Trustworthy Cyber-Physical Networks by Design: Toward a System Scientific Foundation for Security and Resilience in a Connected World

DISSERTATION

Submitted in Partial Fulfillment of

the Requirements for

the Degree of

DOCTOR OF PHILOSOPHY (Electrical Engineering)

at the

NEW YORK UNIVERSITY
TANDON SCHOOL OF ENGINEERING

by

Juntao Chen

May 2020

Trustworthy Cyber-Physical Networks by Design: Toward a System Scientific Foundation for Security and Resilience in a Connected World

DISSERTATION

Submitted in Partial Fulfillment of

the Requirements for

the Degree of

DOCTOR OF PHILOSOPHY (Electrical Engineering)

at the

NEW YORK UNIVERSITY
TANDON SCHOOL OF ENGINEERING

by

Juntao Chen

May 2020

Approved:

Department Chair Signature

Apr 28, 2020

Date

University ID: N14690369
Net ID: jc6412

Approved by the Guidance Committee:

Major: Electrical Engineering

Quanyan Zhu
Quanyan Zhu (Apr 28, 2020)

Quanyan Zhu
Associate Professor of
Electrical and Computer Engineering
Apr 28, 2020
Date

Zhong-Ping Jiang
Zhong-Ping Jiang (Apr 28, 2020)

Zhong-Ping Jiang
Professor of
Electrical and Computer Engineering
Apr 28, 2020
Date

S. S. Panwar

Shivendra Panwar
Professor of
Electrical and Computer Engineering
Apr 28, 2020
Date

Vita

I received my B.Eng. degree in Electrical Engineering and Automation from Central South University, China, in 2014. Since September 2014, I have been with the Department of Electrical and Computer Engineering, Tandon School of Engineering, New York University (NYU), to pursue the Ph.D. degree. During my Ph.D. study, I worked as a research assistant in the Laboratory for Agile and Resilient Complex Systems (LARX) directed by Prof. Quanyan Zhu, and I was also a member of NYU Center for Cybersecurity (CCS). My research interests include cyber-physical systems, cyber security, game and control theory, and artificial intelligence. I was a recipient of the Ernst Weber Ph.D. Fellowship and Dante Youla Award for Graduate Research Excellence from NYU.

Acknowledgements

First of all, I want to express my sincere gratitude to my advisor Prof. Quanyan Zhu. Over the last six years, I have benefited tremendously in many aspects from him, which were beyond becoming a knowledgeable scholar. His guidance and boundless encouragement were inevitable, that helped me through difficulties.

Secondly, I also want to thank my thesis committee members, Prof. Zhong-Ping Jiang and Prof. Shivendra Panwar, for their precious time and efforts in reviewing my dissertation and providing insightful feedback. I also thank Prof. Francisco de Leon and Prof. Farshad Khorrami for their time and help, who served as my Ph.D. qualifying exam committee members.

Thirdly, I was very fortunate to have opportunities to work with Dr. Corinne Touati at INRIA France and my mentor Prof. Tamer Başar at the University of Illinois at Urbana-Champaign. Their help was invaluable, which has yielded fruitful collaborative research outcomes. Furthermore, I feel genuinely honored working in a group with great minds. The Laboratory for Agile and Resilient Complex Systems (LARX) is one of the best in every aspect. My gratitude goes to LARX members: Jeff Pawlick, Zhiheng Xu, Rui Zhang, Linan Huang, Muhammad Junaid Farooq, Yunhan Huang, Guanze Peng, Tao Zhang, Tao Li, Shutian Liu, Shizhou Xu, Yuhan Zhao, Yunfei Ge, Yun Li, and Song Fang.

Last but not least, I give my most enormous gratitude to my family for their unconditional support. I am deeply thankful to my wife, Rui, for her consistent encouragement in the past many years.

Juntao Chen

May 2020

To my family.

ABSTRACT

Trustworthy Cyber-Physical Networks by Design: Toward a System Scientific Foundation for Security and Resilience in a Connected World

by

Juntao Chen

Advisor: Prof. Quanyan Zhu, Ph.D.

Submitted in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy (Electrical Engineering)

May 2020

With the remarkable growth of the information and communication technologies over the past few decades, the Internet of Things (IoT) is enabling ubiquitous connectivity of heterogeneous physical devices with software, sensors, and actuators. These cyber-physical integrations provide an effective solution for the development of smart cities, including industrial control systems, intelligent transportation, smart grids, robotics, and cloud computing systems, all of which can be seen as cyber-physical systems (CPS).

Though IoT enables a highly connected world, the security of IoT-enabled CPS becomes an increasingly critical concern, as the adversarial threats can come from both cyber and physical domains. A significant amount of attention has been attracted from cybersecurity experts to prevent attacks from happening. However, lessons from the advanced persistent threats have highlighted that perfect security is not always possible or cost-prohibitive. Hence, resilience plays a significant role to complement the imperfect security in CPS applications. Achieving security and resilience simultaneously is challenging, especially knowing that CPS networks are multi-layer with complex interdependencies in nature.

In this dissertation, we take a gestalt view and develop a holistic design framework for achieving best-effort security and resilience. The research establishes an interdisciplinary systems and computational science foundation for proactive, agile, and provably-correct security and resilience of CPS. This dissertation leverages techniques from diverse disciplines, including game and control theory, complex networks, artificial intelligence, optimization, economics, and operation research.

After presenting motivation and background on cyber-physical systems' security and resiliency in Chapter 1, we provide some preliminaries on game theory, mechanism design, and network science in Chapter 2. The main component of this dissertation is divided into the following three parts: 1) strategic CPS network design (Chapters 3 and 4), 2) trustworthy decision making over CPS networks (Chapters 5 and 6), and 3) mechanism design for CPS network economics (Chapters 7 and 8).

IoT-enabled CPS are vulnerable to cyber attacks, resulting in link removals in IoT communication networks. Chapter 3 is devoted to developing a heterogeneous multi-layer IoT network design framework in which a network designer can add

links to provide additional communication paths between two nodes or secure links against attacks by investing resources. The goal of the designer is to maintain the connectivity of multi-layer CPS under adversarial threats. We characterize the optimal design of secure IoT network and develop an algorithm to construct networks that satisfy heterogeneous network security specifications. The proposed scheme guarantees the resistance of each layer in the IoT network to a predefined level of malicious attacks with minimum resources.

Cyber attackers are usually strategic in channelizing their attacking resources, aiming to inflict the most damage to the targeted infrastructure system. The defender thus needs to decide how to optimally allocate his constrained security resources. To this end, Chapter 4 establishes a two-player three-stage game to capture the dynamics in the infrastructure protection and recovery phases. With costs for creating and removing links, the two players aim to maximize their utilities while minimizing the costs. We use subgame perfect equilibrium (SPE) to characterize the optimal strategies of the network defender and attacker and derive the SPE explicitly in terms of system parameters. We also give guidelines on the resilience planning for the defender by considering the strategic timing of attack.

In Chapter 5, we investigate the security investment in the IoT network with a consideration of human's bounded rational behavior. This research is motivated by the fact that users cannot be aware of the security policies taken by all its connected neighbors due to the IoT's massive connectivity. Instead, a user makes security decisions based on the cyber risks by observing a selected number of nodes. We propose a model that incorporates this limited attention nature of users/players. Each individual first builds a sparse cognitive network of nodes to respond to and then determines his security investment by minimizing his own real-world security

cost. We propose a games-in-games framework and characterize the decisions of agents by Gestalt Nash equilibrium (GNE). We also design an iterative algorithm to compute the GNE.

After investigating the security measures for static CPS networks, in Chapter 6, we shift our focus to the secure and resilient control of mobile autonomous systems (MAS). Multiple heterogeneous MAS can be integrated together as a multi-layer MAS network to offer holistic services. To design real-time secure operational strategies, we need to address the challenges of the uncoordinated nature between different layers of networks, the evolution of physical systems, and the strategic adversarial attacks. We again establish a games-in-games framework where the inner games capture the local agent-adversary type interactions, and the outer games capture the system-system level interactions. We characterize the solution of the composed game via meta-equilibrium, and design a decentralized algorithm to achieve the desirable secure configuration of MAS.

In Chapter 7, we focus on the mechanism design for on-demand provision of security service in the cloud-enabled Internet of controlled things (IoCT). We establish a holistic framework that integrates the cyber-physical layers of a cloud-enabled IoCT through the lens of contract theory. At the physical layer, the device uses cloud services to operate the system. The quality of cloud services is unknown to the device, and hence the device designs a menu of contracts to enable a reliable and incentive-compatible service. Based on the received contracts, the cloud service provider (SP) serves the device by determining its optimal cyber defense strategy. By focusing on two quality of service types of cloud SPs, we find that the contract design can be divided into two regimes, which are directly related to the requirement on the physical performance by the devices.

Chapter 8 continues to investigate the risk management over CPS networks but from a dynamic contract design perspective by considering the risk evolvement and propagation features. The considered setting includes two parties, asset owner (principal) and cybersecurity professionals (agent), where the principal delegates the risk management tasks to the agent by remunerating him for his efforts that are not directly observable. Under this information pattern, the principal aims to minimize the systemic cyber risks by designing a contract that specifies the compensation flows by taking into account the agent's incentives. We address the challenge of information asymmetry in contract design by proposing a three-step approach: estimation, verification, and control. Under mild conditions, we reveal a separation principle and a new certainty equivalence principle for dynamic principle-agent problems.

As CPS will pervade more facets of our life in the coming decades, they should be designed with a higher level of trustworthiness and confidence. There are many exciting future works to expedite CPS realizations. Chapter 9 explores and outlines a number of these future directions, including the security of learning algorithms for complex CPS, distributed intelligence for large-scale societal CPS, and cyber deception for CPS security.

Contents

List of Figures

List of Tables

Part I

Background and Motivation

Chapter 1

Introduction

1.1 Cyber-Physical System Security

The massive deployment of Internet of Things (IoT) devices enables the effective and workable smart city solutions to improve the quality of life of people. These smart devices create an increasingly connected world by integrating heterogeneous infrastructure, communication, and network components together to offer holistic services, yielding complex cyber-physical systems (CPS). In modern CPS applications, not only does the connectivity of one network itself grow but also networks are interconnected and interdependent. For example, the recent advances in smart grid technologies have witnessed the integration of power grids with communication networks. Transportation networks are connected with social networks through digital platforms for on-demand services. Robotic systems are teaming with humans to execute collaborative mission-critical tasks.

On one hand, the highly interconnected CPS increases the system's efficiency in many aspects including faster information dissemination and efficient coordinated

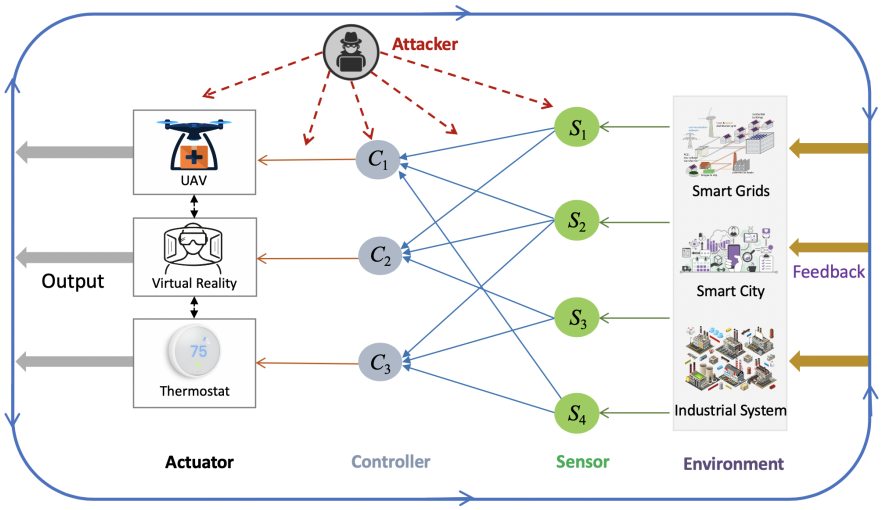


Figure 1.1: Universal adversarial attacks in modern CPS networks where the attack surface includes sensors, comunications, controllers, and actuators. The attacker can exploit the vulnerability in these components and compromise the networks from both the cyber and physical domains.

decision-making. On the other hand, it creates new challenges for the CPS operators to improve the system security and resiliency at different scales against hazards from nature, terrorism, and deliberate cyber attacks. A high level of security and resiliency of CPS is extremely critical as a single point failure in one physical system may cascade to other systems due to their interdependencies. Besides, comparing with direct attacks on physical systems, in modern CPS, the attackers can exploit the vulnerabilities in the cyber domain to achieve their malicious goals remotely. Furthermore, the multi-layer integration offers opportunities for adversaries to launch coordinated cyber-physical attacks, which could lead to more catastrophic outcomes. Figure 1.1 illustrates this phenomenon by showing that the attacker can compromise the CPS through many possible means, including the attacks to sensors, communication channels, and physical control systems of the associated applications. The statistics have shown that the economy loss due to cyberattacks

on critical infrastructure assets can be up to $1 trillion every year with the number expected to increase in 2021 [130].

Therefore, with the prevailing adversarial threats from both cyber and physical domains, safeguarding CPS from attacks is inevitably an urgent task to system operators. Recently, a significant amount of attention has been given to prevent the attacks from happening. However, lessons from the advanced persistent threats have shown that perfect security is not always possible or cost-prohibitive [26, 119]. Therefore, infrastructure operators need to invest in the system's resilience capability, which is an equally important property to complement the imperfect security in CPS applications.

Achieving CPS security and resilience simultaneously is extremely challenging. Instead of designing operational strategies for cyber and physical layers separately, we need to take a holistic view and develop an integrative framework for achieving best-effort security and resilience. To this end, this dissertation focuses on establishing an interdisciplinary systems and computational science foundation for the proactive, agile, and provably-correct security and resilience of CPS. The established frameworks and results aim to contribute to large-scale implementation and management of trustworthy CPS, such as autonomous systems, industrial control systems, transportation systems, and smart grids.

1.2 Enhancing CPS Security and Resiliency

To design modern CPS with built-in security and resiliency, we need to address multiple key challenges. First, the performance of CPS networks relies on collaborative operations of each system component. Hence, how to design the

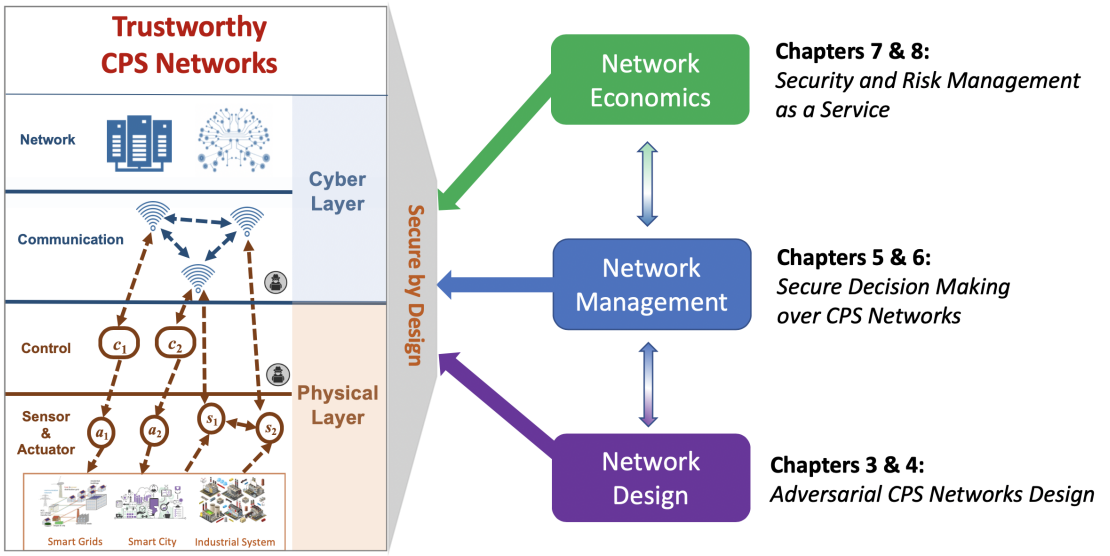


Figure 1.2: Three key aspects in enhancing the CPS security and resiliency: network design, network management, and network economics.

network strategically for maintaining connectivity under the adversarial attacks is a critical task. Second, CPS networks can be dynamic in nature, e.g., robotics and autonomous vehicles. Hence, it is important for the system designer to take into account the complex system dynamics and changing adversarial environment during the trustworthy real-time decision making. Moreover, the dynamic CPS may consist of heterogeneous agents owned by different parties. Thus, the decision should be designed in a decentralized fashion. Third, in the connected massive IoT networks, the users may not observe all the security policies taken by their connected neighbors due to cognitive limitation. Therefore, it is also important to understand how to make security investment optimally to mitigate the cyber risks under the user's bounded rationality. Fourth, risk management as a service is an important concept. As the complexity of managing enterprise assets grows, it becomes harder for asset owners to manage the cyber risks of a large number of devices and the induced systemic risk due to their massive connectivity. There

is a need to outsource the challenging risk management tasks to cybersecurity professionals. The mitigation of the cyber risk involving a third party calls for an appropriate design of cyber contract and cyber insurance mechanisms.

There is no single solution to address all these challenges simultaneously. Instead, it requires us to develop secure strategies for complex CPS networks at different levels, ranging from network design, network management, to network economics. Figure 1.2 depicts the goals of each chapter in this dissertation toward building trustworthy CPS networks.

1.2.1 Strategic Network Design

The connectivity of IoT networks plays an important role in information dissemination. On the one hand, devices can communicate directly with other devices in the underlaid network for local information. On the other hand, devices can also communicate with the infrastructure networks to maintain a global situational awareness. In addition, for IoT devices with insufficient on-board computational resources, such as wearables and drones, they can outsource heavy computations to the data centers through cloud networks, and hence extend the battery lifetime. IoT-enabled CPS networks are vulnerable to cyber attacks including the denial-of-service (DoS) and jamming attacks. These adversarial attacks can lead to communication link removals in IoT networks.

Therefore, to maintain the connectivity of devices, IoT networks need to be secure and resistant to malicious attacks. For example, V2V communication links of a car can be jammed. As a result, it loses the real-time traffic information of the road which may further cause traffic delays and accidents especially in the futuristic self-driving applications. Internet of Battlefield Things (IoBT) is another

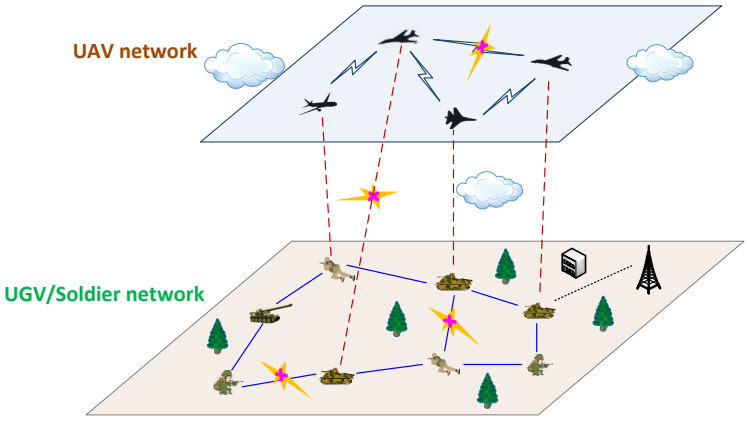


Figure 1.3: In IoBT networks, a team of UAVs and a group of soldiers and UGVs execute missions cooperatively. The agents in the battlefield share critical information through D2D communications. The UAV network and ground network form a two-layer network which faces cyber threats, e.g., jamming attacks which can lead to link removals.

example of mission-critical IoT systems. As depicted in Fig. 1.3, in IoBT networks, a team of unmanned aerial vehicles (UAVs) serves as one layer of wireless relay nodes for a team of unmanned ground vehicles (UGVs) and soldiers equipped with wearable devices to communicate between themselves or exchange critical information with the command-and-control nodes. The UAV network and the ground network naturally form a two-layer network in a battlefield, which can be susceptible to jamming attacks. It is essential to design communication networks that can allow the IoBT networks to be robust to natural failures and secure to cyber attacks in order to keep a high-level situational awareness of agents in a battlefield.

