m^{\mathrm{A}}, \delta^{\mathrm{A}}), \delta^{\mathrm{D}*}(m^{\mathrm{A}}, \delta^{\mathrm{A}})) \in \underset{(m^{\mathrm{D}}, \delta^{\mathrm{D}})}{\arg\max}\, U^{\mathrm{D}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}}, \delta^{\mathrm{D}})), \tag{3.8}$$

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

$$(m^{\mathrm{A}*}, \delta^{\mathrm{A}*}) \in \underset{(m^{\mathrm{A}}, \delta^{\mathrm{A}})}{\arg\max}\, U^{\mathrm{A}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}*}(m^{\mathrm{A}}, \delta^{\mathrm{A}}), \delta^{\mathrm{D}*}(m^{\mathrm{A}}, \delta^{\mathrm{A}}))). \tag{3.9}$$

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.

Remark 3.1. We note that the game used in this chapter and throughout this thesis is repeated games played repeatedly over time. The solution concept used is a standard subgame perfect equilibrium in Stackelberg/sequential game setting represented by extensive form/game tree, which has been widely used [33].

However, in this thesis each game is different due to the difference of the energy used of the players, which are affected by the actions taken by them previously. This formulation with change of strategy space in each time due to the previous actions is relatively new in the game theory field, and is the contribution of our results.

Table 3.1: Possible cases of attack and recovery actions

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

Table 3.2: 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

3.3 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}).

3.3.1 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 $\hat{\lambda}(\mathcal{G})$, $\hat{\lambda}(\mathcal{G}^{\mathrm{A}})$, and $\hat{\lambda}(\mathcal{G}^{\mathrm{D}})$ into three cases shown in Table 3.1. 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 $\hat{\lambda}(\mathcal{G}^{\mathrm{A}}) = \hat{\lambda}(\mathcal{G})$ and $\hat{\lambda}(\mathcal{G}^{\mathrm{D}}) > \hat{\lambda}(\mathcal{G}^{\mathrm{A}})$. Also, note that since by definition $m^{\mathrm{D}} \geq 0$, condition $\hat{\lambda}(\mathcal{G}^{\mathrm{D}}) < \hat{\lambda}(\mathcal{G}^{\mathrm{A}})$ 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 3.1. A summary of the results of the optimal strategies is shown in Table 3.2. 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 3.3: 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	$\mathcal{E}_k^{\mathrm{A2b}*}$	$\underline{\tau}^{\mathrm{D}} - \underline{\tau}^{\mathrm{A}}$			
3	A3	$m^{\mathrm{A3}*}$	$\Delta^{\mathrm{A}}(m^{\mathrm{A3}*})$	D3	$\mathcal{E}^{\mathrm{D3}*}$ $(m^{\mathrm{A3}*})$	ξ

3.3.2 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.

3.3.2.1 Subgame perfect equilibrium analysis in each case

From the problem formulation, since $\hat{\lambda}(\mathcal{G}) \geq \hat{\lambda}(\mathcal{G}^{\mathrm{D}}) \geq \hat{\lambda}(\mathcal{G}^{\mathrm{A}})$, we obtain three cases based on the combinations of $\hat{\lambda}(\mathcal{G})$, $\hat{\lambda}(\mathcal{G}^{\mathrm{A}})$, and $\hat{\lambda}(\mathcal{G}^{\mathrm{D}})$, as shown in Table 3.1. 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 3.3.

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 3.1, the utility function in (3.6) of the defender becomes

$$U^{\mathrm{D}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}}, \delta^{\mathrm{D}})) = \hat{\lambda}(\mathcal{G})\delta^{\mathrm{A}} - \beta^{\mathrm{D}} m^{\mathrm{D}} \delta^{\mathrm{D}}. \tag{3.10}$$

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

$$U^{\mathrm{D}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*})) = \hat{\lambda}(\mathcal{G})\delta^{\mathrm{A}}. \tag{3.11}$$

This strategy $m^{\mathrm{D}*} = 0$ and $\delta^{\mathrm{D}*} = 0$ for the defender is named **Strategy D1** (see Table 3.3).

Likewise, for the attacker, the utility function in (3.5) becomes

$$U^{\mathrm{A}}((m^{\mathrm{A}},\delta^{\mathrm{A}}),(m^{\mathrm{D}*},\delta^{\mathrm{D}*}))=(-\hat{\lambda}(\mathcal{G})-\beta^{\mathrm{A}}m^{\mathrm{A}})\delta^{\mathrm{A}}. \tag{3.12}$$

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

$$U^{\mathrm{A}}((m^{\mathrm{A}*},\delta^{\mathrm{A}*}),(m^{\mathrm{D}*},\delta^{\mathrm{D}*}))=0=:\hat{U}^{\mathrm{A1}}, \tag{3.13}$$

$$U^{\mathrm{D}}((m^{\mathrm{A}*},\delta^{\mathrm{A}*}),(m^{\mathrm{D}*},\delta^{\mathrm{D}*}))=0=:\hat{U}^{\mathrm{D1}}. \tag{3.14}$$

From (3.7), because $m^{\mathrm{A}}=m^{\mathrm{D}}=0$, it follows that the game ends at $\bar{t}=\underline{t}+\gamma^{\mathrm{A}}+\gamma^{\mathrm{D}}$. 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 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 $\hat{\lambda}(\mathcal{G}^{\mathrm{D}})=\hat{\lambda}(\mathcal{G}^{\mathrm{A}})$, the utility function of the defender with $m^{\mathrm{D}*},\delta^{\mathrm{D}*}=0$ as in (3.11) is given by

$$U^{\mathrm{D}}((m^{\mathrm{A}},\delta^{\mathrm{A}}),(m^{\mathrm{D}*},\delta^{\mathrm{D}*}))=\hat{\lambda}(\mathcal{G}^{\mathrm{A}})\delta^{\mathrm{A}}. \tag{3.15}$$

For the attacker, from (3.5) with $\delta^{\mathrm{D}}=0$, we have

$$U^{\mathrm{A}}((m^{\mathrm{A}},\delta^{\mathrm{A}}),(m^{\mathrm{D}*},\delta^{\mathrm{D}*}))=(-\hat{\lambda}(\mathcal{G}^{\mathrm{A}})-\beta^{\mathrm{A}}m^{\mathrm{A}})\delta^{\mathrm{A}}. \tag{3.16}$$

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

$$U^{\mathrm{A}}((m^{\mathrm{A}},\delta^{\mathrm{A}*}),(m^{\mathrm{D}*},\delta^{\mathrm{D}*}))=(-\hat{\lambda}(\mathcal{G}^{\mathrm{A}})-\beta^{\mathrm{A}}m^{\mathrm{A}})\Delta^{\mathrm{A}}=:\hat{U}^{\mathrm{A2a}}(m^{\mathrm{A}}). \tag{3.17}$$

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 (3.17), resulting in

$$m^{\mathrm{A2a}*}\in\underset{m^{\mathrm{A}}>0}{\arg\max}\,\hat{U}^{\mathrm{A2a}}(m^{\mathrm{A}}). \tag{3.18}$$

Note that with this strategy, (3.15) becomes

$$U^{\mathrm{D}}((m^{\mathrm{A}*},\delta^{\mathrm{A}*}),(m^{\mathrm{D}*},\delta^{\mathrm{D}*}))=\hat{\lambda}(\mathcal{G}_k^{\mathrm{A2a}*})\Delta^{\mathrm{A}}=:\hat{U}^{\mathrm{D2a}}. \tag{3.19}$$

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 3.1, the generalized edge connectivities satisfy $\hat{\lambda}(\mathcal{G})\geq\hat{\lambda}(\mathcal{G}^{\mathrm{D}})>\hat{\lambda}(\mathcal{G}^{\mathrm{A}})$.

From (3.6), the defender's utility function can be written as

$$U^{\mathrm{D}}((m^{\mathrm{A}},\delta^{\mathrm{A}}),(m^{\mathrm{D}},\delta^{\mathrm{D}}))=\phi\delta^{\mathrm{D}}+\hat{\lambda}(\mathcal{G}^{\mathrm{A}})\delta^{\mathrm{A}}, \tag{3.20}$$

with $\phi:=(\hat{\lambda}(\mathcal{G}^{\mathrm{D}})-\hat{\lambda}(\mathcal{G}^{\mathrm{A}})-\beta^{\mathrm{D}}m^{\mathrm{D}})$ for simplicity. Since $\hat{\lambda}(\mathcal{G}^{\mathrm{A}})<\hat{\lambda}(\mathcal{G}^{\mathrm{D}})$, 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

$$U^{\mathrm{D}}((m^{\mathrm{A}},\delta^{\mathrm{A}}),(m^{\mathrm{D}},\min\{\Delta^{\mathrm{D}},\overline{\tau}^{\mathrm{A}}-\underline{\tau}^{\mathrm{D}}\}))=\phi(\min\{\Delta^{\mathrm{D}},\overline{\tau}^{\mathrm{A}}-\underline{\tau}^{\mathrm{D}}\})+\hat{\lambda}(\mathcal{G}^{\mathrm{A}})\delta^{\mathrm{A}}. \tag{3.21}$$

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 $\overline{\tau}^{\mathrm{D}}=\overline{\tau}^{\mathrm{A}}=\bar{t}$, and the attacker's utility function in (3.5) can be stated as

$$\begin{aligned}U^{\mathrm{A}}&((m^{\mathrm{A}},\delta^{\mathrm{A}}),(m^{\mathrm{D}},(\overline{\tau}^{\mathrm{A}}-\underline{\tau}^{\mathrm{D}})))\\&=(-\hat{\lambda}(\mathcal{G}^{\mathrm{A}})-\beta^{\mathrm{A}}m^{\mathrm{A}})(\underline{\tau}^{\mathrm{D}}-\underline{\tau}^{\mathrm{A}})+(-\hat{\lambda}(\mathcal{G}^{\mathrm{D}})-\beta^{\mathrm{A}}m^{\mathrm{A}})(\overline{\tau}^{\mathrm{A}}-\underline{\tau}^{\mathrm{D}}).\end{aligned} \tag{3.22}$$

(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 (3.5).

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 $\bar{t}=\overline{\tau}^{\mathrm{D}}=\Delta^{\mathrm{A}}+\underline{\tau}^{\mathrm{A}}$. Otherwise, the defender recovers for Δ^{D}, and $\Delta^{\mathrm{D}}+\underline{\tau}^{\mathrm{D}}<\bar{t}=\Delta^{\mathrm{A}}+\underline{\tau}^{\mathrm{A}}$. Hence, we can rewrite (3.21) as

$$U^{\mathrm{D}}((m^{\mathrm{A}},\Delta^{\mathrm{A}}),(m^{\mathrm{D}},\xi))=\phi\xi+\hat{\lambda}(\mathcal{G}^{\mathrm{A}})\delta^{\mathrm{A}}=:\hat{U}^{\mathrm{D3}}(m^{\mathrm{A}},m^{\mathrm{D}}), \tag{3.23}$$

with

$$\xi:=\min\{\Delta^{\mathrm{D}},\Delta^{\mathrm{A}}+\underline{\tau}^{\mathrm{A}}-\underline{\tau}^{\mathrm{D}}\}. \tag{3.24}$$

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

$$\mathcal{E}^{\mathrm{D3}*}(m^{\mathrm{A}})\in\underset{m^{\mathrm{D}}>0}{\arg\max}\,\hat{U}^{\mathrm{D3}}(m^{\mathrm{A}},m^{\mathrm{D}}). \tag{3.25}$$

The utility function of the attacker can be rewritten as

$$\begin{aligned}U^{\mathrm{A}}((m^{\mathrm{A}},\delta^{\mathrm{A}*}),(m^{\mathrm{D}*},\delta^{\mathrm{D}*}))&=-\hat{\lambda}(\mathcal{G}^{\mathrm{A}})(\Delta^{\mathrm{A}}-\xi)-\hat{\lambda}(\mathcal{G}_k^{\mathrm{D3}*}(\mathcal{E}_k^{\mathrm{A}}))\xi-\beta^{\mathrm{A}}m^{\mathrm{A}}\Delta^{\mathrm{A}}\\&=:\hat{U}_k^{\mathrm{A3}}(m^{\mathrm{A}}).\end{aligned} \tag{3.26}$$

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

$$m^{\mathrm{A3}*}\in\underset{m^{\mathrm{A}}>0}{\arg\max}\,\hat{U}_k^{\mathrm{A3}}(m^{\mathrm{A}}). \tag{3.27}$$

Note that to obtain $m^{\mathrm{A3}*}$, the attacker needs to obtain $\mathcal{E}^{\mathrm{D3}*}$ first. Hence, the attacker solves the maximization problem in (3.25) beforehand to obtain $\mathcal{E}^{\mathrm{D3}*}(m^{\mathrm{A}})$. This strategy for the attacker is named as **Strategy A3**.

Finally, after the attacker obtains $m^{\mathrm{A3}*}$, the defender searches for $\mathcal{E}^{\mathrm{D3}*}$, based on $\hat{U}^{\mathrm{D3}}(m^{\mathrm{A3}*},m^{\mathrm{D}})$ in (3.23), as

$$\mathcal{E}^{\mathrm{D3}*}(m^{\mathrm{A3}*})\in\underset{m^{\mathrm{D}}>0}{\arg\max}\,\hat{U}^{\mathrm{D3}}(m^{\mathrm{A3}*},m^{\mathrm{D}}). \tag{3.28}$$

This strategy $m^{\mathrm{D}}=\mathcal{E}^{\mathrm{D3}*}(m^{\mathrm{A3}*})$, $\delta^{\mathrm{D}}=\xi$ 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 $-\hat{\lambda}(\mathcal{G}^{\mathrm{D}}) - \beta^{\mathrm{A}} m^{\mathrm{A}} < 0$ (from the second term of (3.22)), 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

$$U^{\mathrm{A}}((m^{\mathrm{A}}, \delta^{\mathrm{A}*}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*})) = (-\hat{\lambda}(\mathcal{G}^{\mathrm{A}}) - \beta^{\mathrm{A}} m^{\mathrm{A}})(\underline{\tau}^{\mathrm{D}} - \underline{\tau}^{\mathrm{A}}) =: \hat{U}_k^{\mathrm{A2}}(m^{\mathrm{A}}). \tag{3.29}$$

As in the previous strategy, the attacker looks for the optimal number of edges $\mathcal{E}_k^{\mathrm{A2b}*}$ by maximizing the simplified utility function $\hat{U}_k^{\mathrm{A2}}(m^{\mathrm{A}})$. Specifically,

$$\mathcal{E}_k^{\mathrm{A2b}*} \in \arg\max_{m^{\mathrm{A}} > 0} \hat{U}_k^{\mathrm{A2}}(m^{\mathrm{A}}). \tag{3.30}$$

Strategy $m^{\mathrm{A}} = \mathcal{E}_k^{\mathrm{A2b}*}$ 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 (3.20) becomes

$$U^{\mathrm{D}}((m^{\mathrm{A}*}, \delta^{\mathrm{A}*}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*})) = \hat{\lambda}(\mathcal{G}_k^{\mathrm{A2b}*})\Delta^{\mathrm{A}} =: \hat{U}_k^{\mathrm{D2b}}. \tag{3.31}$$

As $\hat{\lambda}(\mathcal{G}^{\mathrm{A}}) < \hat{\lambda}(\mathcal{G})$ and $\hat{\lambda}(\mathcal{G}^{\mathrm{D}}) = \hat{\lambda}(\mathcal{G}^{\mathrm{A}})$, 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)**.

3.3.2.2 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 $\hat{U}^{\mathrm{A1}}$, $\hat{U}^{\mathrm{A2a}*} := \hat{U}^{\mathrm{A2a}}(m^{\mathrm{A2a}*})$, $\hat{U}^{\mathrm{A2b}*} = \hat{U}_k^{\mathrm{A2}}(\mathcal{E}_k^{\mathrm{A2b}*})$, $\hat{U}^{\mathrm{A3}*} := \hat{U}_k^{\mathrm{A3}}(m^{\mathrm{A3}*})$, $\hat{U}^{\mathrm{D1}}$, $\hat{U}^{\mathrm{D2a}}$, $\hat{U}_k^{\mathrm{D2b}}$, and $\hat{U}_k^{\mathrm{D3}*} := \hat{U}^{\mathrm{D3}}(m^{\mathrm{A3}*}, \mathcal{E}^{\mathrm{D3}*}(m^{\mathrm{A3}*}))$.

We first state properties of utility functions in some strategies. In Lemma 3.2, 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 3.3 and 3.4 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 3.2. 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 3.3. For any possible $m^{\mathrm{A2a}*}$ and $m^{\mathrm{A3}*}$, it follows that $\hat{U}^{\mathrm{A2a}*} \geq \hat{U}^{\mathrm{A3}*}$.

Lemma 3.4. $\hat{U}^{\mathrm{A2a}*}$ 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 chapter. 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 functions $\hat{U}^*$. In particular, we use $\hat{U}^{\mathrm{A3-0}}$ and $\underline{\mathcal{E}}_k^{\mathrm{A}*}$ defined by

$$\hat{U}^{\mathrm{A3-0}} := \max_{m^{\mathrm{A}} \in \mathcal{M}} \hat{U}^{\mathrm{A2a}}(m^{\mathrm{A}}), \tag{3.32}$$

$$\underline{\mathcal{E}}_k^{\mathrm{A}*} \in \arg\max_{m^{\mathrm{A}} \in \mathcal{M}} \hat{U}^{\mathrm{A2a}}(m^{\mathrm{A}}), \tag{3.33}$$

where $\mathcal{M} := \{\underline{m}^{\mathrm{A}} \in \{0, |\mathcal{E}|\} : \widehat{\lambda}_{\mathcal{G}}(\underline{\mathcal{E}}_k^{\mathrm{A}}, m^{\mathrm{D3}*}) - \hat{\lambda}(\underline{\mathcal{G}}_k^{\mathrm{A}}) - \beta^{\mathrm{D}}\mathcal{E}^{\mathrm{D3}*} < 0\}$. Furthermore, we let $\hat{U}^{\mathrm{D3-2a}} := \hat{U}^{\mathrm{D3}}(m^{\mathrm{A2a}*}, \mathcal{E}^{\mathrm{D3}*}(m^{\mathrm{A2a}*}))$.

Theorem 3.5. 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) $\hat{U}^{\mathrm{D3-2a}} < \hat{U}^{\mathrm{D2a}}$, or
   (b) $\hat{U}^{\mathrm{D3-2a}} \geq \hat{U}^{\mathrm{D2a}}$ and
      i. $\hat{U}^{\mathrm{A3}*} < \hat{U}^{\mathrm{A2b}*}$ and $\hat{U}^{\mathrm{A3-0}} > \hat{U}^{\mathrm{A2b}*}$, or
      ii. $\hat{U}^{\mathrm{A3}*} \geq \hat{U}^{\mathrm{A2b}*}$ and $\hat{U}^{\mathrm{A3-0}} > \hat{U}^{\mathrm{A3}*}$.

   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 $\underline{\mathcal{E}}_k^{\mathrm{A}*}$, respectively .
3. Combined Strategy 2b is optimal if $\hat{U}^{\mathrm{A2a}*} \geq 0$, $\hat{U}^{\mathrm{D3-2a}} \geq \hat{U}^{\mathrm{D2a}}$, $\hat{U}^{\mathrm{A2b}*} > \hat{U}^{\mathrm{A3}*}$, and $\hat{U}^{\mathrm{A2b}*} > \hat{U}^{\mathrm{A3-0}}$.
4. Combined Strategy 3 is optimal if $\hat{U}^{\mathrm{A3}*} \geq \hat{U}^{\mathrm{A2b}*} \geq 0$, $\hat{U}^{\mathrm{D3-2a}} \geq \hat{U}^{\mathrm{D2a}}$, and $\hat{U}^{\mathrm{A3-0}} \leq \hat{U}^{\mathrm{A3}*}$.

The combined strategies above cover all possible cases.

Possible optimal strategies for both players are illustrated in Figure 3.2, where 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 $(\cdot, \hat{U}^{\mathrm{D3-2a}})$ and $(\cdot, \hat{\lambda}(\mathcal{G}^{\mathrm{A3}*})\Delta^{\mathrm{A}})$ means that those utilities are not considered to find the optimal strategy.

Moreover, combinations of the conditions of the possible optimal strategies in all cases are shown in Table 3.4. We also note that even if the unit costs β^{A} and β^{D}

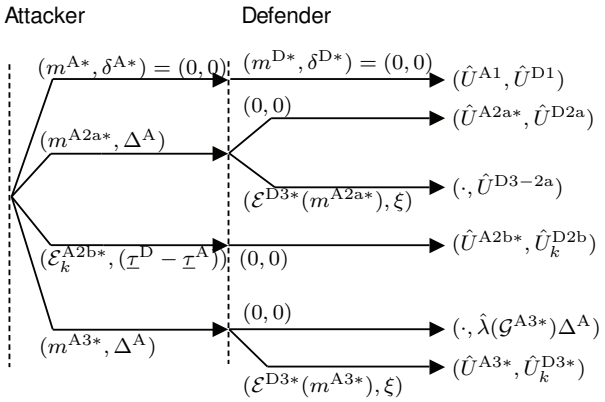


Figure 3.2 Illustration of possible optimal strategies

Table 3.4: Characterization of the optimal strategy of all cases

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

for attacking/recovering one edge per time depend on edges, the procedure to find the optimal combined strategies as in Theorem 3.5 does not change.

From the optimal strategies in Theorem 3.5, 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 3.6. The optimal strategy for the defender is not to recover if $\beta^{D} > 2$.

Corollary 3.7. The optimal strategy for the attacker is not to attack if $\beta^{A} > 1$. Also, under the optimal strategy, if the attacker attacks (i.e., $m^{A}, \delta^{A} > 0$), then $\mathcal{G}^{A}$ always becomes disconnected.

Remark 3.8. If $\hat{\lambda}(\mathcal{G}^{A}) < 0$ (i.e., $\mathcal{G}^{A}$ is disconnected), then in order to make $\hat{\lambda}(\mathcal{G}^{D})$ larger, the defender can reduce the number of connected components by adding links until the graph becomes connected ($\hat{\lambda}(\mathcal{G}^{D}) > 0$). The minimum number of edges to add in order to achieve certain $\hat{\lambda}(\mathcal{G}^{D})$ in a disconnected $\mathcal{G}^{A}$ is given by

$$m^{D} = \hat{\lambda}(\mathcal{G}^{D}) - \hat{\lambda}(\mathcal{G}^{A}), \text{ for } \hat{\lambda}(\mathcal{G}^{D}) < 0, \hat{\lambda}(\mathcal{G}^{A}) < 0. \tag{3.34}$$

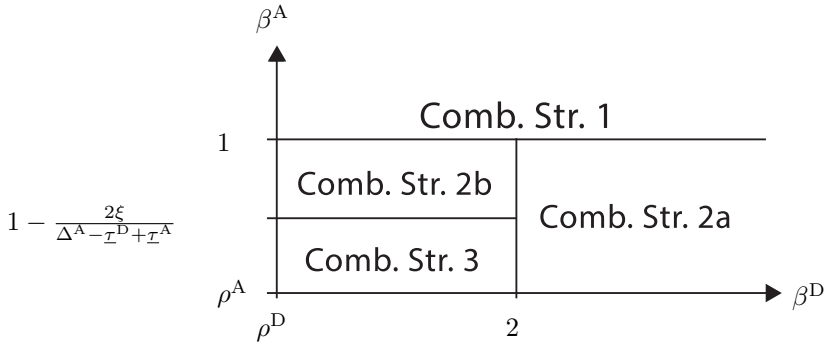


Figure 3.3 Optimal strategies of all cases for $n = 2$

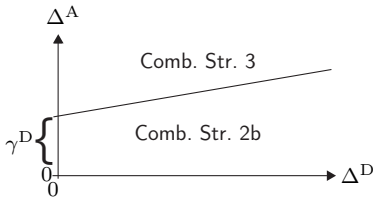


Figure 3.4 Optimal strategies of all cases for $n = 2$ as a function of maximum action durations Δ^{A} and Δ^{D} with $\beta^{\mathrm{A}} \leq 1$ and $\beta^{\mathrm{D}} \leq 2$

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 3.5, the optimal combined strategy can be stated as follows.

Proposition 3.9. 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 3.9 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 Figure 3.3. Similarly, this result can also be expressed in the $(\Delta^{\mathrm{A}}, \Delta^{\mathrm{D}})$ plane with $\beta^{\mathrm{A}} \leq 1$ and $\beta^{\mathrm{D}} \leq 2$ as shown in Figure 3.4; the slope of the line separating Combined Strategy 2b and Combined Strategy 3 is $\frac{2}{1-\beta^{\mathrm{A}}}$, which implies that the unit cost β^{A} further influences the players' decisions. 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 $\overline{\tau}^{\mathrm{D}}$.

3.3.3 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 multiagent systems represented by both connected and disconnected graphs.

3.4 Application to consensus problem

In this section, a consensus problem of a multiagent system [3–5] in the face of jamming attacks is investigated. We apply our game approach to this problem in a repeated manner.

3.4.1 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 3.2. 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 3.2, with subscript k added to all variables, e.g., $\mathcal{E}_k^{\mathrm{A}}$, $\mathcal{E}_k^{\mathrm{D}}$, 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 [17] to model such energy constraints. Specifically, the total energy used by player $p \in \{\mathrm{A}, \mathrm{D}\}$ must satisfy

$$\sum_{l=1}^{k-1} \beta^p m_l^p \delta_l^p + \beta^p m_k^p (t - \underline{\tau}_k^p) \leq \kappa^p + \rho^p t, \tag{3.35}$$

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, as explained in Chapter 2. The left-hand side of (3.35) 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. See also [14, 26] and the references therein for other constraint-based attack models.

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 (3.35) 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

$$\Delta_k^p(m_k^p) := \frac{\kappa^p + \rho^p \underline{\tau}_k^p - \sum_{l=1}^{k-1} \beta^p m_l^p \delta_l^p}{\beta^p m_k^p - \rho^p}. \tag{3.36}$$

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 $\Delta_k^p(m_k^p)$.

3.4.2 Approximate consensus time bound

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

$$\dot{x}_i(t) = \sum_{j \in \mathcal{N}_i(t)} (x_j(t) - x_i(t)), \quad x(0) = x_0, \quad t \geq 0, \tag{3.37}$$

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 $\mathcal{D}_\epsilon := \{x \in \mathbb{R}^n \colon V(x) \leq \epsilon\}$, where

$$V(x) := \max_{i \in \mathcal{V}} x_i - \min_{i \in \mathcal{V}} x_i, \quad x \in \mathbb{R}^n. \tag{3.38}$$

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

$$T_*(x_0) := \inf\{t \geq 0 \colon x(t) \in \mathcal{D}_\epsilon\}. \tag{3.39}$$

In our analysis, we also use the Laplacian matrix $L \in \mathbb{R}^{n\times n}$ associated with graph $\mathcal{G}$. Moreover, let $P \coloneqq e^{-\gamma^{\mathrm{A}}L}$ and $\underline{p} \coloneqq \max_{j\in\{1,\dots,n\}} \min_{i\in\{1,\dots,n\}} P_{i,j},$, where $P_{i,j}$ denotes the (i,j)th entry of the matrix P. Notice that since $\mathcal{G}$ is connected and $\gamma^{\mathrm{A}} > 0$, 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 3.10. Consider the multiagent system (3.37) with the initial condition $x_0 \in \mathbb{R}^n \setminus D_\epsilon$. Under the optimal attack and defense strategies for the resilient graph game in Section 3.3, the approximate consensus time satisfies

$$T_*(x_0) \le \frac{\beta^{\mathrm{A}}(\gamma^{\mathrm{A}}+\gamma^{\mathrm{D}})\left\lceil \frac{\ln\epsilon - \ln V(x_0)}{\ln(1-\underline{p})}\right\rceil + \kappa^{\mathrm{A}}}{\beta^{\mathrm{A}}-\rho^{\mathrm{A}}}. \tag{3.40}$$

Proposition 3.10 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 (3.40), an upper bound of the approximate consensus time can be obtained as $T_*(x_0) \le (\gamma^{\mathrm{A}}+\gamma^{\mathrm{D}})\left\lceil (\ln\epsilon - \ln V(x_0))/(\ln(1-\underline{p}))\right\rceil$. This bound for the attack-free case is clearly smaller than that in (3.40) when the attacker has positive energy resources ($\kappa^{\mathrm{A}}, \rho^{\mathrm{A}} > 0$) and the defender has a nonzero initial waiting duration ($\gamma^{\mathrm{D}} > 0$). Note that with larger values of κ^{A} and ρ^{A}, the bound (3.40) becomes even larger, indicating the possibility of slower consensus due to more damaging attacks.

3.5 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 Figure 3.1 with $n = 4$, and parameters $\beta^{\mathrm{A}} = 0.4$, $\beta^{\mathrm{D}} = 0.6$, $\kappa^{\mathrm{D}} = 1$, $\rho^{\mathrm{D}} = 0.1$, $\gamma^{\mathrm{A}} = 0.1$, and $\gamma^{\mathrm{D}} = 0.3$.

3.5.1 Effect of players' energy on consensus

First, we use the parameters $\kappa^{\mathrm{A}} = 0.5$ and $\rho^{\mathrm{A}} = 0.3$. Figures 3.5 and 3.6 show the states of the agents and properties of the players of the first simulation, with the agents

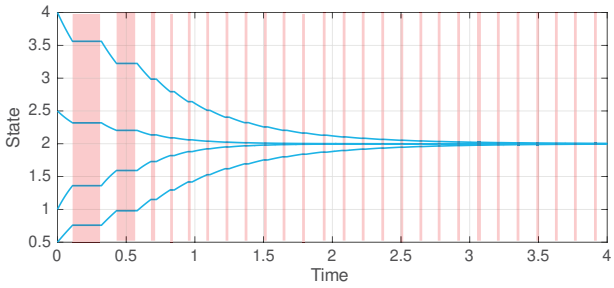


Figure 3.5 State trajectories with $\kappa^{\mathrm{A}} = 0.5$ and $\rho^{\mathrm{A}} = 0.3$. The red areas indicate the intervals where the attacker attacks.

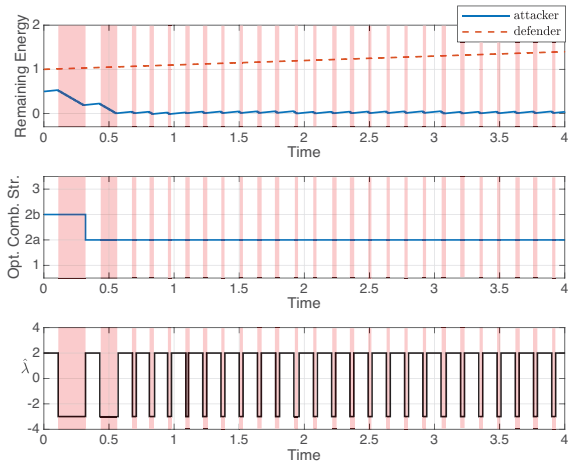


Figure 3.6 Remaining energy and optimal combined strategy for the two players, and the resulting $\widehat{\lambda}$ with $\kappa^{\mathrm{A}} = 0.5$ and $\rho^{\mathrm{A}} = 0.3$

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 Figure 3.6, note that the defender does not recover any edge, and hence the available energy for the defender accumulates continuously. In the second simulation, we use the parameters $\kappa^{\mathrm{A}} = 5$ and $\rho^{\mathrm{A}} = 0.39$. We present the results of this simulation in Figures 3.7 and 3.8, where in the case shown in Figure 3.8, 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.. 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.

3.5.2 Effect of graph structure on consensus

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

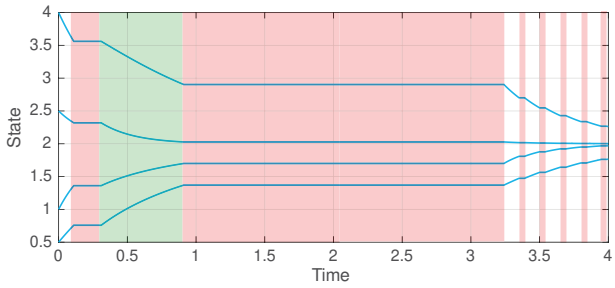


Figure 3.7 State trajectories with $\kappa^{\mathrm{A}} = 5$ and $\rho^{\mathrm{A}} = 0.39$. The green areas indicate the intervals where the defender recovers.

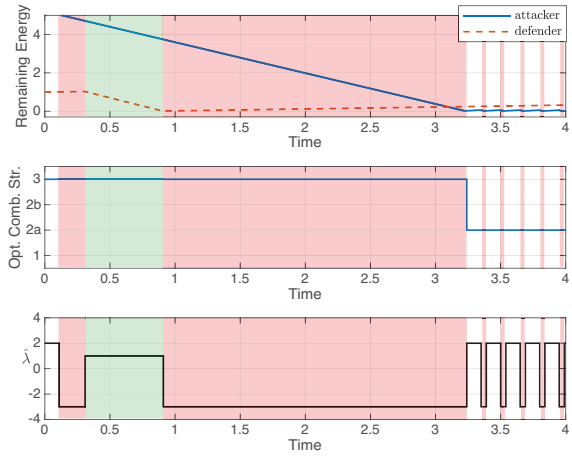


Figure 3.8 Remaining energy and optimal combined strategy for the two players, and the resulting $\widehat{\lambda}$

of four nodes, while all other parameters are set to be the same across these two simulations. Figures 3.9 and 3.10 show the state trajectory for the path graph and the complete graph, respectively. 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 $[\overline{\tau}^{\mathrm{D}}, \overline{\tau}^{\mathrm{A}}]$ interval are not able to compensate the negative payoff that the attacker receives on the $[\overline{\tau}^{\mathrm{D}}, \overline{\tau}^{\mathrm{A}}]$ 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.

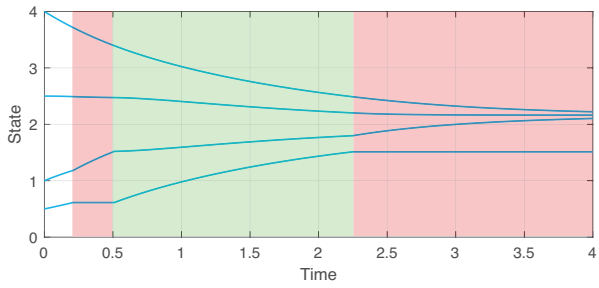


Figure 3.9 State trajectories in the system with the path graph $\mathcal{G}$.

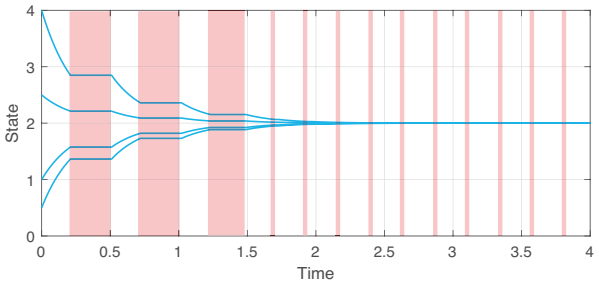


Figure 3.10 State trajectories in the system with the complete graph $\mathcal{G}$.

3.5.3 Effect of players' energy on equilibrium

We also provide an example of how the energy, which affects the maximum attack/recovery durations, influences the equilibrium. We consider the graph in Figure 3.1 with selected values of $\Delta_k^{\mathrm{A}}(m_k^{\mathrm{A}})$ and $\Delta_k^{\mathrm{D}}(m_k^{\mathrm{D}})$ in (3.36) 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 Figure 3.11 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. Figure 3.11 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 Figure 3.12. We note that Figure 3.12 is similar to Figure 3.3 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

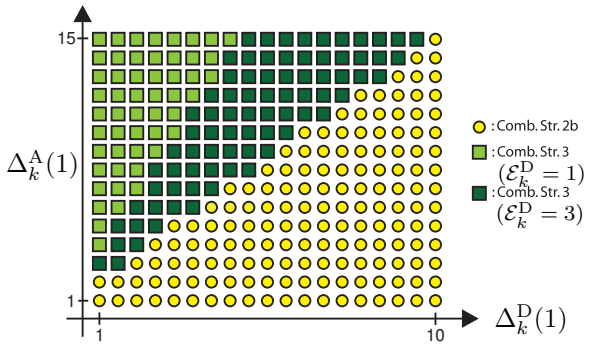


Figure 3.11 Optimal combined strategies for different $\Delta_k^{\mathrm{A}}(\mathcal{E}_k^{\mathrm{A}} = 1)$ and $\Delta_k^{\mathrm{D}}(\mathcal{E}_k^{\mathrm{D}} = 1)$.

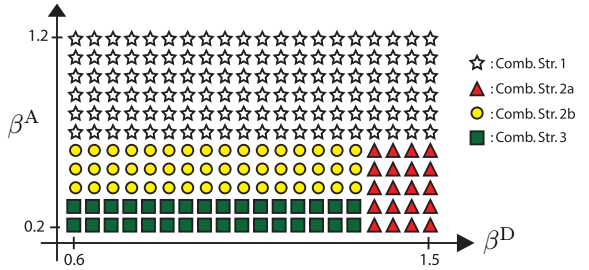


Figure 3.12 Optimal combined strategies for different β^{A} and β^{D}. The optimal numbers of edges are $\mathcal{E}_k^{\mathrm{A}} = 5$, $\mathcal{E}_k^{\mathrm{D}} = 3$ if the players attack or recover.

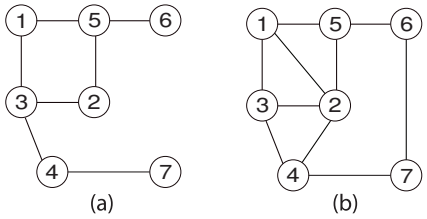


Figure 3.13 Graphs used in the simulations in Section 3.5.4

Corollaries 3.6 and 3.7. These critical values of β^{A} and β^{D} in the simulations are affected by generalized edge connectivity of $\mathcal{G}$ in Figure 3.1.

3.5.4 Effect of graph structure on equilibrium: change between combined strategy 3 and 2b

To investigate the change of equilibrium between Combined Strategy 2b and Combined Strategy 3, we now consider the graphs in Figure 3.13 with selected values of Δ_k^{A} and Δ_k^{D} in (3.36) by changing the total consumed energy up to game $(k-1)$ represented as $\sum_{l=1}^{k-1} \beta^{\mathrm{A}} \mathcal{E}_m^{\mathrm{A}} \delta_m^{\mathrm{A}}$ and $\sum_{l=1}^{k-1} \beta^{\mathrm{D}} \mathcal{E}_m^{\mathrm{D}} \delta_m^{\mathrm{D}}$. The results for the graphs (a) and (b) of Figure 3.13 are shown in Figures 3.14 and 3.15, respectively.

The yellow circles in Figure 3.14 indicate that Combined Strategy 2b is optimal with attacking all seven edges for given Δ_k^{A} and Δ_k^{D}, whereas the squares indicate that Combined Strategy 3 is optimal. From Figure 3.14, we observe that the attacker tends to attack for longer durations if it possesses higher amount of energy relative to the

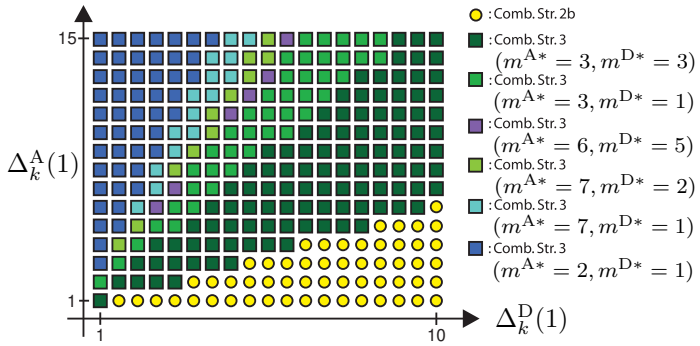


Figure 3.14 Optimal combined strategies for different $\Delta^{\mathrm{A}}(m^{\mathrm{A}} = 1)$ and $\Delta^{\mathrm{D}}(m^{\mathrm{D}} = 1)$ for the graph (a) in Figure 3.13

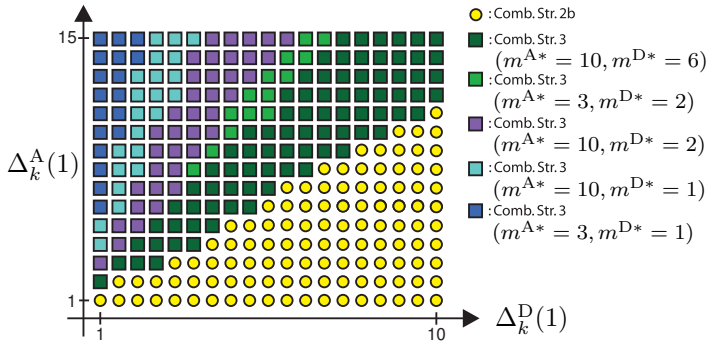


Figure 3.15 Optimal combined strategies for different $\Delta^{\mathrm{A}}(m^{\mathrm{A}} = 1)$ and $\Delta^{\mathrm{D}}(m^{\mathrm{D}} = 1)$ for the graph (b) in Figure 3.13

defender's energy. On the other hand, the defender with more energy will attempt to make the graph connected by recovering more edges.

Similarly, the yellow circles in Figure 3.15 indicate that Combined Strategy 2b is optimal with attacking all 10 edges, whereas the squares indicate that Combined Strategy 3 is optimal. In this setup, the attacker with higher amount of energy relative to the defender also tends to attack less edges for longer durations. On the other hand, the defender with more energy will attempt to make the graph connected by recovering more edges, e.g., by recovering six edges, which is sufficient to make the graph connected.

We note that in the more connected graph, i.e., graph (b) of Figure 3.13, Combined Strategy 2b is more likely to be optimal, as shown by the steeper line separating the squares and the circles in Figure 3.15 compared to Figure 3.14. We also note that Figures 3.14 and 3.15 are similar to Figure 3.4 of the two-agent case. Figures 3.14 and 3.15 can also be useful to estimate the equilibrium based on the past actions and energy parameters.

3.6 Chapter summary

In this chapter, we have considered resilient network problem in the context of multiagent 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 chapter, we have considered the generalized edge connectivity as one specific way to measure the network connectivity. We consider that this formulation with graph connectivity measure is reasonable since the game still admits dynamicity due to the energy constraint of the players. It is also worth investigating other connectivity notions and non-uniform unit costs for practical applications. In Chapter 4, we consider 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.