Due to heterogeneous and multi-tier features of the IoT networks, the required security levels can vary for different networks. For example, in IoBT networks, the connectivity of UAV networks requires a higher security level than the ground network if the UAVs are more likely to be targeted by the adversary. Therefore, it is

imperative to design secure IoT networks resistant to link attacks and maintain the two-layer network connectivity with heterogeneous security requirements simultaneously. To enhance the security and the robustness of the network, an IoT network designer can add extra links to provide additional communication paths between two nodes or secure links against failures by investing resources to protect the links. The goal of the multi-tier network design is to make the network connectivity resistant to link removal attacks by anticipating the worst attack behaviors.

As discussed above, adding link redundancy is an effective approach to increase the security level of CPS networks. However, it becomes expensive when the cost for creating links is costly, especially knowing that the attacker is powerful. Therefore, the system designer also needs to invest on the resiliency to recover the system after its compromise. Recovering the CPS network from attack is a top priority for designers especially in the service-oriented critical infrastructures including electric power and communication networks. With a limited budget of resources, it is essential to develop an optimal post-attack healing mechanism as well as a pre-attack secure mechanism holistically and understand the fundamental tradeoffs between security and resilience in the infrastructures. To this end, dynamic game approach provides a quantitative framework to analyze the interactions between the system defender and attacker, where the CPS network designer aims to keep the network connected before and after the attack, while the objective of the adversary is to keep the network disconnected after the attack.

The resilience of the CPS network is characterized by the capability of the network to maintain connectivity after the attack and the time it takes to heal the network. The security of the CPS is characterized by the capability of the network to combat and withstand the attack before healing. Adding a large number of

redundancies to the network can prevent the attack from disconnecting the network, but this approach can be costly. Hence, it is important to make strategic decisions and planning to yield a joint protection and recovery mechanism for the CPS at a minimum cost.

1.2.2 Trustworthy Decision Making

In cyber networks, security management and practices of users are often viewed as the weakest link [137]. The lack of security awareness and expertise at the user's end creates human-induced vulnerabilities that can be easily exploited by an adversary, exacerbating the insecurity of IoT. Hence, in the IoT, each device owner or system manager needs to allocate resources (e.g. human resources, computing resources, investments or cognition) to secure his applications.

The security policy of one device can have an impact on the security risk of nodes that are connected to it. Since various users own different devices, the security management in IoT is decentralized in nature. Therefore, the process of decentralized security decision making can be modeled as a game problem in which each user strategically allocates his resources to secure the devices. For example, in smart and connected communities as depicted in Fig 1.4, each household needs to safely configure its network and regularly updates its software and password of the IoT devices to secure the network. In this game, the users' risks are reduced when their connected neighbors are of high-level security. Due to the complex and massive connections, users cannot be aware of the security policies taken by all its connected neighbors. Instead, a user can only make security decisions based on the cyber risk by observing a selected number of nodes. This fact indicates that the game model needs to take into account the bounded rationality of players. Therefore, to make

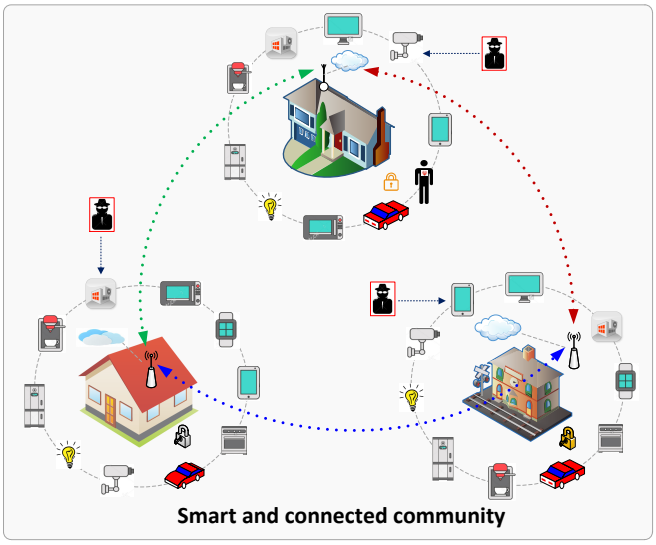


Figure 1.4: IoT-enabled interconnected smart community. The connectivity, on one hand, enhances the situational awareness of smart homes. However, it increses the cyber risks of the community. Hence, the cyber security of each household not only dependents on its own risk management strategy but also the ones of connected neighbors. Secure and decentralized decision making is necessary for each agent in the network.

trustworthy decisions in IoT networks, the users need to determine their security investment as well as allocate their attention resources in a holistic manner.

Other than managing security risks over static IoT networks, providing trustworthy decision support for dynamic CPS is another important topic. Dynamic CPS has a vast number of applications including mobile robotics, autonomous vehicles, etc. Similar to the static CPS networks, the connectivity of multi-agent mobile autonomous systems (MAS) is important, since a higher connectivity enables faster information spreading and hence a high-level of situational awareness. Maintaining the connectivity of MAS network is challenging. First, cybersecurity is a critical concern to MAS, as robots are prone to adversarial attacks; e.g., the communication links between robots can be jammed which decreases the connectivity. Another

challenge comes from the incoordination between different layers of MAS. For example, in the two-layer UAV and UGV mobile networks, though the objectives of two network operators are aligned, the UAVs are operated by one entity while the UGVs is operated by another. The lack of the centralized planning can result in insufficient coordination between two networks and lead to disruptions in connectivity and security vulnerabilities. Therefore, secure control of the multi-layer MAS networks is critical to maintain the global system performance at a high level. Then the objective becomes how to capture the interactions between mobile agents within a network and across networks and enable the design of distributed control algorithms that can maintain the connectivity in both adversarial and non-adversarial environments.

1.2.3 Mechanism Design for Cyber-Physical Risk Transfer

Cyber contract and insurance mechanism design is another approach that can be used to manage risks in CPS. We next describe two scenarios including a static contract mechanism for security as a service in the cloud-enabled IoT and a dynamic contract for systemic cyber risks management in the interdependent enterprise network.

In IoT applications where physical systems play a critical role, such as smart grid and autonomous driving, the sensing, actuation and control of devices in the IoT have given rise to an expanded term: *Internet of Controlled Things* (IoCT). A cloud-enabled IoCT allows heterogeneous components to provide services in an integrated system. However, the cloud layer can be insecure, since it faces cyber threats, and malicious attackers can steal or infer keys used to authenticate devices in the cloud-enabled IoCT. These types of attacks are known as *advanced persistent*

threats (APTs) [129]. The traditional cryptography approaches are not sufficient to deal with this class of attacks, since APTs lead to complete compromise of the cloud without the detection of network administrators. Some real-world examples of APTs include the Stuxnet which broke down approximately one fifth of nuclear centrifuges in Iran [97]. In addition, the operation "Red October" compromised the network systems of a large number of diplomatic, governmental and scientific research organizations to steal credential data in various countries across the world [138]. Due to the stealthiness and persistent nature of APTs, the cyber defense against APTs should shift from the focus on designing perfect security using cryptographic methods to best-effort strategic defense by optimally allocating constrained security resources.

To this end, contract-based game-theoretic framework offers a way to model the security of the cloud. The performance of the physical system is closely related to the security of the cloud. To use the cloud services, the device needs to plan and buy services from the cloud to fulfill its control task. Based on contract theory, the service relationships between the device and cloud SP further create a new paradigm of *security as a service* in the cloud-enabled IoCT. This mechanism design approach enables an on-demand service provision of security and a pricing mechanism to service real-time cloud-enabled IoCT. Furthermore, this paradigm provides reliable ways to deliver critical IT services to future IoTs.

Cyber contract mechanism is also useful in managing dynamic systemic risks. The complex interdependencies between nodes and fast evolution nature of threats have made it challenging to mitigate systemic risks of enterprise network and thus requires expert knowledge from cyber domains. As depicted in Fig. 1.5, the asset owners or system operators can delegate tasks of risk management including

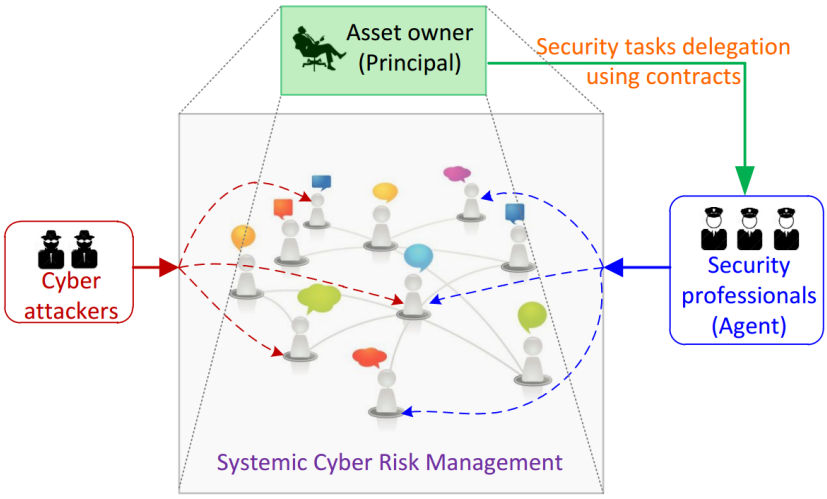


Figure 1.5: Systemic cyber risk management for enterprise network. The asset owner (principal) delegates the risk management tasks, e.g., network monitoring and software patching, to security professionals (agents) by designing a contract which specifies the remuneration schemes. The amount of remuneration is directly related to the systemic risk outcome of the network.

security hardening and risk mitigation to security professionals. The owner can be viewed as a principal who employs a security professional to fulfill tasks that include monitoring the network, patching the software and devices, and recovering machines from failures. The security professionals can be viewed as an agent whose efforts are remunerated by the principal. This principal-agent type of interaction models the service relationships between the two parties. The effort of the agent can be measured by the hours he spends on the security tasks. Moreover, the amount of allocated effort has a direct impact on the systemic cyber risk. For example, with more frequent scans on suspicious files and the Internet traffic at each node, the cyber risk becomes low and less likely to spread. An agent plays an important role in systemic risk as he can determine the amount of his effort and the way of distributing efforts on protecting nodes over the network. Hence, it is essential for the principal to incentivize the agent to distribute his resources

desirably to protect the network.

One feature in designing this type of mechanism is the lack of knowledge of the principal about the effort spent by the agent. This is reflected by the fact that the principal is only able to observe risk outcomes, e.g., the denial or failures of services and conspicuous performance degradation. Moreover, due to the randomness in the cyber network, e.g., the biased assessment of risks and the unknown attack behaviors, the cyber risk evolves under uncertainties, making it difficult for the principal to infer the exact effort of the agent from the observations. This type of incomplete information structure is called *moral hazard* in contracts. The asset owner aims to minimize the systemic cyber risk by providing sufficient incentives to the risk manager through a dynamic contract that specifies the compensation flows and suggested effort, while the risk manager's objective is to maximize his payoff with minimum effort by responding to the agreed contract. This problem can be formulated as a differential game under incomplete information.

1.3 Background and Status Quo

1.3.1 CPS and IoT Security

Due to the increasing cyber threats, IoT security becomes a critical concern nowadays [135]. Depending on the potential of cyber attackers, IoT networks face heterogeneous types of attacks [108]. For example, attackers can target the edge computing nodes in IoT, e.g., RFID readers and sensor nodes. Some typical adversarial scenarios include the node replication attack by replicating one node's identification number [117], DoS by battery draining, sleep deprivation, and outage attacks [91, 134]. The attackers can also launch attacks through the

IoT communication networks. Quintessential examples include the eavesdropping attack where the attacker captures the private information over the channel, and utilizes the information to design other tailored attacks [109]. Another example is the data injection attack where the attacker can inject fraudulent packets into IoT communication links through insertion, manipulation, and replay techniques [144].

With the increasing adoption of information and communication technologies, security is also a critical concern for IoT-enabled CPS [4, 98]. In [27], the authors have used bilevel and trilevel optimization models to design secure critical infrastructure against terrorist attacks. A cross-layer design approach has been proposed in [118, 148] to optimize the performance of cyber-physical control systems where the security is modeled using a game-theoretic framework. Furthermore, [146] has proposed a dynamic game-theoretic approach to investigate the coupling between cyber security policy and robust control design of industrial control systems under cascading failures. In addition, [83] and [100] have designed protective strategies using stochastic games for energy systems under cascading failures due to attacks. Different from the literature, in Chapter 5, we focus on security risk management of IoT networks by capturing bounded rationality of players [45].

In addition to the system security, resilience is another crucial property that needs to be considered by CPS network designers [127]. In [145], the authors have proposed a hybrid framework for robust and resilient control design with applications to power systems by considering both the unanticipated events and deterministic uncertainties. The authors in [5] have studied the resilience aspect of routing problem in parallel link communication networks using a two-player game and designed stable algorithms to compute the equilibrium strategies. [55] has studied the critical infrastructure resilience by focusing on two metrics, optimal

repair time and resilience reduction worth, to measure the criticality of various components in the system. The resilience of critical infrastructures, e.g., smart grid [40, 42], has also been investigated significantly in literature. A recent book [46] has been devoted to study the design of resilient interdependent networks.

Maximizing CPS-IoT network connectivity has been investigated vastly in literature. Some recent advances in this field include adversarial networks design [25, 37, 69] and strategic network formation games [10, 34, 39]. One specific application of CPS is mobile autonomous systems (MAS). When MAS is adopted in mission critical scenarios, such as disaster-affected areas, a higher network connectivity provides a higher level of situational awareness [36]. Connectivity control of mobile robotic network has been addressed in a fully centralized way [80, 105] and completely decentralized way [126]. Our proposed model in Chapter 6 stands in between these two frameworks, and thus results in balanced features in terms of resiliency and optimality.

1.3.2 Game-Theoretic Methods for Cybersecurity

Game-theoretic methods have been extensively used to model the cybersecurity [74, 103, 148]. In [142], the authors have addressed the resource allocation in defending against stealthy attacks through a game model. In addition, game approaches have been adopted in dealing with the emerging IoT security issues, e.g., eHealth [52] and trust in wireless sensor networks [73]. A lot of recent works have been contributed to defending against APTs [26, 129] using game-theoretic approaches [81, 119]. In [119], the authors have addressed the APT threats in cyber-physical systems by proposing a multi-layer `FlipIt` game-based model.

Due to the interconnectivity between different agents, the security of one agent

is also dependent on its connected ones which gives rise to the notion of "interdependent security" [94]. The authors in [41, 44, 119, 139] have further investigated the security interdependencies in multilayer cyber-physical systems using game-theoretic approaches. Huang *et.al* [82, 83] have adopted a stochastic Markov game model to design resilient operating strategies for multilayer interdependent networks.

As the interactions between the defender and attacker evolve over time, there is a need for a dynamic framework to model their strategic behaviors. To this end, dynamic game approaches have been widely used to investigate the network security and resilience. For example, [125] has used a differential game to model the malware defense in wireless sensor networks where the system designer chooses strategies to minimize the overall cost. A stochastic repeated game and an iterative learning mechanism have been adopted for moving target defense in networks [150]. In [49], a multistage Stackelberg game has been studied for developing deceptive routing strategies for nodes in a multihop wireless communication network. Furthermore,[35] has proposed a three-player three-stage game-theoretic framework including two network operators and one attacker to enable the secure design of multi-layer infrastructure networks.

1.3.3 Dynamic Games of Incomplete Information

The contract mechanism design in mitigating evolving systemic risks can be cast as a dynamic game under nonstandard information [43]. Dynamic games of incomplete or imperfect information have been studied within the context of different classes of games, such as repeated games [7], differential games [30], and stochastic games [149]. Many types of information structures that entail incomplete or imperfect information have been investigated in the literature, such as partial or

noisy measurements of system states [8, 16, 75, 86, 87], and asymmetric information for the players [31, 71, 72]. Approaches to control and optimization under classical information structures, also extended to games, include the information state based separation principle [33, 86, 87], belief updates on players' private information [48], generalized belief states of agents [75], and control over networks [141]. Decision-making under nonclassical information structures has also been studied (such as [12, 17, 128]), where the players are coupled through the system dynamics and/or the performance indices do not share the same information and could be memoryless. In this dissertation, Chapter 8 focuses on dynamic risk management over networks by investigating a class of Stackelberg-type differential games under asymmetric information.

1.4 Contributions of the Dissertation

This dissertation establishes *an interdisciplinary systems and computational science foundation for proactive, agile, and provably-correct security and resilience of CPS*. The **contributions** of this dissertation span a number of spectrums, which are summarized as follows.

1. **Models and Frameworks:** We propose multi-layer frameworks for inter-dependent CPS networks, which enable the design of networks with heterogeneous security requirements (Chapter 3) and decentralized real-time decision making of networked agents (Chapter 6). For a holistic study of the infrastructure network security and resiliency, we develop a two-player three-stage dynamic game framework (Chapter 4), capturing the strategic interplay between defender and attacker over networks. We also propose an

integrative framework to investigate the attentionally constrained security management of users in the IoT networks (Chapter 5). Furthermore, we develop innovative paradigms of security and risk management as a service for interconnected CPS networks (Chapters 7 and 8).

2. **Theoretical Advances:** We provide analytical and algorithmic tools for equilibrium analysis in both static and dynamic security games over CPS networks, where the solutions are highly scalable (Chapters 3 and 6). We also characterize fundamental tradeoffs in secure and resilient multi-layer network designs. Furthermore, we advance the theoretical understanding of dynamic mechanism design, which is a stackelberg-type differential game, for systemic cyber risk management of CPS networks under incomplete information, and identify new principles for dynamic principal-agent problems (Chapter 8).

3. **Computationally Efficient Algorithms:** We design a decentralized proximal algorithm to compute the solution containing the security and attention resources allocation of agents (Chapter 5). The algorithm discovers critical phenomena including emergence of partisanship, filling the inattention, and attraction of the mighty in the security risk management of IoT networks. We also propose a resilient and decentralized iterative algorithm with provable convergence to maximize the connectivity performance of dynamic and networked autonomous systems (Chapter 6).