3.7 Appendix

3.7.1 Proof of Lemma 3.2

The utility function in (3.5) can be rewritten as $U^{\mathrm{A}}((m^{\mathrm{A}},\delta^{\mathrm{A}}),(m^{\mathrm{D}},\delta^{\mathrm{D}})) = -\hat{\lambda}(\mathcal{G}^{\mathrm{A}})\delta^{\mathrm{A}} - (\hat{\lambda}(\mathcal{G}^{\mathrm{D}}) - \hat{\lambda}(\mathcal{G}^{\mathrm{A}}))\delta^{\mathrm{D}} - \beta^{\mathrm{A}} m^{\mathrm{A}}\delta^{\mathrm{A}}$. If there is recovery, i.e., $m^{\mathrm{D}}, \delta^{\mathrm{D}} > 0$, then $\hat{\lambda}(\mathcal{G}^{\mathrm{D}}) > \hat{\lambda}(\mathcal{G}^{\mathrm{A}})$ according to the optimal strategy candidates. This implies that $-(\hat{\lambda}(\mathcal{G}^{\mathrm{D}}) - \hat{\lambda}(\mathcal{G}^{\mathrm{A}}))\delta^{\mathrm{D}} < -\hat{\lambda}(\mathcal{G}^{\mathrm{A}})\delta^{\mathrm{D}}$ holds.

3.7.2 Proof of Lemma 3.3

Substitute $m^{\mathrm{A3}*}$ of (3.27) into (3.26) to obtain $\hat{U}^{\mathrm{A3}*} = (\hat{\lambda}(\mathcal{G}^{\mathrm{A3}*}) - \hat{\lambda}(\mathcal{G}^{\mathrm{D3}*}))\xi + \hat{U}^{\mathrm{A2a}}(m^{\mathrm{A3}*})$. Since $\hat{\lambda}(\mathcal{G}^{\mathrm{D3}*}) > \hat{\lambda}(\mathcal{G}^{\mathrm{A3}*})$, it follows that $\hat{U}^{\mathrm{A3}*} \leq \hat{U}^{\mathrm{A2a}}(m^{\mathrm{A3}*})$, and therefore $\hat{U}^{\mathrm{A3}*} \leq \hat{U}^{\mathrm{A2a}*}$.

3.7.3 Proof of Lemma 3.4

First, we show that $\mathrm{sgn}(\hat{U}^{\mathrm{A2a}*}) = \mathrm{sgn}(\hat{U}^{\mathrm{A2b}*})$. We can state $\hat{U}^{\mathrm{A2a}}(m^{\mathrm{A}})$ as $\hat{U}^{\mathrm{A2a}}(m^{\mathrm{A}}) = \hat{U}_k^{\mathrm{A2}}(m^{\mathrm{A}}) + (-\hat{\lambda}(\mathcal{G}^{\mathrm{A}}) - \beta^{\mathrm{A}} m^{\mathrm{A}})(\Delta^{\mathrm{A}} + \underline{\tau}^{\mathrm{A}} - \underline{\tau}^{\mathrm{D}})$. By (3.1), we have $\underline{\tau}^{\mathrm{D}} \leq \overline{\tau}^{\mathrm{A}}$. Consequently, since $\overline{\tau}^{\mathrm{A}} \leq \underline{\tau}^{\mathrm{A}} + \Delta^{\mathrm{A}}$, we have $\Delta^{\mathrm{A}} + \underline{\tau}^{\mathrm{A}} \geq \underline{\tau}^{\mathrm{D}}$ for any possible Δ^{A}. Therefore, if

$-\hat{\lambda}(\mathcal{G}^{\mathrm{A}}) - \beta^{\mathrm{A}} m^{\mathrm{A}} > 0$ is satisfied, then $\hat{U}^{\mathrm{A2a}}(m^{\mathrm{A}}) > 0$ and $\hat{U}_k^{\mathrm{A2}}(m^{\mathrm{A}}) > 0$, and vice versa. Again, since $\Delta^{\mathrm{A}} + \underline{\tau}^{\mathrm{A}} \geq \underline{\tau}^{\mathrm{D}} > \underline{\tau}^{\mathrm{A}}$, it follows that $\hat{U}^{\mathrm{A2b}*} > 0$ if and only if $\hat{U}^{\mathrm{A2a}*} > 0$, since the attacker can always choose edges to make $\hat{U}^{\mathrm{A2a}*}$ and $\hat{U}^{\mathrm{A2b}*}$ positive. By a similar argument, $\hat{U}^{\mathrm{A2b}*} < 0$ if and only if $\hat{U}^{\mathrm{A2a}*} < 0$. Thus, $\mathrm{sgn}(\hat{U}^{\mathrm{A2a}*}) = \mathrm{sgn}(\hat{U}^{\mathrm{A2b}*})$.

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

3.7.4 Proof of Theorem 3.5

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 $\hat{U}^{\mathrm{A1}} = \hat{U}^{\mathrm{D1}} = 0$. Therefore, the attacker chooses the optimal $m^{\mathrm{A}} > 0$ to achieve positive utility. If the attacker attacks $m^{\mathrm{A}*}$, then the optimal strategy for the defender is to recover if and only if $U^{\mathrm{D}}((m^{\mathrm{A}*}, \delta^{\mathrm{A}*}), (m^{\mathrm{D}*}, \delta^{\mathrm{D}*} > 0)) > \hat{\lambda}(\mathcal{G}_k^{\mathrm{A}*})\Delta^{\mathrm{A}}$.

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 ($m^{\mathrm{D}} > 0$) for given m^{A}, then the attacker's utility for given m^{A} is $U^{\mathrm{A}}((m^{\mathrm{A}}, \delta^{\mathrm{A}}), (m^{\mathrm{D}}, \delta^{\mathrm{D}} > 0))$.

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

(i) From Lemmas 3.3 and 3.4, since $\hat{U}^{\mathrm{A2a}*} > \hat{U}^{\mathrm{A3}*}$ and $\hat{U}^{\mathrm{A2a}*}$ has the same sign with $\hat{U}^{\mathrm{A2b}*}$, Combined Strategy 1 is optimal if $\hat{U}^{\mathrm{A2a}*} < 0 = \hat{U}^{\mathrm{A1}}$, regardless of the defender's utility. This fact proves point 1) in the theorem.

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

(ii) Combined Strategy 2a with attacking $m^{\mathrm{A2a}*}$ is the optimal combined strategy if $\hat{U}^{\mathrm{D3-2a}} = U^{\mathrm{D}}((m^{\mathrm{A2a}*}, \Delta^{\mathrm{A}}), (m^{\mathrm{D}*}, \Delta^{\mathrm{D}} > 0))$ is less than $\hat{U}^{\mathrm{D2a}} = U^{\mathrm{D}}((m^{\mathrm{A2a}*}, \Delta^{\mathrm{A}}), (0, 0))$, since the defender chooses not to recover ($m^{\mathrm{D}*} = 0$) and $\hat{U}^{\mathrm{A2a}*} = U^{\mathrm{A}}((m^{\mathrm{A2a}*}, \Delta^{\mathrm{A}}), (0, 0))$ is the maximum possible utility for the attacker from Lemmas 3.3 and 3.4. This fact corresponds to point 2)a) in the theorem.

Since the case where $\hat{U}^{\mathrm{D3-2a}} < \hat{U}^{\mathrm{D2a}}$ is covered, beginning from (iii) to (vi), it is further assumed that $\hat{U}^{\mathrm{D3-2a}} \geq \hat{U}^{\mathrm{D2a}}$, i.e., the defender chooses to recover from $m^{\mathrm{A2a}*}$. Since $\mathcal{E}_k^{\mathrm{D2}*} > 0$ and $\hat{U}^{\mathrm{A2a}*} = U^{\mathrm{A}}((m^{\mathrm{A2a}*}, \Delta^{\mathrm{A}}), (0, 0))$, in the subsequent cases, the attacker's optimal number of edges are not $m^{\mathrm{A2a}*}$ (which corresponds to $\hat{U}^{\mathrm{A2a}*}$). In (iii) and (iv), we analyze the case where $\hat{U}^{\mathrm{A3}*} \geq \hat{U}^{\mathrm{A2b}*}$, which means that Strategy A3 yields more or equal utility than Strategy A2b for the attacker.

(iii) Due to the possible jump between $\hat{\lambda}(\mathcal{G}^{\mathrm{D}}) = -1$ to $\hat{\lambda}(\mathcal{G}^{\mathrm{D}}) = 1$ by recovering only one edge, the defender may have different optimal strategies (whether to recover or not)

given different attacked edges. From Lemma 3.2, since the attacker has better utility if the defender does not recover, here the attacker's optimal strategy is to attack $\underline{\mathcal{E}}_k^{\mathrm{A}*}$ if $\hat{U}^{\mathrm{A3-0}} = U^{\mathrm{A}}((\underline{\mathcal{E}}_k^{\mathrm{A}*}, \Delta^{\mathrm{A}}), (0,0))$ is greater than $\hat{U}^{\mathrm{A3}*} = U^{\mathrm{A}}((m^{\mathrm{A3}*}, \Delta^{\mathrm{A}}), (m^{\mathrm{D}}, \Delta^{\mathrm{D}} > 0))$, with $\underline{\mathcal{E}}_k^{\mathrm{A}*}$ being the optimal number of edges among the edges that cannot be recovered if attacked, as in (3.33). 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 $\hat{U}^{\mathrm{A3-0}} \leq \hat{U}^{\mathrm{A3}*}$. Here, the defender's optimal strategy is to recover if the attacker attacks $m^{\mathrm{A3}*}$. Since $\hat{U}^{\mathrm{A3}*} \geq \max\{\hat{U}^{\mathrm{A2b}*}, 0\}$, the attacker has better utility than in Strategies A1, A2a, and A2b.

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

(v) Similar as in (iii), Combined Strategy 2a is the optimal strategy if $\hat{U}^{\mathrm{A3-0}} \geq \hat{U}^{\mathrm{A2b}*}$. In this case, the attacker has better utility than in Strategies A1, A2b, and A3. However, since $\hat{U}^{\mathrm{D3-2a}} \geq \hat{U}^{\mathrm{D2a}}$, the attacker does not attack $m^{\mathrm{A2a}*}$. This fact corresponds to point 2)b)I) in the theorem.

(vi) If $\hat{U}^{\mathrm{A3-0}} < \hat{U}^{\mathrm{A2b}*}$, Strategy A2b is the optimal strategy for the attacker since $\hat{U}^{\mathrm{A2b}*} > \max(\hat{U}^{\mathrm{A3}*}, \hat{U}^{\mathrm{A3-0}})$ and utility $\hat{U}^{\mathrm{A2a}*}$ cannot be achieved because $\hat{U}^{\mathrm{D3-2a}} \geq \hat{U}^{\mathrm{D2a}}$. This corresponds to point 3) in the theorem.

3.7.5 Proof of Corollary 3.6

In Strategy D3, since $\min\{\Delta^{\mathrm{D}}, \Delta^{\mathrm{A}} + \underline{\tau}^{\mathrm{A}} - \underline{\tau}^{\mathrm{D}}\} > 0$, the necessary condition for Strategy D3 to be the optimal strategy is $\beta^{\mathrm{D}} < (\hat{\lambda}(\mathcal{G}^{\mathrm{D3}*}) - \hat{\lambda}(\mathcal{G}^{\mathrm{A3}*}))/\mathcal{E}^{\mathrm{D3}*}$, 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 $(\hat{\lambda}(\mathcal{G}^{\mathrm{D}}) - \hat{\lambda}(\mathcal{G}^{\mathrm{A}}))/m^{\mathrm{D}} = 2$ at most. Thus, if $\beta^{\mathrm{D}} > 2$, then the defender does not recover any edge.

3.7.6 Proof of Corollary 3.7

From Theorem 3.5, the attacker decides to attack if $\hat{U}^{\mathrm{A2a}}(m^{\mathrm{A2a}*}) \geq 0$. Since $\Delta^{\mathrm{A}} > 0$, Strategy A2a is the optimal strategy if $-\hat{\lambda}(\mathcal{G}_k^{\mathrm{A2a}*}) - \beta^{\mathrm{A}} m^{\mathrm{A2a}*} \geq 0$, assuming that the defender cannot recover. By Lemma 3.1, $\hat{U}^{\mathrm{A2a}}(m^{\mathrm{A2a}*}) > \hat{U}_k^{\mathrm{A3}}(m^{\mathrm{A3}*})$, and thus Strategy A1 is the optimal strategy if $-\hat{\lambda}(\mathcal{G}_k^{\mathrm{A2a}*}) - \beta^{\mathrm{A}} m^{\mathrm{A2a}*} < 0$.

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

3.7.7 Proof of Proposition 3.9

Since $|\mathcal{E}| = 1$, the following four facts corresponding to points 1) to 4) in Theorem 3.5 hold:

(i) Combined Strategy 1 is optimal if $\hat{U}^{\mathrm{A2a}*} < 0$. Since $|\mathcal{E}| = 1$, $\hat{\lambda}(\mathcal{G}^{\mathrm{A}}) = -1$ is always true if $m^{\mathrm{A}} > 0$. From (3.17), it is clear that $\hat{U}^{\mathrm{A2a}*} < 0$ if $\beta^{\mathrm{A}} > 1$.

(ii) In order for Combined Strategy 2a to be optimal, a common condition is that $\hat{U}^{\mathrm{A2a}*} \geq 0$, which holds if $\beta^{\mathrm{A}} \leq 1$. The condition $\hat{U}^{\mathrm{D3-2a}} < \hat{U}^{\mathrm{D2a}}$ then holds if $\beta^{\mathrm{D}} > 2$. Note that $\mathcal{M}$ consists of $|\mathcal{E}| = 1$ if $\beta^{\mathrm{D}} > 2$ and empty otherwise. Hence, $\hat{U}^{\mathrm{A3-0}} = \hat{U}^{\mathrm{A2a}*}$ holds if $\beta^{\mathrm{D}} > 2$, otherwise $\hat{U}^{\mathrm{A3-0}} = 0$ holds. Therefore, in point 2)b) in Theorem 3.5, condition $\hat{U}^{\mathrm{D3-2a}} \geq \hat{U}^{\mathrm{D2a}}$ implies that $\hat{U}^{\mathrm{A3-0}} = 0$ holds, which means that the conditions 2)b)I) and 2)b)II) cannot be satisfied (from Lemma 3.4).

(iii) Combined Strategy 2b is optimal if $\hat{U}^{\mathrm{A2a}*} \geq 0$, which holds if $\beta^{\mathrm{A}} \leq 1$. The other condition is that $\hat{U}^{\mathrm{D3-2a}} \geq \hat{U}^{\mathrm{D2a}}$, which holds if $\beta^{\mathrm{D}} \leq 2$. Conditions $\hat{U}^{\mathrm{A2b}*} > \hat{U}^{\mathrm{A3-0}}$ is always true (see point (ii) in this proof above). With $n = 2$, condition $\hat{U}^{\mathrm{A2b}*} > \hat{U}^{\mathrm{A3}*}$ is true if $\beta^{\mathrm{A}} > 1 - \frac{2\xi}{\Delta^{\mathrm{A}} - \underline{\tau}^{\mathrm{D}} + \underline{\tau}^{\mathrm{A}}}$ holds, with ξ defined in (3.24).

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

3.7.8 Proof of Proposition 3.10

The agents do not face any attacks during the intervals $[\underline{t}_k, \underline{\tau}_k^{\mathrm{A}})$, $k \in \mathbb{N}$. Thus, from (3.37), $\dot{x}(t) = -Lx(t)$, $t \in [\underline{t}_k, \underline{\tau}_k^{\mathrm{A}})$, $k \in \mathbb{N}$. Noting that $\underline{\tau}_k^{\mathrm{A}} = \underline{t}_k + \gamma^{\mathrm{A}}$, we obtain $x(\underline{\tau}_k^{\mathrm{A}}) = Px(\underline{t}_k)$, $k \in \mathbb{N}$. Now by using Lemma 12.8 of [5], it follows that

$$V(x(\underline{\tau}_k^{\mathrm{A}})) = V(Px(\underline{t}_k)) \leq (1 - \underline{p})V(x(\underline{t}_k)). \tag{3.41}$$

During the intervals $[\underline{\tau}_k^{\mathrm{A}}, \underline{t}_{k+1})$, $k \in \mathbb{N}$, there may be attacks and the communication between certain agents may be jammed. It then follows from (3.37) that

$$V(x(\underline{t}_{k+1})) \leq V(x(\underline{\tau}_k^{\mathrm{A}})), \quad k \in \mathbb{N}. \tag{3.42}$$

By (3.41) and (3.42), $V(x(\underline{t}_{k+1})) \leq (1 - \underline{p})V(x(\underline{t}_k))$, and thus,

$$V(x(\underline{t}_{k+1})) \leq (1 - \underline{p})^k V(x(\underline{t}_1)) = (1 - \underline{p})^k V(x_0),\ k \in \mathbb{N}. \tag{3.43}$$

Let $k_* \coloneqq \lceil (\ln \epsilon - \ln V(x_0))/\ln(1-\underline{p}) \rceil$. By (3.43), it clearly holds $V(x(\underline{t}_{k_*+1})) \leq \epsilon$, and therefore,

$$x(t) \in \mathcal{D}_\epsilon, \quad t \geq \underline{t}_{k_*+1}. \tag{3.44}$$

Our next goal is to find an upper bound of $\underline{t}_{k_*+1}$. First, by the energy constraint for the attacker given in (3.35), $\beta^{\mathrm{A}} \sum_{k=1}^{k_*} \mathcal{E}_k^{\mathrm{A}} \delta_k^{\mathrm{A}} \leq \kappa^{\mathrm{A}} + \rho^{\mathrm{A}} \underline{t}_{k_*+1}$ holds. As indicated by the optimal strategies derived in Theorem 3.5, $\mathcal{E}_k^{\mathrm{A}} = 0$ implies that $\delta_k^{\mathrm{A}} = 0$. Hence, we have $\mathcal{E}_k^{\mathrm{A}} \delta_k^{\mathrm{A}} \geq \delta_k^{\mathrm{A}}$, which implies

$$\sum_{k=1}^{k_*} \delta_k^{\mathrm{A}} \leq \frac{1}{\beta^{\mathrm{A}}} \beta^{\mathrm{A}} \sum_{k=1}^{k_*} \mathcal{E}_k^{\mathrm{A}} \delta_k^{\mathrm{A}} \leq \frac{\kappa^{\mathrm{A}}}{\beta^{\mathrm{A}}} + \frac{\rho^{\mathrm{A}}}{\beta^{\mathrm{A}}} \underline{t}_{k_*+1}. \tag{3.45}$$

Next, by (3.7), $\underline{t}_{k+1} = \bar{t}_k \leq \underline{t}_k + \gamma^{\mathrm{A}} + \gamma^{\mathrm{D}} + \delta_k^{\mathrm{A}}, \quad k \in \mathbb{N}$. It then follows from (3.45) that $\underline{t}_{k_*+1} = \sum_{k=1}^{k_*} (\underline{t}_{k+1} - \underline{t}_k) \leq (\gamma^{\mathrm{A}} + \gamma^{\mathrm{D}}) k_* + \frac{\kappa^{\mathrm{A}}}{\beta^{\mathrm{A}}} + \frac{\rho^{\mathrm{A}}}{\beta^{\mathrm{A}}} \underline{t}_{k_*+1}$, and hence,

$$\underline{t}_{k_*+1} \leq \frac{(\gamma^{\mathrm{A}} + \gamma^{\mathrm{D}}) \left\lceil \frac{\ln \epsilon - \ln V(x_0)}{\ln(1-\underline{p})} \right\rceil + \frac{\kappa^{\mathrm{A}}}{\beta^{\mathrm{A}}}}{1 - \frac{\rho^{\mathrm{A}}}{\beta^{\mathrm{A}}}}. \tag{3.46}$$

Finally, by (3.44) and (3.46), we obtain (3.40).

Chapter 4

Cluster Forming in Multiagent Consensus in Continuous Time

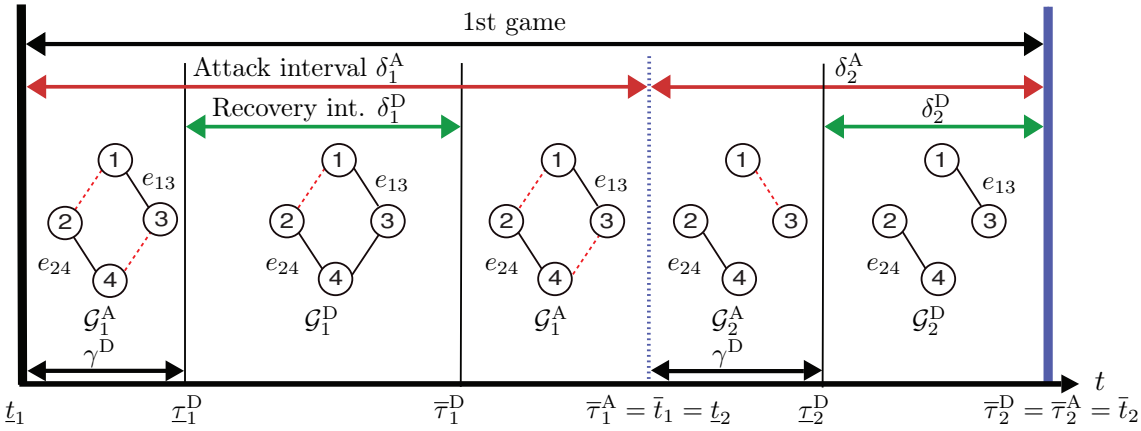


Figure 4.1 Illustration of graph transitions, with $\mathcal{G}$ containing four edges $e_{12}, e_{13}, e_{24}, e_{34}$.

4.1 Introduction

In this chapter, we model the interaction between an attacker and a defender in a two-player game setting played repeatedly over time in the context of multiagent consensus. The attacker is motivated to disrupt the communication among agents by attacking individual links while the defender attempts to recover some or all of them whenever possible. Their utilities are determined by how agents are connected to others during the attacks and recoveries, as well as how these actions affect the states of agents. Both players are constrained in terms of their available energy for the actions of attacks/recoveries. Hence, they must determine whether to attack/defend and if so, for how long.

We formulate the problem based on the one in Chapter 3, which uses graph connectivity to characterize the game and players' strategies (see also [61]). Specifically, in this chapter we address how clusters among agents may form in this security game setting.

In the presence of adversaries, agents in the network under consensus protocol may not converge to the same state; instead, they may be divided into several clusters. Cluster forming in multiagent systems has been studied in, e.g., [71–73], where the weights in the agents' state updates may take negative values, representing the possibly hostile relations among certain agents. In this chapter, we approach clustering from a different viewpoint based on a game-theoretic formulation. Moreover, different from the setting in Chapter 3, here (i) we introduce more options for the attacker's attack strengths and (ii) the game consists of multiple parts, resulting in more complicated attack/defense strategies.

More specifically, with different attack strengths, it is now possible for the attacker to attack the links with stronger attack signals so that the defender is unable to recover those links. In practice, this is possible when the attacker emits stronger jamming signals to particular communication links that results in much lower signal-to-interference-plus-noise ratio (SINR) so that it is not possible for the defender to recover the communication on those links with its limited resources. Such models are employed in [32, 74].

On the other hand, we consider games consisting of multiple parts, where the players need to consider their future conditions when deciding their strategies at any point in time. This has an impact on how the players use their limited energy; it may be possible that the players reduce their intensity of attack/recovery actions at some time to conserve their energy and use it more efficiently later.

This chapter is organized as follows. In Section 4.2, we introduce the framework for the resilient graph game. In Section 4.3, we discuss the effect of some of the parameters on the equilibria and cluster forming. We provide a case study to analyze the better strategies for players in one game in Section 4.4. We then present simulations on the dynamic graph games and the resulting cluster forming in Section 4.5. Finally, we conclude the chapter in Section 4.6. The content in this section appeared in conference articles [C2,C4,O2].

4.2 Problem formulation

In this section, we explain the two-player game formulation between an attacker and a defender in the context of network security. We also explain the characteristics of the

players, such as their energy constraints and how they measure the cluster forming of the agents.

We consider a multiagent system consisting of n agents with the communication topology described by the graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. Every agent i is able to communicate with its neighbors $\mathcal{N}_i(t) \subseteq \mathcal{V}$ in continuous time via the communication links. The underlying graph $\mathcal{G}$, which is undirected and connected, represents the communication topology when there are no attacks.

Each agent has the scalar state x_i whose dynamics are given by

$$\dot{x}_i(t) = \sum_{j \in \mathcal{N}_i(t)} (x_j(t) - x_i(t)), \quad x(0) = x_0, \quad t \geq 0, \tag{2.2}$$

as specified in Chapter 2.

In this chapter, we consider that the attacker has two types of jamming signals in terms of their strength, *strong* and *normal*. We define the attack action by the attacker (both with strong and normal signals) as the removal of edges in graph $\mathcal{G}$. In response to the attacks, the recovery action by the defender is represented by restoring some of the removed edges. The difference between the two jamming signal types is that the edges attacked with strong jamming signals cannot be recovered by the defender. The two types of attacks can be made simultaneously on different edges.

4.2.1 Attack-recovery sequence

The players decide whether to attack/recover in the time interval $[\underline{t}_k, \bar{t}_k]$, with $k \in \mathbb{N}$ and $\bar{t}_k > \underline{t}_k = \bar{t}_{k-1}$. At $\underline{t}_k$, the system is represented by the original graph $\mathcal{G}$. Then, the players may start attacking and recovering certain links sequentially, with the attacker acting before the defender. The attack/recovery durations and the links for the attack/recovery are the action variables to be decided by the players. In this game, the players can make their actions at most once in $[\underline{t}_k, \bar{t}_k]$. Once the attacker stops the attacks (and therefore also ending all recovery attempts), the kth interval ends at $\bar{t}_k$. The next interval then immediately begins, that is, $\underline{t}_{k+1} = \bar{t}_k$.

More specifically, the attacker attacks $\mathcal{G}$ by deleting $\mathcal{E}_k^{\mathrm{A}} \subseteq \mathcal{E}$ (normal jamming signals) and $\overline{\mathcal{E}}_k^{\mathrm{A}} \subseteq \mathcal{E}$ (strong jamming signals) with $\mathcal{E}_k^{\mathrm{A}} \cap \overline{\mathcal{E}}_k^{\mathrm{A}} = \emptyset$ from time $\underline{t}_k$ until $\overline{\tau}_k^{\mathrm{A}}$, whereas the defender recovers $\mathcal{E}_k^{\mathrm{D}} \subseteq \mathcal{E}_k^{\mathrm{A}}$ from $\underline{\tau}_k^{\mathrm{D}}$ until $\overline{\tau}_k^{\mathrm{D}}$, with $\underline{t}_k < \underline{\tau}_k^{\mathrm{D}} \leq \overline{\tau}_k^{\mathrm{D}} \leq \bar{t}_k$. Because of the presence of the attacks, $\mathcal{G}$ is changed to $\mathcal{G}_k^{\mathrm{A}} := (\mathcal{V}, \mathcal{E} \setminus (\overline{\mathcal{E}}_k^{\mathrm{A}} \cup \mathcal{E}_k^{\mathrm{A}}))$ beginning from $\underline{t}_k$. Similarly, because of the recovery action by the defender, $\mathcal{G}_k^{\mathrm{A}}$ is changed to $\mathcal{G}_k^{\mathrm{D}} := (\mathcal{V}, (\mathcal{E} \setminus (\overline{\mathcal{E}}_k^{\mathrm{A}} \cup \mathcal{E}_k^{\mathrm{A}}) \cup \mathcal{E}_k^{\mathrm{D}})$ from $\underline{\tau}_k^{\mathrm{D}}$ until $\overline{\tau}_k^{\mathrm{D}}$. The graph $\mathcal{G}_k^{\mathrm{D}}$ changes back to $\mathcal{G}_k^{\mathrm{A}}$ from $\overline{\tau}_k^{\mathrm{D}}$ to $\overline{\tau}_k^{\mathrm{A}}$, if the defender ends its recovery before the attacker ends its attack.

Otherwise, if the attacker ends its attack first, then the defender can only recover until $\overline{\tau}_k^{\mathrm{A}}$, i.e., $\overline{\tau}_k^{\mathrm{A}} = \overline{\tau}_k^{\mathrm{D}}$. The graph becomes $\mathcal{G}$ again when the attacker stops jamming, as the new (k+1)th interval begins. For attacking/recovering links, both players spend energy in proportion to the attack/recovery duration. In this formulation, we consider a constant waiting time (representing the time needed for the defender to recognize the attack) $\gamma^{\mathrm{D}} \geq 0$ between $\underline{t}_k$ and $\underline{\tau}_k^{\mathrm{D}}$, unless the attacker ends attacking earlier, which is specified by $\underline{\tau}_k^{\mathrm{D}} = \min(\overline{\tau}_k^{\mathrm{A}}, \underline{t}_k + \gamma^{\mathrm{D}})$. The attack and recovery durations denoted respectively by δ_k^{A} and δ_k^{D}, are given as

$$\delta_k^{\mathrm{A}} := \overline{\tau}_k^{\mathrm{A}} - \underline{t}_k, \quad \delta_k^{\mathrm{D}} := \overline{\tau}_k^{\mathrm{D}} - \underline{\tau}_k^{\mathrm{D}}. \tag{4.1}$$

The end time $\bar{t}_k$ of the kth interval is specified by

$$\bar{t}_k := \begin{cases} \overline{\tau}_k^{\mathrm{A}}, & \text{if } (\overline{\mathcal{E}}_k^{\mathrm{A}} \cup \mathcal{E}_k^{\mathrm{A}}) \neq \emptyset, \\ \underline{t}_k + \gamma^{\mathrm{D}}, & \text{otherwise.} \end{cases} \tag{4.2}$$

This indicates that the attacker ends the game at the end of a nonzero attack interval. Otherwise, the attacker does not attack, in which case the game ends at $\underline{t}_k + \gamma^{\mathrm{D}}$.

In this game, players attempt to choose the best strategies in terms of edges attacked/recovered and attack/recovery durations ($(\bar{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}})$ and $(\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}})$) to maximize their own utility functions of the game defined over multiple intervals. Specifically, in this chapter we consider the simplest case, which is the game defined over two intervals $[\underline{t}_k,\bar{t}_k]$ and $[\underline{t}_{k+1},\bar{t}_{k+1}]$ as explained in Section 4.2.4 below.

Fig. 4.1 illustrates the sequences of the attack and recovery actions described so far. As shown in this figure, a game consists of two attack parts. The blue dashed line indicates the end of the first part, while the blue solid line the end of the second part (and hence the game). In the graphs, the solid and dashed lines indicate edges connected and disconnected, respectively; no lines in e_{12} and e_{24} in the second part indicate that those edges are attacked strongly. the attacker attacks two edges e_{12} and e_{34} in the time interval $[\underline{t}_1, \bar{t}_1]$, but the defender recovers one of them. The attacker attacks different edges with different attack strength in $[\underline{t}_2, \bar{t}_2]$, and the defender can only recover e_{13}, which is attacked normally. The attacker ends attacking before the defender ends recovering in the second interval in this example, and therefore the interval ends at $\overline{\tau}_2^{\mathrm{D}} = \overline{\tau}_2^{\mathrm{A}}$.

4.2.2 Energy constraints

As explained in Chapter 2, the players cannot keep sending signals to all edges for infinite duration as players have energy constraints. Here, we suppose that the attacker has two types of jamming signals. The strong attacks on $\overline{\mathcal{E}}_k^{\mathrm{A}}$ take $\overline{\beta}^{\mathrm{A}}$ per unit time, or $s := \overline{\beta}^{\mathrm{A}}/\beta^{\mathrm{A}} > 1$, $s \in \mathbb{R}$, times more energy per edge per unit time compared to the normal attacks on $\mathcal{E}_k^{\mathrm{A}}$. In our numerical examples and analysis given below, we consider the case where $s = 2$, i.e., attacking an edge strongly takes twice the energy. The total energy used for the attacker is constrained as

$$\sum_{m=1}^{k-1}(\overline{\beta}^{\mathrm{A}}|\overline{\mathcal{E}}_m^{\mathrm{A}}| + \beta^{\mathrm{A}}|\mathcal{E}_m^{\mathrm{A}}|)\delta_m^{\mathrm{A}} + (\overline{\beta}^{\mathrm{A}}|\overline{\mathcal{E}}_k^{\mathrm{A}}| + \beta^{\mathrm{A}}|\mathcal{E}_k^{\mathrm{A}}|)(t - \underline{t}_k)\kappa^{\mathrm{A}} + \rho^{\mathrm{A}}t, \tag{4.3}$$

for any $t \in [\underline{t}_k, \underline{t}_{k+1}]$, with $\kappa^{\mathrm{A}} \geq 0$, $\overline{\beta}^{\mathrm{A}} > \beta^{\mathrm{A}} > 0$, and $\beta^{\mathrm{A}}|\mathcal{E}| > \rho^{\mathrm{A}} > 0$. The parameters κ^{A} and ρ^{A} denote the attacker's initial energy and its recharge rate, respectively, whereas β^{A} denotes the attacker's unit cost of attacking one edge per time.

Since from (4.3) it is possible that $\rho^{\mathrm{A}} > \beta^{\mathrm{A}}$, i.e., the attacker recharges its energy faster than it consumes, the attacker can attack up to a certain number of edges for infinite time. We denote that number of edges as $\bar{m}^{\mathrm{A}} := \lfloor \rho^{\mathrm{A}}/\beta^{\mathrm{A}} \rfloor$, where the attacker can attack edges $\overline{\mathcal{E}}_k^{\mathrm{A}}$ and $\mathcal{E}_k^{\mathrm{A}}$ satisfying $(\overline{\beta}^{\mathrm{A}}/\beta^{\mathrm{A}})|\overline{\mathcal{E}}_k^{\mathrm{A}}| + |\mathcal{E}_k^{\mathrm{A}}| \leq \bar{m}^{\mathrm{A}}$ for infinite duration. Otherwise, we obtain the maximum attack duration Δ^{A} where the left-hand side of (4.3) is equal to the right-hand side as

$$\Delta^{\mathrm{A}} := \frac{\kappa^{\mathrm{A}} + (\overline{\beta}^{\mathrm{A}}|\overline{\mathcal{E}}_k^{\mathrm{A}}| + \beta^{\mathrm{A}}|\mathcal{E}_k^{\mathrm{A}}|)\underline{t}_k}{(\overline{\beta}^{\mathrm{A}}|\overline{\mathcal{E}}_k^{\mathrm{A}}| + \beta^{\mathrm{A}}|\mathcal{E}_k^{\mathrm{A}}|) - \rho^{\mathrm{A}}} - \frac{\sum_{m=1}^{k-1}(\overline{\beta}^{\mathrm{A}}|\overline{\mathcal{E}}_m^{\mathrm{A}}| + \beta^{\mathrm{A}}|\mathcal{E}_m^{\mathrm{A}}|)\delta_m^{\mathrm{A}}}{(\overline{\beta}^{\mathrm{A}}|\overline{\mathcal{E}}_k^{\mathrm{A}}| + \beta^{\mathrm{A}}|\mathcal{E}_k^{\mathrm{A}}|) - \rho^{\mathrm{A}}} - \underline{t}_k. \tag{4.4}$$

This energy consumption model for the attacker is illustrated in Fig. 4.2, where the black dashed line with slope ρ^{A} represents the right-hand side of the inequality (4.3) and the black solid line with slope $\overline{\beta}^{\mathrm{A}}|\overline{\mathcal{E}}_k^{\mathrm{A}}| + \beta^{\mathrm{A}}|\overline{\mathcal{E}}_k^{\mathrm{A}}|$ represents the actual energy consumed by the attacker, shown in the left-hand side in (4.3). The attacker runs out of energy when the solid line touches the dashed line. It is then possible for the attacker to never run out of energy if the dashed line is steeper than the solid line, i.e., the attacker attacks only a few edges so that $\overline{\beta}^{\mathrm{A}}|\overline{\mathcal{E}}_k^{\mathrm{A}}| + \beta^{\mathrm{A}}|\mathcal{E}_k^{\mathrm{A}}| \leq \rho^{\mathrm{A}}$. However, the attacker may want to maximize the damage on the multiagent system by attacking more edges (and spending more energy) in some attack intervals. In the game structure explained later, we consider the scenarios where the attacker always attacks more edges and hence runs out of energy every two attack intervals, as also illustrated in Fig. 4.2 where the actual energy consumed by the attacker (black solid line) reaches the energy limit (black dashed

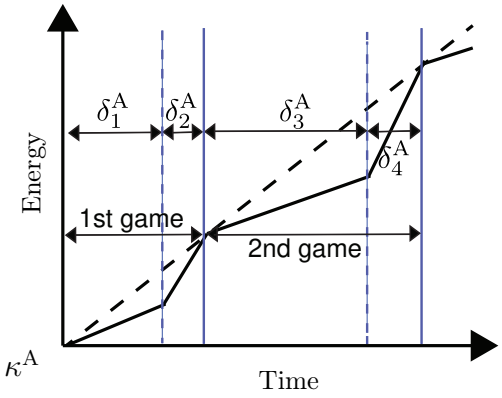


Figure 4.2 The attacker's energy consumption model, with $\kappa^{\mathrm{A}} = 0$. The vertical blue lines indicate the end time of each attack interval: dashed lines for the end of the first parts and solid lines for the second parts.

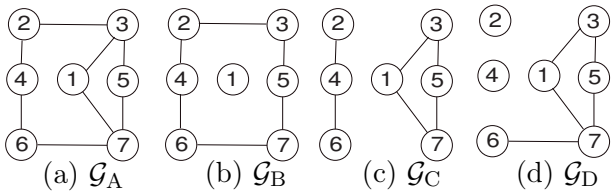


Figure 4.3 Graphs and their agent-group indices: (a) $c(\mathcal{G}_{\mathrm{A}}) = 0$, (b) $c(\mathcal{G}_{\mathrm{B}}) = -12$, (c) $c(\mathcal{G}_{\mathrm{C}}) = -24$, and (d) $c(\mathcal{G}_{\mathrm{D}}) = -22$. Note that $c(\mathcal{G}_{\mathrm{D}})$ is larger than $c(\mathcal{G}_{\mathrm{C}})$, even with more clusters.

line) at the end of every δ_k^{A} with even k.

The energy constraint of the defender, which is similar to (4.3), is given by

$$\sum_{m=1}^{k-1} \beta^{\mathrm{D}} |\mathcal{E}_m^{\mathrm{D}}| \delta_m^{\mathrm{D}} + \beta^{\mathrm{D}} |\mathcal{E}_k^{\mathrm{D}}| (t - \underline{\tau}_k^{\mathrm{D}}) \leq \kappa^{\mathrm{D}} + \rho^{\mathrm{D}} t, \tag{4.5}$$

for any $t \in [\underline{\tau}_k^{\mathrm{D}}, \underline{\tau}_{k+1}^{\mathrm{D}}]$, with $\kappa^{\mathrm{D}} > 0$ and $\beta^{\mathrm{D}} > \rho^{\mathrm{D}} > 0$. We also obtain maximum recovery duration Δ^{D} as

$$\Delta^{\mathrm{D}} := \frac{\kappa^{\mathrm{D}} + \beta^{\mathrm{D}} |\mathcal{E}_k^{\mathrm{D}}| \underline{\tau}_k^{\mathrm{D}} - \sum_{m=1}^{k-1} \beta^{\mathrm{D}} |\mathcal{E}_m^{\mathrm{D}}| \delta_m^{\mathrm{D}}}{\beta^{\mathrm{D}} |\mathcal{E}_k^{\mathrm{D}}| - \rho^{\mathrm{A}}} - \underline{\tau}_k^{\mathrm{D}}. \tag{4.6}$$

4.2.3 Agent clustering and state difference

By attacking, the attacker makes the graph disconnected and in turn separates the agents into clusters. Specifically, in a given graph $\mathcal{G}'$, the agents are grouped into $\tilde{c}(\mathcal{G}')$ number of clusters, with the clusters $\mathcal{V}_1^{\mathcal{G}'}, \mathcal{V}_2^{\mathcal{G}'}, \ldots, \mathcal{V}_{\tilde{c}(\mathcal{G}')}^{\mathcal{G}'}$ being a partition of $\mathcal{V} = \{1, 2, \ldots, n\}$ with $\cup_{l=1}^{\tilde{c}(\mathcal{G}')} \mathcal{V}_l^{\mathcal{G}'} = \mathcal{V}$ and $\mathcal{V}_l^{\mathcal{G}'} \cap \mathcal{V}_m^{\mathcal{G}'} = \emptyset,\ l \neq m$.

Here, we are interested in the case where the attacker is also concerned about the number of agents in each cluster, as an extension of the formulation in Chapter 2. The

attacker does not want too many agents to be together in the same cluster in order to minimize the spread of information, while on the other hand the defender wants as many agents as possible in the same cluster in order to maximize it. Hence, the distribution of agents among clusters becomes important. For example, if there are 12 agents: 1) the attacker can choose to separate the agents into 3 clusters with ten agents in cluster 1 and one agent each in both clusters 2 and 3, or 2) the attacker can also divide those agents into two clusters with both clusters 1 and 2 consisting of six agents each. The option 2) may be better than 1) for the attacker despite having fewer clusters, because the agents are distributed more evenly so that most of them are not grouped together in the same cluster.

Motivated by the example above, here we define the agent-group index $c(\cdot)$ as

$$c(\mathcal{G}') := \sum_{l=1}^{\tilde{c}(\mathcal{G}')} |\mathcal{V}_l^{\mathcal{G}'}|^2 - n^2 (\leq 0). \tag{4.7}$$

The value of $c(\mathcal{G}')$ is 0 if $\mathcal{G}'$ is connected, since there is only one cluster with n agents inside. A larger value (closer to 0) of $c(\mathcal{G}')$ implies that there are fewer clusters in graph $\mathcal{G}'$, with each cluster having more agents. Since $\mathcal{G}_k^{\mathrm{A}} \subseteq \mathcal{G}_k^{\mathrm{D}} \subseteq \mathcal{G}$, it follows that $c(\mathcal{G}_k^{\mathrm{A}}) \leq c(\mathcal{G}_k^{\mathrm{D}}) \leq 0$. The agent-group index of some graphs are shown in Fig. 4.3. Here, it is interesting that $c(\mathcal{G}_{\mathrm{C}})$ is smaller than $c(\mathcal{G}_{\mathrm{D}})$, even though $\mathcal{G}_{\mathrm{D}}$ has more clusters. Thus, for an attacker who tries to reduce the maximum number of agents grouped together in one cluster, the topology $\mathcal{G}_{\mathrm{C}}$ is preferable to $\mathcal{G}_{\mathrm{D}}$.

In this setting the players also consider the effects of their actions on the agent states when attacking/recovering, similar to the formulation in Chapter 2. For example, the attacker may want to separate agents having state values with more difference in different clusters. We specify the agents' state difference z_k of the kth interval as

$$z_k((\overline{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{A}}, \delta_k^{\mathrm{A}}), (\mathcal{E}_k^{\mathrm{D}}, \delta_k^{\mathrm{D}})) := x^{\mathrm{T}}(\bar{t}_k) L_{\mathrm{c}} x(\bar{t}_k), \tag{4.8}$$

Note that the value of z_k does not increase over time [5].