4. **Applications:** Our obtained design and operational guidelines for CPS networks contribute a number of critical application fields, including resilient critical infrastructures (Chapter 4), smart and connected communities (Chapter 5), assured autonomy (Chapter 6), secure cloud-enabled Internet

of controlled things (Chapter 7), and interdependent enterprise networks (Chapter 8).

1.5 Organization of the Dissertation

The rest of this dissertation is organized as follows. Chapter 2 presents preliminaries on game theory, mechanism design, and network science. The main component of the dissertation includes the following three parts: 1) strategic CPS network design (Chapters 3 and 4), 2) trustworthy decision making over CPS networks (Chapters 5 and 6), and 3) mechanism design for CPS network economics (Chapters 7 and 8). Finally, Chapter 9 concludes the dissertation and outlines a number of future research directions.

Chapter 2

Background on Game Theory, Mechanism Design, and Network Science

In this chapter, we introduce the basics of game theory, mechanism design, and network science, which are all important in latter chapters. To design trustworthy CPS networks, understanding and analyzing the behaviors of adversaries is an important step. Game theory provides a scientific and quantitative framework to model and predict the strategic interactions between the system operator and malicious attacker. With the massive connectivity enabled by the IoT, modern CPS become more complex and interdependent. Hence, the operators need to design secure strategies by considering the heterogeneity of network components, where network science plays a critical role in facilitating the decision making over networks. Enhancing cybersecurity of CPS networks is a challenging task. It is possible to outsource the risk management of CPS to security professional. To this

end, mechanism design theory becomes critical in establishing the delegated risk management paradigm.

2.1 Introduction to Game Theory

Game theory is widely used in modeling and analyzing strategic interactions between a number of independent agents (also called *players*) [61, 115]. A game $\mathcal{G}$ can be generally defined by a tuple $\mathcal{G} := \{\mathcal{N}, (\mathcal{A}_i)_{i\in\mathcal{N}}, (U_i)_{i\in\mathcal{N}}\}$, where $\mathcal{N}$ is the set of players, $\mathcal{A}_i$ is the action set of player i, and U_i is the the utility function of player i. Specifically, we consider an N-player game, where $\mathcal{N} := \{1, 2, ..., N\}$. The decision variable of player $i \in \mathcal{N}$ is denoted by $a_i \in \mathcal{A}_i$. Note that the action set can be finite (infinite) such that players have a finite (infinite) number of possible actions. For convenience, we denote the action of all N players as $a := (a_1, a_2, ..., a_N)$. In addition, denote by $\mathcal{A}$ the Cartesian product in the form of $\mathcal{A}_1 \times \mathcal{A}_2 \times ... \times \mathcal{A}_N$.

The utility function of player i can be explicitly written as $U_i(a_i, a_{-i}) : \mathcal{A} \to \mathbb{R}$, where a_{-i} denotes the action profile of all players except the ith one. Furthermore, we denote by $\Omega \subset \mathcal{A}$ the feasible action set of all players after capturing the possibly coupled constraints. Thus, a feasible a needs to satisfy $a \in \Omega$. We further denote by Ω_i the constrained action set of player i. A game is finite, in contrast to infinite games (or continuous-kernel games), if both the action set and the number of players are finite.

2.1.1 Finite Nash Games

In finite games, each player chooses actions from a finitely countable action set, either in pure strategy or mixed-strategy sense, to maximize its utility. A

pure strategy indicates that the player chooses a single action with certainty. In comparison, a mixed-strategy is represented by a probability distribution over the action set which specifies the probability of taking each action.

To characterize the strategic behaviors of players, we adopt Nash equilibrium (NE) as the solution concept, which is defined as follows.

Definition 2.1 (Nash Equilibrium)**.** *An N-tuple action profile $a^* \in \Omega$ constitutes a Nash equilibrium (NE) of game $\mathcal{G}$ if, for all $i \in \mathcal{N}$,*

$$U_i(a_i^*, a_{-i}^*) \geq U_i(a_i, a_{-i}^*), \ \forall a_i \in \mathcal{A}_i, \text{ such that } (a_i, a_{-i}^*) \in \Omega. \tag{2.1}$$

Since a finite N-player game may not have an NE in pure strategy, the solution concept can be extended to mixed-strategy NE. The mixed-strategy of player i is denoted by p_i which assigns the probability of taking each action. In search of a mixed-strategy equilibrium, U_i is replaced by its expected value taken with respect to the mixed-strategy choices of the players, which we denote for player i by $L_i(p_1, ..., p_N)$, where $L_i : [0,1]^{|\mathcal{A}_1|} \times [0,1]^{|\mathcal{A}_1|} \times ... \times [0,1]^{|\mathcal{A}_N|} \to \mathbb{R}$. Denote $\mathcal{P}_i$ by the set of all probability distributions on $\mathcal{A}_i$. Then, the definition of mixed-strategy NE is given as follows.

Definition 2.2 (Mixed-Strategy Nash Equilibrium)**.** *An N-tuple action profile $(p_1^*, ..., p_N^*)$ constitutes a mixed-strategy NE of game $\mathcal{G}$ if, for all $i \in \mathcal{N}$,*

$$L_i(p_i^*, p_{-i}^*) \geq L_i(p_i, p_{-i}^*), \ \forall p_i \in \mathcal{P}_i. \tag{2.2}$$

The existence of NE in finite Nash games is presented below whose proof can be found in [111].

Theorem 2.1. *Every finite N-player nonzero-sum game has a Nash equilibrium in mixed-strategies.*

2.1.2 Infinite Nash Games

In an N-player infinite game, the action set $\mathcal{A}_i$ is a finite-dimensional space instead of a finitely countable set, $\forall i \in \mathcal{N}$. The utility function U_i is a function on the finite-dimensional product space $\mathcal{A}$. The definition of NE strategies of infinite games is the same as the ones in Definitions 2.1 and 2.2 with only slightly differences on the redefined action sets.

The results of existence of NE strategy are summarized in the following Theorems 2.2 and 2.3 which can be found in [67].

Theorem 2.2. *In the N-player nonzero-sum infinite game, if the constrained action set Ω_i for player i is a closed and bounded subset of a finite-dimensional Euclidean space, and $U_i(a_i, a_{-i})$ is continuous for each $i \in \mathcal{N}$, then there exists an NE in mixed-strategies.*

Theorem 2.3. *In the N-player nonzero-sum infinite game, if the constrained set Ω is a closed, bounded, and convex subset of a finite-dimensional Euclidean space, and $U_i(a_i, a_{-i})$ is strictly concave in a_i for each a_{-i} and each $i \in \mathcal{N}$, then there exists an NE in pure strategies.*

2.1.3 Stackelberg Games

The Nash equilibrium solution concept provides a noncooperative equilibrium solution for nonzero-sum games when the roles of the players are symmetric. However, when one of the players has the ability to enforce his strategy on the

others, one needs to introduce a hierarchical equilibrium solution concept. Following the terminology in [9], we call the player who dominates the game the *leader*, and the others reacting to the leader's strategy the *followers*. For the sake of clarity in exposition, we focus on presenting a two-person Stackelberg games in this section, i.e., one leader and one follower. A number of extensions of the Stackelberg solution concept to N-person static games with different levels of hierarchy can be found in [9].

Before presenting the solution concept for Stackelberg game, we introduce the following definition.

Definition 2.3 (Best Response)**.** *In a two-person static game, the set* $BR_2(a_1) \subset \Omega_2$ *defined for each* $a_1 \in \Omega_1$ *by*

$$BR_2(a_1) \subset \Omega_2 = \{\zeta \in \Omega_2 : U_2(a_1, \zeta) \geq U_2(a_1, a_2),\ \forall a_2 \in \Omega_2\} \tag{2.3}$$

is the best response set of player 2 to the strategy $a_1 \in \Omega_1$ *of player 1.*

Based on the best response definition, we define Stackelberg equilibrium solution concept as follows.

Definition 2.4 (Stackelberg Equilibrium)**.** *In a two-person game with player 1 as the leader, a strategy* $a_1^* \in \Omega_1$ *is called a Stackelberg equilibrium strategy for the leader if*

$$\min_{a_2 \in BR_2(a_1^*)} U_1(a_1^*, a_2) = \max_{a_1 \in \Omega_1} \min_{a_2 \in BR_2(a_1)} U_1(a_1, a_2). \tag{2.4}$$

Remark: If $BR_2(a_1)$ is a singleton for each $a_1 \in \Omega_1$, i.e., the best response function of player 2 is described completely by a reaction curve $l_2 : \Omega_1 \to \Omega_2$, then

(2.4) can be replaced by

$$U_1(a_1^*, l_2(a_1^*)) = \max_{a_1 \in \Omega_1} U_1(a_1, l_2(a_1)). \tag{2.5}$$

The existence of Stackelberg equilibrium is summarized below. More discussions on the properties on Stackelberg equilibrium can be found in [9].

Theorem 2.4. *The following statements hold:*

(1) Every two-person finite game admits a Stackelberg strategy for the leader, and the follower's strategy is characterized by the best response.

(2) In two-person infinite games, let Ω_1 and Ω_2 be compact subsets, and U_i be continuous on $\Omega_1 \times \Omega_2$, $i = 1, 2$. Let there exist a finite family of continuous mappings $l_i : \Omega_1 \to \Omega_2$, with $i \in I := \{1, ..., M\}$, such that $BR_2(a_1) = \{a_2 \in \Omega_2 : a_2 = l_i(a_1), i \in I\}$. Then, the two-person nonzero-sum infinite game admits a Stackelberg equilibrium strategy.

2.1.4 Differential Games

The previous introduction has focused on the static game. In many cases, players' interactions may exist over a period of time (can be finite or infinite), which requires a dynamic game framework. Depending on the time scale, dynamic games are defined either in discrete time, in which case there exists a finite number of levels of play, or in continuous time, which includes a continuum of levels of play. That is, the players act only at discrete instants of time in a discrete-time dynamic game, while act throughout a time interval in the continuous-time counterpart. According to the dimension of action space of players, the dynamic games can be

further categorized into finite and infinite ones. In this section, we will introduce the continuous-time infinite dynamic games, or differential games in the literature.

In differential games, differential equations are used to capture the evolution of the underlying decision process. The solutions to these functional equations, also called state equations, determine the possible paths of actions of players. A differential game can be formally defined as follows.

Definition 2.5 (Differential Game)**.** *An N-person differential game with a pre-specified fixed duration involves the following components:*

i) A set $\mathcal{N}$ of N players, where $\mathcal{N} := \{1, 2, ..., N\}$.

ii) A time interval $[0, T]$ which is specified a priori, denoting the duration of the game.

iii) An n-dimensional differential equation:

$$\dot{x}(t) = f(t, x(t), u^1(t), u^2(t), ..., u^N(t)), x(0) = x_0, \tag{2.6}$$

whose solution describes the state trajectory of the game. Specifically, the state satisfies $x(t) \in \mathcal{S}^0$, $t \in [0, T]$, where $\mathcal{S}^0$ is a subset of a finite-dimensional vector space, $\mathbb{R}^n$. $u^i(t) \in \mathcal{U}^i$, $i \in \mathcal{N}$, is the control/action of player i at time t, where $\mathcal{U}^i$ is a subset of real space of appropriate dimension, denoting player i's action space.

iv) Two functionals $q^i : \mathcal{S}^0 \to \mathbb{R}$ and $g^i : [0, T] \times \mathcal{S}^0 \times \mathcal{U}^1 \times ... \times \mathcal{U}^N$ defined for each $i \in \mathcal{N}$. The cost function of player i in the game is defined as:

$$J^i(u^1, ..., u^N) = \int_0^T g^i(t, x(t), u^1(t), u^2(t), ..., u^N(t))dt + q^i(x(T)). \tag{2.7}$$

v) A prespecified class Γ^i *of mapping* γ^i *such that* $u^i(t) = \gamma^i(t, x)$*, where* Γ^i *is the strategy space of player* i*, and each of its element* γ^i *is a permissible strategy for player* i*,* $i \in \mathcal{N}$*.*

To determine the strategies of players in the differential game, another important factor to know beforehand is the player's knowledge of the game. Denote by $\eta^i(t)$ the state information gained and recalled by player i at time $t \in [0, T]$. Then, $\eta^i(\cdot)$ characterizes the information structure of player i, and the collection of these information structures specifies the information structure of the game. We next present a number of information structures within the context of deterministic differential games.

Definition 2.6. *In an* N*-person differential game with a fixed duration* $[0, T]$*, we call that player* i*'s information structure is*

i) open-loop if $\eta^i(t) = \{x_0\}$*,* $t \in \{0, T\}$*,*

ii) closed-loop perfect state if $\eta^i(t) = \{x_s, 0 \leq s \leq t\}$*,* $t \in \{0, T\}$*,*

iii) ϵ*-delayed closed-loop perfect state if* $\eta^i(t) = \begin{cases} \{x_0\}, & 0 \leq t \leq \epsilon \\ \{x_s, 0 \leq s \leq t - \epsilon\}, & \epsilon < t \end{cases}$*,* $t \in \{0, T\}$ *where* $\epsilon > 0$ *is fixed.*

iv) memoryless perfect state if $\eta^i(t) = \{x_0, x(t)\}$*,* $t \in \{0, T\}$*,*

iv) feedback (perfect state) if $\eta^i(t) = \{x(t)\}$*,* $t \in \{0, T\}$*.*

To ensure the existence of a unique state trajectory under players' control and hence a well-defined differential game problem, we require conditions in the following theorem.

Theorem 2.5. *Under the conditions that*

i) $f(t, x(t), u^1(t), u^2(t), ..., u^N(t))$ *is continuous in* $t \in [0, T]$ *for each* x*,*

ii) $f(t, x(t), u^1(t), u^2(t), ..., u^N(t))$ *is uniformly Lipschitz in* x*,* u^1*, ...,* u^N*,*

iii) For $\gamma^i \in \Gamma^i$*,* $\gamma^i(t, x)$ *is continuous in* t *for each* x *and and uniformly Lipschitz in* x*,*

the differential equation (2.6) *admits a unique solution for every* $\gamma^i \in \Gamma^i$*, such that* $u^i(t) = \gamma^i(t, x)$*. In addition, the unique state trajectory is continuous.*

In the following, we present two classes of differential games, including zero-sum differential games and N-person nonzero-sum differential games.

We assume that $f(t, \cdot, u^1(t), u^2(t), ..., u^N(t))$, $g^i(t, \cdot, u^1(t), u^2(t), ..., u^N(t))$, and $q^i(\cdot)$ are continuously differentiable, $\forall t \in [0, T]$.

2.1.4.1 Zero-Sum Differential Games

There are two players, player 1 and player 2, with their control denoted by u and v, respectively. The state equation can be written as

$$\dot{x}(t) = f(t, x(t), u(t), v(t)), x(0) = x_0. \tag{2.8}$$

For notational simplicity and without loss of generality, we assume all variables to be *one-dimensional*. Denote by $\mathcal{U}$ and $\mathcal{V}$ by the feasible action spaces of two players. Further, consider objective function

$$J(u, v) = \int_0^T g(t, x(t), u(t), v(t))dt + q(x(T)). \tag{2.9}$$

In the game, player 1 aims to maximize (2.9), while player 2 seeks to minimize (2.9). Our goal is to find admissible control trajectories satisfying

$$J(u, v^*) \leq J(u^*, v^*) \leq J(u^*, v). \tag{2.10}$$

Note that u^* and v^* are called minimax solution. The necessary condition for u^* and v^* satisfying (2.10) can be obtained using *Pontryagin maximum principle* [93], a well-known result in optimal control theory. Specifically, we can form a Hamiltonian function

$$H(t, x(t), u(t), v(t), \lambda(t)) = g(t, x(t), u(t), v(t)) + \lambda(t) f(t, x(t), u(t), v(t)), \tag{2.11}$$

where $\lambda \in \mathbb{R}$ is the adjoint variable satisfying constraints

$$\begin{aligned} \dot{\lambda}(t) &= -H_x(t, x(t), u(t), v(t), \lambda(t)), \\ \lambda(T) &= q_x(x(T)). \end{aligned}$$

Here, H_x and q_x stand for the partial derivative with respect to the state variable. Denote by $x^*(t)$, $0 \leq t \leq T$, the state trajectory under the minimax control solution. To this end, the necessary condition for (2.10) being hold can be written as follows:

$$H(t, x^*(t), u^*(t), v^*(t), \lambda(t)) = \min_{v \in \mathcal{V}} \max_{u \in \mathcal{U}} H(t, x^*(t), u, v, \lambda(t)). \tag{2.12}$$

Under the scenarios that the action spaces for both players are unconstrained, the necessary conditions can be simplified to: (i) the first-order conditions $H_u = 0$ and $H_v = 0$, and (ii) the second-order conditions $H_{uu} \leq 0$ and $H_{vv} \geq 0$.

2.1.4.2 N-Person Differential Games

We next consider an N-person differential game. Each player i is a minimizer with the cost function given by (2.7). The solution concept to this game is Nash equilibrium. Similar to the solution in N-person finite Nash games, the Nash equilibrium of the N-person differential game satisfies, $\forall i \in \mathcal{N}$,

$$J^i(u^{i*}, u^{-i*}) \leq J^i(u_i, u^{-i*}), \forall u_i \in \mathcal{U}^i, \tag{2.13}$$

with notation u^{-i} representing the strategy profile including all players except the ith one.

Depending on the information structure of the game, the Nash solutions take various forms. We will present the results of two types of the ones listed in Definition 2.6: open-loop and feedback strategies.

Theorem 2.6. *If $\{\gamma^{i*}(t, x_0) = u^{i*}(t),\ i \in \mathcal{N}\}$ provides an open-loop Nash equilibrium solution to the formulated N-person differential game with the corresponding state trajectory $x^*(t)$, $0 \leq t \leq T$, then the following relationships are satisfied:*

$$\begin{aligned}
\dot{x}^*(t) &= f(t, x^*(t), u^{1*}(t), u^{2*}(t), ..., u^{N*}(t)),\ x^*(0) = x_0, \\
\gamma^{i*}(t, x_0) = u^{i*}(t) &= \arg\min_{u^i \in \mathcal{U}^i} H^i(t, x^*, u^i, u^{-i*}, \lambda^i), \\
\dot{\lambda}^i(t) &= -H^i_x(t, x^*, u^{1*}, ..., u^{N*}), \\
\dot{\lambda}^i(T) &= q^i_x(x^*(T)),\ i \in \mathcal{N},
\end{aligned}$$

where $H^i(t, x, u^1, ..., u^N, \lambda^i) := g^i(t, x, u^1, ..., u^N) + \lambda^i(t) f(t, x, u^1, ..., u^N),\ t \in [0, T]$ is the Hamiltonian function, and $\lambda^i(t)$ is the costate function, $i \in \mathcal{N}$.

The feedback Nash solution is based on the current state of the game, i.e., $u^i(t) = \gamma^i(x(t), t)$, $i \in \mathcal{N}$, for some function γ^i to be determined. We then have the following result.