4.2.4 Two-interval game structure

The players' utility functions of the lth game over $[\underline{t}_{2l-1}, \bar{t}_{2l}]$ take account of the agent-group index $c(\cdot)$ and the difference $z_k(\cdot,\cdot)$ of agents' states, and are defined by

$$U_k^{\mathrm{A}} := \sum_{k=2l-1}^{2l} a z_k \delta_k^{\mathrm{A}} - b(c(\mathcal{G}_k^{\mathrm{A}})(\delta_k^{\mathrm{A}} - \delta_k^{\mathrm{D}}) + c(\mathcal{G}_k^{\mathrm{D}})\delta_k^{\mathrm{D}}), \tag{4.9}$$

$$U_k^{\mathrm{D}} := -U_k^{\mathrm{A}}, \tag{4.10}$$

where $a, b > 0$. These utility functions represent the number of clusters over attack duration for two consecutive attack intervals, since the attacker's energy runs out after the two attack intervals as explained above. The players change their strategies once during the two intervals, i.e., once in a game. These strategies are determined at the beginning of each game, as explained later. From now on, we refer to these two attack intervals as two parts of the lth game.

From the discussion on the energy constraint in Section 4.2.2, it is possible that the attacker never runs out of energy if the attacked edges $\overline{\mathcal{E}}_k^{\mathrm{A}}$ and $\mathcal{E}_k^{\mathrm{A}}$ satisfy $(s|\overline{\mathcal{E}}_k^{\mathrm{A}}| + |\mathcal{E}_k^{\mathrm{A}}|) \leq \bar{m}^{\mathrm{A}}$. Since there is no maximum attack duration Δ^{A}, in this case we suppose that the choices for attack duration are limited to $\delta_k^{\mathrm{A}} \in \{\delta/2, \delta\}$ for simplicity, with constant $\delta > 2\gamma^{\mathrm{D}} > 0$.

In this setting, we assume that in the $(2l-1)$th attack interval (the first part of the lth game) the attacker attacks edges $\bar{\mathcal{E}}_{2l-1}^{\mathrm{A}}$ and $\mathcal{E}_{2l-1}^{\mathrm{A}}$ satisfying $(s|\bar{\mathcal{E}}_{2l-1}^{\mathrm{A}}| + |\mathcal{E}_{2l-1}^{\mathrm{A}}|) \leq \bar{m}^{\mathrm{A}}$, with the choices of $\delta_{2l-1}^{\mathrm{A}} \in \{\delta/2, \delta\}$ specified above. In the next $(2l)$th interval (the second part of the game), we suppose that the attacker chooses to attack $\bar{\mathcal{E}}_{2l}^{\mathrm{A}}$ and $\mathcal{E}_{2l}^{\mathrm{A}}$ satisfying $(s|\bar{\mathcal{E}}_{2l}^{\mathrm{A}}| + |\mathcal{E}_{2l}^{\mathrm{A}}|) > \bar{m}^{\mathrm{A}}$, i.e., more/stronger edges than in the first part, for finite Δ_{2l}^{A} duration as in (4.4), i.e., $\delta_{2l}^{\mathrm{A}} = \Delta_{2l}^{\mathrm{A}}$. Therefore, we have two intervals with different characteristics in each lth game. For simplicity, in this game the defender is only able to recover until either it runs out of energy, or the recovery is interrupted by the stoppage of the attack, i.e., $\delta_k^{\mathrm{D}} \in \{0, \min\{\delta_k^{\mathrm{A}} - \gamma^{\mathrm{D}}, \Delta^{\mathrm{D}}\}\}, k \in \mathbb{N}$.

In order to find the equilibrium, the game is classified into some subgames/decision-making points. The subgame perfect equilibrium must be an equilibrium in every subgame. The optimal strategy of each player is obtained by using a backward induction approach, i.e., by finding the equilibrium from smallest subgames. The subgame perfect equilibrium solution concept is suitable for this problem setting, since players decide their strategies in a sequential manner.

The optimal edges and durations are specified as follows. For the lth game over the

interval $[\underline{t}_{2l-1}, \bar{t}_{2l}]$, the optimal strategies of the players according to the subgame perfect equilibrium principle are given by

$$(\mathcal{E}_{2l}^{\mathrm{D}*}, \delta_{2l}^{\mathrm{D}*}) \in \underset{(\mathcal{E}_{2l}^{\mathrm{D}}, \delta_{2l}^{\mathrm{D}})}{\arg\max}\, U_2^{\mathrm{D}}, \tag{4.11}$$

$$(\bar{\mathcal{E}}_{2l}^{\mathrm{A}*}, \mathcal{E}_{2l}^{\mathrm{A}*}, \delta_{2l}^{\mathrm{A}*}) \in \underset{(\bar{\mathcal{E}}_{2l}^{\mathrm{A}}, \mathcal{E}_{2l}^{\mathrm{A}}, \delta_{2l}^{\mathrm{A}})}{\arg\max}\, U_2^{\mathrm{A}}, \tag{4.12}$$

$$(\mathcal{E}_{2l-1}^{\mathrm{D}*}, \delta_{2l-1}^{\mathrm{D}*}) \in \underset{(\mathcal{E}_{2l-1}^{\mathrm{D}}, \delta_{2l-1}^{\mathrm{D}})}{\arg\max}\, U^{\mathrm{D}}, \tag{4.13}$$

$$(\bar{\mathcal{E}}_{2l-1}^{\mathrm{A}*}, \mathcal{E}_{2l-1}^{\mathrm{A}*}, \delta_{2l-1}^{\mathrm{A}*}) \in \underset{(\bar{\mathcal{E}}_{2l-1}^{\mathrm{A}}, \mathcal{E}_{2l-1}^{\mathrm{A}}, \delta_{2l-1}^{\mathrm{A}})}{\arg\max}\, U^{\mathrm{A}}, \tag{4.14}$$

with U_2^{A} and U_2^{D} being parts of U_k^{A} and U_k^{D} associated with the $(2l)$th interval, respectively. We assume that all parameters and utility functions are known to all players, including the energy parameters ($\kappa^{\mathrm{A}}, \rho^{\mathrm{A}}, \beta^{\mathrm{A}}$ and $\kappa^{\mathrm{D}}, \rho^{\mathrm{D}}, \beta^{\mathrm{D}}$) of the opposing player. This implies that a player is aware of the optimal strategies of other player, e.g., the defender knows which edges are optimally attacked by the attacker given the defender's best response.

Note that to find $(\bar{\mathcal{E}}_{2l-1}^{\mathrm{A}*}, \mathcal{E}_{2l-1}^{\mathrm{A}*}, \delta_{2l-1}^{\mathrm{A}*})$, one needs to obtain $(\mathcal{E}_{2l-1}^{\mathrm{D}*}(\bar{\mathcal{E}}_{2l-1}^{\mathrm{A}}, \mathcal{E}_{2l-1}^{\mathrm{A}}, \delta_{2l-1}^{\mathrm{A}})$, $\delta_{2l-1}^{\mathrm{D}*}(\bar{\mathcal{E}}_{2l-1}^{\mathrm{A}}, \mathcal{E}_{2l-1}^{\mathrm{A}}, \delta_{2l-1}^{\mathrm{A}}))$ beforehand. Likewise, to find $(\mathcal{E}_{2l-1}^{\mathrm{D}*}, \delta_{2l-1}^{\mathrm{D}*})$, one needs to obtain $(\bar{\mathcal{E}}_{2l}^{\mathrm{A}*}(\mathcal{E}_{2l-1}^{\mathrm{D}}, \delta_{2l-1}^{\mathrm{D}}), \mathcal{E}_{2l}^{\mathrm{A}*}(\mathcal{E}_{2l-1}^{\mathrm{D}}, \delta_{2l-1}^{\mathrm{D}})$, $\delta_{2l}^{\mathrm{A}*}(\mathcal{E}_{2l-1}^{\mathrm{D}}, \delta_{2l-1}^{\mathrm{D}}))$. These optimization problems are solved by the players in the beginning of the lth game, i.e., the strategies for the second part ($(2l)$th interval) are decided in the beginning of the previous $(2l-1)$th interval. The players are not able to further change their strategies for the second part of the game ($(2l)$th interval) after it has been determined before at the start of the game. The agents' dynamics and the players' energy condition will affect the players' strategies in each game.

In this chapter, we focus on the cluster forming over different intervals. We are able to find the optimal strategies of the players (4.11)–(4.14) by computing all possible combinations of edges and action durations, since they are both finite. It is also clear that the complexity of the game depends on the graph structure: it takes much longer to solve (4.11)–(4.14) in more complex graphs, since there are more possible combinations of edges.

4.3 Consensus and clustering analysis

In this section, we examine the effect of the attacker's energy model on the cluster forming and multiagent consensus.

We first discuss the defender's optimal strategy on some games with specific conditions.

Lemma 4.1. The defender always recovers in the $(2l)$th interval ($\mathcal{E}^{\mathrm{D}}_{2l} \neq \emptyset$), as long as $\mathcal{E}^{\mathrm{A}}_{2l} \neq \emptyset$.

From the result of $(2l)$th interval above, we are now able to state the result of $(2l_i - 1)$th interval for some l.

Lemma 4.2. There exists an infinite sequence $\bar{l} := \{\bar{l}_1, \bar{l}_2, \ldots\}$ of the game indexes where $\bar{l}_{i+1} > \bar{l}_i$ and $\bar{l}_i \in \mathbb{N}$ such that in the $(\bar{l}_i)$th game, the optimal strategy for the defender in the $(2\bar{l}_i - 1)$th attack interval is to recover from attacks with normal strength, i.e., $\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i-1} \neq \emptyset$ as long as $\mathcal{E}^{\mathrm{A}}_{2\bar{l}_i-1} \neq \emptyset$.

The following result provides a necessary condition for the agents to be separated into multiple clusters for infinitely long durations without achieving consensus. The results in Lemmas 4.1 and 4.2, which characterize the defender's optimal strategies in each interval of a game, enable us to derive the following result.

Proposition 4.3. The necessary condition to prevent the consensus from happening is $\bar{m}^{\mathrm{A}} \geq s\lambda$, with λ denoting the edge connectivity of $\mathcal{G}$.

However, the necessary condition in Proposition 4.3 is not sufficient for preventing consensus, since even with $\bar{m}^{\mathrm{A}}$ large enough, the attacker may decide to strongly attack fewer edges instead. This is related to the attacker's energy usage, as we see in the next section.

4.4 Case study on attacker's energy usage

In this section, we investigate how the attacker uses its energy by comparing several attack strategies that characterize different energy consumption profiles. With the ability to attack edges using strong jamming signals, the attacker is able to prevent consensus by attacking some appropriate edges strongly at all times, with the downside that it consumes more energy. However, here we will show that under some conditions related to the energy usage, the attacker chooses not to attack edges strongly. While this attack strategy may be optimal according to U^{A}_k defined over interval $[\underline{t}_{2l-1}, \bar{t}_{2l}]$, it will be unsuccessful in preventing consensus.

Here, we discuss a special case where there are three agents (agents 1, 2, and 3) in a line/path graph 1–2–3. Specifically, we investigate the effect of different initial states

and different energy parameters to the clustering process. Throughout this section, we set $\delta = \beta^{\mathrm{A}} = \beta^{\mathrm{D}} = a = b = 1$, $\kappa^{\mathrm{A}} = \gamma^{\mathrm{D}} = 0$, and initial states $x_0 = [x', 0, -x']^{\mathrm{T}}$. We choose this setting for simplicity, but we will see that the implications hold under other conditions.

4.4.1 Effect of initial states x_0

Here we will investigate the effect of different x_0 on the value of U_k^{A} in the first game ($l = 1$). We also set $\rho^{\mathrm{A}} = 2.5$, implying that $\bar{m}_{\mathrm{A}} = 2$. In this setting, the attacker has at least two strategy choices in $l = 1$: **(1a)** $|\overline{\mathcal{E}}_1^{\mathrm{A}}| = 1$, $|\mathcal{E}_1^{\mathrm{A}}| = 0$, and **(1b)** $|\overline{\mathcal{E}}_1^{\mathrm{A}}| = 0$, $|\mathcal{E}_1^{\mathrm{A}}| = 1$, with $\delta_1^{\mathrm{A}} = |\overline{\mathcal{E}}_2^{\mathrm{A}}| = |\mathcal{E}_1^{\mathrm{A}}| = 1$ in both cases. It is clear that in Case (1b) the attacker attacks fewer edges in the first part to save its energy that will be used in the second part. We assume that the defender with $\kappa^{\mathrm{D}} = 1$ and $\rho^{\mathrm{D}} = 0.5$ always recovers whenever the attacker attacks with normal jamming signals. Other strategies are not discussed due to space limitation.

Case (1a): We notice that in this case $|\mathcal{E}_1^{\mathrm{D}}| = 0$, since $|\mathcal{E}_1^{\mathrm{A}}| = 0$. With the parameters specified above, we have $U_k^{\mathrm{A}} = z_1 + 4 + z_2\Delta_2^{\mathrm{A}} - (-4(\Delta_2^{\mathrm{A}} - \delta_2^{\mathrm{D}}) + c(\mathcal{G}_2^{\mathrm{D}})\delta_k^{\mathrm{D}})$. The value $c(\mathcal{G}_1^{\mathrm{A}}) = -4$ is from the fact that regardless of the attacked edges, there are always two clusters: one cluster has one agent and the other has two agents.

From $|\mathcal{E}_k^{\mathrm{A}}|$, $|\overline{\mathcal{E}}_k^{\mathrm{A}}|$, and $|\mathcal{E}_k^{\mathrm{D}}|$ above, we obtain the attack and recovery durations $\Delta_2^{\mathrm{A}} = 1$ and $\Delta_2^{\mathrm{D}} = 3$. With $x_0 = [x', 0, -x']^{\mathrm{T}}$, if one agent is disconnected for $k = 1$, the function z_k becomes $z_1 = (e^{-2\delta}x')^2 + [((3 - e^{-2\delta})x')^2 + ((3 + e^{-2\delta})x')^2]/4$ from (2.2).

Now, since the defender recovers one edge for $k = 2$ (since $|\mathcal{E}_2^{\mathrm{A}}| = 1$), the graph for $k = 2$ is the same as that for $k = 1$: one agent gets disconnected from the other two. With $|\overline{\mathcal{E}}_2^{\mathrm{A}}| = 1$, it is obvious that $\overline{\mathcal{E}}_1^{\mathrm{A}} = \overline{\mathcal{E}}_2^{\mathrm{A}}$ is better for the attacker than strongly attacking the other edge. By changing δ to $\delta + \Delta_2^{\mathrm{A}}$, we are able to obtain z_k for $k = 2$ as for $k = 1$ specified above.

Finally, we substitute z_1 and z_2 into U^{A} and obtain

$$U_k^{\mathrm{A}} = \frac{3(1 + e^4 + 6e^8)(x')^2}{2e^8} + 8 \approx 9.028(x')^2 + 8. \tag{4.15}$$

Case (1b): Under the assumption that the defender recovers ($|\mathcal{E}_1^{\mathrm{D}}| > 0$), we first obtain $\Delta_1^{\mathrm{D}} = 2$, which implies that the defender recovers for δ duration for $k = 1$ and as a result $c(\mathcal{G}_1^{\mathrm{D}}) = 0$. Therefore, we have $U_k^{\mathrm{A}} = z_1 + z_2\Delta_2^{\mathrm{A}} - (c(\mathcal{G}_2^{\mathrm{A}})(\Delta_2^{\mathrm{A}} - \delta_2^{\mathrm{D}}) + c(\mathcal{G}_2^{\mathrm{D}})\delta_2^{\mathrm{D}})$.

In this case, we obtain $\Delta_2^{\mathrm{A}} = 3$, which is longer than in Case (1a) above, since in this case the attacker is using less energy for $k = 1$. We also obtain $\Delta_2^{\mathrm{D}} = 1$, which is shorter than in Case (1a) for the same reason.

Since the graph remains connected for $k = 1$, from the consensus dynamics in (2.2) we obtain the function z_k where all agents are connected in the path graph as $z_1 = 6(e^{-\delta}x')^2$, with the agents' states becoming $x(t) = [e^{-t}x',\ 0,\ -e^{-t}x']^{\mathrm{T}}$. Since the defender recovers and hence one agent is disconnected from the other agents for Δ_2^{D} duration for $k = 2$, we find z_2 as in Case (1a) above, by replacing x' to $e^{-1}x'$ and δ to $\Delta_2^{\mathrm{D}} = 1$. Note that the value of z_2 does not change after $\underline{t}_2 + \Delta_2^{\mathrm{D}}$, since $\Delta_2^{\mathrm{A}} > \Delta_2^{\mathrm{D}}$. We substitute z_1 and z_2 in U_k^{A} to get

$$U_k^{\mathrm{A}} = \frac{3(3 + 13e^4)(x')^2}{2e^6} + 16 \approx 2.650(x')^2 + 16. \tag{4.16}$$

We then compare (4.15) and (4.16) to obtain a condition on x' for selecting strategies. Specifically, the attacker's strategy $|\overline{\mathcal{E}}_1^{\mathrm{A}}| = 1, |\mathcal{E}_1^{\mathrm{A}}| = 0$ is better than $|\overline{\mathcal{E}}_1^{\mathrm{A}}| = 0, |\mathcal{E}_1^{\mathrm{A}}| = 1$ if $x' > 1.12$. Otherwise, the strategy in Case (1b) is better.

This example shows that the initial state x_0 influences the players' strategies. In general, the attacker tends to save its energy in the first part by attacking fewer edges, if the agents' states are sufficiently close. This also affects the consensus process, where consensus may still happen if the attacker does not attack with strong jamming signals, despite with high enough $\bar{m}^{\mathrm{A}}$.

4.4.2 Effect of attacker's recharge rate ρ^{A} (smaller $\bar{m}^{\mathrm{A}}$)

We next investigate U_k^{A} in the first game ($l = 1$) by varying ρ^{A}. Here we set $2 < \rho^{\mathrm{A}} < 3$, and we also assume that the defender has large enough κ^{D} and ρ^{D} so that it recovers all attacked edges $\mathcal{E}_k^{\mathrm{A}}$ for the entire attack duration δ_k^{A}, i.e., $\delta_k^{\mathrm{D}} = \delta_k^{\mathrm{A}}$, for any k. We again compare two cases of strategy choices as above: **(2a)** $|\overline{\mathcal{E}}_1^{\mathrm{A}}| = 1$, $|\mathcal{E}_1^{\mathrm{A}}| = 0$, and **(2b)** $|\overline{\mathcal{E}}_1^{\mathrm{A}}| = 0$, $|\mathcal{E}_1^{\mathrm{A}}| = 1$, with $\delta_1^{\mathrm{A}} = |\overline{\mathcal{E}}_2^{\mathrm{A}}| = |\mathcal{E}_1^{\mathrm{A}}| = 1$ in both cases. Here we assume that $x_0 = [1, 0, -1]^{\mathrm{T}}$.

Case (2a): The utility function here is $U_k^{\mathrm{A}} = z_1 + 4 + z_2\Delta_2^{\mathrm{A}} - (-4(\Delta_2^{\mathrm{A}} - \delta_2^{\mathrm{D}}) + c(\mathcal{G}_2^{\mathrm{D}})\delta_2^{\mathrm{D}})$. From $|\mathcal{E}_1^{\mathrm{A}}|$ and $|\bar{\mathcal{E}}_1^{\mathrm{A}}|$, we obtain $\Delta_2^{\mathrm{A}} = \frac{\rho^{\mathrm{A}}-2}{3-\rho^{\mathrm{A}}}$, z_1, and z_2, resulting in

$$U_k^{\mathrm{A}} = \frac{3(3 + e^{-4})}{2} + 4 + \frac{\rho^{\mathrm{A}} - 2}{3 - \rho^{\mathrm{A}}}\Big(\frac{3(3 + e^{-4(\frac{\rho^{\mathrm{A}}-2}{3-\rho^{\mathrm{A}}})})}{2} + 4\Big). \tag{4.17}$$

Case (2b): With $\Delta_2^{\mathrm{A}} = \frac{\rho^{\mathrm{A}}-1}{3-\rho^{\mathrm{A}}}$, since the graph remains connected for $k = 1$, we obtain $z_1 = 6e^{-2}$ where all agents are connected, with $x(\underline{t}_2) = [e^{-1},\ 0,\ -e^{-1}]$. Since the defender recovers and hence one agent is disconnected from the other agents for the entire Δ_2^{A}, we use the same approach as in Cases (1a) and (1b) to obtain the value of z_2.

By substitution, we then obtain

$$U_k^{\mathrm{A}} = 6e^{-2} + \frac{\rho^{\mathrm{A}} - 1}{3 - \rho^{\mathrm{A}}}\Big(\frac{3(3 + e^{-4(\frac{\rho^{\mathrm{A}}-1}{3-\rho^{\mathrm{A}}})})}{2e^2} + 4\Big). \tag{4.18}$$

From (4.17) and (4.18), the attacker's strategy in Case (2a) is better than the one in Case (2b) if $\rho^{\mathrm{A}} < 2.812$.

We note that from this example, the higher the attacker's recharge rate ρ^{A} is, the more likely the attacker attacks fewer edges in the first part. This has an interesting implication, where the consensus is more likely to happen for some higher ρ^{A}. This is because the attack duration δ_k^{A} contributes much to the value of U_k^{A}, where δ_k^{A} is multiplied by z_k.

4.4.3 Effect of attacker's recharge rate ρ^{A} (larger $\bar{m}^{\mathrm{A}}$)

We now discuss a scenario with varying ρ^{A} and higher $\bar{m}^{\mathrm{A}}$, compared to Cases (1b) and (2b) above. Specifically, we set $3 < \rho^{\mathrm{A}} < 4$, implying $\bar{m}_{\mathrm{A}} = 3$. We also assume that the defender has enough energy to recover all possible $\mathcal{E}_k^{\mathrm{A}}$ for δ_k^{A} at any kth interval. The initial states are $x_0 = [1, 0, -1]^{\mathrm{T}}$. The compared strategies are: **(3a)** $|\overline{\mathcal{E}}_1^{\mathrm{A}}| = 1$, $|\mathcal{E}_1^{\mathrm{A}}| = 0$, and **(3b)** $|\overline{\mathcal{E}}_1^{\mathrm{A}}| = 0$, $|\mathcal{E}_1^{\mathrm{A}}| = 1$, with $\delta_1^{\mathrm{A}} = 1$, $|\overline{\mathcal{E}}_2^{\mathrm{A}}| = 2$, and $|\mathcal{E}_1^{\mathrm{A}}| = 0$ in both cases.

With the same approach as in Cases (2a) and (2b) above, we obtain utility functions for Case (3a) as $U_k^{\mathrm{A}} = \frac{3(3+e^{-4})}{2} + 4 + \frac{\rho^{\mathrm{A}}-2}{4-\rho^{\mathrm{A}}}\Big(\frac{3(3+e^{-4})}{2} + 6\Big)$, and for Case (3b) as $U_k^{\mathrm{A}} = 6e^{-2} + \frac{\rho^{\mathrm{A}}-1}{4-\rho^{\mathrm{A}}}\Big(6e^{-2}+6\Big)$. By comparing these two functions, we observe that for any value of ρ^{A} with $3 < \rho^{\mathrm{A}} < 4$, the attacker's strategy in Case (3a) is always better than the one in Case (3b). This shows that attacking with stronger signals, which may prevent consensus, may be better for the attacker if $\bar{m}^{\mathrm{A}}$ is large enough.

4.5 Numerical simulation of dynamic games

4.5.1 Effect of attacker's recharge rate ρ^{A}

In our simulations, we use the graph shown in Fig. 4.4 with five vertices/agents with parameters $\beta^{\mathrm{A}} = 1.1$, $\beta^{\mathrm{D}} = 0.6$, $\kappa^{\mathrm{A}} = 0$, $\kappa^{\mathrm{D}} = 5$, $\rho^{\mathrm{D}} = 0.5$, $\gamma^{\mathrm{D}} = 0.1$, $a = 0.1$, $b = 1$, and $x_0 = [1.8, 5.2, 0.1, 2.7, 2.0]^{\mathrm{T}}$. Figs. 4.5 and 4.6 show the states of the agents with $\rho^{\mathrm{A}} = 5$ and $\rho^{\mathrm{A}} = 2.5$, respectively. Since $\lambda = 1$ in this graph, note that ρ^{A} in both simulations satisfy the condition needed in order not to achieve consensus in Proposition 4.3. The line colors in Figs. 4.5 and 4.6 correspond to the colors of the agents in Fig. 4.4. In Figs. 4.5–4.8 discussed in this section, the vertical blue lines indicate the end time of each part

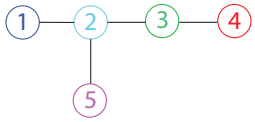


Figure 4.4 Graph used for simulations in Section 4.5

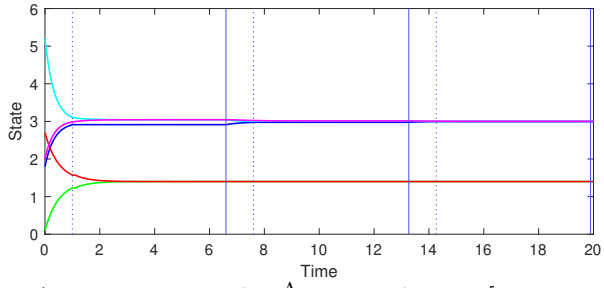


Figure 4.5 Agent states with $\rho^{\mathrm{A}} = 5$ and $x_0 = [1.8, 5.2, 0.1, 2.7, 2.0]^{\mathrm{T}}$

(attack interval), with the dashed lines indicating the end times of the first parts, and the solid lines indicating the end times of the second part of the games. The black lines indicate which graph represents the communication network at the corresponding time. The shown graphs illustrate which edges are connected and disconnected; they do not show the intensity (strong/normal) of the attacks.

In the first simulation, we have $\bar{m}^{\mathrm{A}} = \lfloor \rho^{\mathrm{A}}/\beta^{\mathrm{A}} \rfloor = 4$, whereas $\bar{m}^{\mathrm{A}} = 2$ in the second simulation. This has an impact on the consensus, where in the second simulation consensus is achieved although the attacker has the capability to disconnect an agent with strong jamming signals. On the other hand, in the first simulation, agents are divided into different clusters and do not converge to the same state. Specificallly, the agents are divided into different parts: agents 1,2,5 have the same states, separated from agents 3 and 4 in the different cluster.

4.5.2 Effect of initial states x_0

Here, we continue with mostly the same setting; the only difference is in the initial states x_0. In the first simulation, we use the same $x_0 = [1.8, 5.2, 0.1, 2.7, 2.0]^{\mathrm{T}}$, whereas $x_0 = [5.2, 0.7, 3.0, 2.0, 3.1]^{\mathrm{T}}$ in the second simulation. We set $\rho^{\mathrm{A}} = 5$ in both simulations, so that the first simulation here is the same with the one in Section 4.5.1.

Fig. 4.7 shows the agents' states with the different initial states as specified above. We observe that while agents do not reach consensus in both simulations, the resulting clusters are different. In the second simulation, agent 1 is separated from the other agents, since the players know that agent 1 has further initial states compared to others. On the other hand, while agent 2 has the furthest initial state in the first simulation, it is relatively harder to isolate agent 2 since it is connected to more agents.

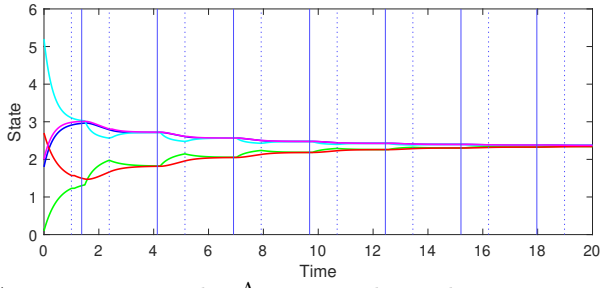


Figure 4.6 Agent states with $\rho^{\mathrm{A}} = 2.5$, where the agents achieve consensus

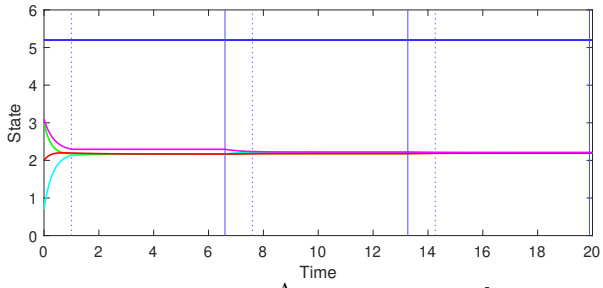


Figure 4.7 Agent states with $\rho^{\mathrm{A}} = 5$ and $x_0 = [5.2, 0.7, 3.0, 2.0, 3.1]^{\mathrm{T}}$.

Fig. 4.8 shows the cluster formations for different x_0, with the resulting graphs shown in the bottom part of the figure. In both simulations the agents are separated into two, three, or four clusters depending on the players' strategies. Note that if the attacker attacks edges with normal jamming signals, the defender is able to reconnect some agents by recovering some of the edges, therefore reducing the number of clusters. From this figure, we can also observe that the attacker may attack different edges in different intervals.

In order to prevent consensus, some edges need to be attacked continuously (depending on λ) without being recovered. It is also shown in Fig. 4.8 that one edge is continuously attacked (e_{23} in the first simulation and e_{12} in the second). Also, note that even if $\bar{m}^{\mathrm{A}} = 4$, it does not imply that the attacker attacks at least $\bar{m}^{\mathrm{A}}/s = 2$ edges with strong jamming signals continuously at all time instants.

4.6 Chapter summary

In this chapter we have formulated a two-player game in a cybersecurity problem of multiagent systems, where the players consider the impact of their actions on future communication topology and future agent states. The optimal strategies of the players have been analyzed. We have also discussed the impact of initial agent states $x(0)$ and the attacker's recharge rate ρ^{A} on cluster forming among agents.

We remark that it may be possible to have a short extension of this formulation in this chapter with slightly different consensus protocol of agents. Specifically, if the agents

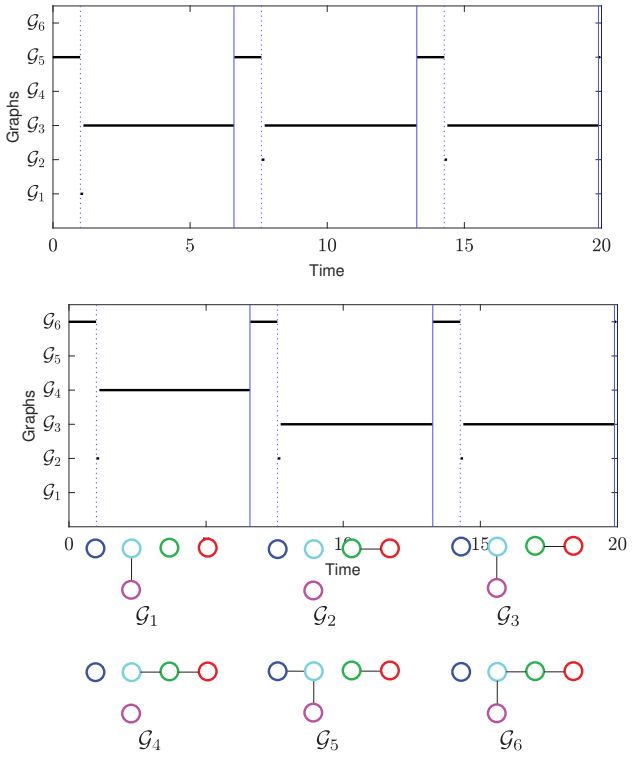


Figure 4.8 The graphs resulting from the attack-recovery actions of Section 4.5.2: first simulation (top), second simulation (middle)

are still expected to converge at infinite time albeit with different speed compared to the original protocol used in the thesis, then the same state difference values $z_k(\bar{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}})$ can still be used by the players, and thus the rest of the results may still hold.

4.7 Appendix

4.7.1 Proof of Lemma 4.1

Since a game consists of two attack intervals, the second part of the game corresponds to the last decision-making point of the game, in which the players' strategies cannot influence the decision already made in the first part of the same game. Hence, in the second part of a game the players do not save their energy by not attacking/recovering. The utility function U^{D} in (6.24) only consists of z_k and $c(\cdot)$. Since $z_{2l}((\bar{\mathcal{E}}_{2l}^{\mathrm{A}}, \mathcal{E}_{2l}^{\mathrm{A}}, \delta_{2l}^{\mathrm{A}}), (\mathcal{E}_{2l}^{\mathrm{D}} \neq \emptyset, \delta_{2l}^{\mathrm{D}} > 0)) < z_{2l}((\bar{\mathcal{E}}_{2l}^{\mathrm{A}}, \mathcal{E}_{2l}^{\mathrm{A}}, \delta_{2l}^{\mathrm{A}}), (\emptyset, 0))$ and $c(\mathcal{G}_{2l}^{\mathrm{A}})(\delta_{2l}^{\mathrm{A}} - \delta_{2l}^{\mathrm{D}}) + c(\mathcal{G}_{2l}^{\mathrm{D}})\delta_{2l}^{\mathrm{D}} \geq c(\mathcal{G}_{2l}^{\mathrm{A}})$, the function U_2^{D} always has a higher value if $\mathcal{E}_{2l}^{\mathrm{D}} \neq \emptyset$.

4.7.2 Proof of Lemma 6.13

We first consider a case where the defender does not recover from nonzero normal attacks in the first part (not recovering in the second part is never optimal, as shown in Lemma 4.1), i.e., $\mathcal{E}^{\mathrm{D}}_{2l-1} = \emptyset, \mathcal{E}^{\mathrm{A}}_{2l-1} \neq \emptyset$. Under this setting, we observe that the worst scenario is that eventually agents will be grouped in different states, with agents in the same group having zero state difference. If the defender recovers in the first part, then z_k obtained may become lower, and agents in the same group eventually have zero state difference as well (this includes the case where there is only one group consisting of all agents).

In this case, if agents are grouped, then the defender does not get any incentives by recovering edges attacked normally, i.e., $\mathcal{E}^{\mathrm{A}}_k$, inside the group. Specifically, there exist games with index $\bar{l}_i$, where

$$z_{2\bar{l}_i}(\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i} \neq \emptyset) = z_{2\bar{l}_i}(\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i} = \emptyset) = z_{2\bar{l}_i-1}(\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i-1} = \emptyset) \tag{4.19}$$

is satisfied given the optimal edges $\mathcal{E}^{\mathrm{A}*}_{2\bar{l}_i}$. Therefore, the defender's decision whether to recover or not only depends on the cluster distribution function $c(\mathcal{G}^{\mathrm{D}}_{2\bar{l}_i})$.

We then show that in this case the defender chooses to recover in the first part, i.e., $(2\bar{l}_i - 1)$th interval, if possible. Without recovery in the $(2\bar{l}_i - 1)$th interval, from (6.24) we can see that the value of both z_k and $c(\cdot)$ associated with the $(2\bar{l}_i - 1)$th interval becomes worse for the defender, since without recovery there will be more clusters and the state difference does not decrease faster. Hence, in the $(2\bar{l}_i - 1)$th game with the same attack strategy, we have

$$U^{\mathrm{D}}_1(\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i-1} = \emptyset) < U^{\mathrm{D}}_1(\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i-1} \neq \emptyset), \tag{4.20}$$

with U^{D}_1 being part of U^{D} associated with the $(2l-1)$th interval.

If the defender does not recover in the first part, then for the same $\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i}$, the duration interval $\delta^{\mathrm{D}}_{2\bar{l}_i}$ becomes longer, which may increase the defender's utility U^{D}_2. However, as mentioned above, with the unchanged z_k as in (4.19), the defender's optimal strategy is decided by $c(\mathcal{G}^{\mathrm{D}}_k)$.

Since it is assumed that the attacker always attacks fewer edges in the first part compared to the second part, as a result, if $\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i-1} \neq 0$, then from (6.24) we have

$$\begin{aligned}&(c(\mathcal{G}^{\mathrm{D}}_{2\bar{l}_i-1}) - c(\mathcal{G}^{\mathrm{A}}_{2\bar{l}_i-1}))\delta^{\mathrm{D}}_{2\bar{l}_i-1} + (c(\mathcal{G}^{\mathrm{D}}_{2\bar{l}_i}) - c(\mathcal{G}^{\mathrm{A}}_{2\bar{l}_i}))\delta^{\mathrm{D}}_{2\bar{l}_i} \\ &\geq (c(\mathcal{G}^{\mathrm{D}}_{2\bar{l}_i}(\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i-1} = \emptyset)) - c(\mathcal{G}^{\mathrm{A}}_{2\bar{l}_i}(\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i} = \emptyset)))\delta^{\mathrm{D}}_{2\bar{l}_i},\end{aligned} \tag{4.21}$$

with the left-hand side of the inequality associated with $(\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i-1} \neq \emptyset)$, and the right-hand

side associated with ($\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i-1} = \emptyset$). The inequalities (4.19)–(4.21) then imply that in any ($\bar{l}_i$)th game, $U^{\mathrm{D}}(\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i-1} = \emptyset) < U^{\mathrm{D}}(\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i-1} \neq \emptyset)$ is satisfied. In other words, there are always games in which the defender recovers nonzero edges in the $(2\bar{l}_i - 1)$th interval whenever possible, i.e., $\mathcal{E}^{\mathrm{A}}_{2\bar{l}_i-1} \neq \emptyset$.

Since it is always possible for the attacker to attack such that the defender gains no utility by recovering edges connecting agents with the same state, this optimal strategy for the defender is the same for the next games with indices $\bar{l}_{i+1}$, $\bar{l}_{i+2}$, and so on.

4.7.3 Proof of Proposition 4.3

We will prove the proposition by contrapositive; especially, we will prove that consensus always happens if $\bar{m}^{\mathrm{A}} < h\lambda$, which is equivalent to the statement in the proposition above.

We first notice that $\bar{m}^{\mathrm{A}} < h\lambda$ implies that for each positive integer l, the attacker can attack at most $\lambda - 1$ number of edges with strong jamming signals in the $(2l-1)$th interval. This indicates that if $\bar{m}^{A} < h\lambda$, then strong attacks by themselves cannot make the graph disconnected.

By Lemma 3.2 above, we show that there exist a sequence $\bar{l}$ of positive integers, for which the defender recovers nonzero normally attacked edges in the $(2\bar{l}_i - 1)$th interval, i.e., $\mathcal{E}^{\mathrm{D}}_{2\bar{l}_i-1} \neq \emptyset$ are optimal given that $\mathcal{E}^{\mathrm{A}}_{2\bar{l}_i-1} \neq \emptyset$.

From the definitions in (5.3) and (6.24), we can see that the defender obtains a higher utility if the agents are closer, which means that given a nonzero number of edges to recover (in the $(2\bar{l}_i - 1)$th interval described above), the defender recovers the edges connecting farther agents. This implies that when recovering, the defender always chooses the further disconnected agents, and since by communicating with the consensus protocol as in (3.37) the agents' states are getting closer, the defender will choose different edges to recover if the states of agents connected by recovered edges $\mathcal{E}^{\mathrm{D}}_k$ becoming close enough. Consequently, if $\bar{m}^{A} < h\lambda$, then there exists $j \in \mathbb{N}$ where the union of graphs, i.e., the graph having the union of the edges of each graph, $(\mathcal{V}, \bigcup((\mathcal{E} \setminus (\overline{\mathcal{E}}^{\mathrm{A}} \cup \mathcal{E}^{\mathrm{A}}_k)) \cup \mathcal{E}^{\mathrm{D}}_k))$ over $[\underline{t}_{2\bar{l}_i}, \underline{t}_{2\bar{l}_{i+j}})$ becomes a connected graph. These intervals $[\underline{t}_{2\bar{l}_i}, \underline{t}_{2\bar{l}_{i+j}})$ occur infinitely many times, and since the length is lower bounded by δ^{A}_k, the total time when the graph is connected becomes infinite in length.

It is shown in [3] that with consensus protocol as in (3.37), the agents achieve consensus in the time-varying graph as long as the union of the graphs over bounded time intervals is a connected graph. In the context of our problem setting, this implies that

consensus is achieved if $(\mathcal{V}, \bigcup((\mathcal{E}\setminus(\overline{\mathcal{E}}^{\mathrm{A}}\cup\mathcal{E}_k^{\mathrm{A}}))\cup\mathcal{E}_k^{\mathrm{D}}))$ is connected over $[\underline{t}_{2\bar{l}_i}, \underline{t}_{2\bar{l}_{i+j}})$, implying that if $\bar{m}^{\mathrm{A}} < h\lambda$ then consensus is achieved. This completes the proof.

Chapter 5

Consensus and Clustering with Repeated Games under Rolling Horizon Approach

5.1 Introduction

Rolling/receding horizon control has been used to handle systems with uncertainties. It is also studied in the context of networked control [75, 76], where there may be additional uncertainties related to communications among agents in the networks. Rolling horizon approaches are also discussed in noncooperative security game settings in [77, 78], where horizon lengths affect the resilience of the system. Rolling horizon approaches have also been used to handle the constraints in the system, e.g., in an agent with obstacle avoidance constraints [79, 80].

In this chapter, we consider a security problem in a two-player game setting between an attacker, who is motivated to disrupt the communication among agents by attacking communication links, and a defender, who attempts to recover some of the attacked links. The game in this chapter is played repeatedly over discrete time in the context of multiagent consensus. Here we consider a more dynamic rolling horizon approach, where players may change their strategies (that have been determined beforehand) at several points in time, in order to adapt to the changing condition of the systems.

In the face of the malicious adversaries, agents with consensus protocols may not be able to converge; instead, they are divided into clusters, i.e., groups of agents with the same states for agents in the same cluster. Cluster forming in multiagent systems has

been studied in, e.g., [71–73], where the relations among certain agents may be hostile. In this chapter, we approach clustering from a different viewpoint based on a game-theoretic formulation. Specifically, the players of the game consider network effect/network externality [81] to form clusters among agents. Their utilities are determined by how the network is disconnected into groups of agents as well as how the players' actions affect the states of the agents at each time.

Receding horizon with agents clustering have been studied in [82], whereas receding horizon in Level-k games is studied in [83].

Moreover, in comparison to [61], our contribution is threefold: (i) We introduce more options for the attacker's jamming signal strengths; (ii) the game consists of multiple attack-recovery actions, resulting in more complicated strategies; and (iii) we consider a rolling horizon approach for the players so that their strategies may be modified as they obtain new knowledge of the status of the system.

More specifically, it is now possible for the attacker to disable links with stronger intensity of attack signals so that the defender is unable to recover those links; this feature is motivated by [32, 84]. On the other hand, we consider games consisting of multiple parts, where the players need to consider their future utilities and energy constraints when deciding their strategies at any point in time. The players recalculate and may override their strategies as time goes on, according to the rolling horizon approach.

This chapter is organized as follows. We explain the attack-recovery sequence, utility function structure, and game structure with rolling horizon in Section 5.2, 5.3, and 5.4, respectively. The analysis of the agent consensus and clustering at infinite time is written in Section 5.5 and 5.6, respectively. In Section 5.7, we examine the euilibrium of the game in a single discrete-time step. Finally, we provide several numerical examples in Section 5.8 and conclude the chapter in Section 5.9. The problem formulation The content in this chapter can be found in the conference proceedings [O3,C5] as well as in the manuscript submitted to a journal publication [O4].

5.2 Attack/recovery characterization for multiagent systems

We consider a multiagent system of n agents communicating to each other in discrete time in the face of jamming attacks. The agents are aiming to converge to a consensus state by interacting with each other over the communication network. The network topology for the normal operation is given by an undirected and connected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. The edge connectivity [5] of the connected graph $\mathcal{G}$ is denoted by λ.