Theorem 2.7. *For an N-person differential game of prescribed fixed duration $[0, T]$, and under either memoryless perfect state or closed-loop perfect state information structure, the strategy profile $\{\gamma^{i*} \in \Gamma^i, i \in \mathcal{N}\}$ provides a feedback Nash equilibrium solution if there exist functions $V^i : [0, T] \times \mathbb{R}^n \to \mathbb{R}$, $i \in \mathcal{N}$, satisfying the partial differential equations*

$$\begin{aligned} -\frac{\partial V^i(t,x)}{\partial t} &= \min_{u^i \in \mathcal{U}^i} \left(\frac{\partial V^i(t,x)}{\partial x} \tilde{f}^{i*}(t, x, u^i) + \tilde{g}(t, x, u^i) \right) \\ &= \frac{\partial V^i(t,x)}{\partial x} \tilde{f}^{i*}(t, x, \gamma^{i*}(t,x)) + \tilde{g}(t, x, \gamma^{i*}(t,x)), \\ V^i(t,x) &= q^i(x), \ \ i \in \mathcal{N}, \end{aligned} \tag{2.14}$$

where $\tilde{f}^{i*}(t, x, u^i) := f(t, x, \{\gamma^*_{-i}(t,x), u^i\})$, $\tilde{g}^{i*}(t, x, u^i) := g(t, x, \{\gamma^*_{-i}(t,x), u^i\})$, and $\{\gamma^*_{-i}(t,x), u^i\} := \gamma^{1*}(t,x), ..., \gamma^{i-1*}(t,x), u^i, \gamma^{i+1*}(t,x), ..., \gamma^{N*}(t,x)$.

It is also possible to obtain the closed-form solutions to a number of special classes of differential games, such as N-person affine-quadratic differential games defined as follows.

Definition 2.7. *An N-person differential game of fixed prescribed duration is*

affine-quadratic if the functionals in (2.6) and (2.7) admit the following forms:

$$f(t,x,u^1,...,u^N) = A(t)x + \sum_{i\in\mathcal{N}} B^i(t)u^i + c(t),$$
$$g^i(t,x,u^1,...,u^N) = \frac{1}{2}\left(x^\mathsf{T} Q^i(t)x + \sum_{j\in\mathcal{N}} u^{j\mathsf{T}} R^{ij}(t)u^j\right),$$
$$q^i(x) = \frac{1}{2}x^\mathsf{T} Q^i_f x,$$

where 'T' denotes the matrix transpose operator; $A(\cdot)$, $B^i(\cdot)$, $Q^i(\cdot)$, $R^{ij}(\cdot)$ are matrices of appropriate dimensions; $c(\cdot)$ is an n-dimensional vector. All are defined on $[0,T]$, and with continuous entries. In addition, Q^i_f, $Q^i(\cdot)$ are symmetric, and $R^{ii}(\cdot)$ is positive definite, $i \in \mathcal{N}$. Note that an affine-quadratic game becomes a linear-quadratic one when $c = 0$.

The following result characterizes the analytical solution of feedback Nash equilibrium strategies in an N-person affine-quadratic differential game.

Corollary 2.1. *In an N-person affine-quadratic differential game with $Q^i(\cdot) \geq 0$, $Q^i_f(\cdot) \geq 0$, $R^{ij}(\cdot) \geq 0$, where $i,j \in \mathcal{N}$ and $i \neq j$, let there exist a set of matrix valued functions $Z^i(\cdot) \geq 0$, $i \in \mathcal{N}$, satisfying the following N coupled Riccati differential equations:*

$$\dot{Z}^i + Z^i\tilde{F} + \tilde{F}^\mathsf{T} Z^i + \sum_{j\in\mathcal{N}} Z^j B^j {R^{jj}}^{-1} R^{ij} {R^{jj}}^{-1} B^{j\mathsf{T}} Z^j + Q^i = 0, \tag{2.15}$$
$$Z^i(T) = Q^i_f, \tag{2.16}$$

where $\tilde{F}(t) := A(t) - \sum_{i\in\mathcal{N}} B^i(t)R^{ii}(t)^{-1}B^i(t)^\mathsf{T} Z^i(t)$. Then, under either memoryless perfect state or closed-loop perfect state information structure, the differential

game admits a feedback Nash equilibrium solution in the following form:

$$\gamma^{i*}(t,x) = -R^{ii}(t)^{-1}B^i(t)^{\mathsf{T}}[Z^i(t)x(t)+\zeta^i],\ i\in\mathcal{N}, \tag{2.17}$$

where ζ_i, $i\in\mathcal{N}$, are the unique solution of the following coupled linear differential equations:

$$\zeta^i + \tilde{F}^{\mathsf{T}}\zeta^i + \sum_{j\in\mathcal{N}} Z^j B^j R^{jj^{-1}} R^{ij} R^{jj^{-1}} B^{j\mathsf{T}}\zeta^j + Z^i\beta = 0,\ \zeta^i(T)=0, \tag{2.18}$$

with $\beta := c - \sum_{i\in\mathcal{N}} B^i R^{ii^{-1}} B^{i\mathsf{T}}\zeta^i$. Furthermore, the corresponding values of the cost functionals are

$$J^{i*} = V^i(0,x_0) = \frac{1}{2}x_0^{\mathsf{T}}Z^i(0)x_0 + x_0^{\mathsf{T}}\zeta^i(0) + n^i(0), \tag{2.19}$$

where $n^i(\cdot)$, $i\in\mathcal{N}$, are obtained from

$$n^i + \beta^{\mathsf{T}}\zeta^i + \sum_{j\in\mathcal{N}} \zeta^j B^j R^{jj^{-1}} R^{ij} R^{jj^{-1}} B^{j\mathsf{T}}\zeta^j = 0,\ n^i(T)=0. \tag{2.20}$$

There are other types of differential games, e.g., Stackleberg differential games. The readers interested in a more complete introduction of this type of differential games can refer to [9] (Chapter 7) for more details.

2.2 Introduction to Mechanism Design

To goal of mechanism design is to devise implementable and efficient solutions to the a non-cooperative game that involves multiple players, and each has private

information on their preferences. There are many problems in practice that can be described as a mechanism design problem, where the decision maker faces a scenario in which its payoff-related information is held privately by another agent. Mechanism design theory can also be seen as a sub-field of game theory. Due to agent's private information, mechanism designer needs to solve a game under incomplete information. In these games, if the designed mechanism is not efficient, the agents then can take advantage of their private information (e.g., lying about their preferences) to receive a higher payoff. For the purpose of promoting truth-revelation from agents, it is crucial for the mechanism designer to provide appropriate incentives and hence efficient mechanisms to achieve the desirable outcome of the game.

There is a vast literature on different types of mechanism design problems. Here, we focus on a quintessential class of problems called contract mechanisms, which have been widely used in real-world applications, such as CPS security [38], cyber risk management [47], power systems [54], mobile crowdsourcing [143], and supply chain [65].

2.2.1 Contract Theory

Contract theory has a very rich history. Its study started in 1960s and since then, it has received a significant amount of attention from economists and game theorists. Contract theory has also been widely applied to real-world economic problems, and its importance has been well recognized, including the Nobel Prize in Economic Sciences, which was awarded to Oliver Hart and Bengt Holmström jointly for their contributions to contract theory in 2016. Furthermore, contract theory is very related to mechanism design whose importance is also widely acknowledged;

e.g., Leonid Hurwicz, Eric Maskin and Roger Myerson were awarded the 2007 Nobel Prize in Economics for their contributions to mechanism design theory.

A major force that facilitates the development of contract theory is the failure of general equilibrium theory when the economic problem includes asymmetric information between players. For example, customers know more about their preferences than the service providers; service providers know more about their costs than the government; and all agents' actions taken can be partially observable. In the seller/buyer example, the information asymmetry refers to the fact that the seller does not have perfect knowledge about the characteristics of the buyer. Tools from contract theory can be leveraged to combat this information asymmetry from the seller's perspective, where he can offer appropriate incentives to the buyer by providing an efficient pricing scheme in the contract.

Another classical application scenario of contract theory lies in labor/organizational economics, in which the employer needs to design a reward mechanism for the work that the employee has done, despite the fact that employee's effort is hidden to the employer. The employer's goal is to maximize his payoff function by designing a menu of contracts for employee based on some publicly observable signals, e.g., work outcomes. This mechanism design problem can be formulated as an constrained optimization program; i.e., the employer maximizes his chosen objective function while considering the employee's incentives. Specifically, there are two major types of constraints that the employee needs to take into account. One is incentive compatibility constraint capturing the rational behavior of employee in maximizing his own payoff when selecting the contract. The other one is individual rationality constraint indicating that under the chosen contract, the employee's benefit should be no less than his reservation payoff.

The models in contract theory can be categorized into several classes of problems based on whether they are static or dynamic, whether they capture a bilateral or multilateral relationships, whether the contractual terms are one-dimensional or multi-dimensional, etc. Furthermore, these models generally fall into a principal-agent paradigm that involves two parties: an informed party and an uninformed party, which we will describe in detail below.

2.2.2 Principal-Agent Models

In the principal-agent models, one party has the bargaining power by proposing a contract, and the other party can choose to either accept it or not but is not free to propose another contract. The principal-agent problem thus can be regarded as a Stackelberg-type game in which the principal who proposes the contract is the leader and the agent who chooses to accept or reject is the follower.

The principal-agent models can be categorized according to whether the initiative in contract design belongs to the uninformed party or the informed one. We next discuss two major types of them, namely adverse selection and moral hazard.

2.2.2.1 Adverse Selection

In adverse selection framework, some characteristics of the agent are imperfectly observed by the principal. For example, in labor market, the employer may not know the level of competence of the employees. Depending on which party designs the contract, the adverse selection problems can be further classified into two classes: screening and signaling. In the screening problem, the contract mechanism is offered by the uninformed party. In contrast, the informed party devises the contract in the signaling problem.

To give a more concrete idea on the features of the adverse selection, we leverage the employer/employee as an running example. In the screening problems, the employer/uninformed party, acting as the principal, designs the contract in a manner to screen the private information owned by the employee/agent. The principal can achieve his goal by offering a menu of contracts, in which each item includes a required outcome/performance from the agent and a corresponding reward for agent's effort. In this game, different types of informed agents can choose according to their private characteristics. In the signaling problems, the informed party acts first by sending a signal that may reveal information related to its type. In the example, the employee becomes the principal and designs the contract. The contracted terms can include an action taken by the employee and an associated reward required from the employer. The computational complexity of optimal contract mechanisms can be remarkably reduced by only focusing on the incentive compatible and direct revelation mechanisms thanks to the revelation principle [110].

We next present a mathematical formulation where the agents have private information about their types, and thus can be called hidden-type problems. Let us consider N types of agents in the problem, where the type parameter is denoted by θ_i, $i \in \mathcal{N} : \{1, 2, .., N\}$. In the employer/employee example, the type can be employee's ability and competence level. The principal does not know the type information of agents explicitly. Instead, he only knows that an agent is of type θ_i with probability $\sigma_i \geq 0$, where $\sum_{i \in \mathcal{N}} \sigma_i = 1$.

The contract designed by the principal for agents of type θ_i includes two terms: required agent's outcome q_i and reward r_i. The objective function of the principal

then can be written as

$$U_p = \sum_{i \in \mathcal{N}} \sigma_i (q_i - r_i). \tag{2.21}$$

We next define by $v(\theta_i, r_i)$ the valuation of agents of type θ_i in receiving r_i reward. Then, the objective function of type θ_i agents is

$$U_a^i = v(\theta_i, r_i) - q_i. \tag{2.22}$$

There are two types of constraints to consider in the contract design: incentive compatibility (IC) and individual rationality (IR). The IC ensures that the agents receive the highest payoff when selecting the contract designed specifically for their own types. The IR guarantees the participation of all types agents by ensuring a nonnegative utility.

Definition 2.8 (Incentive Compatibility)**.** *The designed contract should be incentive-compatible; i.e., the following constrains need to be satisfied:*

$$v(\theta_i, r_i) - q_i \geq v(\theta_i, r_j) - q_j, \ \forall i, j \in \mathcal{N}, \ i \neq j. \tag{2.23}$$

Definition 2.9 (Individual Rationality)**.** *The designed contract should satisfy the following individual rationality constrains:*

$$v(\theta_i, r_i) - q_i \geq 0, \ \forall i \in \mathcal{N}. \tag{2.24}$$

The principal's goal is to maximize his utility U_p by designing contracts satisfying the above incentive constraints. To this end, the principal's problem can be formulated as follows:

$$\max_{q_i, r_i, i \in \mathcal{N}} \sum_{i \in \mathcal{N}} \sigma_i (q_i - r_i)$$
$$\text{s.t. IC (2.23), IR (2.24).} \tag{2.25}$$

Note that there are $|\mathcal{N}|^2$ number of constraints in (2.25). Therefore, with more types of agents considered, the complexity in solving (2.25) will grow quadratically. Depending on the structure of agent's valuation functional v, (2.25) could be simplified further by reducing the number of IC and IR constraints.

2.2.2.2 Moral Hazard

Another principal-agent model in parallel with the adverse selection is called moral hazard. The unique feature of this type of mechanism design problems is that the agent's actions are hidden to the principal. Furthermore, in moral hazard, the principal (uninformed party) acts first and is imperfectly informed of the actions taken by the agent (informed party). To deal with this kind information asymmetry, the principal invokes the revelation principle, and designs a menu of contracts specifying the action-reward pairs.

We consider a discrete version formulation of moral hazard in which the agent can choose between N possible actions: $\{a_i, \ \forall i \in \mathcal{N}\}$. Each action can lead to one among M outcomes: $\{x_i, \ \forall i \in \mathcal{N}\}$, where $\mathcal{M} := \{1, 2, ..., M\}$. The principal cannot differentiate the agents solely based on the observed outcome. Instead, the principal only has 'vague' information. That is, when agent chooses action a_i, the principal observes outcome x_j with probability $p_{ij} \geq 0$, satisfying $\sum_{j \in \mathcal{M}} p_{ij} = 1$, $\forall i \in \mathcal{N}$. To design an efficient contract, the principal should design the incentive

scheme that is based on the observable outcome. To this end, we denote by r_j the reward/payment that the principal delivers to the agent when he observes outcome x_j.

Therefore, the agent's utility, denoted by U_a^i, under action a_i and induced outcome x_j can be in the following form:

$$U_a^i = u(r_j) - a_i, \tag{2.26}$$

where $u : \mathbb{R}_+ \to \mathbb{R}_+$ is the agent's valuation on the reward. When the principal aims to improve the the welfare of the agents, his utility by observing outcome x_j can take the form of $x_j - r_i$.

Under a given menu of contracts $\{r_i,\ \forall i \in \mathcal{N}\}$, the agent determines his action by solving the following optimization program:

$$\max_{a_i,\ i\in\mathcal{N}} \sum_{j=1}^{M} p_{ij} u(r_j) - a_i.$$

When the agent prefers a_i, then the following inequalities characterize the IC constraints:

$$\sum_{j=1}^{M} p_{ij} u(r_j) - a_i \geq \sum_{j=1}^{M} p_{sj} u(r_j) - a_s,\ \forall s \in \mathcal{N},\ s \neq i. \tag{2.27}$$

We can also write the IR constraints, if the agent prefers action a_i, as

$$\sum_{j=1}^{M} p_{ij} u(r_j) - a_i \geq 0,\ \forall i \in \mathcal{N}. \tag{2.28}$$

In moral hazard, the principal solves the following optimization problem:

$$\max_{w_j, j\in\mathcal{N},\ i} \sum_{j=1}^{M} p_{ij}(x_j - r_j)$$
$$\text{s.t. IC (2.27), IR (2.28).} \tag{2.29}$$

The obtained a_i from 2.29 is the action chosen at the optimum, yielding the largest payoff to the principal. Though not directly controllable, the principal can affect the the actions of agents through the reward design in the contracts.

The readers interested in a comprehensive intruduction of contract theory and mechanism design can refer to [24, 96].

2.3 Introduction to Network Science

2.3.1 Modeling of Networks

An undirected graph G is defined by a pair of sets (V, E), where V is a non-empty countable set of elements, called *nodes* or *vertices*, and E is a set of unordered pairs of different nodes, called *edges* or *links*. The link (i, j) joins nodes i and j. The total number of nodes in the graph is equal to the cardinality of the set V denoted by $|V|$ which is also referred as the size of the graph G. The cardinality of the set E is equal to the number of edges. Note that in a graph with n nodes, the maximum number of links is equal to $\frac{n(n-1)}{2}$. When all pairs of nodes are connected, then G is called a complete graph.

Suppose that $G(V, E)$ consists of n nodes and interconnected by m links. *Adjacency matrix* is usually used to represent an undirected graph $G(V, E)$. Denote the adjacency matrix of G by $\mathbf{A} \in \mathbb{R}^{n\times n}$. The element of $\mathbf{A}$ is denoted by a_{ij} taking

values as follows:

$$a_{ij} = \begin{cases} w_{ij}, \text{ nodes } i \text{ and } j \text{ are connected;} \\ 0, \text{ nodes } i \text{ and } j \text{ are not connected;} \end{cases} \tag{2.30}$$

where $w_{ij} \in \mathbb{R}_+$ is the link weight. If G is an unweighted graph where links are homogeneous, then $w_{ij} = 1$ if link $(i, j) \in E$, and otherwise $w_{ij} = 0$. When G is a weighted graph where each link (i, j) is associated with a weight w_{ij} representing the intensity of its connection, then the entry in $\mathbf{A}$ becomes $a_{ij} = w_{ij}$ if link $(i, j) \in E$, and otherwise $a_{ij} = 0$.

There are a number of metrics to quantify the performance of graph for different purposes, including the node degree, nearest neighbors, reachability, shortest path, and diameter. We focus on a metric called *algebraic connectivity* [57] which is an indicator of how well a graph is connected. Algebraic connectivity is based on the Laplacian matrix of a graph. Consider a graph consists of n nodes and m links. For a link l that connects nodes i and j where the link weight equaling to w_{ij}, we define two n-dimensional vectors $\mathbf{a}_l$ and $\mathbf{b}_l$, where $\mathbf{a}_l(i) = 1$, $\mathbf{a}_l(j) = -1$, $\mathbf{b}_l(i) = w_{ij}$, $\mathbf{b}_l(j) = -w_{ij}$, and all other entries 0. When G is unweighted, $w_{ij} = 1$. Then, the Laplacian matrix $\mathbf{L}$ of network G can be expressed as

$$\mathbf{L} = \sum_{l=1}^{m} \mathbf{a}_l \mathbf{b}_l^{\mathsf{T}}. \tag{2.31}$$

Intuitively, the ith diagonal entry $\mathbf{L}_{ii}$ in the Laplacian matrix is equal to the degree of node i, i.e., $\mathbf{L}_{ii} = \sum_{j \in \mathcal{N}_i} w_{ij}, \ \forall i \in V$, where $\mathcal{N}_i$ denotes the set of nodes that connects with node i. In addition, $\mathbf{L}_{ij} = -w_{ij}, \ \forall i \neq j \in V$, if nodes i and j are connected; otherwise $\mathbf{L}_{ij} = 0$. Additionally, Laplacian matrix is positive

semidefinite, and $\mathbf{L1} = 0$, where $\mathbf{1}$ is an n-dimensional vector with all one entries. Thus, by arranging the eigenvalues of $\mathbf{L}$ in an increasing order, we obtain

$$0 = \lambda_1 \leq \lambda_2 \leq ... \leq \lambda_n, \tag{2.32}$$

where the smallest eigenvalue $\lambda_1(\mathbf{L}) = 0$, and $\lambda_2(\mathbf{L})$ is called algebraic connectivity (or Fiedler value) of G [57]. Further, $\lambda_2(\mathbf{L}) = 0$ when G is not connected. For a graph with Laplacian $\mathbf{L}$, the algebraic connectivity $\lambda_2(\mathbf{L})$ can be computed from the Courant-Fisher theorem [79] as follows:

$$\lambda_2(\mathbf{L}) = \min\{z^{\mathsf{T}}\mathbf{L}z | z \in \mathbf{1}^{\perp}, ||z||_2 = 1\}, \tag{2.33}$$

where $||\cdot||_2$ denotes the standard L_2 norm.