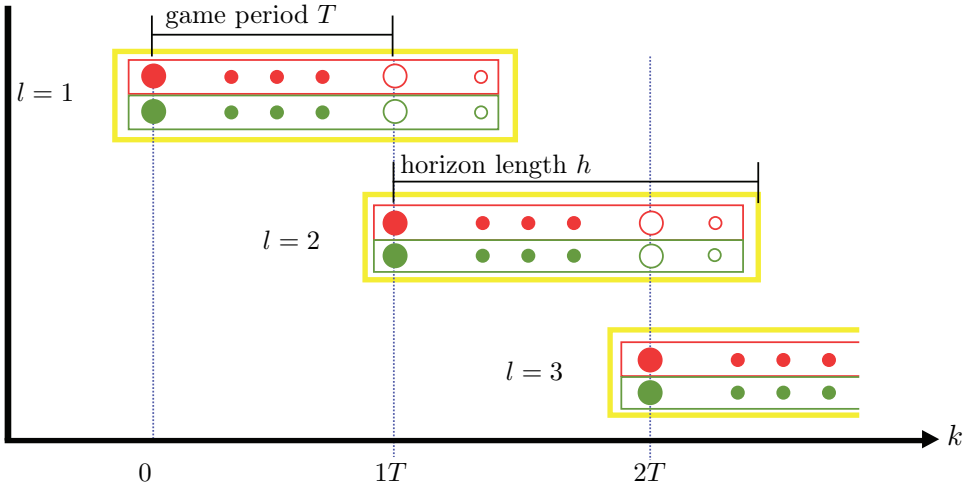


Figure 5.1 Illustration of the games played over discrete time k with rolling horizon approaches by the players.

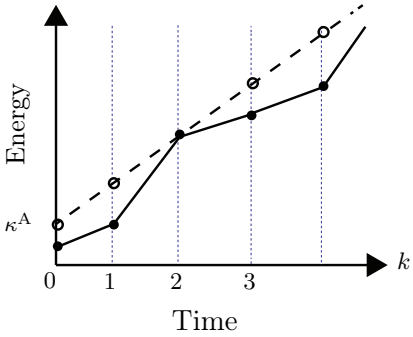


Figure 5.2 Energy constraint of the attacker considered in the formulation. The dashed line represents the total supplied energy to spend. The filled circles representing the actual energy consumed by the player should be below the dashed line.

Each agent i has the scalar state $x_i[k]$ following the discrete-time update rule at time $k \in \mathbb{N}_0$ given by

$$x_i[k+1] = x_i[k] + u_i[k], \quad x[0] = x_0, \tag{2.3}$$

$$u_i[k] = \sum_{j \in \mathcal{N}_i[k]} a_{ij}(x_j[k] - x_i[k]),, \tag{2.4}$$

as specified in Chapter 2.

From this sequence of attacks and recoveries, we characterize the attack-recovery process as a two-player game between the *attacker* and the *defender* in terms of the communication links in the network. As discussed in previous chapters, the graph characterizing the networked system is *resilient* if the group of agents is able to recover from the damages caused by the attacker. However, there may be cases where the resiliency level of the graph is reduced if the jamming signals are sufficiently strong such that the defender cannot recover. Note that to achieve consensus, the agents need *not* be connected for *all* time.

In this chapter, we consider the case where the attacker has two types of jamming signals in terms of their strength, *strong* and *normal*. The defender is able to recover only the edges that are attacked with normal strength. In the following subsections, we first describe the sequence of attacks and recoveries and characterize some constraints on the players' energy and computational ability that we need to impose as well as how the objective of the problem is formulated.

5.2.1 Attack-recovery sequence

In our setting, at each discrete time k the attacker attacks $\mathcal{G}$ by deleting the edges $\mathcal{E}_k^{\mathrm{A}} \subseteq \mathcal{E}$ with normal jamming signals and $\overline{\mathcal{E}}_k^{\mathrm{A}} \subseteq \mathcal{E}$ with strong jamming signals with $\mathcal{E}_k^{\mathrm{A}} \cap \overline{\mathcal{E}}_k^{\mathrm{A}} = \emptyset$, whereas the defender recovers $\mathcal{E}_k^{\mathrm{D}} \subseteq \mathcal{E}_k^{\mathrm{A}}$. As mentioned earlier, the defender is not able to recover the edges attacked with strong jamming signals, i.e., $\mathcal{E}_k^{\mathrm{D}} \cap \overline{\mathcal{E}}_k^{\mathrm{A}} = \emptyset$. Due to the attacks and then the recoveries, the network changes from $\mathcal{G}$ to $\mathcal{G}_k^{\mathrm{A}} := (\mathcal{V}, \mathcal{E} \setminus (\mathcal{E}_k^{\mathrm{A}} \cup \overline{\mathcal{E}}_k^{\mathrm{A}}))$ and further to $\mathcal{G}_k^{\mathrm{D}} := (\mathcal{V}, (\mathcal{E} \setminus (\mathcal{E}_k^{\mathrm{A}} \cup \overline{\mathcal{E}}_k^{\mathrm{A}})) \cup \mathcal{E}_k^{\mathrm{D}})$ at time k. The agents then communicate to their neighbors $\mathcal{N}_i[k]$ based on this resulting graph $\mathcal{G}_k^{\mathrm{D}}$.

In this game, the players attempt to choose the best strategies in terms of edges attacked/recovered $(\overline{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{A}})$ and $\mathcal{E}_k^{\mathrm{D}}$ to maximize their own utility functions. Here, the games are played every T time steps and the lth game is defined over the horizon of h steps from time $(l-1)T$ to $(l-1)T+h-1$, with $l \in \mathbb{N}$ and $1 \leq T \leq h$. The players make decisions in a *rolling horizon* fashion; the optimal strategies obtained at $(l-1)T$ for the future time may be overridden when the players recalculate their strategies at time lT when the next game starts. Fig. 5.1 illustrates the discussed sequence over time with $h = 8$ and $T = 4$, where the filled circles indicate the implemented strategies and the empty circles indicate the strategies of the game that are discarded. The rolling horizon game structure will be discussed in Section 5.4 in more detail.

5.2.2 Energy constraints

The actions of the attacker and the defender are affected by the constraints on their energy resources, as explained in Chapter 2. Here we suppose that the players initially possess certain amount of energy κ^{A} and κ^{D} for the attacker and the defender, respectively.

For the attacker, the strong attacks on $\overline{\mathcal{E}}_k^{\mathrm{A}}$ take $\overline{\beta}^{\mathrm{A}} > 0$ energy per edge per unit time whereas the normal attacks on $\mathcal{E}_k^{\mathrm{A}}$ take $\beta^{\mathrm{A}} > 0$ cost per edge, with $\overline{\beta}^{\mathrm{A}} > \beta^{\mathrm{A}}$. The total

energy used by the attacker is constrained as

$$\sum_{m=0}^{k} (\overline{\beta}^{\mathrm{A}} |\overline{\mathcal{E}}_m^{\mathrm{A}}| + \beta^{\mathrm{A}} |\mathcal{E}_m^{\mathrm{A}}|) \leq \kappa^{\mathrm{A}} + \rho^{\mathrm{A}} k \tag{5.1}$$

for any time k, where $\kappa^{\mathrm{A}} \geq \rho^{\mathrm{A}} > 0$. This implies that the total energy spent by the attacker cannot exceed the available energy characterized as the sum of the initial energy κ^{A} and the supplied energy $\rho^{\mathrm{A}} k$ by time k. This energy constraint restricts the number of edges that the attacker can attack. The condition $\kappa^{\mathrm{A}} \geq \rho^{\mathrm{A}}$ allows the attacker to have at least the same attack ability at time $k = 0$.

Fig. 5.2 illustrates the energy constraint of the attacker, where the dashed line with slope ρ^{A} represents the total supplied energy and the filled circles indicate the total energy spent. A critical case is when $\beta^{\mathrm{A}} < \rho^{\mathrm{A}}$, since it is possible for the attacker to attack at least one edge for all times. This will have implications on the consensus and cluster forming of the agents, as we will discuss later.

The energy constraint for the defender is similar to (5.1):

$$\sum_{m=0}^{k} \beta^{\mathrm{D}} |\mathcal{E}_m^{\mathrm{D}}| \leq \kappa^{\mathrm{D}} + \rho^{\mathrm{D}} k, \tag{5.2}$$

with $\kappa^{\mathrm{D}} \geq \rho^{\mathrm{D}} > 0$ and $\beta^{\mathrm{D}} > 0$. Note that there is a single term on the left-hand side because there is only one type of recovery signals for the agents.

5.3 Utility functions with cluster forming and agent-group index

In our game setting, the attacker tries to make the graph disconnected to separate the agents into clusters. Here, we introduce a few notions related to grouping/clustering of agents. In a given subgraph $\mathcal{G}' = (\mathcal{V}, \mathcal{E}')$ of $\mathcal{G}$, the agents may be divided into $\overline{n}(\mathcal{G}')$ number of *groups*, with the groups $\mathcal{V}'_1, \mathcal{V}'_2, \ldots, \mathcal{V}'_{\overline{n}(\mathcal{G}')}$ being a partition of $\mathcal{V}$ with $\cup_{p=1}^{\overline{n}(\mathcal{G}')} \mathcal{V}'_p = \mathcal{V}$ and $\mathcal{V}'_p \cap \mathcal{V}'_q = \emptyset$, if $p \neq q$. There is no edge connecting different groups, i.e., $e_{i',j'} \notin \mathcal{E}', \forall i' \in \mathcal{V}'_p, j' \in \mathcal{V}'_q$. We also call each subset of agents taking the same state at infinite time as a *cluster*, i.e., $\lim_{k\to\infty}(x_i[k] - x_j[k]) = 0$ implies that agents i and j belong to the same cluster.

In the considered game, we follow the notion of network effect/network externality, where the utility of an agent in a certain group depends on how many other agents belong to that particular group. As specified in Chapter 4, we consider a measure called

agent-group index, given by

$$c(\mathcal{G}') := \sum_{p=1}^{\overline{n}(\mathcal{G}')} |\mathcal{V}'_p|^2 - |\mathcal{V}|^2 \quad (\leq 0). \tag{4.7}$$

The value of $c(\mathcal{G}')$ is 0 if $\mathcal{G}'$ is connected, since there is only one group (i.e., $\overline{n}(\mathcal{G}') = 1$). A larger value (closer to 0) of $c(\mathcal{G}')$ implies that there are fewer groups in graph $\mathcal{G}'$, and/or each group has more agents.

In our problem setting, the players also consider the effects of their actions on the agent states when attacking/recovering, similar to the formulation in Chapter 4. For example, the attacker may want to separate agents having state values with more differences in different groups. We specify the agents' state difference z_k as

$$z_k(\overline{\mathcal{E}}^{\mathrm{A}}_k, \mathcal{E}^{\mathrm{A}}_k, \mathcal{E}^{\mathrm{D}}_k) := x^{\mathrm{T}}[k+1] L_{\mathrm{c}} x[k+1], \tag{5.3}$$

with L_{c}, for simplicity, being the Laplacian matrix of the complete graph with n agents. That is, (5.3) represents the sum of squares of the state differences of all the agent pairs. The attacked and recovered edges $(\overline{\mathcal{E}}^{\mathrm{A}}_k, \mathcal{E}^{\mathrm{A}}_k, \mathcal{E}^{\mathrm{D}}_k)$ will affect $x[k+1]$ in accordance with (2.3) and (2.4), and in turn the value of z_k. Note that the value of z_k is nonincreasing over time [5] even if some agents are left disconnected from other agents under attacks because of the protocol given in (2.3) and (2.4).

Now, we combine the two measures in (4.7) and (5.3) to construct the utility functions for the game in a zero-sum manner. Specifically, for the lth game starting at time $k = (l-1)T$, the attacker and the defender's utility functions take account of the agent-group index $c(\cdot)$ and the difference z_k of agents' states over h horizon length from time $(l-1)T$ to $(l-1)T + h - 1$. With weights $a, b \geq 0$, the utilities for the lth game U^{A}_k for the attacker and U^{D}_k for the defender are, respectively, defined by

$$U^{\mathrm{A}}_k := \sum_{k=(l-1)T}^{(l-1)T+h-1} (a z_k - b c(\mathcal{G}^{\mathrm{D}}_k)), \tag{5.4}$$

$$U^{\mathrm{D}}_k := -U^{\mathrm{A}}_k. \tag{5.5}$$

In our setting both players attempt to maximize their utilities at the start of each game l.

5.4 Rolling horizon game structure

We are interested in finding the subgame perfect equilibrium [33] of this game outlined in Section 5.3. To this end, the game is divided into some subgames/decision-making points. The subgame perfect equilibrium must be an equilibrium in every subgame. The optimal strategy of each player is obtained by using a backward induction approach, i.e., by finding the equilibrium from the smallest subgames. The tie-break condition happens when the players' strategies result in the same utility. In this case, we suppose that the players choose to save their energy by attacking/recovering less edges unless they have enough energy to attack/recover all edges in every subsequent steps, in which case they attack/recover more edges.

Due to the nature of the rolling horizon approach, the strategies obtained from the lth game, i.e., attacked and recovered edges, are applied only from time $(l-1)T$ to $lT-1$. Specifically, in the lth game for time $(l-1)T$ to $(l-1)T+h-1$, the strategies of both players are denoted by $((\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{D}}_{l,1}), \ldots, (\overline{\mathcal{E}}^{\mathrm{A}}_{l,h}, \mathcal{E}^{\mathrm{A}}_{l,h}, \mathcal{E}^{\mathrm{D}}_{l,h}))$, with $(\overline{\mathcal{E}}^{\mathrm{A}}_{l,\bar{l}}, \mathcal{E}^{\mathrm{A}}_{l,\bar{l}}, \mathcal{E}^{\mathrm{D}}_{l,\bar{l}})$ indicating the strategies at the $\bar{l}$th step of the lth game with $\bar{l} \in \{1, \ldots, h\}$. Note that here we show the strategies with two subscripts representing the game and the step indices along the time axis. From the above set of strategies, only $((\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{D}}_{l,1}), \ldots, (\overline{\mathcal{E}}^{\mathrm{A}}_{l,T}, \mathcal{E}^{\mathrm{A}}_{l,T}, \mathcal{E}^{\mathrm{D}}_{l,T}))$ is applied. Recall that h is taken to be greater than or equal to T. Therefore, for the lth game from time $(l-1)T$ to $lT-1$, the strategy applied will be written as $((\overline{\mathcal{E}}^{\mathrm{A}}_{(l-1)T}, \mathcal{E}^{\mathrm{A}}_{(l-1)T}, \mathcal{E}^{\mathrm{D}}_{(l-1)T}), \ldots, (\overline{\mathcal{E}}^{\mathrm{A}}_{lT-1}, \mathcal{E}^{\mathrm{A}}_{lT-1}, \mathcal{E}^{\mathrm{D}}_{lT-1})) := ((\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{D}}_{l,1}), \ldots, (\overline{\mathcal{E}}^{\mathrm{A}}_{l,T}, \mathcal{E}^{\mathrm{A}}_{l,T}, \mathcal{E}^{\mathrm{D}}_{l,T}))$.

We look at how the optimal edges can be found by an example with $h = 2$ and $T = 1$ or 2. In this case, for the lth game over time $(l-1)T$ and $(l-1)T+1$, the optimal strategies of the players are given by

$$\mathcal{E}^{\mathrm{D}*}_{l,2}(\overline{\mathcal{E}}^{\mathrm{A}}_{l,2}, \mathcal{E}^{\mathrm{A}}_{l,2}) \in \underset{\mathcal{E}^{\mathrm{D}}_{l,2}}{\arg\max}\, U^{\mathrm{D}}_{l,2}, \tag{5.6}$$

$$(\overline{\mathcal{E}}^{\mathrm{A}*}_{l,2}(\mathcal{E}^{\mathrm{D}}_{l,1}), \mathcal{E}^{\mathrm{A}*}_{l,2}(\mathcal{E}^{\mathrm{D}}_{l,1})) \in \underset{(\overline{\mathcal{E}}^{\mathrm{A}}_{l,2}, \mathcal{E}^{\mathrm{A}}_{l,2})}{\arg\max}\, U^{\mathrm{A}}_{l,2}, \tag{5.7}$$

$$\mathcal{E}^{\mathrm{D}*}_{l,1}(\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1}) \in \underset{\mathcal{E}^{\mathrm{D}}_{l,1}}{\arg\max}\, U^{\mathrm{D}}_{l}, \tag{5.8}$$

$$(\overline{\mathcal{E}}^{\mathrm{A}*}_{l,1}, \mathcal{E}^{\mathrm{A}*}_{l,1}) \in \underset{(\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1})}{\arg\max}\, U^{\mathrm{A}}_{l}, \tag{5.9}$$

where $U^{\mathrm{A}}_{l,\bar{l}}$ and $U^{\mathrm{D}}_{l,\bar{l}}$ are defined as parts of U^{A}_{k} and U^{D}_{k}, respectively, calculated from the $\bar{l}$th step to the last (hth) step of the lth game, i.e., $U^{\mathrm{A}}_{l,\bar{l}} = -U^{\mathrm{D}}_{l,\bar{l}} := \sum_{(l-1)T+\alpha-1}^{(l-1)T+h-1}(az_k - bc(\mathcal{G}^{\mathrm{D}}_k))$. In this case with $h = 2$, the functions $U^{\mathrm{A}}_{l,2}$ and $U^{\mathrm{D}}_{l,2}$ are based on the values of az_k and $b\mathcal{G}^{\mathrm{D}}_k$ at $k = (l-1)T+1$ only. Note that to find $(\overline{\mathcal{E}}^{\mathrm{A}*}_{l,1}, \mathcal{E}^{\mathrm{A}*}_{l,1})$, one needs to obtain $\mathcal{E}^{\mathrm{D}*}_{l,1}(\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1})$

beforehand. Likewise, to find $\mathcal{E}^{\mathrm{D}*}_{l,1}$, one needs to obtain $(\overline{\mathcal{E}}^{\mathrm{A}*}_{l,2}(\mathcal{E}^{\mathrm{D}}_{l,1}), \mathcal{E}^{\mathrm{A}*}_{l,2}(\mathcal{E}^{\mathrm{D}}_{l,1}))$. Similarly, to find $(\overline{\mathcal{E}}^{\mathrm{A}*}_{l,2}, \mathcal{E}^{\mathrm{A}*}_{l,2})$, the edges $\mathcal{E}^{\mathrm{D}*}_{l,2}(\overline{\mathcal{E}}^{\mathrm{A}}_{l,2}, \mathcal{E}^{\mathrm{A}}_{l,2})$ must be obtained beforehand.

For $h > 2$, the players' optimal strategies consist of $2h$ parts similar to those in (5.6)–(5.9), with one time step consisting of two parts of strategies corresponding to the number of players. They are solved by the players at every time $k = (l-1)T$ of the lth game, $l \in \mathbb{N}$. With $T = h$, the players do not have chance to override their strategies, which removes the rolling horizon aspect of the game.

We will find the optimal strategies of the players by computing all possible combinations, since the choices of edges are finite. To address scalability issues, we may find edges that are easier to attack first, i.e., edges that result in the formation of new groups if attacked, and limit the strategy choices over those edges only.

In the previous chapters we consider related games in continuous time, where the timings for launching attack/defense actions are also part of the decision variables. This aspect complicated the formulation, making it difficult to study games over a time horizon. In this chapter, we simplify the timing issue and instead introduce the rolling horizon feature. This enables the players to consider the cluster forming in a longer time range, which is especially important when consensus among agents is obstructed by adversaries.

5.5 Consensus analysis

In this section, we examine the effect of the game structure and players' energy constraints on consensus.

We will begin the analysis by looking at the case of certain energy conditions of the players. Specifically, if a player has enough energy to attack/recover all edges from a certain step of the game, then it will use all of their energy to attack/recover as many edges as they can in the subsequent steps. We will confirm this point formally in the following. For simplicity, we denote the total energy that the defender consumed before the lth game as $\tilde{\beta}^{\mathrm{D}}_l := \sum_{k=0}^{(l-1)T-1} \beta^{\mathrm{D}} |\mathcal{E}^{\mathrm{D}}_k|$ and the total energy that the defender may consume from the 1st to the $\bar{l}$th step of the lth game as $\hat{\beta}^{\mathrm{D}}_{\bar{l}} := \sum_{m=1}^{\bar{l}} \beta^{\mathrm{D}} |\mathcal{E}^{\mathrm{D}}_{l,m}|$, where we omit the index l from the left-hand side, with a slight abuse of notation. Similarly, for the attacker we denote $\tilde{\beta}^{\mathrm{A}}_l := \sum_{m=0}^{(l-1)T-1} (\beta^{\mathrm{A}} |\mathcal{E}^{\mathrm{A}}_m| + \overline{\beta}^{\mathrm{A}} |\overline{\mathcal{E}}^{\mathrm{A}}_k m|)$ and $\hat{\beta}^{\mathrm{A}}_{\bar{l}} := \sum_{m=1}^{\bar{l}} (\beta^{\mathrm{A}} |\mathcal{E}^{\mathrm{A}}_{l,m}| + \overline{\beta}^{\mathrm{A}} |\overline{\mathcal{E}}^{\mathrm{A}}_{l,m}|)$.

We discuss in Lemma 5.1 (resp., Lemma 5.2) the optimal strategy of the defender (resp., attacker) at the αth step of the game given certain energy conditions mentioned

in Section 5.2. This characterization of optimal strategy of the defender (resp., attacker) will be useful to obtain the necessary (resp., sufficient) conditions for consensus not to happen.

5.5.1 Necessary conditions for not reaching Consensus

This subsection discusses necessary conditions for the agents to be separated into different clusters for infinitely long duration without achieving overall consensus. We first discuss the defender's optimal strategy on some games with specific conditions in Lemmas 5.1 and 5.2. In Lemma 5.1, we state the defender's optimal strategy at any step of the lth game given a certain energy condition.

Lemma 5.1. If the defender's total energy $\tilde{\beta}_l^{\mathrm{D}} + \hat{\beta}_{\hat{\bar{l}}-1}^{\mathrm{D}}$ consumed before the $\hat{\bar{l}}$th step of the lth game satisfies

$$\tilde{\beta}_l^{\mathrm{D}} + \hat{\beta}_{\hat{\bar{l}}-1}^{\mathrm{D}} \leq \kappa^{\mathrm{D}} + \rho^{\mathrm{D}}((l-1)T + \hat{\bar{l}} - 1) - (h - \hat{\bar{l}} + 1)|\mathcal{E}|\beta^{\mathrm{D}}, \tag{5.10}$$

then $\mathcal{E}_{l,\bar{l}}^{\mathrm{D}*} = \mathcal{E}_{l,\bar{l}}^{\mathrm{A}*}$ for all $\bar{l} \geq \hat{\bar{l}}$, i.e., the defender will recover all normally attacked edges from the $\hat{\bar{l}}$th step.

Note that if the defender's strategy is *not* to recover all normally attacked edges given even if (5.10) is satisfied, i.e., $\mathcal{E}_{l,\alpha}^{\mathrm{A}} = \hat{\mathcal{E}}^{\mathrm{A}} \neq \mathcal{E}_{l,\alpha}^{\mathrm{D}}$, then the attacker will not attack $\hat{\mathcal{E}}^{\mathrm{A}}$ set of edges in the first place. This is because by attacking $\hat{\mathcal{E}}^{\mathrm{A}}$ (and considering $\mathcal{E}_{l,\alpha}^{\mathrm{D}} \neq \hat{\mathcal{E}}^{\mathrm{A}}$) the attacker's utility for step $\bar{l} \geq \hat{\bar{l}}$ becomes $U_{l,\alpha}^{\mathrm{A}}(\cdot, \hat{\mathcal{E}}^{\mathrm{A}}, \mathcal{E}_{l,\alpha}^{\mathrm{D}} \neq \hat{\mathcal{E}}^{\mathrm{A}}) < U_{l,\alpha}^{\mathrm{A}}(\cdot, \emptyset, \emptyset)$, since $U_{l,\alpha}^{\mathrm{D}}(\cdot, \hat{\mathcal{E}}^{\mathrm{A}}, \mathcal{E}_{l,\alpha}^{\mathrm{D}} \neq \hat{\mathcal{E}}^{\mathrm{A}}) > U_{l,\alpha}^{\mathrm{D}}(\cdot, \emptyset, \emptyset) = U_{l,\alpha}^{\mathrm{D}}(\cdot, \hat{\mathcal{E}}^{\mathrm{A}}, \hat{\mathcal{E}}^{\mathrm{A}})$ and $U_k^{\mathrm{D}} = -U_k^{\mathrm{A}}$.

We also remark that in order to derive the same optimal strategy for the defender the quantity $(h - \bar{l} + 1)|\mathcal{E}|$ in the right-hand side of inequality (5.10) can be relaxed to the maximum number of edges that the attacker can attack from step $\hat{\bar{l}}$ to step h given its energy condition. However, this number of edges may change every game, making the inequality complicated to express.

Lemma 5.2 gives an interval over which, at least once, either not attacking with normal signals or recovering nonzero edges is optimal.

Lemma 5.2. There is at least one occurrence of either $\mathcal{E}_k^{\mathrm{D}} \neq \emptyset$ or $\mathcal{E}_k^{\mathrm{A}} = \emptyset$ every $\lceil \frac{h|\mathcal{E}|\beta^{\mathrm{D}} - \rho^{\mathrm{D}}}{\rho^{\mathrm{D}} T} + 1 \rceil$ time steps.

Lemmas 5.1 and 5.2 above imply that the defender is guaranteed to make recoveries from normal attacks every certain interval. Hence, the attacker needs to attack some

edges strongly to prevent the recovery in order to separate agents into different clusters, as we discuss next.

The following two results provide necessary conditions for consensus not to take place. We consider a more general condition in Proposition 5.3, whereas in Theorem 5.4 we consider a more specific situation for the utility functions that leads to a tighter condition. Recall that λ represents the connectivity of $\mathcal{G}$.

Proposition 5.3. A necessary condition for consensus not to happen is $\rho^{\mathrm{A}}/\beta^{\mathrm{A}} \geq \lambda$.

We now limit the class of utility functions in (5.4), (5.5) to the case of $b = 0$ in the weights. This means that the players do not take account of the agent-group index in the graph, but only the states in consensus. In this case, the attacker may need more energy to prevent consensus as shown in the next theorem.

Theorem 5.4. Suppose that $b = 0$. A necessary condition for consensus not to happen is $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq \lambda$.

The result in Theorem 5.4 only holds for $b = 0$, since with $b > 0$ the defender may choose to recover the edges connecting agents that already have similar states to maximize $c(\mathcal{G}_k^{\mathrm{D}})$ (instead of those connecting further agents). In such a case, the network may remain disconnected and thus the agents may converge to different states. As we see from these results, the weight values affect the necessary conditions to prevent consensus, whereas the effect of the weights on the sufficient condition (discussed later) is less straightforward. The effect of the values of a and b on consensus is illustrated in Section 5.8.

5.5.2 Sufficient condition to prevent consensus

The next result provides a sufficient condition for preventing consensus. It shows that the attacker can prevent consensus if it has sufficiently large recharge rate ρ^{A} given the network topology $\mathcal{G}$. We first state Lemma 5.5 about the attacker's optimal strategy under some energy conditions, similar to the discussion on the defender's case above.

Lemma 5.5. The attacker's optimal strategy is $\overline{\mathcal{E}}_{l,\alpha}^{\mathrm{A}*} = \mathcal{E}$ if

- the attacker's recharge rate satisfies $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq |\mathcal{E}|$, or
- the attacker's total energy $\tilde{\beta}_l^{\mathrm{A}} + \hat{\beta}_{\bar{l}-1}^{\mathrm{A}}$ that it consumes before $\bar{l}$th step of the lth game satisfies

$$\tilde{\beta}_l^{\mathrm{A}} + \hat{\beta}_{\bar{l}-1}^{\mathrm{A}} \leq \kappa^{\mathrm{A}} + \rho^{\mathrm{A}}((l-1)T + \bar{l} - 1) - (h - \bar{l} + 1)\overline{\beta}^{\mathrm{A}}|\mathcal{E}|. \tag{5.11}$$

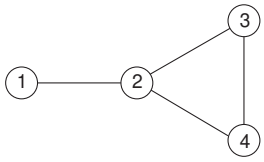


Figure 5.3 Graph $\mathcal{G}$ used in the case study.

Proposition 5.6. A sufficient condition for all agents not to achieve consensus at infinite time is that the attacker's parameters satisfy $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq |\mathcal{E}|$.

5.5.3 Effect of graph structure on a sufficient condition for preventing consensus

Theorem 5.4 considered the case where $b = 0$, i.e., players take account of only the states when attacking/recovering and not the agent-group index. In this subsection we first provide an example that shows that the necessary condition in Theorem 5.4 is not sufficient for preventing consensus.

Here we suppose that the defender is very strong (i.e., ρ^{D} is much larger than β^{D}) such that it can recover any normally-attacked edges at any k (note that the condition in Theorem 5.4 only consists of the attacker's parameters). This will force the attacker to attack with strong jamming signals to disconnect any agent.

We consider a graph $\mathcal{G}$ as in Fig. 5.3, with $x[0] = [1, 0, -20, 1]$, $h = 2$, and $\kappa^{\mathrm{A}} = \rho^{\mathrm{A}}$. We set that $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} = 1$, which satisfies the condition in Theorem 5.4. To prevent consensus, the attacker needs to attack e_{12} (min-cut edge of $\mathcal{G}$) at all times, since it is the only edge which, if attacked, will make the graph disconnected.

We then compare two cases:

a) the attacker attacks e_{12} for both steps $\bar{l} = 1, 2$, and

b) the attacker does not attack at $\bar{l} = 1$ and attacks two edges at $\bar{l} = 2$.

Suppose that the attacker attacks e_{23} and e_{34} in Case b) at $\bar{l} = 2$, since agent 3 has the furthest state from other agents at the initial time.

Now, in Case a): $U_k^{\mathrm{A}} = z_{1,1} + z_{1,2} = 231.5 + 165.72 = 397.22$, whereas in Case b): $U_k^{\mathrm{A}} = z_{1,1} + z_{1,2} = 220.5 + 179.16 = 399.66$. Note that Case b) is better in this example, implying that even with $b = 0$ the attacker may not attack the same edges at all times. From this example, we see how the graph structure affects the consensus by affecting the strategy of one game.

As the last result of the section, we state that for a special case with the complete graph under $b = 0$ and $h = 1$, i.e., a single-step game without rolling horizon, the condition in Theorem 5.4 is also sufficient.

Proposition 5.7. Suppose that $b = 0$ and $h = 1$. In the complete graph $\mathcal{G}$, a sufficient condition for consensus not to happen is $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq n - 1$.

We remark that it is possible to extend this result on the complete graph to more general class of graphs, however distribution of initial states of agents becomes important, since from the utility functions the attacker will want to separate agent with farthest states. In the complete graph case, the attacker is always able to isolate the farthest agents by attacking $(n - 1)$ edges.

5.6 Clustering analysis

In this section, we derive some results on the number of formed clusters of agents at infinite time. From Proposition 5.6, the result implies the simple case where if the attacker has enough energy such that $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq |\mathcal{E}|$, then the attacker can attack all the edges of the underlying topology $\mathcal{G}$ so that the number of clusters is n (i.e., all the agents are separated).

The next result discusses a relation between the attacker's cost and energy recharge rate with the maximum number of clusters that the attacker may create through jamming. In the subsequent results of this section, we suppose that $b = 0$.

We first define a vector which characterizes the maximum number of clusters of $\mathcal{G}$, given the parameters ρ^{A} and $\overline{\beta}^{\mathrm{A}}$. Specifically, we define a vector $\Theta \in \mathbb{R}^{|\mathcal{E}|}$ with elements $\Theta_j := \max_{|\mathcal{E}^{\mathrm{A}}|=j} \overline{n}(\mathcal{V}, \mathcal{E} \setminus \mathcal{E}^{\mathrm{A}})$, with $\overline{n}(\mathcal{V}, \mathcal{E} \setminus \mathcal{E}^{\mathrm{A}})$ being the number of agent groups of $(\mathcal{V}, \mathcal{E} \setminus \mathcal{E}^{\mathrm{A}})$.

Proposition 5.8. An upper bound on the number of formed clusters at infinite time is $\Theta_{\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor}$.

In Proposition 5.8, we use the information of the graph structure to obtain the vector Θ. We remark that if the graph structure $\mathcal{G}$ is not known, then the number of clusters at infinite time is in general upper bounded by $\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor + 1$. This is because the attacker can attack continuously at all time at most $\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor$ number of edges, and in the most vulnerable graph with $\lambda = 1$, i.e., tree graphs, any attacked edge will result in a new group.

We illustrate the results in Proposition 5.8 by looking at the graph in Fig. 5.3 from the last section. Specifically, the vector Θ is $\Theta = [2, 2, 3, 4]^{\mathrm{T}}$, whereas the values of $\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor + 1$ are 2, 3, 4, 5 for $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} = 1$, 2, 3, and 4, respectively. Note that for any value of $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}$, inequality $\Theta_{\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor} \leq \lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor + 1$ is always satisfied, indicating that knowing the graph structure helps to better estimate the upper bound of the number of clusters.

We continue by addressing a special case where all the agents in the network are connected with each other.

Lemma 5.9. In the complete graph $\mathcal{G}$, the attacker cannot divide the agents into more than

$$1 + \sum_{j=1}^{(n-1)} \min\Big\{1, \Big\lfloor \frac{2\rho^{\mathrm{A}}}{j\overline{\beta}^{\mathrm{A}}(2n-j-1)} \Big\rfloor \Big\} \tag{5.12}$$

number of clusters.

5.7 Equilibrium characterization

In this game the strategy choices are all finite in form of edges attacked and recovered. Here, we characterize the equilibrium/optimal strategies of the players in certain situations for the case where the players' horizon length is 1 so that they myopically update their strategies every time step.

In this section, we state some results when $a = 0$, i.e., when the players do not consider the agents' states but agent-group index in determining their strategies so that the defender (resp., attacker) has higher (resp., lower) utility when more agents belong to the same group. Similar to the analysis in Chapter 3, here we explore some possible optimal strategy candidates for the players in a game. However, since a game consists of several steps in this formulation, the subgame perfect equilibrium is more involved to characterize, compared to the case of a game consisting of one step as in Chapter 3.

In the $\bar{l}$th step of each game, there are three possibilities in function $c(\cdot)$ as shown in Table 5.1 (Cases 1, 2, and 3). From this table, we characterize the optimal strategies of both players in each case:

- **Case 1:** When $c(\mathcal{G}) = c(\mathcal{G}_k^{\mathrm{D}})$, the attacker's utility in one time step is $c(\mathcal{G})$, which implies that the attacker should not attack any edge either with normal signals or strong signals, with the utilities of both players equal to zero. The players' strategies in this case are called Combined Strategy 1.

Table 5.1: Possible cases of attack and recovery actions

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

- **Case 2:** When $c(\mathcal{G}_k^{\mathrm{D}}) = c(\mathcal{G}_k^{\mathrm{A}})$, the defender does not recover any attacked edge, whereas the attacker should attack some edges either with strong or normal signals. The players' strategies in this case are classified as Combined Strategy 2.

- **Case 3:** Here both players will attack/recover nonzero number of edges. In particular, the attacker will attack with normal signals and potentially with strong signals. The players' strategies here are called Combined Strategy 3.

We will then discuss the equilibrium for this game in Proposition 5.10 below. For simplicity, we only consider the case when $h = 1$. The case of $h > 1$ can be examined based on the characterization here for $h = 1$.

Proposition 5.10. The optimal strategies for the players with $h = 1$ satisfy the following:

1. Combined Strategy 1 if $\tilde{\beta}_l^{\mathrm{A}} + \beta^{\mathrm{A}} > \kappa^{\mathrm{A}} + \rho^{\mathrm{A}}(l-1)T$,

2. Otherwise,

   (a) Combined Strategy 2 if

      i. $\tilde{\beta}_l^{\mathrm{D}} + \beta^{\mathrm{D}} > \kappa^{\mathrm{D}} + \rho^{\mathrm{D}}(l-1)T$, or

      ii. $\tilde{\beta}_l^{\mathrm{D}} + \beta^{\mathrm{D}} \leq \kappa^{\mathrm{D}} + \rho^{\mathrm{D}}(l-1)T$ and $U_k^{\mathrm{A}}(\lfloor(\kappa^{\mathrm{A}} + \rho^{\mathrm{A}}(l-1)T - \tilde{\beta}_l^{\mathrm{A}})/\overline{\beta}^{\mathrm{A}}\rfloor, \emptyset, \emptyset) = \max_{\overline{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}}} U_k^{\mathrm{A}}(\overline{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}})$,

   (b) Combined Strategy 3 if $\tilde{\beta}_l^{\mathrm{D}} + \beta^{\mathrm{D}} \leq \kappa^{\mathrm{D}} + \rho^{\mathrm{D}}(l-1)T$ and $U_k^{\mathrm{A}}(\lfloor(\kappa^{\mathrm{A}} + \rho^{\mathrm{A}}(l-1)T - \tilde{\beta}_l^{\mathrm{A}})/\overline{\beta}^{\mathrm{A}}\rfloor, \emptyset, \emptyset) \neq \max_{\overline{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}}} U_k^{\mathrm{A}}(\overline{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}})$.

We remark that the result in Proposition 5.10 also holds for a more general class of agent-group indices other than the one defined in (4.7). Specifically, it holds for those that belong to the class given by

$$\mathcal{C} := \{\tilde{c} : 2^{\mathcal{V}} \times 2^{\mathcal{E}} \to \mathbb{R} : \tilde{c}((\mathcal{V}, \overline{\mathcal{E}} \cup \mathcal{E}')) \geq \tilde{c}((\mathcal{V}, \overline{\mathcal{E}})), \overline{\mathcal{E}}, \mathcal{E}' \subseteq \mathcal{E}\}. \tag{5.13}$$

The condition $\tilde{c}((\mathcal{V}, \overline{\mathcal{E}} \cup \mathcal{E}')) \geq \tilde{c}((\mathcal{V}, \overline{\mathcal{E}}))$ implies that not attacking/recovering results in the least value of the attacker/defender, respectively. This condition is necessary for en-

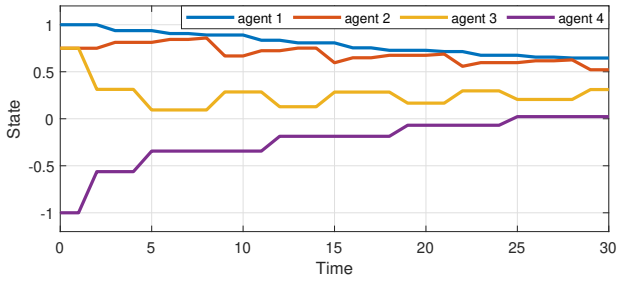


Figure 5.4 Agent states with $a = 0.1$ and $b = 0.9$

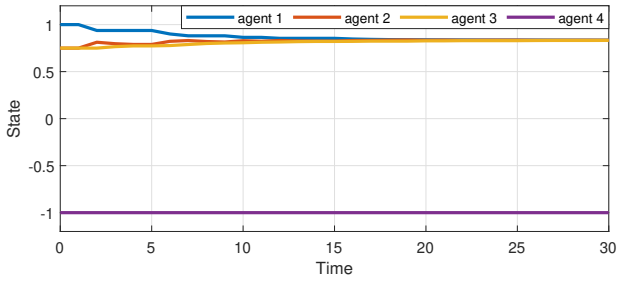


Figure 5.5 Agent states with $a = 0.9$ and $b = 0.1$

suring the equilibrium as in Proposition 5.10 since otherwise Combined Strategies 1 and 2 will be optimal in more cases, regardless of the energy condition of the players.

In general, since the cases discussed above are for one step only, for longer $h > 1$ the optimal strategies will take form of a set of combined strategies. For example, if $h = 3$, the sequence of optimal strategies may be {Combined Strategy 1, Combined Strategy 2, Combined Strategy 2}. On the other hand, for $a > 0$, the condition in Proposition 5.10 becomes more complicated to characterize since attacking more edges does not necessarily result in the highest possible utility.

5.8 Simulation results

5.8.1 Consensus and clustering across parameters

Here we show how the consensus varies across different weights of the utility functions and the initial states.

5.8.1.1 Varying weights a and b

We consider the 4-agents line/path graph 1–2–3–4 with initial states $x_0 = [1, 0.75, 0.75, -1]^{\mathrm{T}}$. The parameters are $\beta^{\mathrm{A}} = \beta^{\mathrm{D}} = 1$, $h = \overline{\beta}^{\mathrm{A}} = 2$, $\kappa^{\mathrm{A}} = \rho^{\mathrm{A}} = 2.6$, $\rho^{\mathrm{D}} = 0.3$, and $\kappa^{\mathrm{D}} = 0.8$, which satisfy the necessary condition in Proposition 5.3. With $b = 1 - a$, Figs. 5.4 and 5.5 show the agent states with small a (at $a = 0.1$) and large a (at $a = 0.9$), respectively.

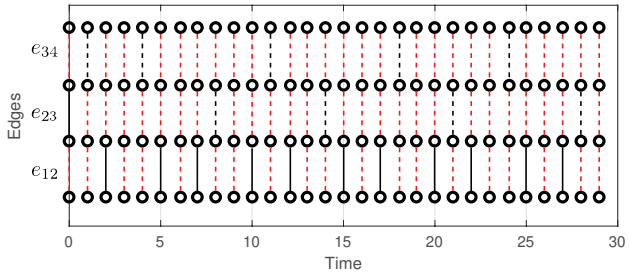


Figure 5.6 Attacked and recovered edges with $a = 0.1$ and $b = 0.9$

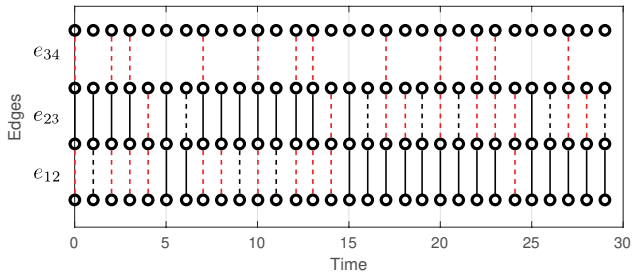


Figure 5.7 Attacked and recovered edges with $a = 0.9$ and $b = 0.1$

Figs. 5.6 and 5.7 illustrate the status of the edges in $\mathcal{G}_k^{\mathrm{D}}$ over discrete time k. There, no line in the corresponding edge implies that the edge is strongly attacked; likewise, dashed red lines: normally attacked, dashed black lines: recovered, and solid black lines: not attacked.

We observe that for small a, the attacker more often divides the agents into more groups, indicated by more dashed red lines in Fig. 5.6. As a result, the attacker fails to prevent consensus among the agents (Fig. 5.4), despite the condition in Proposition 5.3 being satisfied. On the other hand, with large a, the attacker is more focused to make the difference among agents' states larger while separating the agents into fewer groups compared to the case with small a. These features can be seen in Fig. 5.7, where there are no black lines in the edge e_{34}, and thus no consensus among the agents in Fig. 5.5.

We next present a comparison in the optimal state difference $z_k(\overline{\mathcal{E}}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{D}*})$ and agent-group index $c(\mathcal{G}_k^{\mathrm{D}})$ across different a and $b = 1 - a$ in Fig. 5.8. We observe that with larger a, the attacker successfully prevents consensus among agents (shown with larger value of z_k) at time $k = 20$. On the other hand, with smaller a (corresponding to larger b), the attacker obtains higher $c(\mathcal{G}_k^{\mathrm{D}})$ at the cost of low z_k, implying that the attacker fails to prevent consensus. It is interesting that the values of z_k and $\sum c(\mathcal{G}_k^{\mathrm{D}})$ remain almost constant for some different a, implying that there is a critical value of weights a and b that determine the consensus and the number of clusters at infinite time; in this case, the critical value of a is located in $0.4 < a < 0.5$.

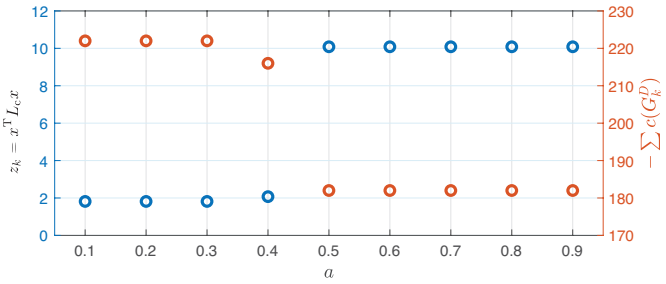


Figure 5.8 Comparison of z_k and $-\sum c(\mathcal{G}_k^{\mathrm{D}})$ $(k = 20)$ versus a

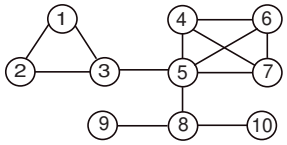


Figure 5.9 Graph used for simulation in Section 5.8.1.2

5.8.1.2 Varying initial states x_0

We also observe how the initial states x_0 affect the agent-group index of the agents. We consider the graph shown in Fig. 5.9, which consists of 10 agents. All parameters other than the initial states are set to be the same and satisfy the conditions in Proposition 5.3. Specifically, we set $\beta^{\mathrm{A}} = \beta^{\mathrm{D}} = 1, \overline{\beta}^{\mathrm{A}} = 2, \kappa^{\mathrm{A}} = \rho^{\mathrm{A}} = 2.1, \kappa^{\mathrm{D}} = \rho^{\mathrm{D}} = 0.7$, and $a = 1-b = 0.9$. The state trajectories of the agents with varying x_0 are shown in Figs. 5.10–5.12. Here we consider three cases of initial states x_0:

1. $x_0 = [1, 0.9, 0.8, 0.4, 0.44, 0.35, 0.48, 0.2, 0.19,\ 0.28]^{\mathrm{T}}$,
2. $x_0 = [1, 0.9, 0.8, 0.4, 0.44, 0.35, 0.48, -0.5, -0.1, -0.2]^{\mathrm{T}}$,
3. $x_0 = [0.6, 0.5, 0.8, 0.4, 0.44, 0.35, 0.48, 0.58, 0.8, 0.75]^{\mathrm{T}}$.

Note that in Case (1), agents 1–3 have closer initial states and are far from the other agents. Similarly, in Case (2), agents 8–10 have initial states that are different from the other agents. However, in Case (3), agent states are distributed approximately evenly in the range $[0.35, 0.8]$ so that it is hard for the attacker to divide them into clusters.

From Fig. 5.10, we can see that in Case (1), agents 1–3, which have weak connection to other agents (only connected by one edge), are grouped together and converge to the same state. This occurs by attacking the edge connecting agents 3 and 5. On the other hand, in Fig. 5.11 for Case (2), agents 8–10 are separated from the others because the edge connecting agents 5 and 8 is attacked continuously. Clearly, in Cases (1) and (2) it is easier for the attacker to separate agents since their initial states form clusters matching the network topology.

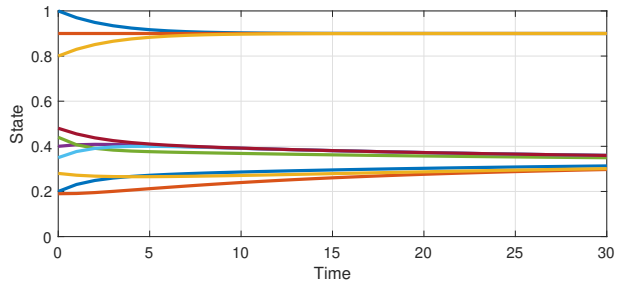


Figure 5.10 Agent states in Case 1

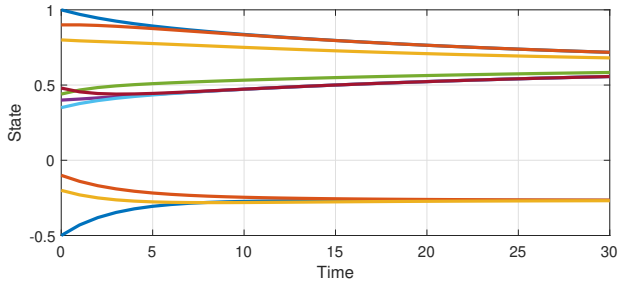


Figure 5.11 Agent states in Case 2

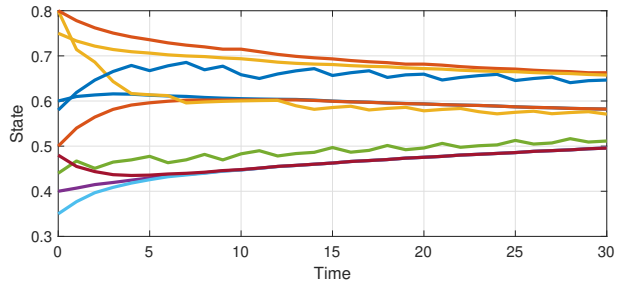


Figure 5.12 Agent states in Case 3

In Case (3), however, the initial state values do not exhibit such properties and as a result, the states converge towards the same value as shown in Fig. 5.12. In this simulation, the attacker is not able to effectively attack certain edges at all times; as a consequence, the agents are not divided into clusters and thus consensus happens. The attacker may be able to prevent consensus with higher weight a, as discussed in Section 5.8.1.1 above.

For obtaining Figs. 5.10–5.12, we solve combinatorial optimization problems to find optimal strategies of the players. We remark that the computational complexity of this problem depends on the number of edges $\mathcal{E}$ of $\mathcal{G}$. We have reduced the complexity by disregarding some combinations of edges that are clearly not optimal; for example, attacking only the edge connecting agents 4 and 7 does not disconnect the graph, and thus cannot be the best move for the attacker.

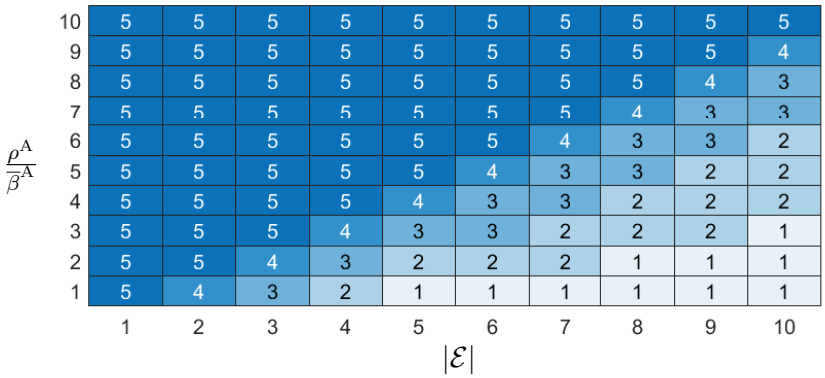


Figure 5.13 Number of clusters at $k = 50$ with $b = 0$. The underlying graphs used are those with 5 agents with maximum 10 edges.

5.8.1.3 Varying energy and cost parameters

We continue by discussing the effect of the attacker's recharge rate ρ^{A} and unit costs of attacks β^{A} and $\overline{\beta}^{\mathrm{A}}$ on the consensus and cluster forming. Recall that in the theoretical results in Sections 5.5 and 5.6, the ratios of ρ^{A} to $\overline{\beta}^{\mathrm{A}}$ and ρ^{A} to β^{A} are used to derive the necessary conditions and sufficient conditions for preventing consensus as well as the upper bound of the number of clusters formed at infinite time.

Assuming that $b = 0$, the number of clusters is dictated by $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}$ as discussed in Proposition 5.8. We show the number of clusters over different topologies of the underlying graph $\mathcal{G}$ in Fig. 5.13. We consider networks with $n = 5$, with the edges positioned to yield the most connected topology, i.e., maximum λ, given the same number of edges $|\mathcal{E}|$. Note that, with $n = 5$, there are at most $n(n-1)/2 = 10$ number of edges in the underlying graph $\mathcal{G}$ (which happens for the complete graph $\mathcal{G}$). We observe that with $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq |\mathcal{E}|$, the agents are divided into 5 clusters (all agents are separated) as shown in the upper left area of the figure indicated by "5" as derived in Proposition 5.6 whereas in the lower right area indicated by "1" the agents converge to the same cluster. It is clear that in a more connected graph, the agents are more likely to converge to a fewer number of clusters.

5.8.2 Players' performance under varying horizon length and game period

In this subsection, we evaluate the players' performance under varying horizon length h and game period T. To evaluate the performance of the players, we introduce the *applied utilities* $\hat{U}_k^{\mathrm{A}} := az_k(\overline{\mathcal{E}}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{D}*}) - bc(\mathcal{G}_k^{\mathrm{D}*})$ and $\hat{U}_k^{\mathrm{D}} := -az_k(\overline{\mathcal{E}}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{D}*}) + bc(\mathcal{G}_k^{\mathrm{D}*})$, with $\mathcal{G}_k^{\mathrm{D}*} = (\mathcal{V}, ((\mathcal{E} \setminus (\overline{\mathcal{E}}_k^{\mathrm{A}*} \cup \mathcal{E}_k^{\mathrm{A}*})) \cup \mathcal{E}_k^{\mathrm{D}*})$. These are elements of utility functions U_k^{A} and U_k^{D} corresponding to the $\bar{l}$th step, $\bar{l} = k \bmod T + 1$, of the game with index

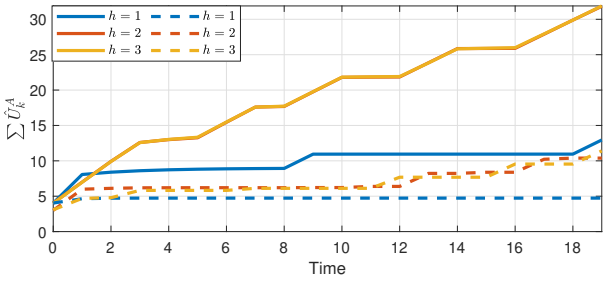


Figure 5.14 $\sum_k \hat{U}_k^{\mathrm{A}}$ in the path graph (solid lines) and the complete graph (dashed lines) for varying value of h

Table 5.2: Difference in the optimal actions and the resulting utilities in the path graph $\mathcal{G}$ between $h = 2$ and $h = 3$

Initial states	$\lvert\overline{\mathcal{E}}_0^{\mathrm{A}*}\rvert$		$\sum_{k=0}^{19} \hat{U}_k^{\mathrm{A}}$	
	$h=2$	$h=3$	$h=2$	$h=3$
$[0.824,\ -0.798,\ -0.413]^{\mathrm{T}}$	2	2	37.74	
$[-0.983,\ 0.649,\ 0.535]^{\mathrm{T}}$	2	2	39.89	
$[-0.787,\ -0.786,\ -0.265]^{\mathrm{T}}$	2	1	28.41	30.00
$[0.624,\ 0.629,\ -0.821]^{\mathrm{T}}$	2	1	37.92	43.45

$l = \lfloor k/T \rfloor + 1$, where the obtained strategies $(\overline{\mathcal{E}}^{\mathrm{A}*}_{(l-1)T+\bar{l}-1}, \mathcal{E}^{\mathrm{A}*}_{(l-1)T+\bar{l}-1}, \mathcal{E}^{\mathrm{D}*}_{(l-1)T+\bar{l}-1}) = (\overline{\mathcal{E}}^{\mathrm{A}*}_{l,\bar{l}}, \mathcal{E}^{\mathrm{A}*}_{l,\bar{l}}, \mathcal{E}^{\mathrm{D}*}_{l,\bar{l}})$ are applied. Since $U_k^{\mathrm{A}} = -U_k^{\mathrm{D}}$, having higher applied utility for the attacker implies lower applied utility for the defender. Note that the values of h and T are uniform among the players.

In this subsection, we consider the weight $a_{ij} = \hat{a}$, $\hat{a} < 1/n$ in (2.4) which implies that different agents have different convergence speeds depending on the number of their neighbors. Furthermore, we consider various initial states x_0 for the agents in order to more accurately evaluate the attacker's performance and the pattern of applied utilities $\hat{U}_k^{\mathrm{A}}$. We use up to 1000 randomly generated initial states in this simulation for each agent ranging from -1 to 1. Throughout this subsection, we use parameters $n = 3$, $\rho^{\mathrm{A}} = 1.1$, $\kappa^{\mathrm{A}} = 7$, $\overline{\beta}^{\mathrm{A}} = 2\beta^{\mathrm{A}} = 1$.

5.8.2.1 Varying horizon length

We now consider the case of varying value of horizon length h when the network is a path graph and a complete graph. Note that the value of h is still uniform among the attacker and the defender. The evolutions of the attacker's applied utility $\hat{U}_k^{\mathrm{A}}$ with varying h (with $T = 1$ for every h) are shown in Fig. 5.14, where in the figure the applied utility for $h = 2$ and $h = 3$ in the path graph is almost identical.

Since the path graph is the least connected graph, the attacker will be able to make multiple groups of agents relatively easily compared to more connected graphs. As a

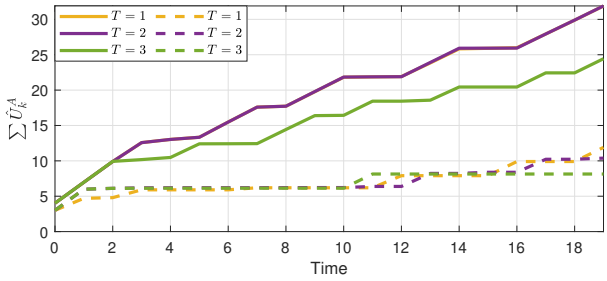


Figure 5.15 $\sum_k \hat{U}_k^{\mathrm{A}}$ in the path graph (solid lines) and the complete graph (dashed lines) for varying T. The applied utility for $h = 1$ and $h = 2$ in the path graph is almost identical.

result, the attacker may not need to have a very long horizon length h to improve its utility since it does not need to save energy as much compared to the case of the complete graph. This is shown with the overlapping red and yellow solid lines in the Fig. 5.14, implying that the horizon length $h = 3$ is already as good as the case of $h = 2$. On the other hand, the blue solid line is far below the red and the yellow ones, implying that having h being too short can result in a worse utility for the attacker over time.

The differences of the attacker's strategies for some notable cases in the path graph $\mathcal{G}$ between $h = 2$ and $h = 3$ are shown in Table 5.2. Here, we see the difference in the optimal actions between the attacker with $h = 2$ and $h = 3$ in the path graph $\mathcal{G}$ even though the plots of applied utilities in Fig. 5.14 are very similar. We observe that when the initial states of some agents are sufficiently close, the attacker with $h = 2$ keeps attacking both edges at $k = 0$, whereas the attacker with $h = 3$ chooses to save its energy by attacking fewer edges. At $k = 19$ the attacker with $h = 3$ obtains higher applied utility, indicating that it is able to better use its energy than the attacker with $h = 2$ by attacking later.

On the other hand, since the complete graph is the most connected graph, here the attacker will need more energy to disconnect the graph and obtain some utility. Consequently, even with longer h, the difference of $\sum \hat{U}_k^{\mathrm{A}}$ is smaller compared to the path graph case. The difference between the red and the yellow dashed lines is clearer however, suggesting that the attacker still benefits by having $h = 3$ (compared to the very little difference in the path graph case). The attacker's different behavior for the path graph and the complete graph $\mathcal{G}$ suggests that in a less connected graph, the effectiveness of longer h may saturate from a lower value compared to the one in a more connected graph $\mathcal{G}$, given the attacker's energy parameters.

In general, we observe that having a longer h may result in a better applied utility for the attacker over time due to its role as a leader of the game, i.e., the attacker moves first and is able to choose its strategy that minimizes the defender's best response. Additionally, there is also a clear pattern on when $\sum \hat{U}_k^{\mathrm{A}}$ increases; this implies that the

Table 5.3: Average total number of edges attacked in the path graph $\mathcal{G}$

h	T	$\sum_{m=0}^{k} \lvert\mathcal{E}_m^{\mathrm{A}*}\rvert$ (Normal)		$\sum_{m=0}^{k} \lvert\overline{\mathcal{E}}_m^{\mathrm{A}*}\rvert$ (Strong)	
		$k=9$	$k=19$	$k=9$	$k=19$
1	1	7	16	5	6
2		0	0	8	13.959
3		0	0	7.993	13.971
	2	0	0	8	13.970
	3	2.970	4.970	7.003	11.015

variation of initial states may not affect the attacker's optimal strategy, except in some cases as explained above.

5.8.2.2 Varying game period

We then continue by simulating the case of varying value of game period T (value of h is set to be $h = 3$ for both players so that the assumption $T \leq h$ is always satisfied). The average value of $\sum \hat{U}_k^{\mathrm{A}}$ over time is shown in Fig. 5.15, where in general, the attacker with shorter game period T has higher applied utility especially at later time for both the path graph and the complete graph $\mathcal{G}$.

The attacker with shorter T will be more adaptive to the changes of the agents' and players' conditions. In the context of this game, the attacker with shorter T may delay the attack further to maximize its utility later. This in turn increases the attacker's utility at later time, similar to the case of longer h discussed above. Note that the yellow dashed and solid lines are the same as the yellow lines in Fig. 5.14, and we observe that the green and the purple lines do not differ as much as the red and the blue lines in Fig. 5.14, indicating that for the attacker, having a large value of T may not be as disadvantageous as having short h.

Table 5.3 shows the average number of edges attacked by normal and strong jamming signals given different values of h and T. It is interesting to note that for $h > T$, the attacker never attacks any edge with normal signals, indicating that it prefers to save its energy to use it later for more powerful attacks. Consequently, the number of edges attacked strongly with $h > T$ becomes more than those in the case of $h = T$, which results in the larger applied utilities as described above. We can also observe that in the case of $h = 3$ and $T = 1$, the attacker is able to strongly attack more edges than the other cases in Table 5.3 in average at $k = 19$, even though at $k = 9$ it attacks slightly fewer edges than the case of closer values of h and T. This suggests that the attacker tends to save its energy more in the case of larger value of h and smaller T.

5.9 Chapter summary

In this chapter, we have formulated a two-player game in a cluster forming of resilient multiagent systems played over time. The players consider the impact of their actions on future communication topology and agent states, and adjust their strategies according to a rolling horizon approach. Necessary conditions and sufficient conditions for forming clusters among agents have been derived. We have discussed the effect of the weights of the utility functions and different initial states on cluster forming, and evaluated the effects of varying horizon length and game period on the players' performance.

We note that it is not straightforward to state the theoretical results of the defender's energy parameters, since the attacker is the first-mover of the game. However, we derive some important results that are needed to derive the necessary conditions and sufficient conditions which are based on the attacker's energy parameters. For example, the necessary conditions and the sufficient conditions in this chapter are based on the results on the defender's optimal strategies which state that the defender will always recover on the last step of the game, e.g., Lemma 5.3.

5.10 Appendix

5.10.1 Proof of Lemma 5.1

We first look at the last (hth) step of the lth game. Since the game consists of a horizon of h steps, the last step of the game corresponds to the last decision-making point, in which the players' strategies cannot influence the decision already made in the previous steps of the same game. Hence, in the last step of the lth game the players do not save their energy by attacking/recovering less edges.

From the defender's energy constraint (5.2), it is clear that at any time k, the set of edges that the defender recovers is bounded as $|\mathcal{E}_k^{\mathrm{D}}| \leq \frac{\kappa^{\mathrm{D}}+\rho^{\mathrm{D}}k-\sum_{m=0}^{k-1}\beta^{\mathrm{D}}|\mathcal{E}_m^{\mathrm{D}}|}{\beta^{\mathrm{D}}}$. Thus, at the hth step, recovered edges satisfy $|\mathcal{E}_{l,h}^{\mathrm{D}}| \leq |\mathcal{E}_{l,h}^{\mathrm{D}\prime}|$ with $|\mathcal{E}_{l,h}^{\mathrm{D}\prime}| := \min\{\lfloor(\kappa^{\mathrm{D}} + \rho^{\mathrm{D}}((l-1)T + h - 1) - (\tilde{\beta}_l^{\mathrm{D}} + \hat{\beta}_{h-1}^{\mathrm{D}}))/\beta^{\mathrm{D}}\rfloor, |\mathcal{E}_{l,h}^{\mathrm{A}*}|\}$.

Depending on which edges are normally attacked, the defender may not recover the maximum number $|\mathcal{E}_{l,h}^{\mathrm{D}\prime}|$ of edges. If the defender's optimal strategy given normally attacked edges $\mathcal{E}_{l,h}^{\mathrm{A}}$ is not to recover $|\mathcal{E}_{l,h}^{\mathrm{D}\prime}|$ number of edges, i.e., recover less, then the defender will be able to obtain more utility $U_{l,h}^{\mathrm{D}}(\overline{\mathcal{E}}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{D}}) > U_{l,h}^{\mathrm{D}}(\overline{\mathcal{E}}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{D}\prime})$. However, under (5.10) with $\alpha = h$ the defender has sufficiently high energy, and thus the utility becomes $U_{l,h}^{\mathrm{D}}(\overline{\mathcal{E}}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{D}}) > U_{l,h}^{\mathrm{D}}(\overline{\mathcal{E}}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{A}}) = U_{l,h}^{\mathrm{D}}(\overline{\mathcal{E}}_{l,h}^{\mathrm{A}}, \emptyset, \emptyset)$. It then follows

that as long as the defender has enough energy, it will recover all optimal edges attacked normally at the hth step, i.e., $\mathcal{E}^{\mathrm{D}*}_{l,h} = \mathcal{E}^{\mathrm{A}*}_{l,h}$.

Next, we investigate the effect of this property on the earlier steps of the lth game. Since the defender's strategy at the hth step is not affected by its strategy at the previous (i.e., $(h-1)$th) step when $\kappa^{\mathrm{D}} + \rho^{\mathrm{D}}((l-1)T + h - 1) - (\tilde{\beta}^{\mathrm{D}}_{l} + \hat{\beta}^{\mathrm{D}}_{h-1}) \geq \beta^{\mathrm{D}}|\mathcal{E}|$, here the defender does not need to recover fewer edges at the $(h-1)$th step to save energy; this is because it already has enough energy to recover $\mathcal{E}^{\mathrm{A}*}_{l,h}$ at the hth step.

Now, we derive that if $\kappa^{\mathrm{D}} + \rho^{\mathrm{D}}((l-1)T + h - 2) - (\tilde{\beta}^{\mathrm{D}}_{l} + \hat{\beta}^{\mathrm{D}}_{h-2}) \geq 2\beta^{\mathrm{D}}|\mathcal{E}|$ at the $(h-1)$th step, then the defender will also recover $\mathcal{E}^{\mathrm{D}*}_{l,h-1} = \mathcal{E}^{\mathrm{A}*}_{l,h-1}$. To recover all attacked edges at steps $\bar{l} \geq \hat{\bar{l}}$, it is then sufficient that the defender's energy satisfies (5.10) so that $\kappa^{\mathrm{D}} + \rho^{\mathrm{D}}((l-1)T + \bar{l} - 1) \geq \tilde{\beta}^{\mathrm{D}}_{l} + \hat{\beta}^{\mathrm{D}}_{\bar{l}-1} + \beta^{\mathrm{D}}|\mathcal{E}|$, i.e., the worst-case scenario of the energy constraint (5.2) when the defender recovers all edges, is always satisfied when $\bar{l} \geq \hat{\bar{l}}$.

5.10.2 Proof of Lemma 5.2

It follows from Lemma 5.1 that in a game with index l' where (5.10) is satisfied for $\bar{l} = 1$, the defender always recovers edges that are attacked normally in the 1st step, i.e., $\mathcal{E}^{\mathrm{D}}_{l',1} \neq \emptyset$ if $\mathcal{E}^{\mathrm{A}}_{l',1} \neq \emptyset$. We then investigate in which game inequality (5.10) is satisfied for $\bar{l} = 1$. Since the defender gains ρ^{D} every time k, if $\mathcal{E}^{\mathrm{D}}_{k} = \emptyset$ for any $k \in \{0, \ldots, (l'-1)T-1\}$, then (5.10) at the first step of the l'th game can be written as $\frac{\kappa^{\mathrm{D}} + \rho^{\mathrm{D}}(l'-1)T}{\beta^{\mathrm{D}}} \leq h|\mathcal{E}|$. With $\kappa^{\mathrm{D}} = \rho^{\mathrm{D}}$ as a worst-case scenario, the left-hand side becomes $\frac{\rho^{\mathrm{D}}(1+(l'-1)T)}{\beta^{\mathrm{D}}}$, and we then obtain $l' \geq \lceil \frac{h|\mathcal{E}|\beta^{\mathrm{D}} - \rho^{\mathrm{D}}}{\rho^{\mathrm{D}}T} + 1 \rceil$.

Note that the above fact holds when the defender does not recover any edge for any $k \in \{(j-1)(l'-1)T, \ldots, j(l'-1)T - 1\}, j \in \mathbb{N}$. If the defender recovers one or more attacked edges at any $k \in \{0, \ldots, (l'-1)T - 1\}$, then the above result may not hold, i.e., the defender may not be able to recover all $\mathcal{E}^{\mathrm{A}}_{l'}$. However, it follows that during time $k \in \{(j-1)(l'-1)T, \ldots, j(l'-1)T - 1\}$, either 1) the defender recovers nonzero edges ($\mathcal{E}^{\mathrm{D}}_{k} \neq \emptyset$), or 2) the attacker attacks no edges with normal signals ($\mathcal{E}^{\mathrm{A}}_{k} = \emptyset$) at least once.

5.10.3 Proof of Proposition 5.3

We note that, without any recovery from the defender ($\mathcal{E}^{\mathrm{D}}_{k} = \emptyset$), the attacker must attack at least λ number of edges with normal signals at any time k to make $\mathcal{G}^{\mathrm{D}}_{k}$ disconnected. If the attacker attacks λ edges with normal jamming signals at all times, the energy constraint (5.1) becomes $(\beta^{\mathrm{A}}\lambda - \rho^{\mathrm{A}})k \leq \kappa^{\mathrm{A}}$. Thus, the condition $\rho^{\mathrm{A}}/\beta^{\mathrm{A}} \geq \lambda$ has to be satisfied for all k.

5.10.4 Proof of Theorem 5.4

We prove by contrapositive; especially, we prove that consensus always happens if $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda$.

We first suppose that the attacker attempts to attack λ edges strongly at all times to disconnect the graph $\mathcal{G}_k^{\mathrm{D}}$. From (5.1), the energy constraint of the attacker at time k becomes $(\overline{\beta}^{\mathrm{A}}\lambda - \rho^{\mathrm{A}})k \leq \kappa^{\mathrm{A}}$. This inequality is not satisfied for sufficiently large k if $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda$, since $\overline{\beta}^{\mathrm{A}}\lambda - \rho^{\mathrm{A}}$ becomes positive and κ^{A} is finite. Therefore, the attacker cannot attack λ edges strongly at all times if $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda$, and is forced to disconnect the graph by attacking with normal jamming signals instead.

Next, by Lemma 5.2 above, we show that there exists an interval of time where the defender always recovers if there are edges attacked normally, i.e., $\mathcal{E}_{l'}^{\mathrm{D}} \neq \emptyset$ is optimal given that $\mathcal{E}_{l'}^{\mathrm{A}} \neq \emptyset$.

From the definitions in (5.4), (5.5), given that $b = 0$, we can see that the defender obtains a higher utility if the agents are closer. This means that given a nonzero number of edges to recover (at time $jl'T$ described above), the defender recovers the edges connecting further agents. Specifically, for some $i \in \mathbb{N}$, for interval $[jl'T, (j+i)l'T]$, there is a time step where $U_k^{\mathrm{D}}(\mathcal{E}_k^{\mathrm{D}} = \mathcal{E}_1) \geq U_k^{\mathrm{D}}(\mathcal{E}_2)$, with edges $\mathcal{E}_1$ connecting agents with further states than agents connected by $\mathcal{E}_2$. This fact implies that when recovering, the defender always chooses the further disconnected agents. Since by communicating with the consensus protocol as in (2.3) the agents' states are getting closer, the defender will choose different edges to recover if the states of agents connected by recovered edges $\mathcal{E}_k^{\mathrm{D}}$ become close enough. Consequently, if $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda$, then there exists $i \in \mathbb{N}$ where the union of graphs, i.e., the graph having the union of the edges of each graph $(\mathcal{V}, \bigcup((\mathcal{E} \setminus (\overline{\mathcal{E}}_k^{\mathrm{A}} \cup \mathcal{E}_k^{\mathrm{A}})) \cup \mathcal{E}_k^{\mathrm{D}}))$ over the time interval $[j(l'-1)T, (j+i)(l'-1)T]$, becomes a connected graph, where $l' = \lceil \frac{h|\mathcal{E}|\beta^{\mathrm{D}} - \rho^{\mathrm{D}}}{\rho^{\mathrm{D}}T} + 1 \rceil$ as in Lemma 5.2 above. These intervals $[j(l'-1)T, (j+i)(l'-1)T]$ occur infinitely many times, since the defender's energy bound keeps increasing over time.

It is shown in [3] that with protocol (2.3), the agents achieve consensus in the time-varying graph as long as the union of the graphs over bounded time intervals is a connected graph. This implies that consensus is achieved if $(\mathcal{V}, \bigcup((\mathcal{E} \setminus (\overline{\mathcal{E}}_k^{\mathrm{A}} \cup \mathcal{E}_k^{\mathrm{A}})) \cup \mathcal{E}_k^{\mathrm{D}}))$ is connected over $[l_i', l_i'+1, \ldots, l_{i+j}']$. Thus, if $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda$ then consensus is achieved.

5.10.5 Proof of Lemma 5.5

We first observe that in the hth step of the lth game the attacker does not save their energy by attacking fewer edges. Since $z_{l,h}(\mathcal{E}, \emptyset, \emptyset) > z_{l,h}(\overline{\mathcal{E}}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{D}})$ and $c((\mathcal{V}, \emptyset)) \geq$

$c((\mathcal{V},(\mathcal{E}\setminus(\overline{\mathcal{E}}^{\mathrm{A}}_{l,h}\cup\mathcal{E}^{\mathrm{A}}_{l,h})\cup\mathcal{E}^{\mathrm{D}}_{l,h})))$ are always satisfied for any edges $\overline{\mathcal{E}}^{\mathrm{A}}_{l,h},\mathcal{E}^{\mathrm{A}}_{l,h},\mathcal{E}^{\mathrm{D}}_{l,h}$, the function U^{A}_h always has the highest value if the attacker strongly attacks all edges $\mathcal{E}$. It then follows that the attacker with enough energy, i.e., $\kappa^{\mathrm{A}}+\rho^{\mathrm{A}}((l-1)T+h-1)-(\tilde{\beta}^{\mathrm{A}}_l+\hat{\beta}^{\mathrm{A}}_{h-1})\geq\overline{\beta}^{\mathrm{A}}|\mathcal{E}|$ is satisfied, will choose to attack all edges with strong signals.

Similar to the proof in Lemma 5.1, inequalities $z_{l,\alpha}(\mathcal{E},\emptyset,\emptyset)>z_{l,\alpha}(\overline{\mathcal{E}}^{\mathrm{A}}_{l,\alpha},\mathcal{E}^{\mathrm{A}}_{l,\alpha},\mathcal{E}^{\mathrm{D}}_{l,\alpha})$ and $c((\mathcal{V},\emptyset))\geq c((\mathcal{V},(\mathcal{E}\setminus(\overline{\mathcal{E}}^{\mathrm{A}}_{l,\alpha}\cup\mathcal{E}^{\mathrm{A}}_{l,\alpha})\cup\mathcal{E}^{\mathrm{D}}_{l,\alpha})))$ are always satisfied for any step α. Hence, the attacker will choose to attack all edges with strong signals in any step α given enough energy. This can be achieved if the attacker has high enough stored energy, i.e., (5.11) is satisfied, or if the attacker has high enough recharge rate, i.e., $\rho^{\mathrm{A}}\geq\overline{\beta}^{\mathrm{A}}|\mathcal{E}|$. These conditions enable the attacker to attack all edges strongly while still satisfying the energy constraint (5.1) above for all steps.

5.10.6 Proof of Proposition 5.6

By Lemma 5.5, the attacker always strongly attacks all edges with strong signals in a game at any step α given either sufficient recharge rate or sufficient stored energy at the beginning of the game. Consequently, if the attacker's recharge rate satisfies $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}\geq|\mathcal{E}|$, the attacker will attack $\mathcal{E}$ with stronger jamming signals at all steps of all games, separating every agent at all times. As a result, there are n clusters formed, and hence, obviously, consensus is not reached.

5.10.7 Proof of Lemma 5.7

With $h=1$, the attacker will spend all of its energy at the only step of the game. With $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}\geq n-1$, the attacker is always able to disconnect the complete graph $\mathcal{G}$.

In the complete graph $\mathcal{G}$, every agent has the same degree and the same position, implying that there is no agent that can be prioritized to be isolated by the attacker (different from the example shown before). Then, with $b=0$, the attacker is ensured to separate the furthest agent. This implies that, at each game (and at each k), the attacker will always attack the same edges, resulting in disconnected $\mathcal{G}^{\mathrm{D}}_k$ at each time.

5.10.8 Proof of Lemma 5.8

The vector Θ consists of the maximum number of formed groups $\overline{n}(\mathcal{V},\mathcal{E}\setminus\mathcal{E}^{\mathrm{A}})$ given the number of attacked edges as the element index. Since some edges need to be attacked consistently in order to divide the agents into different clusters, the number of formed clusters at infinite time is never more than the maximum number of groups at any time k given the same number of strongly attacked edges.

Recall that $\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor$ is the maximum achievable number of edges that can be strongly attacked at all times. Given the known graph topology $\mathcal{G}$, we then can imply that $\Theta_{\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor}$ gives the maximum number of clusters at infinite time.

5.10.9 Proof of Lemma 5.9

In the complete graph, every agent is connected to all other $n-1$ agents. Thus $n-1$ edges must be attacked to have two clusters. Furthermore, to separate the agents into three clusters, the attacker needs to attack at least $n-2$ more edges, as all connected agents are now connected to other $n-2$ agents. Based on the approach of Proposition 5.8, we can derive $\Theta = [1, \ldots, n-1, n]^{\mathrm{T}}$, where the value of the $(n-1)$th entry is 2, the value of the $((n-1)+(n-2))$th entry is 3, and so on. The value of the $\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor$th entry for the complete graph can be written as in (5.12) above, where the number of strongly attacked edges $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}$ is divided by the sum of edge connectivities of the graphs after the attack. This value determines the upper bound of the number of clusters.

5.10.10 Proof of Proposition 5.10

With $a = 0$, we observe that the defender always recovers from the optimal attack at the last step given sufficient energy, which implies that it always recovers for $h = 1$ if $\tilde{\beta}_l^{\mathrm{D}} + \beta^{\mathrm{D}} \leq \kappa^{\mathrm{D}} + \rho^{\mathrm{D}}((l-1)T)$ is satisfied. Similar to the defender, the attacker obtains the least utility, i.e., zero, by not attacking for the case of $h = 1$. Therefore, the attacker will attack at least one edge as long as it has enough energy to do so. We prove each point of the proposition statement as below.

(1): We now suppose that $\tilde{\beta}_l^{\mathrm{A}} + \beta^{\mathrm{A}} > \kappa^{\mathrm{A}} + \rho^{\mathrm{A}}((l-1)T)$ (point (1) in the statement) is satisfied, i.e., the attacker does not have enough energy to even attack one edge normally. In this case, Combined Strategy 1 becomes optimal since there is no other choice, i.e., the attacker cannot attack even one edge with normal signals. In the rest of the proof, we assume that $\tilde{\beta}_l^{\mathrm{A}} + \beta^{\mathrm{A}} \leq \kappa^{\mathrm{A}} + \rho^{\mathrm{A}}((l-1)T)$ is satisfied.

(2*a*(*i*)): We now continue by providing the conditions for Combined Strategy 2. Similarly to the attacker above, we observe that the defender cannot recover any edge if $\tilde{\beta}_l^{\mathrm{D}} + \beta^{\mathrm{D}} > \kappa^{\mathrm{D}} + \rho^{\mathrm{D}}((l-1)T)$, implying that $c(\mathcal{G}_k^{\mathrm{A}}) < c(\mathcal{G})$ and $c(\mathcal{G}_k^{\mathrm{D}}) = c(\mathcal{G}_k^{\mathrm{A}})$ (corresponds to point $(2a(i))$).

(2*a*(*ii*)): We then suppose that $\tilde{\beta}_l^{\mathrm{D}} + \beta^{\mathrm{D}} \leq \kappa^{\mathrm{D}} + \rho^{\mathrm{D}}((l-1)T)$ is satisfied. It then follows that given enough energy for the defender, the attacker needs to attack nonzero number of edges with strong signals to satisfy $c(\mathcal{G}_k^{\mathrm{A}}) < c(\mathcal{G})$ and $c(\mathcal{G}_k^{\mathrm{D}}) = c(\mathcal{G}_k^{\mathrm{A}})$. In order for Combined Strategy 2 to be optimal, the attacker then needs to attack

edges strongly without attacking with normal signals at all, i.e., $\mathcal{E}_k^{\mathrm{A}} = \emptyset$. Thus, $\overline{\beta}^{\mathrm{A}}$ needs to be sufficiently low to make strong attack feasible. Specifically, $U_k^{\mathrm{A}}(\overline{\mathcal{E}}_k^{\mathrm{A}\prime}, \emptyset, \emptyset) = \max_{\overline{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}}} U_k^{\mathrm{A}}(\overline{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}})$, with $|\overline{\mathcal{E}}_k^{\mathrm{A}\prime}| = \lfloor (\kappa^{\mathrm{A}} + \rho^{\mathrm{A}}((l-1)T) - \tilde{\beta}_l^{\mathrm{A}})/\overline{\beta}^{\mathrm{A}} \rfloor$ indicating the maximum number of edges the attacker attacks strongly. This corresponds to point $(2a(ii))$.

(2b): Consequently, if $\tilde{\beta}_l^{\mathrm{D}} + \beta^{\mathrm{D}} \leq \kappa^{\mathrm{D}} + \rho^{\mathrm{D}}((l-1)T)$ and $U_k^{\mathrm{A}}(\overline{\mathcal{E}}_k^{\mathrm{A}\prime}, \emptyset, \emptyset) \neq \max_{\overline{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}}} U_k^{\mathrm{A}}(\overline{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}})$ are true, then the attacker normally attacks nonzero number of edges and the defender recovers nonzero number of edges, which imply that Combined Strategy 3 is optimal (point $2b$).

Chapter 6

Players' Performance, Consensus, and Clustering with Non-uniform Horizons

6.1 Introduction

Receding/rolling horizon control has been employed to deal with multiagent systems with uncertainties and state constraints. It is used for achieving consensus of a linear multiagent system [76]. It is also studied in noncooperative security game settings in [78], where horizon lengths affect the resilience of the system. Rolling horizon approach has also been followed to obtain better planning, e.g., in an agent with obstacle avoidance constraints [79] and in a multivehicle competitive scenarios for self-driving cars [85].

In this chapter, we consider a security problem in a two-player game setting between an attacker, who is motivated to disrupt the communication among agents by attacking communication links, and a defender, who attempts to recover some of the attacked links. This game is played repeatedly over discrete time where the players recalculate and may change their strategies as time goes on, according to the rolling horizon approach. The players' utilities are determined by how agents are divided into clusters.

We formulate the problem based on [61], which use graph connectivity to characterize the game and players' strategies. Specifically, we address how clusters among agents may form in this security game setting. In this chapter, we approach clustering from a viewpoint based on a game-theoretic formulation. This approach can be related to the concept of network effect/externality [81], where the utility of an agent in a certain cluster

depends on how many other agents belong to that particular cluster. Such concepts have been used to analyze grouping of agents on, e.g., social networks and computer networks, as discussed in [86, 87].

Moreover, in comparison to our works in the previous chapters, our contributions in this chapter can be stated as follows: (i) we consider the difference in the capabilities of the players, represented by non-uniform values of horizon parameters, and (ii) we analyze the consensus and clustering of agents under non-uniform horizons setting which impacts how players allocate its resources.

Here we focus on evaluating the players' performance given different computational resources represented by *horizon lengths* (how long in the future the players can plan their strategies) and *game periods* (how long the players apply the obtained strategies without updating). As a consequence of these non-uniform horizons, the player with shorter horizon length can no longer perfectly observe the opponent's planned action in the future time. Therefore, it is then possible that the player does not perfectly execute the strategies planned before, since its strategy space depends on the opponent's action. This may result in a waste of the player's limited resources since each attack/recovery takes certain amount of resources. Similar energy allocation games in the context of cyber security have been discussed in, e.g., [88–90]. This has also been studied in stochastic setting in [91]. Related formulation of asymmetric information of the players is studied in [92, 93]. While [34, 61] consider jamming in similar multiagent system settings, the notion of wasted resources was not considered there. We discuss in this chapter that this notion is particularly useful in energy allocation games.

The chapter is organized as follows. In Section 6.2, we describe the general problem formulation of the attack-recovery sequence. We then specify the non-uniform horizon length approach for games played over time in Section 6.3 and discuss some theoretical results in Section 6.4. We then continue by discussing the formulations with non-uniform game periods in Section 6.5. The simulation results on players' performance is provided in Section 6.6. In Section 6.7, we discuss how the non-uniform horizon parameters affect consensus and clustering of agents. Numerical examples in these consensus and clustering topic is provided in Section 6.8. We conclude the chapter in Section 6.9. Lastly, in Section 6.10, we provide a brief discussion regarding the ongoing work of incomplete games formulation.

In regard to the representations associated with players' actions and parameters, we put * and $'$ to denote optimal strategies in some different aspects. On the other hand, subscripts of some notations indicate time indices.