The readers interested in more detailed and formal discussions on graph theory can refer to [22, 136].

2.3.2 Modeling of Network-of-Networks

To facilitate the analysis and design of resilient interdependent networks, we need to establish a model for network-of-networks. We consider two interdependent networks $G_1(V_1, E_1)$ and $G_2(V_2, E_2)$, where networks 1 and 2 are represented by the graphs $G_i,\ i = 1, 2$, respectively. Network i, for $i \in \{1, 2\}$, is composed of $n_i = |V_i|$ nodes and $m_i = |E_i|$ links. The set of links denoted by E_i are called the *inter-links* of individual network i. The two networks can also be connected using *intra-links* which create the interdependencies between two networks. Let E_{12} be the set of m_{12} intra-links between G_1 and G_2, with $m_{12} = |E_{12}|$. Hence, the global network

can be represented by the combined graph $G = (V_1 \cup V_2, E_1 \cup E_2 \cup E_{12})$. Note that we also use E_{21} to denote the set of intra-links in G for convenience later, and thus $E_{21} = E_{12}$. Let $n = n_1 + n_2$ and $m = m_1 + m_2 + m_{12}$. The adjacency matrix $\mathbf{A} \in \mathbb{R}^{n \times n}$ of the global networks G has the entry a_{ij} defined in (2.30).

Let $\mathbf{A}_1 \in \mathbb{R}^{n_1 \times n_1}$ and $\mathbf{A}_2 \in \mathbb{R}^{n_2 \times n_2}$ be the adjacency matrices of G_1 and G_2. When these two networks are disconnected, $\mathbf{A}$ takes the following form

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_1 & \mathbf{0}_{n_1 \times n_2} \\ \mathbf{0}_{n_2 \times n_1} & \mathbf{A}_2 \end{bmatrix},$$

where $\mathbf{0}_{n_1 \times n_2}$ is an $n_1 \times n_2$-dimensional matrix with all zero entries. When $E_{12} \neq \emptyset$, the adjacency matrix of the network G becomes

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_1 & \mathbf{B}_{12} \\ \mathbf{B}_{12}^{\mathsf{T}} & \mathbf{A}_2 \end{bmatrix},$$

where $\mathbf{B}_{12} \in \mathbb{R}^{n_1 \times n_2}$ is an off-diagonal block matrix used to capture the effect of intra-links between networks.

The Laplacian matrix $\mathbf{L}$ can be rewritten as adjacent matrices $\mathbf{A}_1$ and $\mathbf{A}_2$. Let $\mathbf{D}_1 \in \mathbb{R}^{n_1 \times n_1}$ and $\mathbf{D}_2 \in \mathbb{R}^{n_2 \times n_2}$ be two diagonal matrices associated with network 1 and 2, respectively, which are defined as follows:

$$\begin{cases} (\mathbf{D}_1)_{ii} = \sum_j (\mathbf{B}_{12})_{ij}, \\ (\mathbf{D}_2)_{ii} = \sum_j (\mathbf{B}_{12}^{\mathsf{T}})_{ij}. \end{cases}$$

Then, by using $\mathbf{L} = \mathbf{D} - \mathbf{A}$, the Laplacian matrix of G is

$$\mathbf{L} = \begin{bmatrix} \mathbf{L}_1 + \mathbf{D}_1 & -\mathbf{B}_{12} \\ -\mathbf{B}_{12}^{\mathsf{T}} & \mathbf{L}_2 + \mathbf{D}_2 \end{bmatrix}, \tag{2.34}$$

where $\mathbf{L}_i = \mathbf{D}_i - \mathbf{A}_i, i = 1, 2$, are Laplacians associated with G_1 and G_2, respectively.

Note that depending on the modeling and decomposition of network-of-networks, the above two-layer network model can be directly extended to multi-layer ones. The off-diagonal blocks in the adjacency matrix capture the complex interdependencies between all those connected layers.

Part II

Strategic CPS Network Design

Chapter 3

Optimal Secure Multi-Layer CPS-IoT Network Design

3.1 Introduction

Internet of Things (IoTs) networks can be viewed as multi-layer networks with the existing infrastructure networks (e.g., cloud and cellular networks) and the underlaid device networks, and hence with cyber-physical features. In this chapter, we focus on a two-layer IoT network and aim to design each network resistant to different number of link failures with minimum resources. We characterize the optimal strategy of the secure network design problem by first developing a lower bound on the number of links a secure network requires for a given budget of protected links. Then, we provide necessary and sufficient conditions under which the bounds are achieved and present a method to construct an optimal network that satisfies the heterogeneous network design specifications with the minimum cost. Furthermore, we characterize the robust network topologies which optimally satisfy

a class of security requirements. These robust optimal networks are applicable to the cases when the cyber threats are not perfectly perceived or change dynamically, typically happening in the mission-critical scenarios when the attacker's action is partially observable.

The proposed framework can be applied to many mission-critical scenarios. In the case studies, we consider a battlefield scenario in which the UAV network collaborates with the soldier network to execute tasks. We investigate how the optimal network changes as the cost of forming a protected communication link varies. We also study the dynamic reconfiguration and resilience of the UAV network as nodes leave and join the battlefield.

3.2 Heterogeneous Two-Layer IoT Network Design Formulation

In this section, we formulate a two-layer secure IoT network design problem. Due to the heterogeneous features of IoT networks, the devices at each layer face different levels of cyber threats. To maintain the global situational awareness, the designer aims to devise an IoT network with a minimum cost, where each layer of IoT network should remain connected in the presence of a certain level of adversarial attacks.

Specifically, we model the two-layer IoT network with two sets of devices or nodes[1] denoted by $\mathcal{S}_1$ and $\mathcal{S}_2$. Each set of nodes is of a different type. Specifically, denote by $n_1 := |\mathcal{S}_1|$ and $n_2 := |\mathcal{S}_2|$ the number of nodes of type 1 and 2, respectively,

[1]Nodes and vertices in the IoT network refer to the devices, and they are used interchangeably. Similar for the terms edges and links.

where $|\cdot|$ denotes the cardinality of a set. We unify them to $n = n_1 + n_2$ *vertices* that are numbered from 1 to n starting from nodes in $\mathcal{S}_1$. Thus, a node labeled i is of type 1 if and only if $i \leq n_1$. Note that each set of nodes forms an IoT subnetwork. Together with the interconnections between two sets of nodes, the subnetworks form a two-layer IoT network. Technically, the communication protocols between nodes within and across different layers can be either the same or heterogeneous depending on the adopted technology by considering the physical distance constraints. Furthermore, the nodes' functionality can be different in two subnetworks depending on their specific tasks. In this chapter, our focus lies in the high-level of network connectivity maintenance.

In standard graph theory, an *edge* (or a *link*) is an unordered pair of vertices: $(i, j) \in [\![1, n]\!]^2$, $i \neq j$, where $[\![1, n]\!]^2$ is a set including all the pairs of integers between 1 and n. We recall that two vertices (nodes) i_0 and i_L are said *connected* in a graph of nodes $\mathcal{S}_1 \cup \mathcal{S}_2$ and a set of edges $\mathcal{E}$ if there exists a path between them, i.e., a finite alternating sequence of nodes and distinct links: i_0, (i_0, i_1), i_1, (i_1, i_2), i_2, ..., (i_{L-1}, i_L), i_L, where $i_l \in \mathcal{S}_1 \cup \mathcal{S}_2$ and $(i_{l-1}, i_l) \in \mathcal{E}$ for all $1 \leq l \leq L$.

In our IoT networks, the communication links (edges) are vulnerable to malicious attacks, e.g., jamming and DoS, which result in link removals. To keep the IoT network resistant to cyber attacks, the network designer can either invest (i) in redundancy of the path, i.e., using extra links so that two nodes can communicate through different paths, or (ii) in securing its links against failures where we refer to these special communication edges as *protected links*. These protected links can be typically designed using moving target defense (MTD) strategies, where the designer randomizes the usage of communication links among multiple created

channels between two nodes [147]. More precisely, we consider that for the designer, the cost per non-protected link created is c_{NP} and the cost per protected link created is c_P. It is natural to have $c_{NP} \leq c_P$ since creation of a protected link is more costly than that of a non-protected one. For clarity, we assume that the costs of protected or non-protected links at two different layers are the same. If the costs of creating links are different in two subnetworks, then the network designer needs to capture this link creation difference in his objective. Let $\mathcal{E}_{NP} \subseteq \mathcal{E}$ be the set of non-protected links and $\mathcal{E}_P \subseteq \mathcal{E}$ be the set of protected links in the IoT network, and $\mathcal{E}_{NP} \cup \mathcal{E}_P = \mathcal{E}$. In this chapter, we assume that the protection is perfect, i.e., links will not fail under attacks if they are protected. Therefore, an adversary does not have an incentive to attack protected links. Denote the strategy of the attacker by $\mathcal{E}_A$, then it is sufficient to consider attacks on a set of links $\mathcal{E}_A \subseteq \mathcal{E}_{NP}$. Furthermore, we assume that the network designer can allocate links between any nodes in the network. In the scenarios that setting up communication links between some nodes is not possible, then the network designer needs to take into account this factor as constraints when designing networks.

The heterogeneous features of IoT networks naturally lead to various security requirements for devices in each subnetwork. Hence, we further consider that the nodes in IoT network have different criticality levels (k_1 and k_2 for nodes of type 1 and 2, respectively, with $k_1, k_2 \in [\![0, |\mathcal{E}_{NP}|]\!]$, where $[\![a, b]\!]$ denotes a set of integers between a and b). It means that subnetworks 1 and 2 should remain connected after the compromise of *any* k_1 and k_2 links in $\mathcal{E}_{NP}$, respectively. Thus, the designer needs to prepare for the worst case of link removal attacks when designing the two-layer IoT network. Our problem is beyond the robust network design where the link communication breakdown is generally caused by nature failures. In this

chapter, we consider the link removal which is a consequence of cyber attacks, e.g., jamming and DoS attack. Furthermore, in our problem formulation, the network designer can allocate protected links which can be seen as a security practice, and he takes into account the strategic behavior of attackers, and designs the optimal secure networks. Without loss of generality, we have the following two assumptions:

(A1) $k_1 \leq k_2$.

(A2) $n_1 \geq 1$, $n_2 \geq 1$.

Specifically, (A1) indicates that the IoT devices in subnetwork 2 are relatively more important than those in subnetwork 1, and thus subnetwork 2 should be more resistant to cyber attacks. Another interpretation of (A1) can also be that subnetwork 2 faces a higher level of cyber threats, and the network designer needs to prepare a higher security level for subnetwork 2. In addition, (A2) ensures that no IoT subnetwork is empty.

More precisely, consider a set of vertices $\mathcal{S}_1 \cup \mathcal{S}_2$ and edges $\mathcal{E}_P \cup \mathcal{E}_{NP}$. The IoT network designer needs to guarantee the following two cases:

(a) if $|\mathcal{E}_A| \leq k_1$, then all nodes remain attainable in the presence of attacks, i.e., $\forall i, j \in \mathcal{S}_1 \cup \mathcal{S}_2$, there exists a path in the graph $(\mathcal{S}_1 \cup \mathcal{S}_2, \mathcal{E}_P \cup \mathcal{E}_{NP} \backslash \mathcal{E}_A)$ between i and j.

(b) if $|\mathcal{E}_A| \leq k_2$, nodes of type 2 remain attainable after attacks, i.e., $\forall i, j \in \mathcal{S}_2$, there exists a path in the graph $(\mathcal{S}_1 \cup \mathcal{S}_2, \mathcal{E}_P \cup \mathcal{E}_{NP} \backslash \mathcal{E}_A)$ between i and j.

Remark: We denote the designed network satisfying (a) and (b) above by $s^D := (\mathcal{S}_1 \cup \mathcal{S}_2, \mathcal{E}_P \cup \mathcal{E}_{NP})$, and call such heterogeneous IoT networks (k_1, k_2)-*resistant* (with $k_1 \leq k_2$). The proposed $(k1, k2)$-resistant metric provides a flexible network

design guideline by specifying various security requirements on different network components. Furthermore, in this chapter, we care about each node's degree which requires an explicit agent-level quantification. Then, the (k_1, k_2)-resistant metric is more preferable than measure of the proportion of links in each subnetwork, where the latter metric only gives a macroscopic description of the link allocation over two subnetworks.

Given the system's parameters $\mathcal{S}_1$, $\mathcal{S}_2$, k_1, and k_2, an optimal strategy for the IoT network designer is the choice of a set of links $\mathcal{E}_P \cup \mathcal{E}_{NP}$ which solves the optimization problem:

$$\begin{aligned} \min_{\mathcal{E}_P, \mathcal{E}_{NP}} \quad & c_p|\mathcal{E}_P| + c_{NP}|\mathcal{E}_{NP}| \\ \text{s.t.} \quad & \mathcal{E}_P \subseteq [\![1, n]\!]^2, \mathcal{E}_{NP} \subseteq [\![1, n]\!]^2, \\ & \mathcal{E}_P \cap \mathcal{E}_{NP} = \emptyset, \\ & s^D = (\mathcal{S}_1 \cup \mathcal{S}_2, \mathcal{E}_P \cup \mathcal{E}_{NP}) \text{ is } (k_1, k_2)-\text{resistant}. \end{aligned}$$

From the above optimization problem, the optimal network design cost directly depends on c_P and c_{NP}. In addition, as we will analyze in Section 3.3, the cost ratio $\frac{c_P}{c_{NP}}$ plays a critical role in the optimal strategy design.

Under the optimal design strategy, compromising a node with low degree, i.e., k_1 degree in subnetwork 1 and k_2 degree in subnetwork 2, is not feasible for the attacker, since the degree of any nodes without protected link in the network is larger than k_1 or k_2 depending on the nodes' layers.

Note that the above designer's constrained optimization problem is not straightforward to solve. First, the size of search space increases exponentially as the number of nodes in the IoT network grows. Therefore, we need to find a scalable

method to address the optimal network design. Second, the heterogeneous security requirements make the problem more difficult to solve. On the one hand, two subnetworks are separate since they have their own design standards. On the other hand, we should tackle these two layers of network design in a holistic fashion due to their natural couplings.

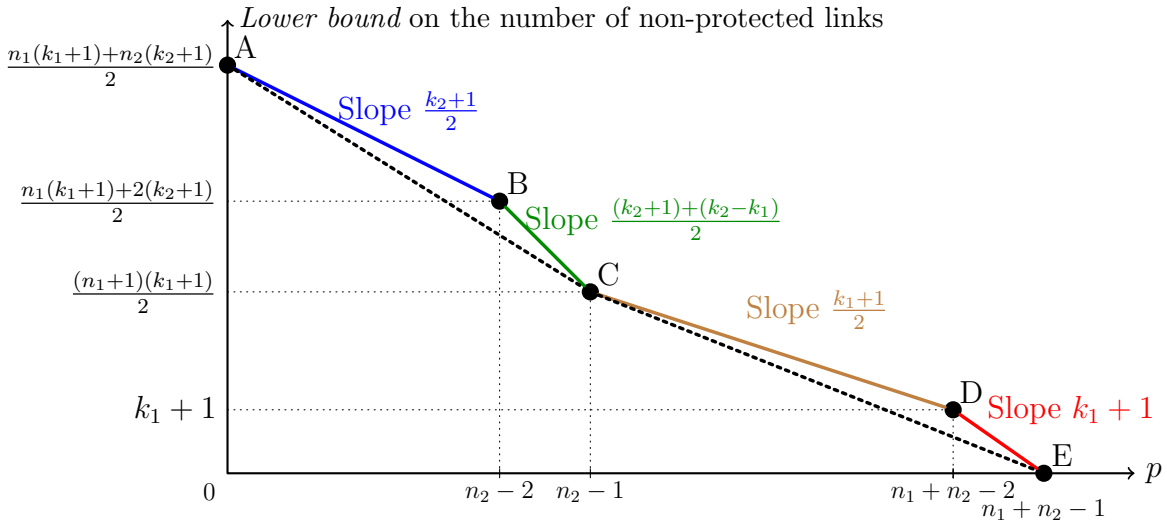


Figure 3.1: Lower bound on the number of non-protected links as a function on the number of protected links in the IoT network. Note that all the slopes of lines are quantified in their absolute value sense for convenience.

3.3 Analytical Results and Optimal IoT Network Design

In this section, we provide an analytical study of the designer's optimal strategy, i.e., the optimal two-layer IoT network design.

We first develop, for given system parameters $\mathcal{S}_1$, $\mathcal{S}_2$, k_1, k_2, c_P and c_{NP}, and for each possible number of protected links $p = |\mathcal{E}_P|$, a lower bound on the number

of non-protected links that have any (k_1, k_2)-resistant network with p protected links (Section 3.3.1). Then, we study three important cases, namely when p takes values 0, $n_2 - 1$ and $n_1 + n_2 - 1$, and present for each of them sufficient conditions under which the lower bounds are attained (Section 3.3.2). Based on this study, we can obtain the main theoretical results of this chapter, which include the optimal strategy for the designer, i.e., a (k_1, k_2)-resistant IoT network with the minimal cost, as well as the robust optimal strategy, and constructive methods of an optimal IoT network (Section 3.3.3).

3.3.1 A Lower Bound on the Number of (Non-Protected) Links

Recall that the system parameters are $\mathcal{S}_1$, $\mathcal{S}_2$, k_1, k_2, c_P and c_{NP} (corresponding to the set of nodes of criticality level 1 and 2, the values of criticality, and the unitary cost of creating protected and non-protected links). We first address the question of a lower bound on the cost for the designer with an additional constraint on the number of protected links p in the network. Since the cost is linear with the number of non-protected links, it amounts to finding a lower bound on the number of non-protected links that are required in any (k_1, k_2)-resistant network with p protected links.

Let $\tilde{s}_p^D$ be a (k_1, k_2)-resistant network containing p protected links. Then, we have the following proposition on the lower bound $|\mathcal{E}_{NP}|$.

Proposition 3.1 (Lower bound on $|\mathcal{E}_{NP}|$)**.** *The number of non-protected links of* $\tilde{s}_p^D$ *is at least of*

(i) $\dfrac{n_1(k_1+1) + (n_2 - p)(k_2+1)}{2}$, *if* $0 \leq p \leq n_2 - 2$,

(ii) $\dfrac{(n-p)(k_1+1)}{2}$, *if* $n_2 - 1 \leq p \leq n_1 + n_2 - 2$,

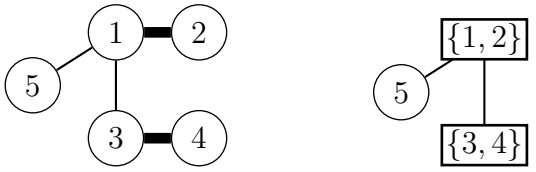
(iii) 0, *if* $p = n_1 + n_2 - 1$.

Note that p takes integer values in each regime. The results are further illustrated in Fig. 3.1.

Before proving Proposition 3.1, we first present the notion of network contraction in the following.

Network Contraction: Let $g = (\mathcal{S}_1 \cup \mathcal{S}_2, \mathcal{E}_P \cup \mathcal{E}_{NP})$ be a network. Given a link $(i,j) \in \mathcal{E}_P$, the network denoted by $g \oslash (i,j)$ refers to the one obtained by contracting the link (i,j); i.e., by merging the two nodes i and j into a single node $\{i,j\}$ (supernode). Note that any node a is adjacent to the (new) node $\{i,j\}$ in $g \oslash (i,j)$ if and only if a is adjacent to i or j in the original network g. In other words, all links, other than those incident to neither i nor j, are links of $g \oslash (i,j)$ if and only if they are links of g. Then $\hat{g}$, the contraction of network g, is the (uniquely defined) network obtained from g by sequences of link contractions for all links in $\mathcal{E}_P$ [25].

For clarity, we illustrate the contraction of a network g in Fig. 3.2. This example consists of 5 nodes and 2 protected links (represented in bold lines between nodes 1 and 2 and between nodes 3 and 4). The link $(1,2)$ is contracted and thus both nodes 1 and 2 in g are merged into a single node denoted by $\{1,2\}$ in $\hat{g}$. Similarly the link $(3,4)$ is contracted. The resulting network thus consists of node 5 and supernodes $\{1,2\}$ and $\{3,4\}$. Since g contains a link between nodes 5 and 1 in g, then nodes 5 and $\{1,2\}$ are connected through a link in network $\hat{g}$. Similarly, since nodes 1 and 3 are adjacent in g, then supernodes $\{1,2\}$ and $\{3,4\}$ are adjacent in network $\hat{g}$.



(a) Network $g = (N, \mathcal{E}_P \cup \mathcal{E}_{NP})$

(b) Contraction network $\hat{g}$

Figure 3.2: Illustration of network contraction. The protected links $(1, 2)$ and $(3, 4)$ in network g are contracted in network $\hat{g}$.

Based on network contraction, we present the proof of Proposition 3.1 as follows.

Proof. Consider an IoT network g including p protected links, and $\hat{g}$ as its contraction. Let

(1) ν_1 be the number of nodes of type 1 in $\hat{g}$ (and supernodes containing only nodes of type 1),

(2) ν_2 be the number of nodes of type 2 in $\hat{g}$ (and supernodes containing only nodes of type 2),

(3) ν_0 be the number of supernodes in $\hat{g}$ that contains nodes of both type 1 and 2.

Note that if $\nu_1 + \nu_2 + \nu_0 = 1$, (i.e., if there is a unique supernode containing all nodes of the network), then no non-protected link is needed to ensure any level of (k_1, k_2)-resistancy. Otherwise, for the IoT network to be (k_1, k_2)-resistant, each element of ν_1, ν_2 and ν_0 must have a degree of (at least) $k_1 + 1$. Further, if there exist more than one element not in ν_1; i.e., if $\nu_0 + \nu_2 \geq 2$, then each of them should have a degree of (at least) $k_2 + 1$.

Thus, a lower bound on the number of non-protected links in $\tilde{s}_p^D$ is

$$\Phi = \begin{cases} \dfrac{\nu_1(k_1+1)+(\nu_0+\nu_2)(k_2+1)}{2}, & \text{if } \nu_2+\nu_0 > 1, \\ 0, & \text{if } \nu_1+\nu_2+\nu_0 = 1, \\ \dfrac{(\nu_1+1)(k_1+1)}{2}, & \text{if } \nu_1 \geq 1 \text{ and } \nu_2+\nu_0 = 1. \end{cases}$$

Next, we focus on the study of parameters ν_0, ν_1 and ν_2. If no protected link is used, i.e., $p = 0$, then $\nu_1 = n_1$, $\nu_2 = n_2$ and $\nu_0 = 0$ and $\nu_0 + \nu_1 + \nu_2 = n_1 + n_2 = n$. Adding any protection allows to decrease the total number of elements $\nu_1 + \nu_2 + \nu_0$ by 1 (or to remain constant if the link induce a loop in a protected component of g). Thus $\nu_0 + \nu_1 + \nu_2 \geq n - p$. Similarly, for each subnetwork, we have $\nu_0 + \nu_1 \geq n_1 - p$ and $\nu_0 + \nu_2 \geq n_2 - p$. Further, the number of elements of ν_1 and ν_2 are upper bounded by the number of nodes of type 1 n_1 and type 2 n_2, respectively, i.e., $\nu_1 \leq n_1$ and $\nu_2 \leq n_2$. Finally, since $n_1 \geq 1$ then $\nu_1 + \nu_0 \geq 1$, and since $n_2 \geq 1$ then $\nu_2 + \nu_0 \geq 1$. Thus, for any p, a lower bound on the number of non-protected links in $\tilde{s}_p^D$ can be obtained by solving the following optimization problem:

$$\begin{aligned} \min_{\nu_1,\nu_2,\nu_0} \quad & \Phi \\ \text{s.t.} \quad & \nu_0 + \nu_1 + \nu_2 \geq n - p, \\ & \nu_0 + \nu_1 \geq n_1 - p, \ \nu_0 + \nu_2 \geq n_2 - p, \\ & \nu_1 \leq n_1, \ \nu_2 \leq n_2, \\ & \nu_1 + \nu_0 \geq 1, \ \ \nu_2 + \nu_0 \geq 1. \end{aligned} \tag{3.1}$$

To solve this optimization problem, we consider three cases.

Case 1: First, assume that $p < n_2 - 1$. From $\nu_0 + \nu_1 + \nu_2 \geq n - p$, we obtain that $\nu_0 + \nu_2 > 1$. Thus, (3.1) reduces to $\min_{\nu_1,\nu_2,\nu_0} \ \frac{\nu_1(k_1+1)+(\nu_0+\nu_2)(k_2+1)}{2}$ with the

same constraints as in (3.1) except $\nu_0 + \nu_2 > 1$.

Since $k_2 \geq k_1$, then the minimum of the objective is obtained when $\nu_0 + \nu_2$ is minimized, i.e., when all protections involve nodes of type 2. Then, $\nu_0 + \nu_2 = n_2 - p$. Thus, the lower bound is equal to $\frac{n_1(k_1+1)+(n_2-p)(k_2+1)}{2}$. This result is illustrated by the line joining points A and B in Fig. 3.1.

Case 2: Assume that $n_2 - 1 \leq p \leq n_1 + n_2 - 2$. Then $n - p \leq n_1 + 1$. Therefore, for a given p, i.e., for a given minimal value of $\nu_0 + \nu_1 + \nu_2$, we can have either $\nu_0 + \nu_2 > 1$ or $\nu_0 + \nu_2 = 1$. Then, the lower bound of the number of non-protected links is $\min\left\{\frac{n_1(k_1+1)+(n_2-p)(k_2+1)}{2}, \frac{(n-p)(k_1+1)}{2}\right\}$. Recall that $k_2 \geq k_1$, and therefore the lower bound achieves at $\frac{(n-p)(k_1+1)}{2}$. This observation is illustrated by the line in Fig. 3.1 joining points C and D.

Case 3: Finally, when $p = n - 1$, $\nu_0 + \nu_1 + \nu_2 = 1$, and thus no non-protected link is needed, which is represented by point E in Fig. 3.1. □

Based on Proposition 3.1, we further comment on the locations where protected and non-protected links are placed in the two-layer IoT networks.

Corollary 3.1. *When $0 \leq p \leq n_2 - 2$, the protected links purely exist in subnetwork 2. When $n_2 - 1 \leq p \leq n_1 + n_2 - 2$, subnetwork 2 only contains protected links, and non-protected links appear in subnetwork 1 or between two layers. When $p = n_1 + n_2 - 1$, then all nodes in the two-layer IoT network are connected with protected links.*

Corollary 3.1 has a natural interpretation that the protected link resources are prior to be allocated to a subnetwork facing higher cyber threats, i.e., subnetwork 2 in our setting.

3.3.2 Networks with Special Values of p Protected Links

In the previous Section 3.3.1, we have studied for each potential number of protected links p, a lower bound $m(p)$ on the minimum number of non-protected links for an IoT network with sets of nodes $\mathcal{S}_1$ and $\mathcal{S}_2$ being (k_1, k_2)-resistant. Then, the cost associated with such networks is

$$C(p, m(p)) = pc_P + m(p)c_{NP},$$

where $C : \mathbb{N} \times \mathbb{N} \to \mathbb{R}_+$. Since the goal of the designer is to minimize its cost, we need to investigate the value of p minimizing such function $C(p, m(p))$.

In Fig. 3.1, we note that the plot of a network of equal cost (*iso-cost*) K is a line of equation $\frac{K-pc_P}{c_{NP}}$. It is thus a line of (negative) slope c_P/c_{NP} that crosses the y-axis at point K/c_{NP}. Recall also that the graph that shows $m(p)$ as a function of p is on the upper-right quadrant of its lower bound. Thus, the optimal value of p corresponds to the point where an iso-cost line meets the graph $m(p)$ for the minimal value K. From the shape of the lower bound drawn in Fig. 3.1, the points A, C and E are selected candidates leading to the optimal network construction cost. We thus investigate in the following the condition under which the lower bounds are reached at these critical points as well as the corresponding configuration of the optimal two-layer IoT networks.

Remark: Denote by s_p^D a (k_1, k_2)-resistant IoT network with p protected links and the *minimum* number of non-protected links.

Before presenting the result, we first present the definition of Harary network in the following. Recall that for a network containing n nodes being resistant to k link attacks, one necessary condition is that each node should have a degree of

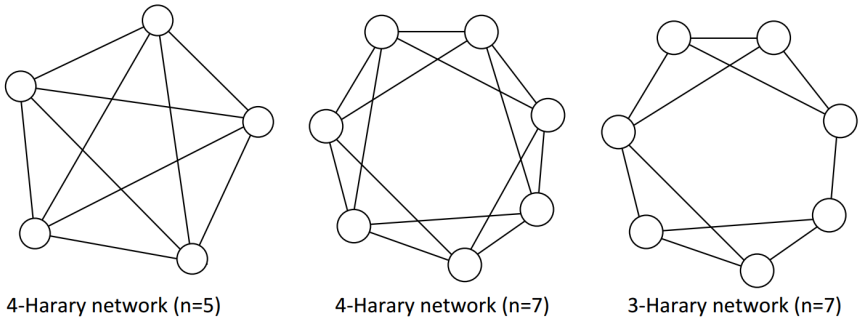


Figure 3.3: Illustration of Harary networks with different number of nodes and security levels.

at least $k+1$, yielding the total number of links more than $\left\lceil \frac{(k+1)n}{2} \right\rceil$. Here, $\lceil \cdot \rceil$ denotes the ceiling operator. Harary network below can achieve this bound.

Definition 3.1 (Harary Network [76])**.** *In a network containing n nodes, Harary network is the optimal design that uses the minimum number of links equaling $\left\lceil \frac{(k+1)n}{2} \right\rceil$ for the network still being connected after removing any k links.*

The constructive method of general Harary network can be described with cycles as follows. It first creates the links between node i and node j such that $(|i-j| \mod n) = 1$, and then $(|i-j| \mod n) = 2$, etc. When the number of nodes is odd, then the last cycle of link creation is slightly different since $\frac{(k+1)n}{2}$ is not an integer. However, the bound $\left\lceil \frac{(k+1)n}{2} \right\rceil$ can be still be achieved. For clarity, we illustrate three cases in Fig. 3.3 with $n = 5, 7$ under different security levels $k = 2, 3$. Since Harary network achieves the bound $\left\lceil \frac{(k+1)n}{2} \right\rceil$, its computational cost of the construction is linear in both the number of nodes n and the security level k.

Then, we obtain the following result.

Proposition 3.2. *For the number of protected links p taking values of $n-1$, n_2-1, and 0, we successively have:*

(i) *each* s_{n-1}^D *contains exactly* 0 *non-protected link.*

(ii) *each* $s_{n_2-1}^D$ *contains exactly* $\left\lceil \frac{(n_1+1)(k_1+1)}{2} \right\rceil$ *non-protected links if and only if* $k_1+1 \leq n_1$.

(iii) *if we have the following asumptions: (i)* $k_1 \mod 2 = 1$, *where* mod *denotes the modulus operator, (ii)* $n_2 > k_2 - k_1$ *and (iii)* $n_2 \frac{k_1+1}{2} \leq n_1$, *then each* s_0^D *contains exactly* $\left\lceil \frac{n_1(k_1+1)+n_2(k_2+1)}{2} \right\rceil$ *non-protected links.*

Proof. We successively prove the three items in the proposition in the following.

(i) Note that s_{n-1}^D contains exactly $p = n-1$ protected links. It is thus possible to construct a tree network among the set $\mathcal{S}_1 \cup \mathcal{S}_2$ of nodes that consists of only protected links. Thus, no non-protected link is required, and the lower bound (point E in Fig. 3.1) can be reached.

(ii) Suppose that $p = n_2 - 1$. If $k_1 + 1 \leq n_1$, we can construct any tree protected network on the nodes of $\mathcal{S}_2$. Further, construct a (k_1+1)-Harary network on the nodes of $\mathcal{S}_1 \cup \{n_1+1\}$, that is the nodes of type 1 and one node of type 2. Such construction is possible since $k_1 + 2 \leq n_1 + 1$. The total number of non-protected links is then exactly $\left\lceil \frac{(n_1+1)(k_1+1)}{2} \right\rceil$ (point C in Fig. 3.1). Therefore, each node in $\mathcal{S}_1 \cup \{n_1+1\}$ is connected to k_1+1 other nodes, and the IoT network cannot be disconnected after removing k_1 non-protected links. In addition, the subnetwork 2 is resistant to any number of attack since it is constructed using all protected links. Note that the constructed Harary network here is optimal, in the sense that its configuration uses the least number of links for the IoT network being (k_1, k_2)-resistant.

Next, if $k_1 + 1 > n_1$, then suppose that a network g achieves the lower bound $\left\lceil \frac{(n_1+1)(k_1+1)}{2} \right\rceil$. Consider its associated contracted network $\hat{g}$. Since g contains $n_2 - 1$

protected links, then $\hat{g}$ is such that $\nu_0 + \nu_1 + \nu_2 \geq n_1 + 1$. From the shape of the lower bound Φ in the proof of Proposition 3.1, then necessarily $\nu_0 + \nu_2 = 1$ and $\nu_1 = n_1$. Thus, all nodes in $\mathcal{S}_2$ need to be connected together by protected links. Since $|\mathcal{S}_2| = n_2$, then it requires at least $n_2 - 1$ protected links, which equals p. Thus, there cannot be any protected link involving nodes in set $\mathcal{S}_1$. In addition, each node in $\mathcal{S}_1$ needs to be connected to at least $k_1 + 1$ other nodes in the IoT network. Since $k_1 + 1 > n_1$, then every node in $\mathcal{S}_1$ should connect to at least $(k_1 + 1) - (n_1 - 1) \geq 2$ number of nodes in $\mathcal{S}_2$. Recall that in a complete network of m nodes, each node has a degree of $m - 1$, and the total number of links is $\frac{m(m-1)}{2}$. Hence, our IoT network admits a completed graph in $\mathcal{S}_1$ with some extra $n_1((k_1 + 1) - (n_1 - 1))$ non-protected links between two subnetworks, and in total at least $\frac{n_1(n_1-1)}{2} + n_1((k_1 + 1) - (n_1 - 1)) = n_1(k_1 + 1) - \frac{n_1(n_1-1)}{2}$ non-protected links. Then, comparing with the lower bound, the extra number of links required is $n_1(k_1 + 1) - \frac{n_1(n_1-1)}{2} - \frac{(n_1+1)(k_1+1)}{2} = \frac{n_1-1}{2}(k_1 + 1 - n_1) > 0$. Thus, $s^D_{n_2-1}$ does not achieve the lower bound (point C in Fig. 3.1) when $k_1 + 1 > n_1$.

(iii) Finally, suppose that $p = 0$. We renumber the nodes in the network according to the following sequence: $1, 2, \cdots, \frac{k_1+1}{2}, n_2, \frac{k_1+1}{2} + 1, \cdots, k_1 + 1, n_2 + 1, k_1 + 2, \cdots, 3\frac{k_1+1}{2}, n_2 + 2, \cdots$. Intuitively, we interpose one node in $\mathcal{S}_2$ after every $\frac{k_1+1}{2}$ nodes in $\mathcal{S}_1$. Then, we first build a $(k_1 + 1)$-Harary network among all the nodes in $\mathcal{S}_1$ and $\mathcal{S}_2$. Note that since $n_2\frac{k_2+1}{2} \leq n_1$, then the last $\frac{k_1+1}{2}$ indices of the sequence only contain nodes of type 1. Thus, by construction, there are no links between any two nodes in $\mathcal{S}_2$. Then, we can further construct a $(k_2 - k_1)$-Harary network on the nodes in $\mathcal{S}_2$, which is possible since $n_2 > k_2 - k_1$. Thus, the constructed IoT network is (k_1, k_2)-resistant, and it is also optimal since it uses the minimum number of non-protected links. □

Proposition 3.2 and Fig. 3.1 indicate that depending on the system parameters (k_1, k_2, n_1, n_2) and for a given budget, the optimal IoT network can achieve at either point A, C or E with $p = 0, n_2 - 1, n - 1$ protected links, respectively. Notice that when $k_1 + 1 > n_1$, $s^D_{n_2-1}$ is not optimal at point C and the lower bound on the number of non-protected links is not attained. Instead, in this case, $s^D_{n_2-1}$ requires $\frac{n_1(2k_1-n_1+3)}{2}$ non-protected links in which $n_1(k_1 - n_1 + 2)$ are allocated between two subnetworks, introducing protection redundancy for nodes in $\mathcal{S}_2$. For the IoT network containing 0 protected link, it reaches the lower bound (point A) if we can construct a (k_1+1)-Harary network for all nodes and an additional (k_2-k_1)-Harary network for nodes only in $\mathcal{S}_2$. As mentioned before, the Harary network admits an optimal configuration with the maximum connectivity given a number of links [76].

3.3.3 Optimal Strategy and Construction of IoT Networks

We investigate the optimal strategy and the corresponding construction for the IoT network designer in this section.

3.3.3.1 Optimal Strategy

Before presenting the main result, we comment on the scenarios that we aim to study regarding the IoT networks.

(1) First, the number of nodes is relatively large comparing with the link failure risks, i.e., $n_1 \geq k_1 + 1$ and $n_2 \geq k_2 - k_1 + 1$. Indeed, these two conditions indicate that the designer can create a secure two-layer IoT network solely using non-protected links.

(2) We further have the condition $n_2 \frac{k_1+1}{2} \leq n_1$, indicating that the type 2 nodes

with higher criticality levels in $\mathcal{S}_2$ constitute a relatively small portion in the IoT network comparing with these in $\mathcal{S}_1$. This condition also aligns with the practice that the attacker has preferences on the nodes to compromise in the IoT which generally only contain a small subset of the entire network.