The content in this chapter regarding the players' performance is published in a

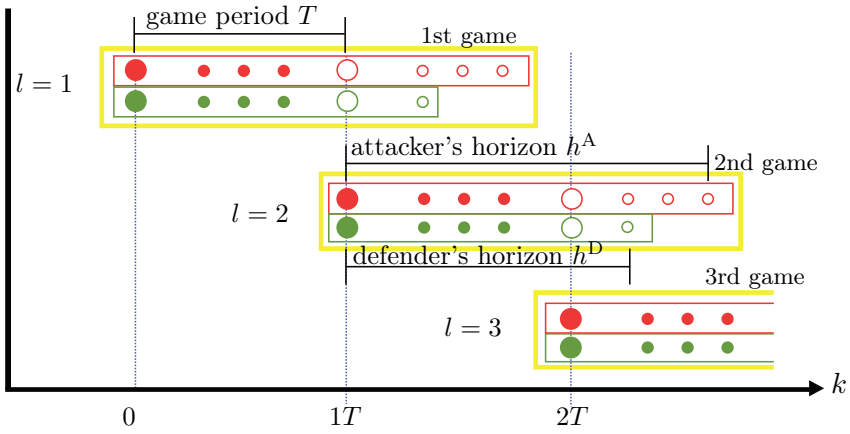


Figure 6.1 Illustration of the games played over discrete time k with rolling horizon approach for the players, where the players have different horizon lengths h^{A} and h^{D}.

journal article [J2], which is a short extension of a conference article [C6]. On the other hand, the discussion on clustering and consensus given non-uniform horizon is part of a manuscript submitted for conference publication [O5].

6.2 Problem formulation

We explore a multiagent system of n agents communicating to each other in discrete time in the face of jamming attacks. The network topology for the normal operation is given by an undirected and connected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. Each agent i has the scalar state x_i following the discrete consensus update rule at time $k \in \mathbb{N}_0$ (2.3)-(2.4) as explained in Chapter 2 and also used in Chapter 5.

The attacker is capable to block the communication by jamming some targeted edges, represented by the removal of edges in $\mathcal{G}$. On the other hand, we suppose that there is a defender that has the capability to maintain the communication among the agents, e.g., by asking agents to send even stronger communication signals to overcome the jamming signals. These are represented by the action of rebuilding some of the attacked edges.

From this occurence of attacks and recoveries, we characterize the attack-recovery process as a two-player game between the attacker and the defender in terms of the communication among the agents of the network. In other words, we may say that the graphs characterizing the networked system are *resilient* if the group of agents is able to recover from the damages caused by the attacker. However, there may be cases where the resiliency of the graph is reduced due to the stronger attack signals. In this chapter, we consider the case where the attacker has two types of jamming signals in terms of their strength, *strong* and *normal*. The defender is able to recover only the edges that are attacked with normal strength. In the following subsections, we first describe the

order of attack and recovery actions in one sequence and characterize some constraints that we impose as well as the objective of the problem.

6.2.1 Attack-recovery sequence

In our setting, the players make their attack/recovery actions at every discrete time $k \in \mathbb{N}_0$. At time k, the players decide to attack/recover certain edges in the two stages, with the attacker acting first, followed by the defender. Specifically, at time k the attacker attacks $\mathcal{G}$ by deleting $\mathcal{E}_k^{\mathrm{A}} \subseteq \mathcal{E}$ with normal jamming signals and $\overline{\mathcal{E}}_k^{\mathrm{A}} \subseteq \mathcal{E}$ with strong jamming signals with $\mathcal{E}_k^{\mathrm{A}} \cap \overline{\mathcal{E}}_k^{\mathrm{A}} = \emptyset$, whereas the defender recovers $\mathcal{E}_k^{\mathrm{D}} \subseteq \mathcal{E}$ (note that the defender may attempt to recover the edges that are either unattacked or attacked strongly). Due to the attacks and then the recoveries at time k, the network changes from $\mathcal{G}$ to $\mathcal{G}_k^{\mathrm{A}} := (\mathcal{V}, \mathcal{E} \setminus (\mathcal{E}_k^{\mathrm{A}} \cup \overline{\mathcal{E}}_k^{\mathrm{A}}))$ and further to $\mathcal{G}_k^{\mathrm{D}} := (\mathcal{V}, (\mathcal{E} \setminus (\mathcal{E}_k^{\mathrm{A}} \cup \overline{\mathcal{E}}_k^{\mathrm{A}})) \cup (\mathcal{E}_k^{\mathrm{D}} \cap \mathcal{E}_k^{\mathrm{A}}))$. The agents then communicate to their neighbors at time k based on this resulting graph $\mathcal{G}_k^{\mathrm{D}}$.

In this chapter, we formulate the game where the players attempt to choose the best strategies in terms of edges attacked/recovered to maximize their own utility functions. With $l \in \mathbb{N}$, here the lth game is defined over the horizon of h^{A} and h^{D} steps for the attacker and the defender, respectively, and played every T steps of game period from time $(l-1)T$ to $(l-1)T + \max\{h^{\mathrm{A}}, h^{\mathrm{D}}\} - 1$. Since the game period should be within the horizon, we assume that $1 \leq T \leq \min\{h^{\mathrm{A}}, h^{\mathrm{D}}\}$. The players make decisions in a rolling horizon fashion as explained more in Section 6.3; the optimal strategies obtained at $(l-1)T$ for the future time may change when the players recalculate their strategies at the future time lT. Figure 6.1 illustrates the discussed rolling horizon game over time; the filled circles indicate the applied strategies and the empty circles indicate the strategies of the game that are discarded.

When a player has a longer horizon length, it indicates that it has a better computational ability relative to its opponent, since the computational burden is directly related to the horizon length (explained in Section 6.3 later). It is expected that the player with a longer horizon length can perform better in general. This topic on the relationship between the ability of players to calculate several strategies in the future and their performance is discussed, e.g., in chess, where better players search for a move more extensively and deeply [94]. A related approach to calculate players' optimal strategies in such games is discussed in [95].

6.2.2 Energy constraints

The actions of the attacker and the defender are affected by the constraints on the energy availability, which is assumed in this chapter to increase linearly in time; furthermore, the energy consumed by the players is proportional to the number of the planned attacked/recovered edges, as explained in Chapter 2, with initial energy κ^{A} and κ^{D} and constant supply rates ρ^{A} and ρ^{D} for the attacker and the defender, respectively. For example, this models devices which are able to supply energy wirelessly to obstruct/retain communication signals between the agents.

Recall that the attacker has two types of jamming signals, strong and normal. Here, the strong attacks on $\overline{\mathcal{E}}_k^{\mathrm{A}}$ take $\overline{\beta}^{\mathrm{A}} > 0$ energy per edge per unit time compared to the normal attacks on $\mathcal{E}_k^{\mathrm{A}}$, which take $\beta^{\mathrm{A}} > 0$ where $\overline{\beta}^{\mathrm{A}} > \beta^{\mathrm{A}}$. The total energy used by the attacker is constrained as

$$\sum_{m=0}^{k} (\overline{\beta}^{\mathrm{A}} |\overline{\mathcal{E}}_m^{\mathrm{A}}| + \beta^{\mathrm{A}} |\mathcal{E}_m^{\mathrm{A}}|) \leq \kappa^{\mathrm{A}} + \rho^{\mathrm{A}} k \tag{6.1}$$

for any time k, where $\kappa^{\mathrm{A}} \geq \rho^{\mathrm{A}} > 0$. This energy constraint restricts and upper bounds the number of edges that the attacker can attack.

The energy constraint of the defender, which is similar to (6.1), is given by

$$\sum_{m=0}^{k} \beta^{\mathrm{D}} |\mathcal{E}_m^{\mathrm{D}}| \leq \kappa^{\mathrm{D}} + \rho^{\mathrm{D}} k \tag{6.2}$$

with $\kappa^{\mathrm{D}} \geq \rho^{\mathrm{D}} > 0$, $\beta^{\mathrm{D}} > 0$. Recall that the defender can recover only the edges in $\mathcal{E}_k^{\mathrm{A}}$ under normal jamming attacks. With $\mathcal{E}_k^{\mathrm{D}} \subseteq \mathcal{E}$, it is possible that the defender wastes its resources by recovering the strongly attacked edges, for example. The effect of the energy usage of the players, especially the defender, on the networks is discussed later in this chapter. These constraints can also be illustrated by Fig. 5.2 in Chapter 5.

6.2.3 Agents clustering

By attacking, the attacker makes the graph disconnected and separates the agents into clusters (i.e., sets of agents). We introduce a few notions related to grouping/clustering of agents. For a given subgraph $\mathcal{G}' = (\mathcal{V}, \mathcal{E}')$ where $\mathcal{E}' \subseteq \mathcal{E}$, we say that the agents are grouped into $\overline{n}(\mathcal{G}')$ number of *groups*, if the sets of agents $\mathcal{V}_1', \mathcal{V}_2', \ldots, \mathcal{V}_{\overline{n}(\mathcal{G}')}' \subseteq \mathcal{V}$ satisfy $\cup_{a=1}^{\overline{n}(\mathcal{G}')} \mathcal{V}_a' = \mathcal{V}$ and $\mathcal{V}_a' \cap \mathcal{V}_b' = \emptyset$ if $a \neq b$. There is no edge connecting different groups, i.e., $e_{ij} \notin \mathcal{E}'$ for $i \in \mathcal{V}_a', j \in \mathcal{V}_b'$.

Here, we also use the notion of agent-group index as previously explained in Chapter 4, which is given by

$$c(\mathcal{G}') := \sum_{a=1}^{\overline{n}(\mathcal{G}')} |\mathcal{V}'_a|^2 - |\mathcal{V}|^2. \tag{4.7}$$

Note that $c(\mathcal{G}')$ is always negative when $\mathcal{G}'$ is disconnected, whereas $c(\mathcal{G}') = 0$ if $\mathcal{G}'$ remains connected.

The attacker and the defender's utility functions of the lth game (lth decision-making opportunity), $l \in \mathbb{N}$, starting at time $k = (l-1)T$, take account of the agent-group index $c(\cdot)$ over time horizons $h^{\mathrm{A}}, h^{\mathrm{D}} \geq 1$ from time $(l-1)T$ to $(l-1)T + \max\{h^{\mathrm{A}}, h^{\mathrm{D}}\} - 1$. Specifically, the utility functions at the lth game are defined by

$$U_k^{\mathrm{A}} := \sum_{k=(l-1)T}^{(l-1)T+h^{\mathrm{A}}-1} -c(\mathcal{G}_k^{\mathrm{D}}), \tag{6.3}$$

$$U_k^{\mathrm{D}} := \sum_{k=(l-1)T}^{(l-1)T+h^{\mathrm{D}}-1} c(\mathcal{G}_k^{\mathrm{D}}). \tag{6.4}$$

With the rolling horizon approach, the players will be able to manage the usage of their energy better. The player with a longer horizon length is expected to use their energy more efficiently, and thus obtain a higher utility over time.

6.3 Game structure with non-uniform rolling horizon lengths

We are interested in finding the subgame perfect equilibrium of this game. To find the equilibrium, the game is divided into some subgames/decision-making points. The subgame perfect equilibrium must be an equilibrium in every subgame. The optimal strategy of each player is obtained by using a backward induction approach, i.e., by finding the equilibrium from the smallest subgames. The tie-break condition happens when the players' strategies result in the same utility. In this case, we suppose that the players choose to save their energy by attacking/recovering less edges; otherwise, i.e., they have enough energy to attack/recover all edges in every subsequent steps, then they will attack/recover more edges, given the same resulting utility.

In this chapter we consider the situation where the attacker and the defender have different horizon lengths denoted by h^{A} and h^{D}, respectively. The difference in the horizon lengths corresponds to the different ability of the players to solve the game.

Due to the nature of the rolling horizon approach, the strategies obtained for the lth

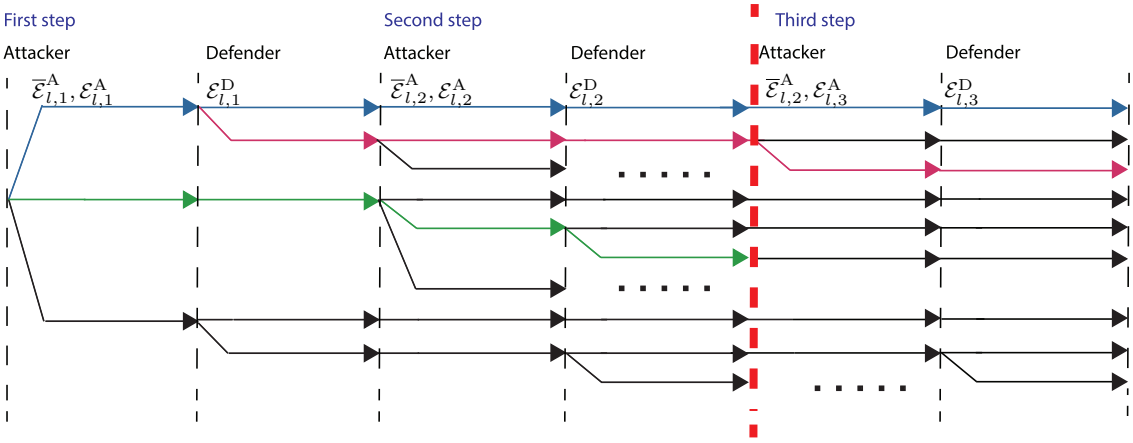


Figure 6.2 Extensive-form game for $h^{\mathrm{A}} = 3$ and $h^{\mathrm{D}} = 2$.

game, i.e., attacked and recovered edges, are applied only from time $(l-1)T$ to $lT-1$ with $T \leq \min\{h^{\mathrm{A}}, h^{\mathrm{D}}\}$. Note that T is set to be the same for the players. The players' strategies at the lth game are specified as $((\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{D}}_{l,1}), \ldots, (\overline{\mathcal{E}}^{\mathrm{A}}_{l,h^{\mathrm{D}}}, \mathcal{E}^{\mathrm{A}}_{l,h^{\mathrm{D}}}, \mathcal{E}^{\mathrm{D}}_{l,h^{\mathrm{D}}}), (\overline{\mathcal{E}}^{\mathrm{A}}_{l,h^{\mathrm{D}}+1}, \mathcal{E}^{\mathrm{A}}_{l,h^{\mathrm{D}}+1}), \ldots, (\overline{\mathcal{E}}^{\mathrm{A}}_{l,h^{\mathrm{A}}}, \mathcal{E}^{\mathrm{A}}_{l,h^{\mathrm{A}}}))$ if $h^{\mathrm{A}} > h^{\mathrm{D}}$, and $((\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{D}}_{l,1}), \ldots, (\overline{\mathcal{E}}^{\mathrm{A}}_{l,h^{\mathrm{A}}}, \mathcal{E}^{\mathrm{A}}_{l,h^{\mathrm{A}}}, \mathcal{E}^{\mathrm{D}}_{l,h^{\mathrm{A}}}), \mathcal{E}^{\mathrm{D}}_{l,h^{\mathrm{A}}+1}, \ldots, \mathcal{E}^{\mathrm{D}}_{l,h^{\mathrm{D}}})$ if $h^{\mathrm{A}} < h^{\mathrm{D}}$, with $\overline{\mathcal{E}}^{\mathrm{A}}_{l,\alpha}, \mathcal{E}^{\mathrm{A}}_{l,\alpha}, \mathcal{E}^{\mathrm{D}}_{l,\alpha}$ indicating the strategies at the αth step of the lth game, $\alpha \in \mathbb{N}$. Note that here we show the strategies with two subscripts representing the game and the step indices along the time axis. If $h^{\mathrm{A}} > h^{\mathrm{D}}$, only the attacker formulates its strategies after h^{D}th step. Similarly, if $h^{\mathrm{A}} < h^{\mathrm{D}}$, only the defender formulates its strategies after h^{A}th step. In the case of $h^{\mathrm{A}} = h^{\mathrm{D}}$, both players obtain their strategies until $(h^{\mathrm{A}} = h^{\mathrm{D}})$th step, denoted by $((\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{D}}_{l,1}), \ldots, (\overline{\mathcal{E}}^{\mathrm{A}}_{l,h^{\mathrm{A}}}, \mathcal{E}^{\mathrm{A}}_{l,h^{\mathrm{A}}}, \mathcal{E}^{\mathrm{D}}_{l,h^{\mathrm{A}}}))$.

However, since the game is played in a rolling horizon fashion, only $((\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{D}}_{l,1}), \ldots, (\overline{\mathcal{E}}^{\mathrm{A}}_{l,T}, \mathcal{E}^{\mathrm{A}}_{l,T}, \mathcal{E}^{\mathrm{D}}_{l,T}))$ is applied (recall that h^{A} and h^{D} are taken to be greater than or equal to T). Here the strategies applied can be written in single subscripts of time indices as $((\overline{\mathcal{E}}^{\mathrm{A}}_{(l-1)T}, \mathcal{E}^{\mathrm{A}}_{(l-1)T}, \mathcal{E}^{\mathrm{D}}_{(l-1)T}), \ldots, (\overline{\mathcal{E}}^{\mathrm{A}}_{lT-1}, \mathcal{E}^{\mathrm{A}}_{lT-1}, \mathcal{E}^{\mathrm{D}}_{lT-1})) = ((\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{D}}_{l,1}), \ldots, (\overline{\mathcal{E}}^{\mathrm{A}}_{l,T}, \mathcal{E}^{\mathrm{A}}_{l,T}, \mathcal{E}^{\mathrm{D}}_{l,T}))$. We assume that the values of h^{A} and h^{D} are known to both players. Note that this game is not necessarily zero-sum.

In what follows, we provide an example of a small scale to detail how the optimal edges can be obtained in our game setting. To this end, suppose that $h^{\mathrm{A}} = 3$ and $h^{\mathrm{D}} = 2$. The optimal strategies $((\overline{\mathcal{E}}^{\mathrm{A}*}_{l,1}, \mathcal{E}^{\mathrm{A}*}_{l,1}, \mathcal{E}^{\mathrm{D}*}_{l,1}), (\overline{\mathcal{E}}^{\mathrm{A}*}_{l,2}, \mathcal{E}^{\mathrm{A}*}_{l,2}, \mathcal{E}^{\mathrm{D}*}_{l,2}), (\overline{\mathcal{E}}^{\mathrm{A}*}_{l,3}, \mathcal{E}^{\mathrm{A}*}_{l,3}))$ of the players at the game with index l are obtained backward in time (from Step $\alpha = 3$ to Step $\alpha = 1$) and is given by:

- Step 3:

$$(\overline{\mathcal{E}}^{\mathrm{A}*}_{l,3}(\mathcal{E}^{\mathrm{D}}_{l,2}), \mathcal{E}^{\mathrm{A}*}_{l,3}(\mathcal{E}^{\mathrm{D}}_{l,2})) \in \underset{(\overline{\mathcal{E}}^{\mathrm{A}}_{l,3}, \mathcal{E}^{\mathrm{A}}_{l,3})}{\arg\max}\, U^{\mathrm{A}}_{l,3}(\mathcal{E}^{\mathrm{D}*}_{l,3}) \tag{6.5}$$

$$\text{where } \mathcal{E}^{\mathrm{D}*}_{l,3}(\overline{\mathcal{E}}^{\mathrm{A}}_{l,3}, \mathcal{E}^{\mathrm{A}}_{l,3}) \in \underset{\mathcal{E}^{\mathrm{D}}_{l,3}}{\arg\max}\, -U^{\mathrm{A}}_{l,3}, \tag{6.6}$$

- Step 2:

$$\mathcal{E}^{\mathrm{D}*}_{l,2}(\overline{\mathcal{E}}^{\mathrm{A}}_{l,2}, \mathcal{E}^{\mathrm{A}}_{l,2}) \in \underset{\mathcal{E}^{\mathrm{D}}_{l,2}}{\arg\max}\, U^{\mathrm{D}}_{l,2}, \tag{6.7}$$

$$(\overline{\mathcal{E}}^{\mathrm{A}*}_{l,2}(\mathcal{E}^{\mathrm{D}}_{l,1}), \mathcal{E}^{\mathrm{A}*}_{l,2}(\mathcal{E}^{\mathrm{D}}_{l,1})) \in \underset{(\overline{\mathcal{E}}^{\mathrm{A}}_{l,2}, \mathcal{E}^{\mathrm{A}}_{l,2})}{\arg\max}\, U^{\mathrm{A}}_{l,2}(\mathcal{E}^{\mathrm{D}*}_{l,2}), \tag{6.8}$$

- Step 1:

$$\mathcal{E}^{\mathrm{D}*}_{l,1}(\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1}) \in \underset{\mathcal{E}^{\mathrm{D}}_{l,1}}{\arg\max}\, U^{\mathrm{D}}_{k}(\overline{\mathcal{E}}^{\mathrm{A}\prime}_{l,2}, \mathcal{E}^{\mathrm{A}'}_{l,2}) \tag{6.9}$$

$$\text{where } (\overline{\mathcal{E}}^{\mathrm{A}\prime}_{l,2}(\mathcal{E}^{\mathrm{D}}_{l,1}), \mathcal{E}^{\mathrm{A}'}_{l,2}(\mathcal{E}^{\mathrm{D}}_{l,1})) \in \underset{(\overline{\mathcal{E}}^{\mathrm{A}}_{l,2}, \mathcal{E}^{\mathrm{A}}_{l,2})}{\arg\max}\, -U^{\mathrm{D}}_{l,2}(\mathcal{E}^{\mathrm{D}*}_{l,2}), \tag{6.10}$$

$$(\overline{\mathcal{E}}^{\mathrm{A}*}_{l,1}, \mathcal{E}^{\mathrm{A}*}_{l,1}) \in \underset{(\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1})}{\arg\max}\, U^{\mathrm{A}}_{k}(\mathcal{E}^{\mathrm{D}*}_{l,1}), \tag{6.11}$$

where $U^{\mathrm{A}}_{l,\alpha} := \sum_{k=(l-1)T+\alpha-1}^{(l-1)T+h^{\mathrm{A}}-1} -c(\mathcal{G}^{\mathrm{D}}_k)$ (resp., $U^{\mathrm{D}}_{l,\alpha} := \sum_{k=(l-1)T+\alpha-1}^{(l-1)T+h^{\mathrm{D}}-1} c(\mathcal{G}^{\mathrm{D}}_k)$) is defined as parts of U^{A}_k (resp., U^{D}_k) calculated from the αth step to the h^{A}th (resp., h^{D}th) step of the lth game.

Once again, these optimization problems are solved backward from the $\max\{h^{\mathrm{A}}, h^{\mathrm{D}}\} =$ 3rd step of the lth game. Note that to find $(\overline{\mathcal{E}}^{\mathrm{A}*}_{l,1}, \mathcal{E}^{\mathrm{A}*}_{l,1})$ in (6.11), one needs to obtain $(\mathcal{E}^{\mathrm{D}*}_{l,1}(\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1}))$ in (6.9) beforehand. Likewise, to find $(\mathcal{E}^{\mathrm{D}*}_{l,1}(\overline{\mathcal{E}}^{\mathrm{A}}_{l,1}, \mathcal{E}^{\mathrm{A}}_{l,1}))$ in (6.9), one needs to obtain $(\overline{\mathcal{E}}^{\mathrm{A}*}_{l,2}(\mathcal{E}^{\mathrm{D}}_{l,1}), \mathcal{E}^{\mathrm{A}*}_{l,2}(\mathcal{E}^{\mathrm{D}}_{l,1}))$ in (6.8), and so on. Also, note that while $\mathcal{E}^{\mathrm{D}*}_{l,3}$ is not part of the defender's strategy, it is still needed for the attacker to obtain $(\overline{\mathcal{E}}^{\mathrm{A}*}_{l,3}, \mathcal{E}^{\mathrm{A}*}_{l,3})$ in (6.5). Therefore, outside the defender's ability characterized by its horizon length h^{D}, here we suppose that the attacker utilizes the strategy that emulates the defender's best response with a longer horizon, i.e., from part of utility functions $-U^{\mathrm{A}}_k$ (which is not equal to U^{D}_l due to the horizon inadequacy).

In the steps with index $\alpha \leq h^{\mathrm{D}}$, the defender assumes that the attacker's optimal edges, e.g., in (6.10), are based on the defender's utility function, which consists of $h^{\mathrm{D}} < h^{\mathrm{A}}$ steps only. Also, in this game the defender's optimal strategies, e.g., in (6.9), are based on the defender's perception of the attacker's optimal strategies, i.e., $(\overline{\mathcal{E}}^{\mathrm{A}\prime}_{l,2}, \mathcal{E}^{\mathrm{A}\prime}_{l,2})$, since the defender is not able to foresee the attacker's strategy beyond h^{D}. For the attacker, since it is able to compute the optimal strategy for the defender as well (due

to longer h^{A}), the attacker's strategies in the steps with index $\alpha \leq h^{\mathrm{D}}$, e.g., (6.8) and (6.11), are based on the defender's optimal edges $\mathcal{E}^{\mathrm{D}*}_{l,\alpha}$.

In this setting, since the defender's strategy depends on the attacker's strategy as well, i.e., the defender can only recover edges attacked normally, it is possible that the defender cannot apply its strategy when the attacker changes its own strategy. In this case, the defender will apply the strategy only on the edges that can be recovered.

The decision-making process of the players in this example is illustrated in the game tree in Figure 6.2, where the blue line indicates the *equilibrium path.* i.e., the strategy taken by the player following backward induction, if $h^{\mathrm{A}} = h^{\mathrm{D}} = 3$. The green line indicates the equilibrium path if $h^{\mathrm{A}} = h^{\mathrm{D}} = 2$ and the magenta line indicates the equilibrium path if $h^{\mathrm{A}} = 3, h^{\mathrm{D}} = 2$. The vertical dashed lines denote the different steps of the game, whereas the dashed red line denotes boundary (min{2,3}) of different players' horizon lengths. The optimization beyond this boundary is done by only the player with a longer horizon (in this case the attacker). In step 2, the attacker assumes that $\mathcal{E}^{\mathrm{D}*}_{l,2}$ comes from utility over $h^{\mathrm{A}} = 3$. The case where $h^{\mathrm{A}} < h^{\mathrm{D}}$ can be similarly described. These optimization problems are solved by the players at every game period T.

It is clear that with a longer T, the players play this game less often and apply their obtained strategies for more time steps. Note that with $T = \min\{h^{\mathrm{A}}, h^{\mathrm{D}}\}$, the player with a shorter horizon length does not change its strategies at all, thus effectively removing the rolling horizon aspect of the player. In this game, we will find the optimal strategies of the players by computing all possible combinations, since the choices of edges are finite.

From the optimization problems in (6.6)–(6.11) above, the player with a shorter horizon length $h_{\mathrm{short}} \in \{h^{\mathrm{A}}, h^{\mathrm{D}}\}$ examines at most $3^{|\mathcal{E}|}2^{|\mathcal{E}|}h_{\mathrm{short}}$ number of combinations for utility evaluations, since the player has to foresee the opponent's response as well. Note that the attacker has three possible actions on an edge: no attack, attack with normal signals, and attack with strong signals. On the other hand, the player with a longer horizon length $h_{\mathrm{long}} \in \{h^{\mathrm{A}}, h^{\mathrm{D}}\}$ examines at most $(3^{|\mathcal{E}|}2^{|\mathcal{E}|})(h_{\mathrm{long}} - h_{\mathrm{short}}) + (3^{|\mathcal{E}|} + 3^{|\mathcal{E}|}2^{|\mathcal{E}|})h_{\mathrm{long}}$ combinations.

In this section, we have explained the problem setting where it is assumed that the players may not have the same computational ability represented by the different values of horizon lengths h^{A} and h^{D}. Without the assumption of the horizon length discrepancy, the most related results are given in Chapter 5 where the players have the same ability to compute their strategies, represented by $h^{\mathrm{A}} = h^{\mathrm{D}} = h$. There, we do not discuss the effect of the horizons on the players' performance; we instead focus

more on the necessary and sufficient condition of agents clustering at infinite time, given the consensus dynamics. Other related papers include [61] which considers the one-shot attack-recovery games. This formulation is the extension of Chapter 3 where the repeated attack-recovery games without rolling horizon approach in continuous time is considered. Specifically, the timings for launching attack/defense actions are also part of the decision variables.

6.4 Players' performance with non-uniform horizon lengths

The utility functions defined in (6.3) and (6.4) are considered for deriving the best strategies for the players. As explained in Section 2.1 above, the last several actions for the players may be discarded from the obtained strategies and replaced by a new set of actions calculated in the next game. As a consequence, the resulting values of the agent-group index at time k is given by $c(\mathcal{G}_k^{\mathrm{D}*})$, with $\mathcal{G}_k^{\mathrm{D}*} = (\mathcal{V}, ((\mathcal{E} \setminus (\overline{\mathcal{E}}_k^{\mathrm{A}*} \cup \mathcal{E}_k^{\mathrm{A}*})) \cup (\mathcal{E}_k^{\mathrm{D}*} \cap \mathcal{E}_k^{\mathrm{A}*}))$. We now characterize how the horizon lengths h^{A} and h^{D} affect the *applied utilities* $\hat{U}_k^{\mathrm{A}} := -c(\mathcal{G}_k^{\mathrm{D}*})$ and $\hat{U}_k^{\mathrm{D}} := c(\mathcal{G}_k^{\mathrm{D}*})$. These are elements of the utility functions U_k^{A} and U_k^{D} corresponding to the αth step, with $\alpha = k \bmod T + 1$, of the game with index $l = \lfloor k/T \rfloor + 1$, where the obtained strategies $(\overline{\mathcal{E}}_{(l-1)T+\alpha-1}^{\mathrm{A}*}, \mathcal{E}_{(l-1)T+\alpha-1}^{\mathrm{A}*}, \mathcal{E}_{(l-1)T+\alpha-1}^{\mathrm{D}*}) = (\overline{\mathcal{E}}_{l,\alpha}^{\mathrm{A}*}, \mathcal{E}_{l,\alpha}^{\mathrm{A}*}, \mathcal{E}_{l,\alpha}^{\mathrm{D}*})$ are applied.

We first state a result implying that when the attacker has large enough energy supply characterized by ρ^{A}, the optimal strategies of both players do not depend on the horizon lengths. Specifically, if $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq |\mathcal{E}|$, then the attacker will attack all edges of the underlying graph $\mathcal{G}$ at any time k, making the optimal strategies independent of h^{A} and h^{D}.

The results afterwards illustrate the performance of the players for different h^{A} and h^{D} in separate subsections assuming that

$$\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < |\mathcal{E}|. \tag{6.12}$$

6.4.1 Attacker's strategies with varying h^{A}

To show the change of the attacker's strategies, we consider certain scenarios where the defender's strategies are less reliant on the attacker's action. Specifically, by assuming certain values of ρ^{D} and β^{D}, it is possible that the defender's optimal strategies are always to recover all $\mathcal{E}_k^{\mathrm{A}}$.

In this subsection, we further assume that

$$\rho^{\mathrm{D}}/\beta^{\mathrm{D}} > |\mathcal{E}|, \tag{6.13}$$

implying that ρ^{D} is large enough so that there is always recovery from normally attacked edges at any step of the game. Furthermore, in Propositions 6.2 and 6.3 below, we suppose for simplicity of obtaining theoretical assertions that

$$\kappa^{\mathrm{A}} = \rho^{\mathrm{A}}, \tag{6.14}$$

i.e., the attacker has the same amount of supplied energy at any k, including at $k = 0$.

We first state a lemma describing a property of a class of graphs under attacks, where it is better for the attacker to attack as soon as it has the energy, rather than saving it to attack more edges later. For the statement of the following results, let $\overline{c}(\xi) := \min_{|\mathcal{E}'|=\xi} c((\mathcal{V}, \mathcal{E} \setminus \mathcal{E}'))$ denote the smallest value of agent-group index given the number of strongly attacked edges $\xi (< n-1)$.

Lemma 6.1. Consider the case where the network topology $\mathcal{G}$ of the agents is given as the star graph and the attacker attacks ξ number of edges with strong signals. Suppose (6.12)–(6.13) hold. Then, for time interval $\hat{k}$, $\hat{k}\overline{c}(\xi) \leq \overline{c}(\hat{k}\xi)$ is always satisfied for any $\hat{k} \leq (n-1)/\xi$.

In Lemma 6.1, we state that in the star graph attacking a few edges every time results in a more negative agent-group index compared to saving energy and only attacking later. For example, attacking one edge for $k = 1, 2$ results in a more negative $c(\mathcal{G}_1^{\mathrm{D}}) + c(\mathcal{G}_2^{\mathrm{D}})$ over $\hat{k} = 2$ interval than attacking two edges only for one time $k = 2$; $(n-1)^2 + (n-1)^2 \leq n^2 + (n-2)^2$ from (4.7) is always satisfied (note that the value of agent-group index is zero if there is no attack).

Proposition 6.2. Consider the case where the network topology $\mathcal{G}$ of the agents is given by any tree graph. Suppose that (6.12)–(6.14) hold. Then, the value of $\sum_{k=0}^{\overline{k}} \hat{U}_k^{\mathrm{A}}$ does not depend on h^{A} or T, for any time $\overline{k}$.

We continue by stating a result on the complete graph $\mathcal{G}$, where in a low energy situation characterized by small $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}$, the attacker with longer h^{A} always has better utility.

Proposition 6.3. Consider the complete graph $\mathcal{G}$. If (6.12)–(6.14) and $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < (n-2)/T$ are satisfied, then $0 = \sum_{k=0}^{\overline{k}} \hat{U}_k^{\mathrm{A}}(h^{\mathrm{A}} = T) \leq \sum_{k=0}^{\overline{k}} \hat{U}_k^{\mathrm{A}}(h^{\mathrm{A}} > T)$ for any $\overline{k}$.

In Proposition 6.4 below, we state that the attacker with a shorter h^{A} in any $\mathcal{G}$ may perform better if we measure the applied utility over a shorter interval.

Proposition 6.4. Suppose that (6.12) and (6.13) are satisfied. In any $\mathcal{G}$, it follows that $\sum_{k=0}^{\overline{k}} \hat{U}_k^{\mathrm{A}}(h^{\mathrm{A}}=1) \geq \sum_{k=0}^{\overline{k}} \hat{U}_k^{\mathrm{A}}(h^{\mathrm{A}}>1)$ for any time $\overline{k} < \lfloor \kappa^{\mathrm{A}}/(|\mathcal{E}|\overline{\beta}^{\mathrm{A}} - \rho^{\mathrm{A}}) \rfloor$.

6.4.2 Defender's strategies with varying h^{D}

In this section, we discuss the characterization of $\hat{U}_k^{\mathrm{D}}$ of the defender given different values of h^{D}. We first state a lemma describing a property of an attacked empty graph $(\mathcal{V}, \emptyset)$, where it is better for the defender to save its energy and use it later to recover more edges. For the statement of the following results, let $c'(\theta) := \max_{|\mathcal{E}'|=\theta} c((\mathcal{V}, \mathcal{E}'))$ denote the largest value of agent-group index given the number of recovered edges θ. As a consequence, $\sum_{k=0}^{\hat{k}} c'(\theta) = \hat{k}c'(\theta)$ indicates the energy consumption when the number of recovered edges is θ for $\hat{k}$ steps.

Lemma 6.5. Assume that the attacker attacks all edges $\mathcal{E}$ with normal signals at all time. Let θ be the number of recovered edges. If (6.12) is satisfied, then

$$\hat{k}c'(\theta) \leq (\hat{k}-1)c'(0) + c'(\hat{k}\theta) \tag{6.15}$$

for any time interval $\hat{k} \leq (n-1)/\theta$ for any $\theta = 1, \ldots, n-1$.

From (6.4), we note that the defender prefers strategies that result in larger value of $c(\mathcal{G}_k^{\mathrm{D}})$ over time. Thus, by Lemma 6.5, we see that recovering later is better for the defender, which is different from Lemma 6.1 for the attacker where attacking immediately is better.

We now continue by assuming certain values of the attacker's energy parameters so that its strategies do not change regardless of the defender's response. Specifically, we now assume that

$$\kappa^{\mathrm{A}} = \rho^{\mathrm{A}} = \beta^{\mathrm{A}}|\mathcal{E}|, \quad \overline{\beta}^{\mathrm{A}}/\beta^{\mathrm{A}} > h^{\mathrm{A}}|\mathcal{E}| \tag{6.16}$$

are satisfied, i.e., attacking with strong signals takes much energy so that it is not affordable for the attacker to take such actions at any time. Note that with $\rho^{\mathrm{A}} = \beta^{\mathrm{A}}|\mathcal{E}|$, the attacker will be able to attack all edges normally at all time; furthermore, with $\overline{\beta}^{\mathrm{A}}/\beta^{\mathrm{A}} > h^{\mathrm{A}}|\mathcal{E}|$ the attacker will never have enough energy to attack any edge with strong signals at any step of the game. Therefore, any attacked edge at any time can be recovered.

In Proposition 6.6, similar to Proposition 6.4 above, we now state that the defender with a shorter h^{D} may perform better if we measure the applied utility over a shorter

interval. Note that this result does not depend on the topology of the underlying graph $\mathcal{G}$, similar to the one in Proposition 6.4 above.

Proposition 6.6. Suppose that $\rho^{\mathrm{D}}/\beta^{\mathrm{D}} < n-1$ and (6.16) are satisfied. Then $\sum_{k=0}^{\overline{k}} U_k^{\mathrm{D}}(h^{\mathrm{D}} = 1) \geq \sum_{k=0}^{\overline{k}} U_k^{\mathrm{D}}(h^{\mathrm{D}} > 1)$ is satisfied, with $\overline{k} < \lfloor \frac{\kappa^{\mathrm{D}}}{(n-1)\beta^{\mathrm{D}} - \rho^{\mathrm{D}}} \rfloor$.

While we do not obtain the general condition that ensures a higher utility for longer h^{A} (resp., longer h^{D}), in Section 6.6 we will show in a numerical simulation that with longer horizons the attacker (resp., the defender) generally obtains more applied utility over longer time.

6.5 Game structure and players' performance with non-uniform game periods

6.5.1 Game structure with non-uniform game periods

Games where players update their strategies in an asynchronous manner can be used to model several real-life interaction. For example, decisions involving firms from various countries cannot be done simultaneously due to different working time in [96, 97]. We extend this approach by discussing how the asynchronous moves represented by non-uniform game periods affect players' performance and agent states over time in the context of multiagent systems.

In this section, we extend the problem formulation by generalizing the game period T into T^{A} and T^{D} for the attacker and the defender, respectively. These periods T^{A} and T^{D} are known by both players for simplicity of the analysis. To ensure that both players are able to obtain their own strategies at any k, we set $T^{\mathrm{A}} \leq h^{\mathrm{A}}$ and $T^{\mathrm{D}} \leq h^{\mathrm{D}}$. Fig. 6.3 illustrates the game with non-uniform game periods; the attacker's and the defender's horizon lengths, i.e., how far in the future players look ahead when determining their strategies, are $h^{\mathrm{A}} = 3$ and $h^{\mathrm{D}} = 2$, respectively, whereas the game periods, i.e., how often players update their strategies, are denoted by $T^{\mathrm{A}} = 1$ and $T^{\mathrm{D}} = 2$. Each of the yellow rectangle indicates a game consisting of the set of *decision-making processes*, which follows a certain pattern. A game is played, i.e., both players simultaneously update their strategies, every lowest common multiple of T^{A} and T^{D} denoted as $\mathrm{lcm}(T^{\mathrm{A}}, T^{\mathrm{D}})$; in Figure 6.3, the game is played every 2 time steps. With this formulation, it is expected that the players have better performance with shorter T^{A} and T^{D} since they can adapt to the changes faster.

From Figure 6.3, we see that the players may not formulate their strategies at the same time. For example, at time $k = 1$, only the attacker updates its strategies, whereas

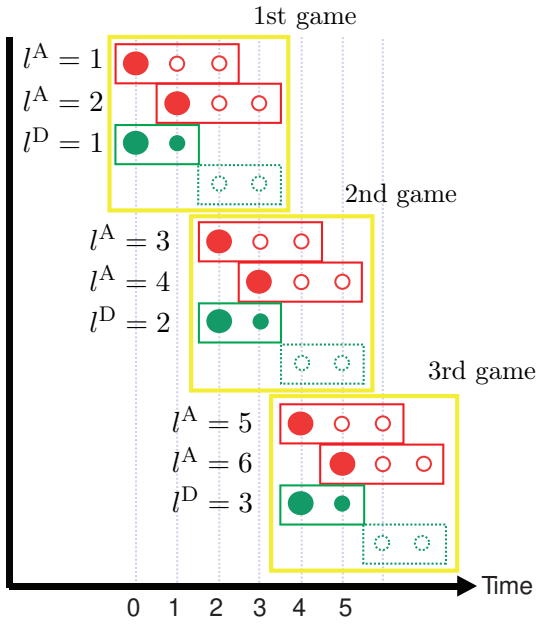


Figure 6.3 Sequence of games with decision-making indices l^{A} and l^{D}: the attacker's horizon (red) and the defender's horizon (green) with non-uniform game periods

the defender does not due to the longer T^{D}. Since T^{A} and T^{D} are known by both players, at $k = 1$ the attacker decides its strategy considering the defender's strategy that is obtained before at $k = 0$. Furthermore, since $h^{\mathrm{A}} = 3$ and $\mathcal{E}^{\mathrm{D}}_{1,2}$ has been determined, here the attacker at $k = 1$ with the ability to compute for three time steps ahead predicts and hence already covers the defender's second decision-making process. This attacker's prediction of the defender's next actions is represented by the green rectangle with dashed lines in Figure 6.3.

Since it is clear that the non-uniform game periods make the players decide their strategies at different times, we specify different decision-making indices l^{A} and l^{D} which occur at times $(l^{\mathrm{A}} - 1)T^{\mathrm{A}}$ and $(l^{\mathrm{D}} - 1)T^{\mathrm{D}}$ for the attacker and the defender, respectively. As a result, the attacker (resp., the defender) does not update its strategy if $k \pmod{T^{\mathrm{A}}} \neq 0$ (resp., $k \pmod{T^{\mathrm{D}}} \neq 0$). The utility functions of the l^{A}th and l^{D}th decision-making processes consisting of α^{A} and α^{D} steps, respectively, are given by

$$U^{\mathrm{A}}_{l^{\mathrm{A}}} := \sum_{k=(l^{\mathrm{A}}-1)T^{\mathrm{A}}}^{(l^{\mathrm{A}}-1)T^{\mathrm{A}}+h^{\mathrm{A}}-1} -c(\mathcal{G}^{\mathrm{D}}_k) = \sum_{\alpha^{\mathrm{A}}=1}^{h^{\mathrm{A}}} -c(\mathcal{G}^{\mathrm{D}}_{l^{\mathrm{A}},\alpha^{\mathrm{A}}}), \tag{6.17}$$

$$U^{\mathrm{D}}_{l^{\mathrm{D}}} := \sum_{k=(l^{\mathrm{D}}-1)T^{\mathrm{D}}}^{(l^{\mathrm{D}}-1)T^{\mathrm{D}}+h^{\mathrm{D}}-1} c(\mathcal{G}^{\mathrm{D}}_k) = \sum_{\alpha^{\mathrm{D}}=1}^{h^{\mathrm{D}}} c(\mathcal{G}^{\mathrm{D}}_{l^{\mathrm{D}},\alpha^{\mathrm{D}}}), \tag{6.18}$$

similar to (6.3) and (6.4) above. Note that different values of these indices for the players may refer to the same time step; e.g., in Figure 6.3, both $l^{\mathrm{A}} = 2$, $\alpha^{\mathrm{A}} = 1$ and $l^{\mathrm{D}} = 1$,

$\alpha^{\mathrm{D}} = 2$ correspond to $k = 1$.