(3) Finally, we have constraints $k_1 \mod 2 = 1$ and $n_2(k_2+1) \mod 2 = 0$ which are only used to simplify the presentation of the chapter (whether the number of nodes and attacks is odd or even). However, they do not affect the results significantly. Note that different cases corresponding to $k_1 \mod 2 = 0$ or $n_2(k_2+1) \mod 2 = 1$ can be studied in a similar fashion as in our current context. The only difference is that for certain system parameters, s_0^D is not an optimal strategy comparing with $s_{n_2-1}^D$ by following a similar analysis in [25].

Therefore, based on the above conditions, the scenarios that we analyze are quite general and conform with the situations in the adversarial IoT networks. Based on Proposition 3.2, we then obtain the following result on the optimal design of secure two-layer IoT networks. Note that the solution in Proposition 3 is optimal to the original optimization problem presented in Section II under the considered scenarios.

Proposition 3.3. *Under the conditions that* $n_1 \geq k_1 + 1$, $n_2 \geq k_2 - k_1 + 1$, $n_2 \frac{k_1+1}{2} \leq n_1$, $k_1 \mod 2 = 1$ *and* $n_2(k_2+1) \mod 2 = 0$, *we have the following results:*

I) Regime I: if $1 + k_1 - n(k_2 - k_1) \leq 0$, *then:*

(1) if $2\frac{c_P}{c_{NP}} \geq k_2 + 1 + \frac{k_2-k_1}{n_2-1}$, *then* s_0^D *are optimal strategies.*

(2) if $k_1+1+\frac{k_1+1}{n_1} \leq 2\frac{c_P}{c_{NP}} < k_2+1+\frac{k_2-k_1}{n_2-1}$, *then* $s^D_{n_2-1}$ *are optimal strategies.*

(3) if $2\frac{c_P}{c_{NP}} < k_1+1+\frac{k_1+1}{n_1}$, *then* s^D_{n-1} *are optimal strategies.*

II) Regime II: if $1+k_1-n(k_2-k_1) > 0$, *then:*

(1) when $k_2-k_1+1 \leq n_2 < \frac{1+k_1}{1+k_1-n_1(k_2-k_1)}$, *the optimal IoT network design strategies are the same as those in regime I.*

(2) otherwise, i.e., $n_2 \geq \frac{1+k_1}{1+k_1-n_1(k_2-k_1)}$, *we obtain*

(i) if $2\frac{c_P}{c_{NP}} \geq \frac{n_1(k_1+1)+n_2(k_2+1)}{n_1+n_2-1}$, *then* s^D_0 *are optimal strategies.*

(ii) if $2\frac{c_P}{c_{NP}} < \frac{n_1(k_1+1)+n_2(k_2+1)}{n_1+n_2-1}$, *then* s^D_{n-1} *are optimal strategies.*

Thus, $s^D_{n_2-1}$ *cannot be optimal in this scenario.*

Proof. From Proposition 3.2 and under the assumptions in the current proposition, s^D_0, $s^D_{n_2-1}$ and s^D_{n-1} achieve the lower bounds of the number of links for the network being (k_1, k_2)-resistant. In Fig. 3.1, note that the slope of the line between points A and C is $\frac{1}{2}(k_2+1+\frac{k_2-k_1}{n_2-1})$, and between points C and E is $\frac{1}{2}(k_1+1+\frac{k_1+1}{n_1})$, where we quantify the slopes in their absolute value sense.

In regime I, i.e., $1+k_1-n(k_2-k_1) \leq 0$, we obtain $(k_2+\frac{k_2-k_1}{n_2-1})-(k_1+\frac{k_1+1}{n_1}) \leq 0$, yielding that the line connecting points A and C has a higher slope than the one joining points C and E. Thus, if the lines of iso-costs have a slope higher than the slope of the line A-C, then the minimum cost is obtained at point A. Similarly, if the slope is less than that of line C-E, then the minimum cost is obtained at point E. Otherwise, the minimum is obtained at point C. Recall that the slope of the lines of iso-costs is equal to c_P/c_{NP} which leading to the result.

In the other regime II, i.e., $1+k_1-n(k_2-k_1) > 0$, the slope of line A-C is not always greater than that of line C-E. Specifically, we obtain a threshold

$n_2 = \frac{1+k_1}{1+k_1-n_1(k_2-k_1)}$ over which the slop of line C-E is greater than line A-C. Therefore, if $n_2 < \frac{1+k_1}{1+k_1-n_1(k_2-k_1)}$, the optimal network design is the same as those in regime I. In addition, when $n_2 \geq \frac{1+k_1}{1+k_1-n_1(k_2-k_1)}$, and if the slop of iso-costs lines, i.e., c_P/c_{NP}, is larger than the slope of the line connecting points A and E, the minimum cost is achieved at point A. Otherwise, if c_P/c_{NP} is smaller than the slop of line A-E, the optimal network configuration is obtained at point E. □

From Proposition 3.3, we can conclude that in regime I, i.e., $1+k_1-n(k_2-k_1) \leq 0$, when the unit cost of protected links is relatively larger than the non-protected ones, then the secure IoT networks admit an s_0^D strategy using all non-protected links. In comparison, the secure IoT networks are constructed with solely protected links when the cost per protected link is relatively small satisfying $c_P < (k_1 + 1 + \frac{k_1+1}{n_1})c_{NP}/2$. Note that the optimal network design strategy in this regime can be achieved by protecting the minimum spanning tree for a connected network. Equivalently speaking, finding a spanning tree method provides an algorithmic approach to construct the optimal network in this regime. Finally, when the cost per protected link is intermediate, the network designer allocates $n_2 - 1$ protected links connecting those critical nodes in set $\mathcal{S}_2$ while uses non-protected links to connect the nodes in $\mathcal{S}_1$. In addition, the intralinks between two subnetworks are non-protected ones.

Note that the specific configuration of the optimal IoT network is not unique according to Proposition 3.3. To enhance the system reliability and efficiency, the network designer can choose the one among all the optimal topology that minimize the communication distance between devices.

Since the cyber threat in subnetwork 2 is more severe than that in subnetwork 1, i.e., $k_2 \geq k_1$, thus the condition of regime II in Proposition 3.3 $(1+k_1-n(k_2-k_1) > 0)$

is not generally satisfied. We further have the following Corollary refining the result of optimal IoT network design in regime II.

Corollary 3.2. *Only when two subnetworks facing the same level of cyber threats, i.e., $k_1 = k_2$, the optimal IoT network design follows the strategies in regime II. Moreover, $s^D_{n_2-1}$ cannot be an optimal network design in regime II.*

Proof. Based on the condition $n_1 \geq k_1 + 1$, we obtain $1 + k_1 - (n_1 + n_2)(k_2 - k_1) \leq n_1 - (n_1 + n_2)(k_2 - k_1)$. Thus, when $k_2 > k_1$, the condition of regime II $(1 + k_1 - n(k_2 - k_1) > 0)$ cannot be satisfied. Since $k_2 \geq k_1$, then only $k_1 = k_2$ yields $1 + k_1 > 0$. Therefore, $n_2 \geq \frac{1+k_1}{1+k_1-n_1(k_2-k_1)} = 1$ always holds which leads to the result. □

We then simplify the conditions leading to regime I and II as follows.

Corollary 3.3. *The IoT network design can be divided into two regimes according to the cyber threat levels. Specifically, when $k_2 > k_1$, the optimal design strategy follows the one in regime I in Proposition 3.3, and otherwise ($k_1 = k_2$) follows the one in regime II.*

We illustrate the optimal design strategies in Fig. 3.4 according to the heterogeneous security requirements and link creation costs ratio.

3.3.3.2 Robust Optimal Strategy

One interesting phenomenon is that some strategies are optimal for a class of security requirements. Thus, these strategies are robust in spite of the dynamics of cyber threat levels. We summarize the results in the following Corollary.

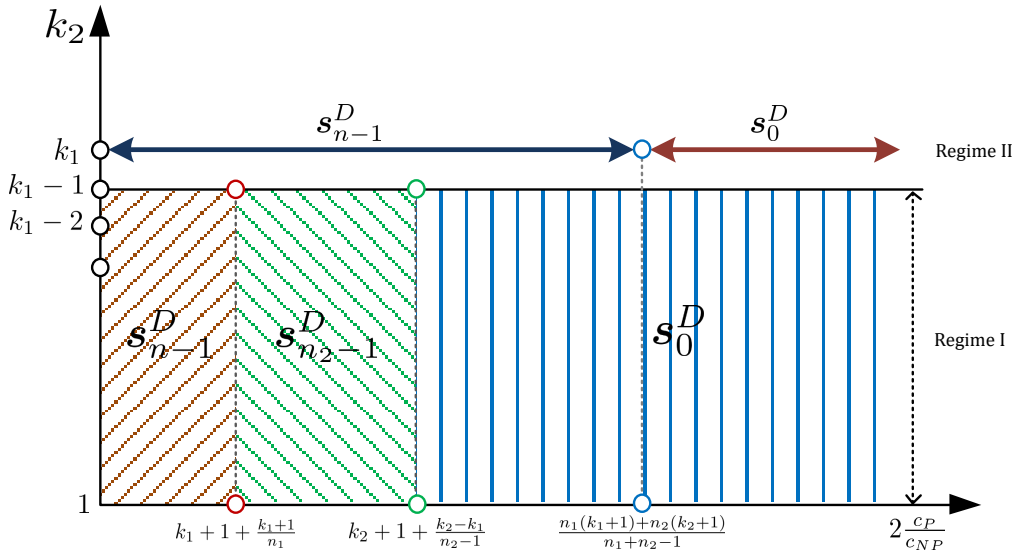


Figure 3.4: Optimal design of two-layer IoT networks in two regimes in terms of system parameters. When $k_2 > k_1$, the optimal network design follows from the strategies in regime I which can be in any s^D_{n-1}, $s^D_{n_2-1}$ or s^D_0 depending on the value of $\frac{c_P}{c_{NP}}$. When $k_2 = k_1$, the IoT network designer chooses strategies from regime II, either of s^D_{n-1} or s^D_0 in term of the link cost ratio $\frac{c_P}{c_{NP}}$.

Corollary 3.4. *Consider to design a (k_1, k_2)-resistant IoT network. If s^D_{n-1} is the optimal strategy, then it is robust and optimal to security requirement for the network being (k'_1, k'_2)-resistant, for all $k'_1 > k_1$ and all $k'_2 > k_2$. If $s^D_{n_2-1}$ is the optimal strategy, then it is robust and optimal to cyber threat levels (k_1, k'_2), for all $k'_2 > k_2$. Furthermore, the optimal strategy s^D_0 is not robust to any other security standards (k'_1, k'_2), for $k'_1 \neq k_1$ and $k'_2 \neq k_2$.*

Corollary 3.4 has a natural understanding on the selection of robust strategies. When the cyber threat level increases, then the optimal network s^D_{n-1} remains to be optimal since the network construction cost does not increase under s^D_{n-1}. Under the optimal $s^D_{n_2-1}$, subnetwork 2 is connected with all protected links and the rest

is connected by a Harary network with the minimum cost. If subnetwork 2 faces more attacks, (k_2 becomes larger), then $s^D_{n_2-1}$ is robust and optimal in the sense that subnetwork 2 remains secure and no other non-protected link is required.

3.3.3.3 Construction of the Optimal Secure IoT Networks

We present the constructive methods of optimal IoT networks with parameters in different regimes based on Proposition 3.3.

Specifically, the optimal s^D_{n-1} can be constructed by any tree network using protected links. In addition, the optimal networks $s^D_{n_2-1}$ can be constructed in two steps as follows. First, we create a tree protected network on the nodes of $\mathcal{S}_2$. Then, we construct a (k_1+1)-Harary network on the nodes of $\mathcal{S}_1 \cup \{n_1+1\}$, i.e., all nodes of type 1 and one node of type 2, where a constructive method of Harary network can be found in [76].

Finally, regarding the optimal network s^D_0, we build it with the following procedure. First, we renumber the nodes according to the sequence: $1, 2, ..., \frac{k_1+1}{2}, n_2, \frac{k_1+1}{2}+1, ..., k_1+1, n_2+1, k_1+2, ..., 3\frac{k_1+1}{2}, n_2+2, ...$ Recall that this renumbering sequence can be achieved by interpolating one node in $\mathcal{S}_2$ after every $\frac{k_1+1}{2}$ nodes in $\mathcal{S}_1$. Then, we build a (k_1+1)-Harary network among all the nodes in $\mathcal{S}_1$ and $\mathcal{S}_2$. Finally, we construct a (k_2-k_1)-Harary network on the nodes in $\mathcal{S}_2$.

3.3.3.4 Consideration of Random Link Failures

In the considered model so far, the non-protected communication link between nodes is removed with probability 1 by the attack and remains connected without attack. In general, the non-protected links face random natural failures. If we consider this random failure factor, then there is a probability that the designed

optimal network will be disconnected under the joint cyber attacks and failures. We assume perfect connection of protected links and denote the random failure probability of a non-protected link by $\kappa \in [0, 1)$. Therefore, in the regime that the optimal network design is of Harary network where all links are non-protected, then under the anticipated level of cyber attacks, a single link failure of non-protected link will result in the network disconnection. Thus, the probability of network connection, i.e., mean connectivity, is equal to $(1-\kappa)^{\left\lceil \frac{n_1(k_1+1)+n_2(k_2+1)}{2} \right\rceil - k_2} \approx (1-\kappa)^{\frac{n_1(k_1+1)+n_2(k_2+1)-2k_2}{2}}$ which is of order $(1-\kappa)^{\frac{n_1k_1+n_2k_2}{2}}$. Similarly, under the regime that the optimal network admits $n_2 - 1$ protected links and $\left\lceil \frac{(k_1+1)(n_1+1)}{2} \right\rceil$ non-protected links, the probability of network connection under link failure is $(1-\kappa)^{\left\lceil \frac{(k_1+1)(n_1+1)}{2} \right\rceil} \approx (1-\kappa)^{\frac{(k_1+1)(n_1+1)}{2}}$ which is of order $(1-\kappa)^{\frac{k_1n_1}{2}}$. We can see that in the above two regimes, when the security requirement is not relatively high and the size of the network is not large, the current designed optimal strategy gives a relatively high mean network connectivity. In the regime that the optimal network is constructed with all protected links, then the mean network connectivity is 1 where the random failure effect is removed.

3.4 Case Studies

In this section, we use case studies of IoBT to illustrate the optimal design principals of secure networks with heterogeneous components. The results in this section are also applicable to other mission-critical IoT network applications.

The IoBT network designer determines the optimal strategy on creating links with/without protection between agents in the battlefield. The ground layer and aerial layer in IoBT generally face different levels of cyber threats which aim to

disrupt the network communications. Since UAVs become more powerful in the military tasks, they are the primal targets of the attackers, and hence the UAV network faces an increasing number of cyber threats. In the following case studies, we investigate the scenario that the IoBT network designer anticipates more cyber attacks on the UAV network than the soldier and UGV networks. The cost ratio between forming a protected link and a unprotected link $\frac{c_p}{c_{NP}}$ is critical in designing the optimal IoBT network. This ratio depends on the number of channels used in creating a safe link though MTD. We will analyze various cases in the following studies.

3.4.1 Optimal IoBT Network Design

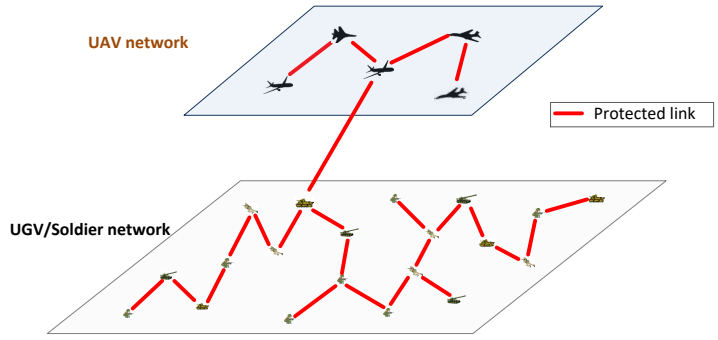
Consider an IoBT network consisting of $n_1 = 20$ soldiers and $n_2 = 5$ UAVs ($n = 25$). The designer aims to design the ground network and the UAV network resistant to $k_1 = 5$ and $k_2 = 9$ attacks, respectively. Hence the global IoBT network is $(5, 9)$-resistant. Based on Proposition 3.3, the system parameters satisfy the condition of regime I. Further, we have two critical points $T_1 := (k_1 + 1 + \frac{k_1+1}{n_1})/2 = 3.15$ and $T_2 := (k_2 + 1 + \frac{k_2-k_1}{n_2-1})/2 = 5.5$, at which the topology of optimal IoBT network encounters a switching. For example, when a protected link adopts 3 channels to prevent from attacks, i.e., $\frac{c_p}{c_{NP}} = 3$, the optimal IoBT network is an s^D_{24} graph as shown in Fig. 3.5(a). When a protected link requires 5 channels to be perfectly secure, i.e., $\frac{c_p}{c_{NP}} = 5$, then the optimal IoBT network is of s^D_4 configuration which is depicted in Fig. 3.5(b). In addition, if the cyber attacks are difficult to defend against (e.g., require 7 channels to keep a link safe, i.e., $\frac{c_p}{c_{NP}} = 7$), the optimal IoBT network becomes an s^D_0 graph as shown in Fig. 3.5(c). The above three types of optimal networks indicate that the smaller the cost of a protected

link is, the more secure connections are formed starting from the UAV network to the ground network.

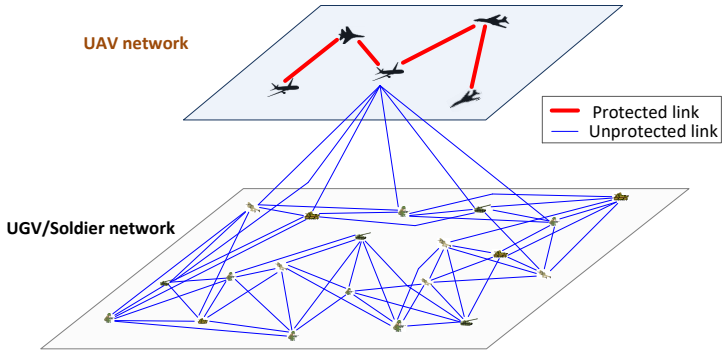
3.4.2 Resilience of the IoBT Network

The numbers of UAVs, UGVs and soldiers can be dynamically changing. To study the resilience of the designed network, we first investigate the scenario that a number of UGVs/soldiers join the battlefield which can be seen as army backups. As n_1 increases, the threshold T_1 decreases slightly while T_2 remains unchanged. Therefore, the optimal IoBT network keeps with a similar topology except that the newly joined UGVs/soldiers connect to a set of their neighbors. To illustrate this scenario, we present the optimal network with $n_1 = 22$ and $\frac{c_p}{c_{NP}} = 5$ in Fig. 3.6(a), and all the other parameters stay the same as those in Section 3.4.1. When n_1 decreases, the network remains almost unchanged except those UGVs/soldiers losing communication links build up new connections with neighbors. An illustrative example with $n_1 = 17$ is depicted in Fig. 3.6(b).