The optimal strategy of the attacker at time $k = 1$ corresponding to $l^{\mathrm{A}} = 2$, i.e., $((\overline{\mathcal{E}}^{\mathrm{A}*}_{2,1}, \mathcal{E}^{\mathrm{A}*}_{2,1}), (\overline{\mathcal{E}}^{\mathrm{A}*}_{2,2}, \mathcal{E}^{\mathrm{A}*}_{2,2}), (\overline{\mathcal{E}}^{\mathrm{A}*}_{2,3}, \mathcal{E}^{\mathrm{A}*}_{2,3}))$ in the case shown in Figure 6.3 (noting that $k \pmod{T^{\mathrm{A}}} = 0$ and $k \pmod{T^{\mathrm{D}}} \neq 0$ for $k = 1$), is obtained backward in time and are given by:

- Step 3 ($k = 3$, $l^{\mathrm{D}} = 2$):

$$(\overline{\mathcal{E}}^{\mathrm{A}*}_{2,3}(\mathcal{E}^{\mathrm{D}}_{2,2}), \mathcal{E}^{\mathrm{A}*}_{2,3}(\mathcal{E}^{\mathrm{D}}_{2,2})) \in \underset{(\overline{\mathcal{E}}^{\mathrm{A}}_{2,3}, \mathcal{E}^{\mathrm{A}}_{2,3})}{\arg\max}\, U^{\mathrm{A}}_{2,3}(\mathcal{E}^{\mathrm{D}\prime}_{2,2}) \tag{6.19}$$
$$\text{where } \mathcal{E}^{\mathrm{D}\prime}_{2,2}(\overline{\mathcal{E}}^{\mathrm{A}}_{2,3}, \mathcal{E}^{\mathrm{A}}_{2,3}) \in \underset{\mathcal{E}^{\mathrm{D}}_{2,2}}{\arg\max} -U^{\mathrm{A}}_{2,3},$$

- Step 2 ($k = 2$, $l^{\mathrm{D}} = 2$):

$$(\overline{\mathcal{E}}^{\mathrm{A}*}_{2,2}(\mathcal{E}^{\mathrm{D}}_{2,1}), \mathcal{E}^{\mathrm{A}*}_{2,2}(\mathcal{E}^{\mathrm{D}}_{2,1})) \in \underset{(\overline{\mathcal{E}}^{\mathrm{A}}_{2,2}, \mathcal{E}^{\mathrm{A}}_{2,2})}{\arg\max}\, U^{\mathrm{A}}_{2,2}(\mathcal{E}^{\mathrm{D}\prime}_{2,1}) \tag{6.20}$$
$$\text{where } \mathcal{E}^{\mathrm{D}\prime}_{2,1}(\overline{\mathcal{E}}^{\mathrm{A}}_{2,2}, \mathcal{E}^{\mathrm{A}}_{2,2}) \in \underset{\mathcal{E}^{\mathrm{D}}_{2,1}}{\arg\max} -U^{\mathrm{A}}_{2,2}(\overline{\mathcal{E}}^{\mathrm{A}*}_{2,3}, \mathcal{E}^{\mathrm{A}*}_{2,3}),$$

- Step 1 ($k = 1$, $l^{\mathrm{D}} = 1$):

$$(\overline{\mathcal{E}}^{\mathrm{A}*}_{2,1}, \mathcal{E}^{\mathrm{A}*}_{2,1}) \in \underset{(\overline{\mathcal{E}}^{\mathrm{A}}_{2,1}, \mathcal{E}^{\mathrm{A}}_{2,1})}{\arg\max}\, U^{\mathrm{A}}_{2}(\mathcal{E}^{\mathrm{D}}_{1}). \tag{6.21}$$

Since the attacker cannot compute more than $h^{\mathrm{A}} = 3$ time steps ahead, in (6.19) and (6.20) above the attacker will use its own utility function $U^{\mathrm{A}}_{l^{\mathrm{A}}}$ to estimate the defender's optimal edges denoted by $\mathcal{E}^{\mathrm{D}\prime}_{2,\alpha}$, i.e., at $l^{\mathrm{D}} = 2$. Since $1 \pmod{T^{\mathrm{D}}} \neq 0$, the defender does not make a new decision and thus will apply the strategy obtained in the previous time instead. Therefore, it is possible for the player with shorter game period (in this case, the attacker) to benefit by changing its strategies; for example, in the case explained above, the attacker may benefit by changing $\mathcal{E}^{\mathrm{A}}_{1}$ to avoid the recovery by the defender $\mathcal{E}^{\mathrm{D}}_{1}$, which has been set and cannot be changed.

The optimization problems explained above vary slightly at each time due to different T^{A} and T^{D}. For example, the optimization problems (6.19)–(6.21) are solved at times $k = i(\mathrm{lcm}(T^{\mathrm{A}}, T^{\mathrm{D}})) + 1$, $i \in \mathbb{N}_0$.

6.5.2 Attacker's strategies with varying T^{A}

In this section, we also explore the performance of the attacker represented by $\hat{U}^{\mathrm{A}}_{k}$ for the non-uniform game periods, similar to the one in Section 6.4 above. We first state

that under some condition, the values of T^{A} and T^{D} do not affect the optimal strategies of the players.

Specifically, we notice that if $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq |\mathcal{E}|$, the attacker attacks all of the edges of $\mathcal{G}$ at any time k, making the optimal strategies, and therefore the applied utilities $\hat{U}_k^{\mathrm{A}}$ and $\hat{U}_k^{\mathrm{D}}$, independent of the values of T^{A} and T^{D}.

We continue by discussing the strategies of the players given that $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < |\mathcal{E}|$, i.e., (6.12), is satisfied. In Corollaries 6.7–6.10 and Proposition 6.8 below, we also suppose that (6.13) and (6.14) are satisfied, for the same reason as in Section 6.4 above. The result in Corollary 6.7 below for the tree graph $\mathcal{G}$ is also similar to the one in Section 6.4, since the optimal strategies for both players do not rely on T^{A}.

Corollary 6.7. Consider the tree graph $\mathcal{G}$. If (6.12)–(6.14) are satisfied, then $\sum_{k=0}^{\overline{k}} \hat{U}_k^{\mathrm{A}}$ does not depend on h^{A} or T^{A}, for any time $\overline{k}$.

We then state the attacker's optimal strategies for $T^{\mathrm{A}} = 1$ under certain situations for the case of the complete graph $\mathcal{G}$, where the attacker with low recharge rate ρ^{A} will not be able to attack any edge at earlier times.

Proposition 6.8. Consider the complete graph $\mathcal{G}$. If (6.12)–(6.14), $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < n-1$, and $T^{\mathrm{A}} = 1$ hold, then the attacker does not attack any edge for $k < \lfloor \frac{(h^{\mathrm{A}}-1)((n-1)-\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}})\rho^{\mathrm{A}}}{\overline{\beta}^{\mathrm{A}}} \rfloor$.

From Proposition 6.8, we are able to characterize the attacker's performance measured by $\sum \hat{U}_k^{\mathrm{A}}$ for different T^{A} values in Corollary 6.9 below.

Corollary 6.9. Consider the complete graph $\mathcal{G}$. If (6.12)–(6.14) and $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < n-1$ hold, then the attacker's applied utilities satisfy $\sum_{k=0}^{\overline{k}} \hat{U}_k^{\mathrm{A}}(T^{\mathrm{A}} = 1) < \sum_{k=0}^{\overline{k}} \hat{U}_k^{\mathrm{A}}(T^{\mathrm{A}} > 1)$, with $\overline{k} < \lfloor (h^{\mathrm{A}} - 1)((n-1) - \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}})(\overline{\beta}^{\mathrm{A}}/\rho^{\mathrm{A}}) \rfloor$.

From Proposition 6.3, we are also able to state that having a shorter T^{A} may help in the situation of low energy characterized by low $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}$.

Corollary 6.10. Consider the complete graph $\mathcal{G}$. If (6.12)–(6.14) and $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < (n-2)/h^{\mathrm{A}}$ are satisfied, then $\sum_{k=0}^{\overline{k}} \hat{U}_k^{\mathrm{A}}(T^{\mathrm{A}} < h^{\mathrm{A}}) \geq \sum_{k=0}^{\overline{k}} \hat{U}_k^{\mathrm{A}}(T^{\mathrm{A}} = h^{\mathrm{A}})$ for any $\overline{k}$.

6.5.3 Defender's strategies with varying T^{D}

In this section, we discuss the optimal strategies of the defender for different T^{D} values. In Proposition 6.11 and Corollary 6.12 below, we suppose that, again for simplicity, (6.16) and $\kappa^{\mathrm{D}} = \rho^{\mathrm{D}}$ are satisfied.

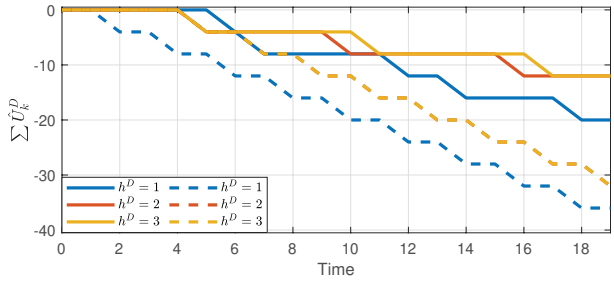


Figure 6.4 Evolution of $\sum \hat{U}_k^{\mathrm{D}}$ for the path graph (solid lines) and the complete graph (dashed lines) with $h^{\mathrm{A}} = 1$; the results for complete graph with $h^{\mathrm{D}} = 2$ and $h^{\mathrm{D}} = 3$ are identical

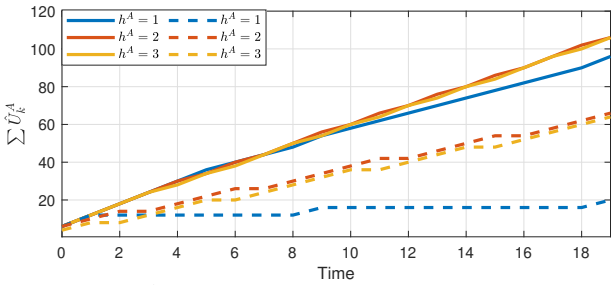


Figure 6.5 Evolution of $\sum \hat{U}_k^{\mathrm{A}}$ with $h^{\mathrm{D}} = 1$ for the path graph (solid lines) and the complete graph (dashed lines)

Proposition 6.11. Suppose that (6.16) and $\kappa^{\mathrm{D}} = \rho^{\mathrm{D}}$ are satisfied. The defender with $T^{\mathrm{D}} = 1$ does not make any recovery for $k < \lfloor \frac{(h^{\mathrm{D}}-1)(n-1-\rho^{\mathrm{D}}/\beta^{\mathrm{D}})\beta^{\mathrm{D}}}{\rho^{\mathrm{D}}} \rfloor$.

From Proposition 6.11, we are able to characterize the defender's performance in Corollary 6.12 below.

Corollary 6.12. Suppose that (6.16) and $\kappa^{\mathrm{D}} = \rho^{\mathrm{D}}$ are satisfied. Then the defender's observed utilities satisfy $\sum_{k=0}^{\overline{k}} \hat{U}_k^{\mathrm{D}}(T^{\mathrm{D}} = 1) < \sum_{k=0}^{\overline{k}} \hat{U}_k^{\mathrm{D}}(T^{\mathrm{D}} > 1)$ for $\overline{k} < \lfloor \frac{(h^{\mathrm{D}}-1)(n-1-\rho^{\mathrm{D}}/\beta^{\mathrm{D}})\beta^{\mathrm{D}}}{\rho^{\mathrm{D}}} \rfloor$.

These theoretical results on the case with varying T^{A} and T^{D} are specific to some values of parameters and class of graphs. We will see the performance of the players on more general graphs and parameters in Section 6.6 below.

6.6 Numerical examples on players' performance

In this section, we provide some numerical examples to illustrate the difference of players' performance for the cases with non-uniform horizon lengths and game periods. In this section we slightly modify the energy constraint of the defender in (6.2) to

$$\sum_{m=0}^{k} \beta^{\mathrm{D}} |\mathcal{E}_m^{\mathrm{D}} \cap \mathcal{E}_m^{\mathrm{A}}| \leq \kappa^{\mathrm{D}} + \rho^{\mathrm{D}} k. \tag{6.22}$$

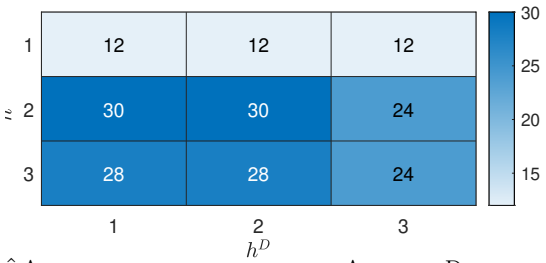


Figure 6.6 $\sum_{k=0}^{20} \hat{U}_k^{\mathrm{A}}$ for different values of h^{A} and h^{D} for the complete graph

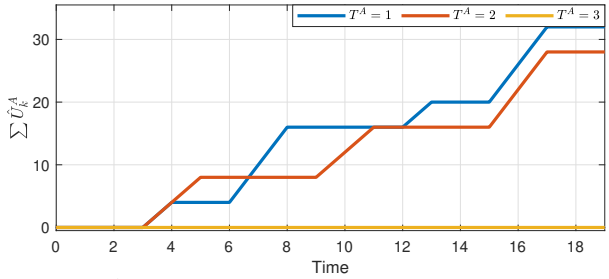


Figure 6.7 Evolution of $\sum \hat{U}_k^{\mathrm{A}}$ for the complete graph with varying T^{A} and fixed $h^{\mathrm{A}} = 3$

6.6.1 Non-uniform horizon lengths h^{A} and h^{D}

Here we discuss the players' strategies when they have non-uniform horizon lengths. It is expected that players will get better utility with longer horizon lengths, especially in the long term. From Figures 6.4 and 6.5 plotting $\sum \hat{U}_k^{\mathrm{A}}$ and $\sum \hat{U}_k^{\mathrm{D}}$ over time with three different values of h^{A} and h^{D}, we see that it is generally the case in this simulation. In Figure 6.4 for varying h^{D}, the parameters used are $n = 3$, $\rho^{\mathrm{A}}/\beta^{\mathrm{A}} = 3.1$, $\overline{\beta}^{\mathrm{A}}/\beta^{\mathrm{A}} = 10$, and $\rho^{\mathrm{D}}/\beta^{\mathrm{D}} = 1.5$. In this figure, we see that both in the path graph and the complete graph $\mathcal{G}$, the defender with $h^{\mathrm{D}} = 2$ and $h^{\mathrm{D}} = 3$ generally obtains more $\sum \hat{U}_k^{\mathrm{D}}$ than the one with $h^{\mathrm{D}} = 1$. The difference between $h^{\mathrm{D}} = 2$ and $h^{\mathrm{D}} = 3$ is not very significant in this simulation; it may be more notable in the case of more complex systems with more agents.

However, if we consider the performance of the players over a certain interval, it is possible that with a shorter horizon length the player can obtain more applied utility. We illustrate this phenomenon in the case of the attacker's applied utilities $\hat{U}_k^{\mathrm{A}}$ over time in Figure 6.5. We now use parameters $\kappa^{\mathrm{A}} = 10.5$, $\overline{\beta}^{\mathrm{A}} = 2$, $\rho^{\mathrm{A}} = 2.5$, $h^{\mathrm{D}} = 3$, and $\rho^{\mathrm{D}}/\beta^{\mathrm{D}} = 5$, so that the condition $\rho^{\mathrm{D}}/\beta^{\mathrm{D}} > |\mathcal{E}|$ in Proposition 6.4 is satisfied. Note that $\kappa^{\mathrm{A}} > \rho^{\mathrm{A}}$ here, which does not satisfy the assumption of some of the results in Section 6.4. We see from Figure 6.5 that the attacker with $h^{\mathrm{A}} = T = 1$ obtains a higher applied utility $\hat{U}_k^{\mathrm{A}}$ in the complete graph $\mathcal{G}$ until $k = 2$ as stated in Proposition 6.4, with $\overline{k} < 3$.

It is interesting to note that the complexity of the graph $\mathcal{G}$ also influences the effectiveness of having a longer horizon. Especially, with more connected $\mathcal{G}$, having a longer

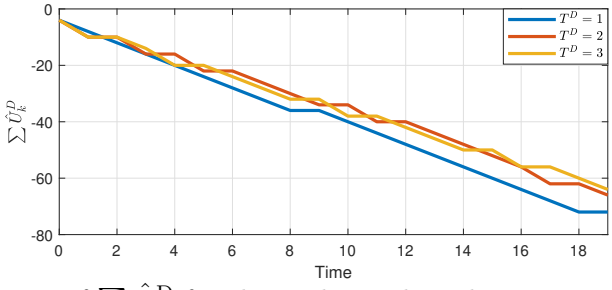


Figure 6.8 Evolution of $\sum \hat{U}_k^{\mathrm{D}}$ for the path graph with varying T^{D} and fixed $h^{\mathrm{D}} = 3$

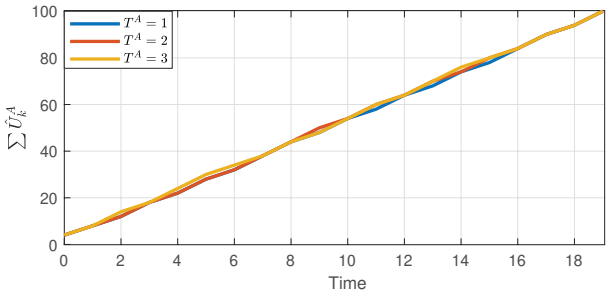


Figure 6.9 Evolution of $\sum \hat{U}_k^{\mathrm{A}}$ for the path graph with varying T^{A} and fixed $h^{\mathrm{A}} = 3$

horizon may be even more beneficial, i.e., resulting in an even higher difference of total applied utility, compared to the case with less connected $\mathcal{G}$. For example, in Figure 6.5, the difference of $\sum \hat{U}_k^{\mathrm{A}}$ in the complete graph is more apparent than in the path graph. The reason is that in the complete graph, since the attacker may attack some unnecessary edges in a short h^{A} case, e.g., attack all edges in $\mathcal{G}$, which makes the attacker have no energy in later time steps.

Figure 6.6 shows $\sum_{k=0}^{20} \hat{U}_k^{\mathrm{A}}$ for several combinations of h^{A} and h^{D} with slightly different parameters, where similar to Figure 6.5, the attacker obtains higher applied utility with $h^{\mathrm{A}} = 2$ and $h^{\mathrm{A}} = 3$, compared to that of $h^{\mathrm{A}} = 1$. Similarly, the defender also obtains more applied utility with a longer h^{D} (recall that $\hat{U}_k^{\mathrm{A}} = -\hat{U}_k^{\mathrm{D}}$).

6.6.2 Non-uniform game periods T^{A} and T^{D}

In the situation where players have non-uniform game periods, we expect that players will get better utility over time with a shorter game period, since they can use their energy more efficiently. However, from Figures 6.7–6.9, we see that the effectiveness of having a shorter game period depends on the underlying graph structure as well. In Figure 6.7, the attacker obtains more applied utility in shorter game periods $T^{\mathrm{A}} = 1$ and $T^{\mathrm{A}} = 2$. On the other hand, in Figure 6.9 the attacker in the path graph $\mathcal{G}$ obtains very similar utilities across different values of T^{A} and in Figure 6.8 the defender with a longer T^{D} has slightly more applied utility over time.

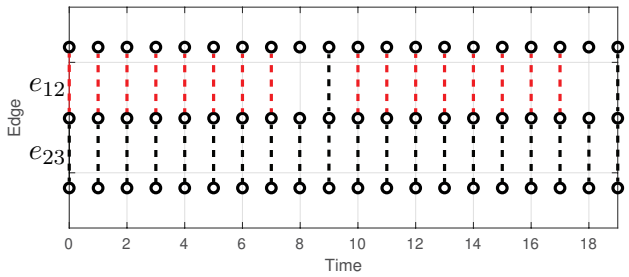


Figure 6.10 Edges attacked and recovered with $T^{\mathrm{D}} = 1$

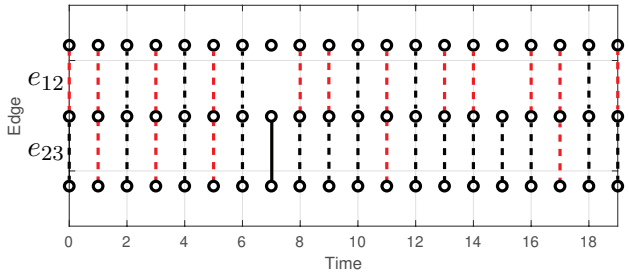


Figure 6.11 Edges attacked and recovered with $T^{\mathrm{D}} = 2$

For the simulation in Figure 6.7, we consider the complete graph, with low recharge rate ρ^{A} for the attacker; specifically, we set $n = 3$, $h^{\mathrm{A}} = 3$, $\rho^{\mathrm{A}} = 0.9$, $\overline{\beta}^{\mathrm{A}} = 2$, and $\rho^{\mathrm{D}}/\beta^{\mathrm{D}} > 3$. Note that here, the attacker cannot attack strongly without saving energy. From Figure 6.7, we see that in a low energy condition, having a long game period $T^{\mathrm{A}} = 3$ results in a lower utility over time. This is in line with Corollary 6.10 above, where having the maximum T^{A}, i.e., $T^{\mathrm{A}} = h^{\mathrm{A}}$, does not yield any additional applied utility, since the attacker becomes wasteful.

On the other hand, in Figures 6.8 and 6.9 for the path graph, we observe that having higher update frequencies, i.e., lower game periods, does not necessarily result in higher utilities for both players. For the simulation considering varying T^{D} whose $\sum \hat{U}_k^{\mathrm{D}}$ is shown in Figure 6.8, we also see the difference in the recovered edges for the path graph in Figures 6.10 and 6.11, where black dashed lines represent recovered edges, red dashed lines represent edges not recovered from normal attacks, black solid lines represent unattacked edges, and no lines represent edges attacked with strong attacks. In the case with $T^{\mathrm{D}} = 1$, the defender recovers only one edge for most of the time, whereas in $T^{\mathrm{D}} = 2$ the defender recovers two edges at some k, resulting in a higher utility (as discussed in Lemma 6.5). This is because in the case with $T^{\mathrm{D}} = 1$, the defender always saves its energy to use it later, causing the recovery to be delayed. This yields a fewer connected $\mathcal{G}_k^{\mathrm{D}}$ over time since the defender tends to apply the recovery of fewer edges more consistently (rather than all edges at more time steps).

6.7 Consensus and clustering analysis

In this section, we examine the effect of the game structure and players' energy constraints on consensus and clustering. Recall that since the defender's strategy space depends on the attacker's strategy at the same step, i.e., the defender can only recover edges attacked normally, it is possible that the defender cannot perfectly apply its strategy. Specifically the defender may not recover some of $\mathcal{E}_k^{\mathrm{D}}$, in which the energy is allocated, when the attacker changes its own strategy. If the defender allocates its energy to the strongly-attacked edges, the edges cannot be rebuilt and the resources will be wasted. Similarly, if the defender allocates its resources to the edges that are not attacked, the resources will also be wasted without any improvement of the network connectivity.In this case, the defender will apply the strategy only on the edges that can be recovered. However, as explained above, we suppose that the recovery on the edges that are not attacked still consumes energy. This will be important to the discussion of consensus and clustering. Note that this possible waste of energy does not happen to the attacker, since the attacker's strategy space does not depend on the defender's strategy.

6.7.1 Utility function structure

For the rest of this chapter, we consider a slightly different utility function structure as in Chapter 5, consisting of agent-group index $c(\cdot)$ (4.7) and state difference z_k (5.3).

The game structure used is illustrated in Fig. 6.3. The attacker's (resp., the defender) utility functions of the l^{A}th (resp., l^{D}th) decision-making index, $l^{\mathrm{A}}, l^{\mathrm{D}} \in \mathbb{N}$, starting at time $k = (l^{\mathrm{A}}-1)T^{\mathrm{A}}$ (resp., $k = (l^{\mathrm{D}}-1)T^{\mathrm{D}}$) take account of the agent-group index $c(\cdot)$ over time horizons $h^{\mathrm{A}}, h^{\mathrm{D}} \geq 1$ from time $(l^{\mathrm{A}}-1)T^{\mathrm{A}}$ to $(l^{\mathrm{A}}-1)T^{\mathrm{A}}+h^{\mathrm{A}}-1$ (resp., from $(l^{\mathrm{D}}-1)T^{\mathrm{D}}$ to $(l^{\mathrm{D}}-1)T^{\mathrm{D}}+h^{\mathrm{D}}-1$). Specifically, the utility functions at the l^{A}th decision-making process for the attacker and at the l^{D}th decision-making process for the defender are defined by

$$U_{l^{\mathrm{A}}}^{\mathrm{A}} := \sum_{k=(l^{\mathrm{A}}-1)T^{\mathrm{A}}}^{(l^{\mathrm{A}}-1)T^{\mathrm{A}}+h^{\mathrm{A}}-1} (az_k - bc(\mathcal{G}_k^{\mathrm{D}})), \tag{6.23}$$

$$U_{l^{\mathrm{D}}}^{\mathrm{D}} := \sum_{k=(l^{\mathrm{D}}-1)T^{\mathrm{D}}}^{(l^{\mathrm{D}}-1)T^{\mathrm{D}}+h^{\mathrm{D}}-1} (-az_k + bc(\mathcal{G}_k^{\mathrm{D}})), \tag{6.24}$$

which are to be maximized by the players. The players with longer horizon length and shorter game period are expected to use their energy more efficiently, and thus obtain a higher utility over time.

Our previous work in Chapter 5 considered special cases where $h^{\mathrm{A}} = h^{\mathrm{D}}$ and $T^{\mathrm{A}} = T^{\mathrm{D}}$, i.e., the players have identical computational ability, and discussed how the agents are divided into clusters at infinite time.

6.7.2 Consensus analysis

We first investigate the defender's optimal strategy on some games in order to state the results for consensus.

Lemma 6.13. There exists an infinite sequence $\bar{l}^{\mathrm{D}} := \{\bar{l}_1^{\mathrm{D}}, \bar{l}_2^{\mathrm{D}}, \ldots\}$ of the defender's decision-making index where $\bar{l}_{i+1}^{\mathrm{D}} > \bar{l}_i^{\mathrm{D}}$ and $\bar{l}_i^{\mathrm{D}} \in \mathbb{N}$ such that in the $\bar{l}_i^{\mathrm{D}}$th decision-making process, the optimal strategy for the defender in the first step is to recover $\mathcal{E}^{\mathrm{D}}_{\bar{l}_i^{\mathrm{D}},1} \neq \emptyset$ as long as $\mathcal{E}^{\mathrm{A}}_{\bar{l}_i^{\mathrm{D}},1} \neq \emptyset$.

The following results provide necessary conditions for the agents to be separated into multiple clusters for infinitely long duration without achieving consensus.

Proposition 6.14. A necessary condition for consensus not to happen is $\rho^{\mathrm{A}}/\beta^{\mathrm{A}} \geq \lambda$, with λ being the connectivity of $\mathcal{G}$.

Proposition 6.15. A necessary condition for consensus not to happen is $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq \lambda$ if either of the following two conditions is satisfied:

(a) $b = 0$, $h^{\mathrm{D}} \geq h^{\mathrm{A}}$ and $\mathrm{lcm}(T^{\mathrm{A}}, T^{\mathrm{D}}) = T^{\mathrm{A}}$; or

(b) $b = 0$ and $h^{\mathrm{D}} = T^{\mathrm{D}} = 1$.

The next result provides a condition for consensus to be completely blocked and all agents are separated from each other. It shows that the attacker should be capable to make strong attacks on all the edges for all time.

Proposition 6.16. A sufficient condition for all agents not to achieve consensus at infinite time is $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq |\mathcal{E}|$.

Note that these conditions are based on the assumption that the unsuccessful recovery, i.e., $\mathcal{E}_k^{\mathrm{D}} \setminus \mathcal{E}_k^{\mathrm{A}}$, still consumes energy as formulated in (6.2). The conditions in the case where the defender does not lose energy from unsuccessful recovery are discussed in a remark below based on Propositions 6.14–6.16.

Remark 6.17. Suppose that the energy consumption of the defender satisfies $\sum_{m=0}^{k} \beta^{\mathrm{D}} |\mathcal{E}_m^{\mathrm{D}} \cap \mathcal{E}_m^{\mathrm{A}}| \leq \kappa^{\mathrm{D}} + \rho^{\mathrm{D}} k$, i.e., only the successful recovery takes the defender's energy. Then, necessary conditions to prevent consensus are $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq \lambda$ if $b = 0$ and $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq \lambda$ otherwise. A sufficient condition is $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq |\mathcal{E}|$.

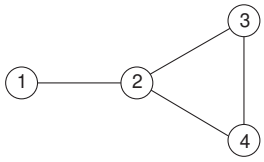


Figure 6.12 Graph $\mathcal{G}$ used in the case study.

The general necessary and sufficient conditions are the same as in Propositions 6.14 and 6.16 above, since the conditions of those results are derived from the attacker's ability rather than the defender, as discussed in the proofs of Propositions 6.14 and 6.16. For the case of $b = 0$, there is a difference from Proposition 6.15 that in a no-waste energy situation, the defender's horizon parameters no longer influence the requirement for obtaining tighter necessary condition. This implies that the defender becomes weaker with energy constraint (6.2), since the necessary conditions to prevent consensus become less tight.

6.7.3 Clustering analysis

Next we derive some results on the number of formed clusters of agents at infinite time. These results are related to the consensus result above, since agents are separated into different clusters when consensus is not reached.

From Proposition 6.16, it is clear that if $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq |\mathcal{E}|$, then the attacker can make n clusters by strongly attacking all edges at all time. Thus, for the result below, we consider the case where $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < |\mathcal{E}|$.

Proposition 6.18. Define a vector $\Theta \in \mathbb{R}^{|\mathcal{E}|}$ with elements $\Theta_i := \max_{|\mathcal{E}^{\mathrm{A}}|=i} \overline{n}((\mathcal{V}, \mathcal{E} \setminus \mathcal{E}^{\mathrm{A}}))$, with $\overline{n}((\mathcal{V}, \mathcal{E} \setminus \mathcal{E}^{\mathrm{A}}))$ being the number of groups of graph $(\mathcal{V}, \mathcal{E} \setminus \mathcal{E}^{\mathrm{A}})$. Then the number of formed clusters at infinite time is upper bounded by

- $\Theta_{\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor}$ if either
  - $b = 0$, $h^{\mathrm{D}} \geq h^{\mathrm{A}}$ and $\mathrm{lcm}(T^{\mathrm{A}}, T^{\mathrm{D}}) = T^{\mathrm{A}}$; or
  - $b = 0$ and $h^{\mathrm{D}} = T^{\mathrm{D}} = 1$,
- $\Theta_{\min\{|\mathcal{E}|, \lfloor \rho^{\mathrm{A}}/\beta^{\mathrm{A}} \rfloor\}}$ otherwise.

We illustrate the results in Proposition 6.18 by looking at the graph in Fig. 6.12 above. In this graph, the vector Θ is $\Theta = [2, 2, 3, 4]^{\mathrm{T}}$. Suppose $\beta^{\mathrm{A}} = 1$, $\overline{\beta}^{\mathrm{A}} = 2$, $\rho^{\mathrm{A}} = 3.5$. In this case, if $b = 0$ and h^{A}, h^{D}, $T^{\mathrm{A}}, T^{\mathrm{D}}$ satisfy the condition in Proposition 6.18, then the maximum number of clusters is $\Theta_1 = 2$; otherwise the maximum number of clusters is $\Theta_3 = 3$. Note that since $\Theta_{i+1} \geq \Theta_i$, the upper bound becomes tighter if the values of horizon lengths and game periods satisfy the condition in Proposition 6.15.

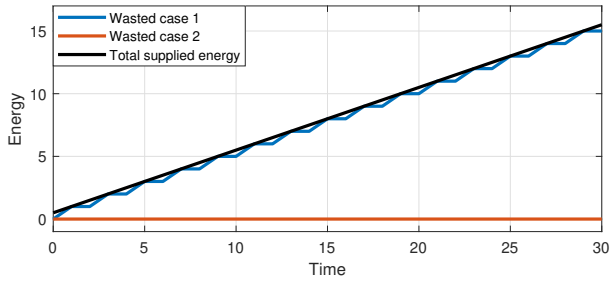


Figure 6.13 Wasted energy and total supplied energy, i.e., $\kappa^{\mathrm{D}} + \rho^{\mathrm{D}} k$, of the defender in Case 1 and Case 2

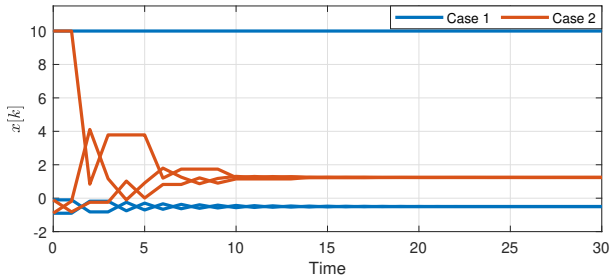


Figure 6.14 Agent states of Case 1 and Case 2

6.8 Numerical examples on consensus and clustering

In this section, we continue by showing the effect of the values of horizon lengths and game periods on the consensus speed and the number of clusters. Specifically, we show the example where consensus may still be prevented if the defender's horizon parameters are sufficiently low, even with relatively low energy parameters for the attacker. This is related to the conditions in Propositions 6.14 and 6.15.

Here, we consider a simple path graph consisting of three agents ($|\mathcal{E}| = 2, \lambda = 1$) with the following parameters:

- Case 1: $h^{\mathrm{A}} = 3$, $h^{\mathrm{D}} = 2$, $T^{\mathrm{A}} = 1$, $T^{\mathrm{D}} = 2$,
- Case 2: $h^{\mathrm{A}} = h^{\mathrm{D}} = T^{\mathrm{A}} = T^{\mathrm{D}} = 2$,

with $b = 0$, $\kappa^{\mathrm{D}} = \rho^{\mathrm{D}} = 0.5$, $\kappa^{\mathrm{A}} = \rho^{\mathrm{A}} = 1.5$, $\overline{\beta}^{\mathrm{A}} = 2$, $\beta^{\mathrm{A}} = \beta^{\mathrm{D}} = 1$ in both cases. Notice that since $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda = 1$, the attacker is not able to strongly attack edges at all time to keep the graph disconnected. Thus, in order to prevent consensus, the attacker needs to continuously change its strategies to make the recovery unsuccessful.

The attacker is stronger than the defender in Case 1, since with $h^{\mathrm{A}} > h^{\mathrm{D}}$ and $T^{\mathrm{A}} < T^{\mathrm{D}}$ the attacker can look further forward and update their strategies more often. Consequently, in this case the attacker may avoid the recovery on $\mathcal{E}_k^{\mathrm{D}}$ either by canceling its planned attack or by changing to strong attack instead. In Case 2, both players have

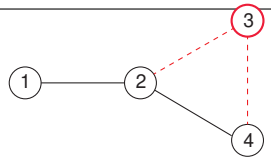


Figure 6.15 Example of node attacks. The attacker attacks node/agent 3, removing edges (3,2) and (3,4). As a result, agent 3 is disconnected from others.

the exact same horizon parameters, implying that the defender never wastes its energy since the attacker is not able to unilaterally change its strategy.

In Fig. 6.13, the defender wastes all of its energy in Case 1 of shorter T^{A} from failing to apply the recoveries. This affects the evolution of the agents' states in Fig. 6.14 where agents are being divided into two separate clusters in Case 1, while on the contrary they converge into the same state in Case 2. Note that the values of the horizon lengths and the game periods in Case 2 satisfy the requirements in Proposition 6.15 to make the necessary condition tighter, i.e., $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq \lambda$ instead of of $\rho^{\mathrm{A}}/\beta^{\mathrm{A}} \geq \lambda$. On the other hand, the horizon parameters in Case 1 do not satisfy that requirements, making the consensus easier to prevent.

6.9 Chapter summary

In this chapter, we have formulated a two-player game in a cluster forming of networks played over time. The players consider the impact of their actions on future network topologies, and adjust their strategies according to a rolling horizon approach. The players may have different computation capabilities represented by different horizon lengths and game periods. The performance of the players are measured by calculating the applied utilities, where in general, the player with a longer horizon length and a shorter game period performs better over longer intervals. We have confirmed that this is especially the case for more connected networks and when the attack/defense energy is more limited.

Additionally, necessary conditions and sufficient conditions for forming clusters among agents have been derived. We have discussed the effect of the horizon parameters on the possible number of clusters and consensus, where in general, the attacker needs to have sufficiently long horizon length and short game period to prevent consensus, in addition to having sufficient energy.

6.10 Extension: Node-attack case

In addition to the attacks and the recoveries based on individual edges as introduced above, we can consider a slightly different setting where the attacker can attack

nodes/agents so that *all* edges adjacent to the attacked agents are disconnected, as shown in Fig. 6.15. Specifically, the attacker's actions are now $\mathcal{E}_k^{\mathrm{A}} \in \mathcal{F}$ and $\overline{\mathcal{E}}^{\mathrm{A}} \in \mathcal{F}$, where $\mathcal{F} := \{\emptyset, F_1, F_2, \ldots, F_n, F_1 \cup F_2, \ldots, \mathcal{E} = \cup_{i\in\mathcal{V}} F_i\}$ and $F_i := \{(i,j) : \ j \in \mathcal{N}_i\}$ represents the set of edges adjacent to agent i. In this case, the attacker effectively attacks a node/agent by attacking all edges adjacent to it.

For this node attack case, the energy constraint of the attacker (6.1) becomes $\sum_{m=0}^{k}(\overline{\beta}_{\mathcal{V}}^{\mathrm{A}}|\overline{\mathcal{V}}_m^{\mathrm{A}}|+ \beta_{\mathcal{V}}^{\mathrm{A}}|\mathcal{V}_m^{\mathrm{A}}|) \leq \kappa^{\mathrm{A}} + \rho^{\mathrm{A}}k$ with energies $\overline{\beta}_{\mathcal{V}}^{\mathrm{A}} > \beta_{\mathcal{V}}^{\mathrm{A}}$, where $\overline{\mathcal{V}}_m^{\mathrm{A}}$ and $\mathcal{V}_m^{\mathrm{A}}$ denote the sets of nodes/agents whose adjacent edges are attacked with strong and normal jamming signals, respectively. Note that in this case, if an edge is attacked by *both* normal signals and strong signals, then that edge cannot be recovered by the defender.

It then follows that in this case, the necessary conditions $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq \lambda$ and $\rho^{\mathrm{A}}/\beta^{\mathrm{A}} \geq \lambda$ in Propositions 6.14 and 6.15 to prevent consensus change to $\rho^{\mathrm{A}}/\overline{\beta}_{\mathcal{V}}^{\mathrm{A}} \geq 1$ and $\rho^{\mathrm{A}}/\beta_{\mathcal{V}}^{\mathrm{A}} \geq 1$, respectively, since the attacker only needs to isolate an agent to prevent consensus.

6.11 Extension: Incomplete information games

In some situation, a player may not exactly know the utility of its opponents, which may be kept as private information. We call this lack of information of a player in the game as *incomplete information* [98, 99]. Bayesian games are commonly used to model incomplete information among players in the game, e.g., Bayesian Nash Equilibrium [100] and Perfect Bayesian Equilibrium [101]. These solution concepts are also recently studied in the context of n-player networks [102–105]. This incomplete information setting is also applied to economic problem, mainly to auctions. [106].

Specifically in the ongoing works, we extend the formulation to consider a more realistic scenario where each agent of the network decides its own strategies, instead of relying on the centralized defender. This decentralized defenses from the agents naturally have several limitations such as their limited knowledge of what happens outside their local environment. Thus, it is natural to consider an incomplete information structure of the game, where an agent does not exactly know the utilities of other agents. This ongoing works are discussed in an under-preparation manuscript [O6].

6.12 Appendix

6.12.1 Proof of Lemma 6.1

In the star graph $\mathcal{G}$, ξ number of strongly attacked edges results in ξ number of isolated agents and a group of $(n-\xi)$ number of agents forming a star graph. Thus,

we have $\overline{c}(\xi) = (n-\xi)^2 + \xi - n^2$ and hence $\overline{c}(\hat{k}\xi) = (n-\hat{k}\xi)^2 + \hat{k}\xi - n^2$ so long as $\hat{k}\xi \leq n-1$. It then follows that the sum of agent-group index over $\hat{k}$ interval becomes $\hat{k}\overline{c}(\xi) = \hat{k}(n-\xi)^2 + \hat{k}\xi - \hat{k}n^2$. It is straightforward to show that $\hat{k}(n-\xi)^2 - \hat{k}n^2 \leq (n-\hat{k}\xi)^2 - n^2$ for any $\hat{k} \leq (n-1)/\xi$.

6.12.2 Proof of Proposition 6.2

Since after the attack of $|\overline{\mathcal{E}}_k^{\mathrm{A}}|$ edges there is still a group of agents consisting of at most $(n - |\overline{\mathcal{E}}_k^{\mathrm{A}}|)$ agents forming a star graph, here the star graph gives the least value of agent-group index among the graphs with n nodes with edge connectivity 1 (tree graphs). Therefore, proving for the star graph is sufficient to show the result for the tree graphs.

Since the immediate attack gives the more negative agent-group index from Lemma 6.1, it then follows that if $\kappa^{\mathrm{A}} = \rho^{\mathrm{A}}$, it will also give the maximum $\sum_{k=0}^{\overline{k}} \hat{U}_k^{\mathrm{A}}$ over any $\overline{k}$. Note that, if $\kappa^{\mathrm{A}} > \rho^{\mathrm{A}}$, i.e., (6.14) is not satisfied, then the attacker may have different ability especially at $k = 0$, which makes the immediate attack more wasteful and no longer optimal in a shorter horizon situation.

6.12.3 Proof of Proposition 6.3

Note that the complete graph has the edge connectivity $n-1$. Since it is assumed that the attacker always spends all of its energy at the last step of the game, there is at most $\overline{\beta}^{\mathrm{A}}$ amount of energy at the beginning of each game from the leftover of the previous games. With $\rho^{\mathrm{A}} T < (n-2)\overline{\beta}^{\mathrm{A}}$, if $h^{\mathrm{A}} = T$, then the attacker will spend all of its energy at the last step of the game without disconnecting any agent, implying that $U_k^{\mathrm{A}} = 0$ for any l and hence $\hat{U}_k^{\mathrm{A}} = 0$ for any k.

6.12.4 Proof of Proposition 6.4

In the case of $h^{\mathrm{A}} = 1$, at time $k = 0$ the attacker will spend all its energy, which is dictated by κ^{A}. In this case, if $\kappa^{\mathrm{A}} > |\mathcal{E}|\overline{\beta}^{\mathrm{A}}$, then the attacker will attack all edges to maximize U_k^{A}. Considering the recharge rate ρ^{A} that changes the attacker's available energy in each time k, the attacker with $h^{\mathrm{A}} = 1$ will attack all edges with strong signals as long as k satisfies $k < \frac{\kappa^{\mathrm{A}} + k\rho^{\mathrm{A}}}{|\mathcal{E}|\overline{\beta}^{\mathrm{A}}}$. It then follows that, since attacking all edges always gives maximum applied utility in a single time step, with $h^{\mathrm{A}} = 1$ the attacker will obtain maximum possible applied utility $\hat{U}_k^{\mathrm{A}}$ for time $k < \frac{\kappa^{\mathrm{A}} + k\rho^{\mathrm{A}}}{|\mathcal{E}|\overline{\beta}^{\mathrm{A}}}$.

6.12.5 Proof of Lemma 6.5

We begin by discussing the right-hand side of (6.15). Recall from (4.7) that $c'(0) = c((\mathcal{V}, \emptyset)) = n - n^2$. Note that, in the last time step of $\hat{k} \leq (n-1)/\theta$ interval, the defender cannot recover more than $(n-1)$ edges given no previous recovery for $\hat{k}-1$ interval. Thus, at the end of the interval, (4.7) becomes $c'(k\theta) = (\hat{k}\theta + 1)^2 + (n - \hat{k}\theta - 1) - n^2$.

On the other hand, if the defender recovers θ number of edges, then we have $c'(\theta) = (\theta+1)^2 + (n-\theta-1) - n^2$. It then follows that $\hat{k}c'(\theta) = \hat{k}[(\theta+1)^2 + (n-\theta-1) - n^2] \leq (\hat{k}-1)c'(0) + c'(\hat{k}\theta) = (\hat{k}-1)n + (\hat{k}\theta+1)^2 + (n - \hat{k}\theta - 1) - \hat{k}n^2$ for any time interval $\hat{k} \leq (n-1)/\theta$.

6.12.6 Proof of Proposition 6.6

Since $\overline{\beta}^{\mathrm{A}}/\beta^{\mathrm{A}}$ is large enough to prevent attacking with strong signals, all attacks in any k are done with normal jamming signals. Since $\rho^{\mathrm{A}}/\beta^{\mathrm{A}} = |\mathcal{E}|$, the attacker is able to attack all edges $\mathcal{E}$ at all k, which is optimal.

Similar to the proof in Proposition 6.4 above, since the defender recovers all of the attacked edges with $h^{\mathrm{D}} = 1$, at $k = 0$ it will obtain maximum applied utility. The assumption $\rho^{\mathrm{D}}/\beta^{\mathrm{D}} < n-1$ means that the defender cannot recover more than $(n-1)$ number of edges at every time k, which results in maximum $c(\mathcal{G}_k^{\mathrm{D}})$ in (4.7). The defender then will recover all edges until time $\lfloor \frac{\kappa^{\mathrm{D}}}{(n-1)\beta^{\mathrm{D}} - \rho^{\mathrm{D}}} \rfloor$.

6.12.7 Proof of Corollary 6.7

The proof is similar to the proof of Proposition 6.2.

6.12.8 Proof of Proposition 6.8

Since $\kappa^{\mathrm{A}} = \rho^{\mathrm{A}} < (n-1)\overline{\beta}^{\mathrm{A}}$, the attacker keeps spending all of its energy and hence it cannot disconnect the graph by attacking with strong signals at any k. This implies that in the complete graph $\mathcal{G}$ the attacker will not attack unless it has enough energy to attack $n-1$ edges at later steps of the decision-making process. Furthermore, to implement the attack strategies, the attacker needs to have enough energy to attack at least $(n-1)h^{\mathrm{A}}$ number of edges (recall that given the same utility, the attacker is assumed to attack less edges at the earlier steps).

We are then looking for the condition that prevents the attacker from attacking at the earliest step (since $T^{\mathrm{A}} = 1$, the only applied strategies are the ones in the first

step). With the ability to attack $\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor$ number of edges every k, the attacker will have $(h^{\mathrm{A}}-1)\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}$ more energy at the end of each game, given no previous attacks. It follows that there is no attack before time $\lfloor ((h^{\mathrm{A}}-1)(n-1)-(h^{\mathrm{A}}-1)\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}})/(\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}) \rfloor$.

6.12.9 Proof of Corollary 6.9

The result is a direct consequence of Proposition 6.8.

6.12.10 Proof of Corollary 6.10

The result is a direct consequence of Proposition 6.3.

6.12.11 Proof of Proposition 6.11

Since $\rho^{\mathrm{A}}/\beta^{\mathrm{A}} = |\mathcal{E}|$ and $\overline{\beta}^{\mathrm{A}}/\beta^{\mathrm{A}} > h^{\mathrm{A}}|\mathcal{E}|$ are satisfied by (6.16), the attacker cannot strongly attack any edge at any k and instead its optimal strategy is to attack $\mathcal{E}$ with normal jamming signals so that $\mathcal{G}_k^{\mathrm{A}}$ is an empty graph.

In this case, it follows from Lemma 6.5 that the defender will not recover any edge at the first step. Since by (4.7) the defender does not receive any additional utility by recovering more than $(n-1)$ edges, it then follows that to obtain the maximum utility of (6.18) in a single decision-making process, the defender has to recover $(n-1)h^{\mathrm{D}}$ number of edges in total ($(n-1)h^{\mathrm{D}}$ number of edges except for the $T^{\mathrm{D}}(=1)$ step(s)).

We continue by looking for the condition that prevents the defender from recovering at the first step. With the ability to recover $\lfloor \rho^{\mathrm{D}}/\beta^{\mathrm{D}} \rfloor$ number of edges every k, the defender projects that it will have $(h^{\mathrm{D}}-1)\rho^{\mathrm{D}}/\beta^{\mathrm{D}}$ more energy at the end of each decision-making process, given no previous recoveries. It then follows that the defender does not make any recovery before $\lfloor ((h^{\mathrm{D}}-1)(n-1)-(h^{\mathrm{D}}-1)\rho^{\mathrm{D}}/\beta^{\mathrm{D}})/(\rho^{\mathrm{D}}/\beta^{\mathrm{D}}) \rfloor$.

6.12.12 Proof of Corollary 6.12

The result is a direct consequence of Proposition 6.11.

6.12.13 Proof of Lemma 6.13

We note that if the defender does not recover from nonzero normal attacks in the first step of the game, the worst scenario is that agent states will eventually converge to different values. Consequently, the attacker needs to keep attacking the edges connecting

the agents with different states to keep them separated from other clusters. Suppose that the agents are separated into clusters at the game with index $\bar{l}_i^{\mathrm{D}}$. Here,

$$z_{\bar{l}_i^{\mathrm{D}},1}(\cdot, \tilde{\mathcal{E}}^{\mathrm{A}}_{\bar{l}_i^{\mathrm{D}},1}, \emptyset) \geq z_{\bar{l}_i^{\mathrm{D}},1}(\cdot, \tilde{\mathcal{E}}^{\mathrm{A}}_{\bar{l}_i^{\mathrm{D}},1}, \mathcal{E}^{\mathrm{D}}_{\bar{l}_i^{\mathrm{D}},1}) \tag{6.25}$$

is always satisfied, with $\tilde{\mathcal{E}}^{\mathrm{A}}_{\bar{l}_i^{\mathrm{D}}}$ being the edges separating agents with different states. In this case, the attacker needs to attack $\tilde{\mathcal{E}}^{\mathrm{A}}_{\bar{l}_i^{\mathrm{D}}}$ to keep the agents separated into different states. Note that (6.25) is a more specific form of $z_k(\emptyset, \mathcal{E}, \emptyset) \geq z_k(\emptyset, \mathcal{E}, \mathcal{E}_k^{\mathrm{D}})$, where attacking all edges always gives maximum value of z_k.

From (6.25), the defender always benefits from recovering nonzero number of edges, since $z_{\bar{l}_i^{\mathrm{D}},2} = z_{\bar{l}_i^{\mathrm{D}},1}$ if the defender does not recover any edge which gives the least value of utility. Since $c(\mathcal{G}^{\mathrm{D}}_{\bar{l}_i^{\mathrm{D}},1})$ also gives the lowest value if the defender does not recover, at the first step of the $\bar{l}_i^{\mathrm{D}}$th game the defender's utility with recovering nonzero edges is always better than the case of not recovering any edge. Since the defender constantly gains ρ^{D} amount of energy at each time, this action for the defender is the same for the next games with indices $\bar{l}^{\mathrm{D}}_{i+1}$, $\bar{l}^{\mathrm{D}}_{i+2}$, and so on.

6.12.14 Proof of Proposition 6.14

We note that, without any recovery from the defender ($\mathcal{E}_k^{\mathrm{D}} = \emptyset$), the attacker must attack at least λ number of edges with normal signals at any time k in order to make $\mathcal{G}_k^{\mathrm{D}}$ disconnected. If the attacker attacks λ edges with normal jamming signals at all times, the energy constraint (6.1) becomes $(\beta^{\mathrm{A}}\lambda - \rho^{\mathrm{A}})k \leq \kappa^{\mathrm{A}}$. Thus, the condition $\rho^{\mathrm{A}}/\beta^{\mathrm{A}} \geq \lambda$ has to be satisfied for all k.

6.12.15 Proof of Proposition 6.15

We prove by contrapositive; especially, we prove that consensus always happens if $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda$ under the specified conditions.

We first suppose that the attacker attempts to attack λ edges strongly at all times to disconnect the graph $\mathcal{G}_k^{\mathrm{D}}$. From (6.1), the energy constraint of the attacker at time k becomes $(\overline{\beta}^{\mathrm{A}}\lambda - \rho^{\mathrm{A}})k \leq \kappa^{\mathrm{A}}$. This inequality is not satisfied for higher k if $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda$, since the left-hand side becomes positive and κ^{A} is finite. Therefore, the attacker cannot attack λ edges strongly at all times if $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda$, and is forced to disconnect the graph by attacking with normal jamming signals instead. As a consequence, it follows from Lemma 6.13 that there exists an interval of time where the defender always recovers, i.e., $\mathcal{E}^{\mathrm{D}}_{\bar{l}_i^{\mathrm{D}},1} \neq \emptyset$, $i = 1, 2, \ldots$, are optimal given that $\mathcal{E}^{\mathrm{A}}_{\bar{l}_i^{\mathrm{D}},1} \neq \emptyset$. Note that this strategy is always applied since it is for the first step of the game.

From the definition of the utility function in (6.24), given that $b = 0$, we can see that the defender obtains a higher utility if the agents are closer, which means that given a nonzero number of edges to recover (at the first step of the games with index $\bar{l}_i^{\mathrm{D}}$ described above), the defender recovers the edges connecting further agents. Specifically, for the sequence of decision-making indices $[\bar{l}_i^{\mathrm{D}}, \bar{l}_{i+1}^{\mathrm{D}}]$, there is a time step where $U_{l^{\mathrm{D}}}^{\mathrm{D}}(\mathcal{E}_{l^{\mathrm{D}},1}^{\mathrm{D}} = \mathcal{E}_1) \geq U_{l^{\mathrm{D}}}^{\mathrm{D}}(\mathcal{E}_2)$, where $\mathcal{E}_1$ and $\mathcal{E}_2$ denote sets of edges connecting agents with further states and closer states, respectively. Since by communicating with the consensus protocol as in (2.3) the agents' states are getting closer, the defender will choose different edges to recover if the states of the agents connected by the recovered edges $\mathcal{E}_k^{\mathrm{D}}$ become close enough.

For Case (a), with $h^{\mathrm{D}} \geq h^{\mathrm{A}}$ and $\mathrm{lcm}(T^{\mathrm{A}}, T^{\mathrm{D}}) = T^{\mathrm{A}}$, it is guaranteed that the defender does not waste any energy by recovering, since by having longer horizon length the defender will accurately predict the attacker's action. The game period $\mathrm{lcm}(T^{\mathrm{A}}, T^{\mathrm{D}}) = T^{\mathrm{A}}$ implies that the attacker will never update its decision alone, i.e., the defender also updates when the attacker updates, which prevents the attacker to unilaterally changes its strategy to avoid the defender's planned recovery. On the other hand, for Case (b), the defender with $h^{\mathrm{D}} = 1$ will be able to perfectly observes the attacker's action that has been done, and hence also removing the possibility of wasting energy.

Consequently, with aforementioned values of the horizon lengths and the game periods, if $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda$ and $b = 0$, then there exists $j \in \mathbb{N}$ depending on i such that the union of graphs, i.e., the graph having the union of the edges of each graph $(\mathcal{V}, \bigcup((\mathcal{E} \setminus (\overline{\mathcal{E}}_k^{\mathrm{A}} \cup \mathcal{E}_k^{\mathrm{A}})) \cup \mathcal{E}_k^{\mathrm{D}}))$, over the decision-making index $[\bar{l}_i^{\mathrm{D}}, \bar{l}_{i+j(i)}^{\mathrm{D}}]$ becomes a connected graph for all i. These intervals $[(\bar{l}_i^{\mathrm{D}} - 1)T^{\mathrm{D}}, (\bar{l}_{i+j(i)}^{\mathrm{D}} - 1)T^{\mathrm{D}}]$, $i = 1, 2, \ldots$, occur infinitely many times, since the defender's energy bound keeps increasing over time.

It is shown in [3] that with protocol (2.3), the agents achieve consensus in the time-varying graph as long as the union of the graphs over bounded time intervals is a connected graph. This implies that consensus is achieved if $(\mathcal{V}, \bigcup((\mathcal{E} \setminus (\overline{\mathcal{E}}_k^{\mathrm{A}} \cup \mathcal{E}_k^{\mathrm{A}})) \cup \mathcal{E}_k^{\mathrm{D}}))$ is connected over $[\bar{l}_i^{\mathrm{D}}, \bar{l}_{i+j(i)}^{\mathrm{D}}]$ for all i.

6.12.16 Proof of Proposition 6.16

Since $z_{l^{\mathrm{A}},\bar{l}^{\mathrm{A}}}(\mathcal{E}, \emptyset, \emptyset) \geq z_{l^{\mathrm{A}},\bar{l}^{\mathrm{A}}}(\overline{\mathcal{E}}_{l^{\mathrm{A}},\bar{l}^{\mathrm{A}}}^{\mathrm{A}}, \mathcal{E}_{l^{\mathrm{A}},\bar{l}^{\mathrm{A}}}^{\mathrm{A}}, \mathcal{E}_{l^{\mathrm{A}},\bar{l}^{\mathrm{A}}}^{\mathrm{D}})$ and $c((\mathcal{V}, \emptyset)) \geq c((\mathcal{V}, \mathcal{E} \setminus (\overline{\mathcal{E}}_{l^{\mathrm{A}},\bar{l}^{\mathrm{A}}}^{\mathrm{A}} \cup \mathcal{E}_{l^{\mathrm{A}},\bar{l}^{\mathrm{A}}}^{\mathrm{A}}) \cup (\mathcal{E}_{l^{\mathrm{A}},\bar{l}^{\mathrm{A}}}^{\mathrm{D}} \cap \mathcal{E}_{l^{\mathrm{A}},\bar{l}^{\mathrm{A}}}^{\mathrm{A}})))$, the function $U_{l^{\mathrm{A}}}^{\mathrm{A}}$ has the highest value if the attacker attacks all edges, i.e., $\overline{\mathcal{E}}_{l^{\mathrm{A}},\bar{l}^{\mathrm{A}}}^{\mathrm{A}} = \mathcal{E}$ or $\mathcal{E}_{l^{\mathrm{A}},\bar{l}^{\mathrm{A}}}^{\mathrm{A}} = \mathcal{E}$. With $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq |\mathcal{E}|$, the attacker can attack all edges of $\mathcal{G}$ with strong jamming signals at any time k. Thus, the attacker will attack $\mathcal{E}$ strongly at the $\bar{l}^{\mathrm{A}}$th step of the l^{A}th decision-making process, i.e., $\overline{\mathcal{E}}_{l^{\mathrm{A}},\bar{l}^{\mathrm{A}}}^{\mathrm{A}*} = \mathcal{E}$, which also

prevents the defender from recovering any edge, i.e., $\mathcal{E}^{\mathrm{D}}_{l^{\mathrm{A}},\bar{l}^{\mathrm{A}}} = \emptyset$, for all $l^{\mathrm{A}}, \bar{l}^{\mathrm{A}}$. Thus the attacker will attack $\mathcal{E}$ with strongly at all time, separating every agent into n clusters.

6.12.17 Proof of Proposition 6.18

The vector Θ consists of the maximum number of formed groups $\overline{n}((\mathcal{V}, \mathcal{E} \setminus \mathcal{E}^{\mathrm{A}}))$ given the number of attacked edges as the element index. Since some edges need to be attacked consistently in order to divide the agents into different clusters, the number of formed clusters at infinite time is never more than the maximum number of groups at any time k given the same number of strongly attacked edges.

Recall from Proposition 6.15 that given certain values of h^{A}, h^{D}, T^{A}, and T^{D}, $\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor$ is the maximum achievable number of edges that can be strongly attacked at all times. On the other hand, if those values do not satisfy the requirement in Proposition 6.15, then from Proposition 6.14, $\lfloor \rho^{\mathrm{A}}/\beta^{\mathrm{A}} \rfloor$ is the maximum achievable number of edges that can be strongly attacked at all times. Given the known graph topology $\mathcal{G}$, we then can imply that depending on the horizon lengths and the game periods, $\Theta_{\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor}$ and $\Theta_{\lfloor \rho^{\mathrm{A}}/\beta^{\mathrm{A}} \rfloor}$ give the maximum number of clusters at infinite time.

Chapter 7

Concluding Remarks

7.1 Conclusion and summary

In this thesis, we have provided a two-player subgame perfect equilibrium analysis under the setting of multiagent system in the face of jamming attacks and recoveries. We focus on the impact of the game on the agents' states following consensus dynamics at infinite time. The results in each chapter are as follows.

In Chapter 3, we provide a graph-based analysis of the game. We have obtained the optimal strategies of the players in terms of edges and durations of action intervals by considering the effect of the attack or recovery actions to the connectivity measures and states of the agents. In a consensus problem, we have explored how the time for the agents to reach approximate consensus is influenced by the parameters of the players and topology of the graph.

In Chapter 4, we discuss a continuous-time setting of clustering, where it has been shown that the attacker with sufficiently high recharge rate may be able to prevent consensus. However, the attacker does not necessarily choose the strategies that focus on the long term due to the finite horizon nature of the formulation.

In Chapter 5, we discuss a discrete-time setting of agent consensus and clustering, where similarly, the attacker with sufficiently high recharge rate has a better chance to prevent consensus. We also derive the upper bound of number of cluster of agents formed at infinite time as a more general case of consensus; the upper bound increases with the better recharge rate by the attacker.

In Chapter 6, we study players' performance under non-uniform horizon parameters by calculating the value of observed utility of the players. It has been shown that players

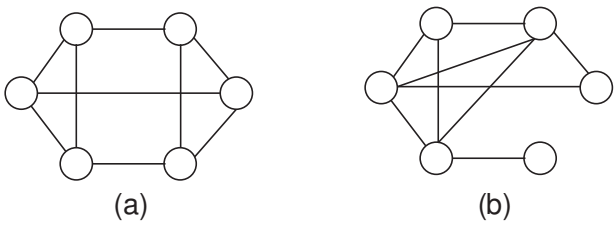


Figure 7.1 Difference of edge connectivity given the same number of edges: (a) $\lambda = 3$, (b) $\lambda = 1$

with longer horizon length and shorter game period are able to obtain better utility at later time, however they may perform worse in a short-time window. Additionally, in this chapter we analyze consensus and agent clustering at infinite time under non-uniform horizon is discussed. We show that, by specifying the necessary conditions for preventing consensus, the attacker with better horizon parameters than the opponent may not need to have as much recharge rate to be able to achieve its goal.

The results obtained in this thesis may be used as a guidelines to design real networks that is resilient to the strategic attacks. For example, the system designer may design a network with a relatively balanced degree across components in order to maximize the value of edge connectivity λ. This high value of λ can in turn minimize the risk of the attacks and help the agents to achieve consensus, as demonstrated in the results in Chapters 4–6.

Furthermore, from the results in Chapter 6, we show it is important for the defender to have sufficiently good horizon parameters. Thus, it is important for the system designers to entrust the system to the defender that is able to think more in the long term.

Figure 7.1 illustrates the edge/link distribution for the underlying graphs. With the same number of edges/links, it is clear that graph (a) is much less connected than graph (b), which impact the attacker's strategies and consensus.

7.2 Future research directions

Noncooperative game-theoretical approach for analyzing network security is an emerging field of study. In this thesis, we focus on the repeated games approach where players may focus on the long term aspect on the game. A two-player game between a centralized attacker and a centralized defender is considered.

A natural future direction of this research is to consider a n-player game where each agent in the network is able to decide its own strategy in the face of a centralized attacker from outside the system. One possible extension is to consider *potential games* [47] to

characterize their coordination among the agents. For a large number of agents $n \to \infty$, *mean-field games* setting for the agents [44] can also be considered.approach can also be used.

In the formulation we proposed, we focus on the deterministic aspect of the game with sequential nature of the players' movement. The players are assumed to have perfect and complete information of the players' parameters, agent states, and network structure. Another natural future work is to consider an incomplete information structure [98, 99] of the players, which is also briefly discussed in the end of Chapter 6.

In incomplete information games (also referred as *Bayesian games*), several solution concept of the games have been proposed, namely Bayesian Nash Equilibrium [100] for the game where players move simultaneously and Perfect Bayesian Equilibrium [101]. These solution concepts are also recently studied in the context of n-player networks [102–105].

Receding horizon control approach for repeated games is also a relatively new approach for addressing players' different abilities. A further investigation on the relationship between horizon parameters and players' long-term and short-term performance in the context of multiagent consensus would be helpful.

Acknowledgments

First and foremost, I would like to show my appreciation to my advisor, Prof. Tomohisa Hayakawa, for his guidance on my study and research during my stay in his lab. He helped me a lot with finding interesting topics to discuss, especially in the field of multiagent system and networked control.

I also would like to thank the other research group members: Prof. Hideaki Ishii, Prof. Ahmet Cetinkaya, and Prof. Quanyan Zhu for the discussions on the research. It is a pleasure to work and write papers together with them during my stay in Tokyo Tech. I also would like to thank Prof. Hiroya Nakao, Prof. Takayuki Ishizaki, and Prof. Takeshi Hatanaka for serving as committee members in my thesis presentation. Moreover, I am also thankful for the comments from Prof. Jun-Ichi Imura, Prof. Kazuhiro Nakadai, and their lab members at the yearly summer and winter presentations.

I would thank my labmates who helped me a lot with the day-to-day life in Tokyo Tech, especially Yan and Ravi. Many thanks also to colleagues from my home country who helped me to adapt and settle in Japan. I also would like to express my gratitude to MEXT for the financial support on my study here.

I have to thank my old friends, especially those from my college clique, for the indirect support. I can only hope that we become wiser men in spite of the different paths that we pursue.

Last but not least, I am deeply indebted to my parents, my sister, and also everyone from my extended families who are always very helpful and supportive throughout my life.

List of Publications

Journal Articles

[J1] Y. Nugraha, A. Cetinkaya, T. Hayakawa, H. Ishii, and Q. Zhu, "Dynamic resilient network games with applications to multiagent consensus", *IEEE Transactions on Control of Network Systems*, vol. 8, pp. 246-259, 2021. (Chapter 3)

[J2] ——, "Rolling horizon games of resilient networks with non-uniform horizons", *European Journal of Control*, vol. 68, pp. 100693, 2022. (Chapter 6)

Peer-reviewed Conference Articles

[C1] Y. Nugraha, A. Cetinkaya, T. Hayakawa, H. Ishii, and Q. Zhu, "Subgame perfect equilibrium analysis for jamming attacks on resilient graphs", in *Proc. American Control Conference*, 2019, pp. 2060-2065. (Chapter 3)

[C2] ——, "Dynamic resilient graph games for state-dependent jamming attacks analysis on multi-agent systems", in *Proc. IFAC World Congress*, 2020, pp. 3421–3426. (Chapter 4)

[C3] ——, "Dynamic resilient network games considering connectivity", in *Proc. IEEE Conf. Decision and Control*, 2020, pp. 3779-3784. (Chapter 5)

[C4] ——, "Cluster formation in multiagent consensus via dynamic resilient graph games", in *Proc. IEEE Conf. on Control Technology and Applications*, 2021, pp. 735-740. (Chapter 4)

[C5] ——, "Rolling horizon games for cluster formation of resilient multiagent systems", in *Proc. IEEE Conf. on Decision and Control*, 2021, pp. 4829-4934. (Chapter 5)

[C6] ——, "Rolling horizon games of resilient networks with non-uniform horizons", in *Proc. European Control Conference*, 2022, pp. 1254-1269. (Chapter 6)

Other Articles

[O1] Y. Nugraha, A. Cetinkaya, T. Hayakawa, H. Ishii, and Q. Zhu, "Two-player subgame perfect equilibrium analysis for jamming attacks on dynamic graphs", in *SICE Int. Systems and Control Symposium* as position paper, 2019. (Chapter 3)

[O2] ——, "Two-player resilient graph games for state-dependent jamming attacks analysis on multi-agent systems", in *SICE Int. Systems and Control Symposium* as position paper, 2020. (Chapter 4)

[O3] ——, "Two-player rolling horizon games for jamming attacks on multiagent systems", in *SICE Int. Systems and Control Symposium* as position paper, 2021. (Chapter 5)

[O4] ——, "A rolling horizon game considering network effect in cluster forming for dynamic resilient multiagent systems", submitted to *Automatica*, under revision. (Chapter 5)

[O5] ——, "Cluster forming of multiagent systems in energy allocation games with non-uniform horizons", *submitted to conference publication.* (Chapter 6)

[O6] ——, "Two-player incomplete games of resilient multiagent systems", *submitted to conference publication.* (Chapter 6)

References

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

[2] Y. Shoham and K. Leyton-Brown, *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations*. Cambridge University Press, 2010.

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

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

[5] F. Bullo, *Lectures on Network Systems*. Kindle Direct Publishing, 2019.

[6] 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.

[7] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Syst. Mag.*, vol. 35, pp. 46–65, 2015.

[8] H. Ishii and Q. Zhu, *Security and Resilience of Control Systems: Theory and Applications, Lecture Notes in Control and Information Sciences*. Springer, 2022, vol. 489.

[9] H. Sedjelmaci, M. Hadji, and N. Ansari, "Cyber security game for intelligent transportation systems," *IEEE Network*, vol. 33, pp. 216 – 222, 2019.

[10] D. Grimsman *et al.*, "A case study of a systematic attack design method for critical infrastructure cyber-physical systems," in *Proc. American Control Conference*, 2016, pp. 296–301.

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

[12] X. Li, J. Xu, H.-N. Dai, Q. Zhao, C. F. Cheang, and Q. Wang, "On modeling eavesdropping attacks in wireless networks," *Journal of Computational Science*, vol. 11, pp. 196–204, 2015.

[13] Y. Li, R. Huang, and L. Ma, "False data injection attack and defense method on load frequency control," *IEEE Internet of Things Journal*, vol. 8, pp. 2910–2919, 2021.

[14] D. Senejohnny, P. Tesi, and C. De Persis, "A jamming resilient algorithm for self-triggered network coordination," *IEEE Transactions on Control of Network Systems*, vol. 5, pp. 981–990, 2018.

[15] Z. Cheng, D. Yue, S. Hu, H. Ge, and L. Chen, "Distributed event-triggered consensus of multi-agent systems under periodic DoS jamming attacks," *Neurocomputing*, vol. 400, pp. 458–466, 2020.

[16] D. Bauso, L. Giarre, and R. Pesenti, "Consensus in noncooperative dynamic games: A multiretailer inventory application," *IEEE Transactions on Automatic Control*, vol. 53, pp. 998–1003, 2008.

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

[18] R. Resmi, S. Mija, and J. Jeevamma, "Model predictive consensus in networked autonomous systems using discrete Laguerre functions and event triggering approach," *European Journal of Control*, vol. 64, p. 100607, 2022.

[19] S. Hu, D. Yue, X. Xie, X. Chen, and X. Yin, "Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks," *IEEE Transactions on Cybernetics*, vol. 49, pp. 4271–4281, 2019.

[20] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 766–781, 2013.

[21] S. M. Dibaji, H. Ishii, and R. Tempo, "Resilient randomized quantized consensus," *IEEE Transactions on Automatic Control*, vol. 63, pp. 2508–2522, 2018.

[22] L. Guerrero-Bonilla, A. Prorok, and V. Kumar, "Formations for resilient robot teams," *IEEE Robotics and Automation Letters*, vol. 2, pp. 841–848, 2017.

[23] Y. Wang and H. Ishii, "Resilient consensus through event-based communication," *IEEE Transactions on Control of Network Systems*, vol. 7, pp. 471 – 482, 2020.

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

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

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

[27] ——, "The effect of time-varying jamming interference of networked stabilization," *SIAM J. Control Optim.*, vol. 56, pp. 2398–2435, 2018.

[28] 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.

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

[30] C. Wang and Z. Lu, *Proactive and Dynamic Network Defense.* Springer International Publishing, 2019.

[31] 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.

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

[33] D. Fudenberg and J. Tirole, *Game Theory.* Cambridge, MA: MIT Press, 1991.

[34] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "SINR-based DoS attack on remote state estimation: A game-theoretic approach," *IEEE Transactions on Control of Network Systems*, vol. 4, pp. 632–642, 2017.

[35] 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 Transactions on Automatic Control*, vol. 60, pp. 2831–2836, 2015.

[36] 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.

[37] L. Jia, Y. Xu, Y. Sun, S. Feng, and A. Anpalagan, "Stackelberg game approaches for anti-jamming defence in wireless networks," *IEEE Wireless Commun.*, vol. 25, pp. 120–128, 2018.

[38] 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.

[39] A. Sanjab and W. Saad, "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective," *IEEE Transactions on Smart Grid*, vol. 7, pp. 2038–2049, 2016.

[40] Y. Li, D. Shi, and T. Chen, "False data injection attacks on networked control systems: A Stackelberg game analysis," *IEEE Transactions on Automatic Control*, vol. 63, pp. 3503–3509, 2018.

[41] S. D'oro, L. Galluccio, G. Morabito, S. Palazzo, L. Chen, and F. Martignon, "Defeating jamming with the power of silence: a game-theoretic analysis," *IEEE Transactions on Wireless Communications*, vol. 14, pp. 2337–2352, 2014.

[42] J. Chen, C. Touati, and Q. Zhu, "Optimal secure two-layer iot network design," *IEEE Transactions on Control of Network Systems*, vol. 7, pp. 398–409, 2020.

[43] I. Kordonis and G. Papavassilopoulos, "Network design in the presence of a link jammer: A zero-sum game formulation," in *IFAC PapersOnLine*, 2017, pp. 9211–9217.

[44] D. Bauso, "Consensus via multi-population robust mean-field games," *Systems & Control Letters*, vol. 107, pp. 76–83, 2017.

[45] M. A. uz Zaman, K. Zhang, E. Miehling, and T. Başar, "Approximate equilibrium computation for discrete-time linear-quadratic mean-field games," in *Proc. American Control Conference*, 2020, pp. 333–339.

[46] F. Parise, B. Gentile, S. Grammatico, and J. Lygeros, "Network aggregative games: Distributed convergence to nash equilibria," in *Proc. IEEE Conference on Decision and Control*, 2015, pp. 2295–2300.

[47] N. Li and J. R. Marden, "Designing games for distributed optimization," *IEEE Journal of Selected Topics in Signal Processing*, vol. 7, pp. 230 – 242, 2013.

[48] M. L. Littman, "Markov games as a framework for multi-agent reinforcement learning," in *Proceedings of the Eleventh International Conference on International Conference on Machine Learning*, 1994, pp. 157–163.

[49] S. Sarıtaş, S. Yüksel, and S. Gezici, "Quadratic multi-dimensional signaling games and affine equilibria," *IEEE Transactions on Automatic Control*, vol. 62, pp. 605 – 619, 2016.

[50] D. Kübler, W. Müller, and H.-T. Normann, "Job-market signaling and screening: An experimental comparison," *Games and Economic Behavior*, vol. 64, pp. 219–236, 2008.

[51] E. Semsar-Kazerooni and K. Khorasani, "Multi-agent team cooperation: A game theory approach," *Automatica*, vol. 45, pp. 2205–2213, 2009.

[52] X. Xu and Q. Zhao, "Distributed no-regret learning in multiagent systems: Challenges and recent developments," *IEEE Signal Processing Magazine*, vol. 37, pp. 84–91, 2020.

[53] X. Kang and Y. Wu, "Incentive mechanism design for heterogeneous peer-to-peer networks: A Stackelberg game approach," *IEEE Transactions on Mobile Computing*, vol. 14, pp. 1018 – 1030, 2014.

[54] B. Li, D. Hao, D. Zhao, and T. Zhou, "Mechanism design in social networks," in *Proc. Thirty-First AAAI Conference on Artificial Intelligence*, 2017, pp. 586–592.

[55] D. Paccagnan, R. Chandan, and J. R.Marden, "Utility and mechanism design in multi-agent systems: An overview," *Annual Reviews in Control*, vol. 53, pp. 315–328, 2022.

[56] X. Huang, Q. Liu, and X. Guo, "n-person nonzero-sum games for continuous-time jump processes with varying discount factors," *IEEE Transactions on Automatic Control*, vol. 64, pp. 2037 – 2044, 2019.

[57] Z. Zhou, P. Glynn, and N. Bambos, "Repeated games for power control in wireless communications: Equilibrium and regret," in *Proc. Conference on Decision and Control*, 2016, pp. 3603–3610.

[58] D. Bauso and M. Cannon, "Consensus in opinion dynamics as a repeated game," *Automatica*, pp. 204–211, 2018.

[59] E. R. Stephens, D. B. Smith, and A. Mahanti, "Game theoretic model predictive control for distributed energy demand-side management," *IEEE Transactions on Smart Grid*, vol. 6, pp. 1394 – 1402, 2015.

[60] S. M. Dibaji, H. Ishii, and R. Tempo, "Resilient randomized quantized consensus," *IEEE Transactions on Automatic Control*, vol. 63, pp. 2508–2522, 2018.

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

[62] B. Bosansky and J. Cermak, "Sequence-form algorithm for computing Stackelberg equilibria in extensive-form games," in *Proc. AAAI Conference on Artificial Intelligence*, 2015, pp. 805–811.

[63] G. Alcantara-Jiménez and J. B. Clempner, "Repeated Stackelberg security games: Learning with incomplete state information," *Reliability Engineering & System Safety*, vol. 195, p. 106695, 2020.

[64] W. Wei, X. Fan, H. Song, X. Fan, and J. Yang, "Imperfect information dynamic Stackelberg game based resource allocation using hidden markov for cloud computing," *IEEE Transactions on Services Computing*, vol. 11, pp. 78–95, 2018.

[65] L. Zheng, T. Fiez, Z. Alumbaugh, B. Chasnov, and L. Ratliff, "Stackelberg actor-critic: Game-theoretic reinforcement learning algorithms," in *Proceedings of the AAAI Conference on Artificial Intelligence*, 2022, pp. 9217–9224.

[66] 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.

[67] I. Drori *et al.*, "Learning to solve combinatorial optimization problems on real-world graphs in linear time," in *Proc. IEEE International Conference on Machine Learning and Applications*, 2020, pp. 19–24.

[68] L. Wang, S. Li, F. Tian, and X. Fu, "A noisy chaotic neural network for solving combinatorial optimization problems: Stochastic chaotic simulated annealing," *IEEE Transactions on Systems, Man, and Cybernetics-Part B: Cybernetics*, vol. 34, pp. 2119–2125, 2004.

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

[70] 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.

[71] C. Altafini, "Consensus problems on networks with antagonistic interactions," *IEEE Transactions on Automatic Control*, vol. 58, pp. 935–946, 2013.

[72] G. De Pasquale and M. E. Valcher, "Consensus for clusters of agents with cooperative and antagonistic relationships," *Automatica*, p. 110002, 2022.

[73] Y. Shang, "Resilient cluster consensus of multiagent systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, pp. 346–356, 2022.

[74] M. A. Maleki Sadr, M. Ahmadian-Attari, R. Amiri, and V. V. Sabegh, "Worst-case jamming attack and optimum defense strategy in cooperative relay networks," *IEEE Control Systems Letters*, vol. 3, pp. 7–12, 2019.

[75] E. Stefansson, J. F. Fisac, D. Sadigh, S. S. Sastry, and K. H. Johansson, "Human-robot interaction for truck platooning using hierarchical dynamic games," in *Proc. European Control Conference*, 2019, pp. 3165–3172.

[76] H. Li and W. Yan, "Receding horizon control based consensus scheme in general linear multi-agent systems," *Automatica*, vol. 56, pp. 12–18, 2015.

[77] M. Zhu and S. Martinez, "Stackelberg-game analysis of correlated attacks in cyber-physical systems," in *Proc. American Control Conference*, 2011, pp. 4063–4068.

[78] ——, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Transactions on Automatic Control*, vol. 59, pp. 804–808, 2014.

[79] T. Schouwenaars, J. How, and E. Feron, "Receding horizon path planning with implicit safety guarantees," in *Proc. American Control Conference*, 2004, pp. 5576–5581.

[80] Y. Kuwata, T. Schouwenaars, A. Richards, and J. How, "Robust constrained receding horizon control for trajectory planning," in *Proc. AIAA Guidance, Navigation, and Control Conference and Exhibit*, 2005, p. 6079.

[81] M. L. Katz and C. Shapiro, "Systems competition and network effects," *Journal of Economic Perspective*, vol. 8, pp. 93–115, 1994.

[82] P. Chanfreut, J. Maestre, T. Hatanaka, and E. F. Camacho, "Fast clustering for multi-agent model predictive control," *IEEE Transactions on Control of Network Systems*, to appear.

[83] S. Karimi and A. Vahidi, "Receding horizon motion planning for automated lane change and merge using monte carlo tree search and Level-K game theory," in *Proc. American Control Conference*, 2020, pp. 1223–1228.

[84] B. Wang, Y. Wu, K. R. Liu, and T. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, pp. 877–889, 2011.

[85] M. Wang, Z. Wang, J. Talbot, J. C. Gerdes, and M. Schwager, "Game-theoretic planning for self-driving cars in multivehicle competitive scenarios," *IEEE Transactions on Robotics*, vol. 37, pp. 1313–1325, 2021.

[86] Y. Li, C. A. Courcoubetis, L. Duan, and R. Weber, "Optimal pricing for peer-to-peer sharing with network externalities," *IEEE/ACM Transactions on Networking*, vol. 29, pp. 148–161, 2021.

[87] X. Gong, L. Duan, X. Chen, and J. Zhang, "When social network effect meets congestion effect in wireless networks: Data usage equilibrium and optimal pricing," *IEEE J. Sel. Areas Commun.*, vol. 35, pp. 449–462, 2017.

[88] H. Mo and G. Sansavini, "Dynamic defense resource allocation for minimizing unsupplied demand in cyber-physical systems against uncertain attacks," *IEEE Transactions on Reliability*, vol. 66, pp. 1253–1265, 2017.

[89] M. Abdallah, P. Naghizadeh, A. R. Hota, T. Cason, S. Bagchi, and S. Sundaram, "Behavioral and game-theoretic security investments in interdependent systems modeled by attack graphs," *IEEE Transactions on Control of Network Systems*, vol. 7, pp. 1585–1596, 2020.

[90] G. S. Aujla, M. Singh, N. Kumar, and A. Y. Zomaya, "Stackelberg game for energy-aware resource allocation to sustain data centers using res," *IEEE Transactions on Cloud Computing*, vol. 7, pp. 1109–1123, 2019.

[91] J. Li, H. Chen, Y. Chen, Z. Lin, B. Vucetic, and L. Hanzo, "Pricing and resource allocation via game theory for a small-cell video caching system," *IEEE Journal on Selected Areas in Communications*, vol. 34, pp. 2115 – 2129, 2016.

[92] Z. Li, D. Marelli, M. Fu, Q. Cai, and W. Meng, "Linear quadratic Gaussian Stackelberg game under asymmetric information patterns," *Automatica*, vol. 125, p. 109406, 2021.

[93] C. Zeng, B. Ren, M. Li, H. Liu, and J. Chen, "Stackelberg game under asymmetric information in critical infrastructure system: From a complex network perspective," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 29, 2019.

[94] N. Charness, "Search in chess: Age and skill differences," *Journal of Experimental Psychology: Human Perception and Performance*, vol. 7, pp. 467–476, 1981.

[95] D. Silver *et al.*, "A general reinforcement learning algorithm that masters chess, shogi, and go through self-play," *Science*, vol. 362, pp. pp. 1140–1144, 2018.

[96] R. Lagunoff and A. Matsui, "Asynchronous choice in repeated coordination games," *Econometrica*, vol. 65, pp. 1467–1477, 1997.

[97] K. Yoon, "A Folk theorem for asynchronously repeated games," *Econometrica*, vol. 69, pp. 191–200, 2001.

[98] I. Cho and D. M. Kreps, "Signaling games and stable equilibria," *The Quarterly Journal of Economics*, vol. 102, pp. 179–222, 1987.

[99] J. H. Harsanyi, "Games with incomplete information played by "Bayesian" players, Part III. The basic probability distribution of the game," *Management Science*, vol. 14, pp. 486–502, 1968.

[100] D. Umsonst, S. Sarıtaş, G. Dán, and H. Sandberg, "A Bayesian Nash equilibrium-based moving target defense against stealthy sensor attacks," 2021, arXiv:2111.06682.

[101] D. Vasal, A. Sinha, and A. Anastasopoulos, "A systematic process for evaluating structured Perfect Bayesian equilibria in dynamic games with asymmetric information," *IEEE Transactions on Automatic Control*, vol. 64, pp. 81–96, 2019.

[102] M. Castiglioni, A. Celli, A. Marchesi, and N. Gatti, "Signaling in Bayesian network congestion games: the subtle power of symmetry," in *Proc. AAAI Conference on Artificial Intelligence*, 2021, pp. 5252–5259.

[103] C. Eksin, P. Molavi, A. Ribeiro, and A. Jadbabaie, "Bayesian quadratic network game filters," *IEEE Transactions on Signal Processing*, vol. 62, pp. 2250–2264, 2014.

[104] G. P. Swann, "The functional form of network effects," *Information Economics and Policy*, vol. 14, pp. 417–429, 2002.

[105] Z. Xiong, S. Feng, D. Niyato, P. Wang, Y. Zhang, and B. Lin, "A Stackelberg game approach for sponsored content management in mobile data market with network effects," *IEEE Internet of Things Journal*, vol. 7, pp. 5184–5201, 2020.

[106] S. Zou, Z. Ma, and X. Liu, "Resource allocation game under double-sided auction mechanism: Efficiency and convergence," *IEEE Transactions on Automatic Control*, vol. 63, pp. 1273 – 1287, 2018.