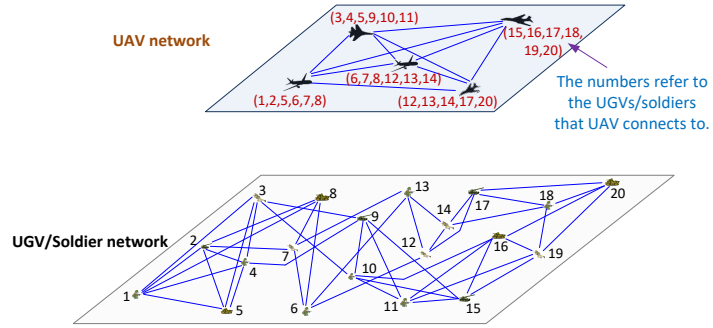
Another interesting scenario is that when the number of UAVs n_2 changes due to backup aerial vehicles joining in and current vehicles leaving the battlefield for maintenance. When n_2 increases, then the threshold T_1 remains the same while T_2 decreases. If the cost ratio $\frac{c_p}{c_{NP}}$ lies in the same regime with respect to T_1 and T_2 even though T_2 decreases, then under $\frac{c_p}{c_{NP}} \leq T_2$, the newly joined UAV will connect with another UAV with a protected link which either creates an S^D_{n-1} or $s^D_{n_2-1}$ graph. Otherwise, if $\frac{c_p}{c_{NP}} > T_2$, the UAV first connects to other UAVs and then connects to a set of UGVs/soldiers both with unprotected links which yields an s^D_0 graph. When a number of UAVs leaving the battlefield, i.e., n_2, decreases, then T_1 stays the same and T_2 will increase under which the cost ratio $\frac{c_p}{c_{NP}}$ previous



(a) s_{24}^D IoBT network

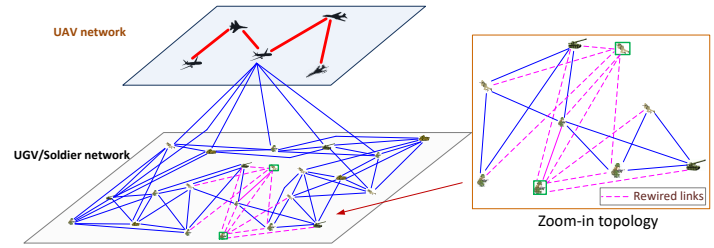


(b) s_4^D IoBT network

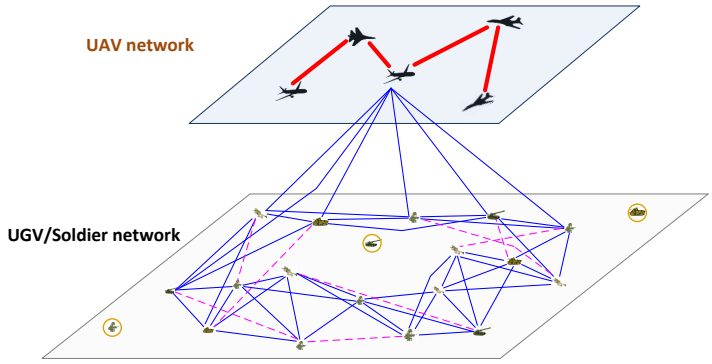


(c) s_0^D IoBT network

Figure 3.5: (a) When $\frac{c_p}{c_{NP}} = 3 < T_1$, the optimal IoBT network is an s_{24}^D graph with all protected links. (b) When $T_1 < \frac{c_p}{c_{NP}} = 5 < T_2$, the optimal network is an s_4^D graph, where the UAV network is connected with protected links and the ground network with all unprotected links. (c) When $\frac{c_p}{c_{NP}} = 7 > T_3$, the optimal IoBT network adopts an s_0^D configuration with all unprotected links.



(a)



(b)

Figure 3.6: (a) and (b) show the optimal IoBT network reconfiguration when two UGVs/soldiers join in and leave the battlefield, respectively.

belonging to interval $\frac{c_p}{c_{NP}} \geq T_2$ may change to interval $T_1 \leq \frac{c_p}{c_{NP}} \leq T_2$. Note that regime switching can also happen when n_2 increases. Therefore, the optimal IoBT network switches from s_0^D to $s_{n_2-1}^D$ (for the increase of n_2 case, the switching is in a backward direction). For example, when the network contains $n_2 = 6$ UAVs and $\frac{c_p}{c_{NP}} = 5.4$, and the other parameters are the same as those in Section 3.4.1, from Proposition 3.3, the optimal IoBT network is an s_0^D graph. However, Fig. 3.5(b) shows that the optimal network adopts an s_4^D topology when $n_2 = 5$. Therefore, by adding a UAV to the aerial layer, the optimal IoBT network switches from s_4^D to s_0^D in this scenario. The interpretation is that a smaller number of UAVs is easier for the aerial network to defend against attacks, and hence protected links are used

between UAVs instead of redundant unprotected links.

3.4.3 Flexible Design and Robust Strategies

In this section, we further investigate the secure IoBT network design in the presence of varying levels of cyber threats. Specifically, the parameters are selected as follows: $n_1 = 20$, $n_2 = 10$, $k_1 = 5$, and $\frac{c_P}{c_{NP}} = 5$. The security requirement k_2 takes a value varying from 5 to 14, modeling the dynamic or uncertain behaviors of the attacker targeting at the critical UAV network. The optimal IoBT network design is depicted in Fig. 3.7, and the corresponding cost is in shown Fig. 3.8. When $k_2 \in [\![5, 8]\!]$, the optimal IoBT network is constructed with all non-protected links. Since k_2 becomes larger, the number of non-protected links used is increasing, and thus the total cost increases. The optimal network topology switches from s_0^D to s_9^D when k_2 exceeds the threshold 8. Then, when $k_2 \in [\![9, 14]\!]$, the optimal IoBT network is unchanged as well as the associated construction cost. Despite the increases in k_2, no addition links are required since the UAV network (subnetwork 2) is connected with all protected links. Note that s_9^D is a robust strategy in the sense that the IoBT network can be $(5, k_2)$-resistant, for all $k_2 \in [\![9, 14]\!]$. This study can be generalized to the cases when the network designer has an uncertain belief on the attacker's strategy. Therefore, the IoBT designer can prepare for a number of attacking scenarios and choose from these designed strategies in the field with a timely and flexible manner.

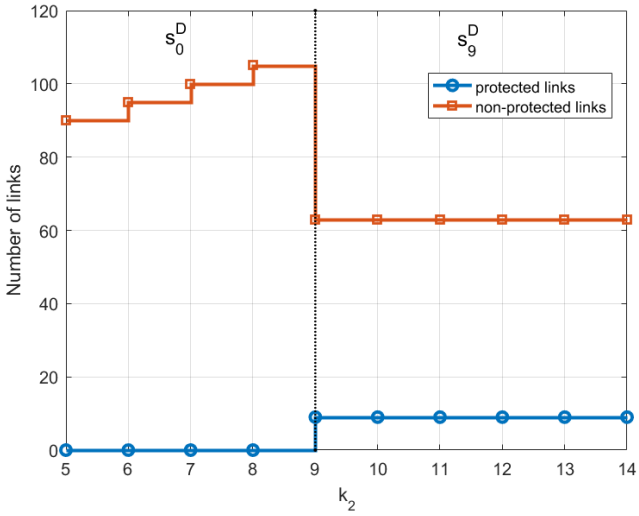


Figure 3.7: Optimal IoBT network design with parameters $n_1 = 20$, $n_2 = 10$, $k_1 = 5$, $\frac{c_P}{c_{NP}} = 5$, and k_2 taking a value from 5 to 14. When $k_2 \in [\![5, 8]\!]$, the optimal network design is in the form of s_0^D. When $k_2 \in [\![9, 14]\!]$, the optimal network admits a strategy of s_9^D. Note that s_9^D is robust to a dynamic or varying number of cyber attacks ranging from 9 to 14.

3.5 Summary

In this chapter, we have studied a two-layer secure network formation problem for IoT networks in which the network designer aims to form a two-layer communication network with heterogeneous security requirements while minimizing the cost of using protected and unprotected links. We have shown a lower bound on the number of non-protected links of the optimal network and developed a method to construct networks that satisfy the heterogeneous network design specifications. We have demonstrated the design methodology in the IoBT networks. It has been shown that the optimal network can reconfigure itself adaptively as nodes enter or leave the system. In addition, the optimal IoBT network configuration may encounter a topological switching when the number of UAVs changes. We have further identified the optimal design strategies that can be robust to a set of security requirements.

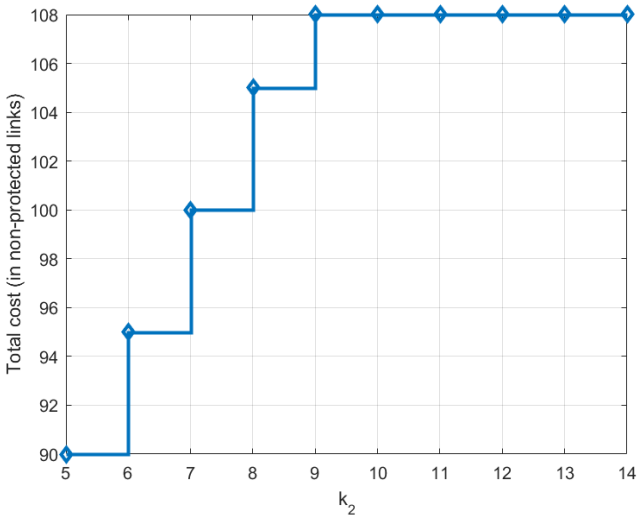


Figure 3.8: The total cost of optimal network design in terms of the number of non-protected links. In the regime of $k_2 \in [\![5, 8]\!]$, with a larger k_2, the IoBT network requires more non-protected links to be resistant to attacks. In the regime of $k_2 \in [\![9, 14]\!]$, the total cost remains the same, since the UAV network is connected with all protected links and no additional non-protected link is required despite of the increasing cyber threats k_2.

As part of the future work, we would extend the single network designer problem to a twoplayer one, where each player designs their own subnetwork in a decentralized way. Another direction will be generalizing the current bi-level network to more than two layers and designing the optimal strategies.

Chapter 4

Proactive Secure and Resilient Co-Design of CPS Network

4.1 Introduction

The previous Chapter 3 has studied the optimal design of multi-layer IoT networks with security considerations. Specifically, it has shown how to protect the network by creating redundant links in the network so that networks can be still connected despite arbitrary removal of a fixed number of links. Adding link redundancy is an effective approach when there is no knowledge of the target of the attacker. However, it becomes expensive and sometimes prohibitive when the cost for creating links is costly, and the attacker is powerful. Therefore, a paradigm shift to emphasize the recovery and response to attacks is critical, and the network resilience becomes essential for developing post-attack mechanisms to mitigate the impacts.

To this end, we establish a two-player dynamic three-stage network game

formation problem in which the CPS network designer aims to keep the network connected before and after the attack, while the objective of the adversary is to keep the network disconnected after the attack. Note that each player has a cost on creating or removing links. Specifically, at the first stage of the game, the CPS network designer first creates a network with necessary redundancies by anticipating the impact of adversarial behavior. Then, an adversary attacks at the second stage by removing a minimum number of links of the network. At the last stage of the game, the network designer can recover the network after the attack by adding extra links to the attacked network.

4.2 Dynamic Game Formulation

In this section, we consider a CPS network represented by a set $\mathcal{N}$ of n nodes. The CPS network designer can design a network with redundant links before the attack for protection and adding new links after the attack for recovery. Note that the attack action of the adversary can be enabled through cyber and physical approaches due to the integration of modern infrastructures with information and communication technologies. The sequence of the actions taken by the designer and the attacker is described as follows:

(i) A Designer (D) aims to create a network between these nodes and protect it against a malicious attack;

(ii) After some time of operation, an Adversary (A) puts an attack on the network by removing a subset of its links;

(iii) Once the D realizes that an attack has been conducted, it has the opportunity

to heal its network by constructing new links (or reconstructing some destroyed ones).

In addition, the timing of the actions also play a significant role in determining the optimal strategies of both players. We normalize the horizon of the event from the start of the preparation of CPS protection to a time point of interest as the time internal $[0, 1]$. This normalization is motivated by the observation made in [114] where the consequences of fifteen major storms occurring between 2004 and 2012 are plotted over a normalized duration of the event. We let τ and τ_R represent, respectively, the fraction of time spent before the attack (system is fully operational) and between the attack and the healing phase. This is illustrated in Fig. 4.1.

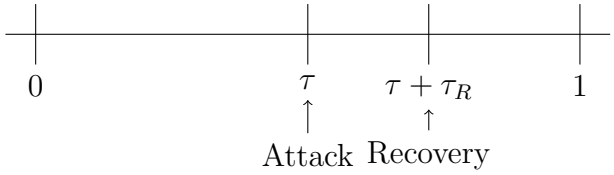


Figure 4.1: Attack and defense time fractions. The attacker compromises the network at time τ, and the defender recovers it after τ_R amount of time.

The goal of the designer or the defender is to create protection and recovery mechanisms to keep its network operational, i.e., connected in this case. Let $\mathcal{E}_1$ be the set of links created by the defender initially (i.e., at time 0). $\mathcal{E}_A \subseteq \mathcal{E}_1$ is the set of links removed (attacked) by the adversary and $\mathcal{E}_2$ is the set of links created by the defender after the attack (at fraction $\tau + \tau_R$ of the time horizon). Regardless of the time stamp, creating (resp. removing) links has a unitary cost c_D (resp. c_A). The adversary aims to disconnect the network. Thus, for any set $\mathcal{E}$, we define $\mathbb{1}_E$ which equals 1 if the graph $(\mathcal{N}, \mathcal{E})$ is connected and 0 otherwise. Values of

τ, τ_R, c_A and c_D are assumed as common knowledge to both D and A first, and later we investigate the strategic selections of τ and τ_R. As a tie-breaker rule, if the output/utility is the same for A, then A chooses to attack the network with the largest number of link removals. Similarly, D chooses not to create links if its utility is the same.

Remark: The link creation cost is treated as identical in the framework. Here, c_D can capture various application scenarios. For example, in a large complex network with heterogeneous link costs, analyzing the strategy of D becomes intractable. A viable choice for D is to consider the mean link creation cost captured by c_D which gives an approximation of the network. Another case is that D considers the largest single link creation cost denoted by c_D, and thus it captures the worst case in which D is conservative in designing the strategies. In sum, considering an identical c_D is reasonable, and also it makes the technical analysis of the problem tractable.

The utility for the designer (resp. adversary) is equal to the fraction of time the network is connected (resp. disconnected) minus the costs of creating (resp. removing) the links. Hence, the payoff functions of the designer and the adversary are represented by U_D and U_A, respectively, as follows:

$$\begin{aligned} U_D(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_A) =& (1-\tau-\tau_R)\mathbb{1}_{E_1 \setminus E_A \cup E_2} + \tau \mathbb{1}_{E_1} \\ & + \tau_R \mathbb{1}_{E_1 \setminus E_A} - c_D(|\mathcal{E}_1| + |\mathcal{E}_2|), \\ U_A(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_A) =& (1-\tau-\tau_R)(1-\mathbb{1}_{E_1 \setminus E_A \cup E_2}) - c_A|\mathcal{E}_A| \\ & + \tau(1-\mathbb{1}_{E_1}) + \tau_R(1-\mathbb{1}_{E_1 \setminus E_A}), \end{aligned}$$

where $|\cdot|$ denotes the cardinality of a set. In addition, $\mathbb{1}_{E_1 \setminus E_A \cup E_2}$ means that a network including $|\mathcal{N}| = n$ nodes contains a set $\mathcal{E}_1 \setminus \mathcal{E}_A \cup \mathcal{E}_2$ of links. Note that if

the fraction of time and the cost of links metrics cannot be directly added up in the utility functions, we can use a conversion factor to transform one metric to the other. Therefore, the formulated utility functions for D and A are still valid.

We adopt subgame perfect Nash equilibrium (SPE) as the solution concept of the dynamic game. Specifically, we study the SPE and analyze the strategies of the players to the sets $(\mathcal{E}_1, \mathcal{E}_A, \mathcal{E}_2)$. Thus, we seek triplets $(\mathcal{E}_1, \mathcal{E}_A, \mathcal{E}_2)$ such that $\mathcal{E}_2$ is a best response to $(\mathcal{E}_1, \mathcal{E}_A)$ and that given $\mathcal{E}_1$, $(\mathcal{E}_A, \mathcal{E}_2)$ is also a SPE. In other words, the SPE involves the analysis of the following three sequentially nested problems starting from the last stage of the designer's recovery problem to the first stage of the designer's protection problem:

(i) Given the strategies $\mathcal{E}_1$ and $\mathcal{E}_A$, player D chooses

$\mathcal{E}_2^*(\mathcal{E}_1, \mathcal{E}_A) \in \arg\max_{\mathcal{E}_2} U_D(\mathcal{E}_1, \mathcal{E}_A, \mathcal{E}_2)$;

(ii) Given $\mathcal{E}_1$, the adversary chooses

$\mathcal{E}_A^*(\mathcal{E}_1) \in \arg\max_{\mathcal{E}_A} U_A(\mathcal{E}_1, \mathcal{E}_A, \mathcal{E}_2^*(\mathcal{E}_1, \mathcal{E}_A))$;

(iii) Player D chooses

$\mathcal{E}_1^* \in \arg\max_{\mathcal{E}_1} U_D(\mathcal{E}_1, \mathcal{E}_A^*(\mathcal{E}_1), \mathcal{E}_2^*(\mathcal{E}_1, \mathcal{E}_A))$.

The equilibrium solution $(\mathcal{E}_1, \mathcal{E}_A, \mathcal{E}_2)$ that solves the above three problems consistently is an SPE of the two-player dynamic game.

Comments on the game formulation: In the established model, the attacking time τ and attacker's cost c_A are assumed to be known by D. More practically, D may have no perfect information on the attacker's parameters, and only the distributions of τ and c_A are available. Then, D can calculate the expected values of τ and c_A. The analysis in the chapter is still valid to design the defensive strategy of D at time 0. However, A's behavior may not be the same as expected by D

which leads to a random network after the attack. Thus, D needs to determine the healing strategy $\mathcal{A}_2$ again at time τ. This creates another layer of decision-making problem for D which is an optimization problem itself instead of a game as A's behavior has been revealed. Other than capturing the unknown parameters τ and c_A through their expected values, we can also model the game by considering the incomplete information directly. This yields a formulation of dynamic Bayesian game with a random type parameter including τ and c_A which is nontrivial to solve.

4.3 Dynamic Game Analysis

In this section, we analyze the possible configurations of the CPS network at SPE.

We first note that c_A should be not too large, since otherwise A cannot be a threat to D. Similarly, c_D should be sufficiently small so that the D can create a connected network:

Lemma 4.1. *If $c_A > 1-\tau$, then A has no incentive to attack any link. In addition, if $c_D > \frac{1}{n-1}$, then D has no incentive to create a connected network.*

Proof. Suppose that $c_A > 1-\tau$. Let $\mathcal{E}_1$ be given and $\phi := \tau(1-\mathbb{1}_{E_1})$. If A decides not to remove any link, then its payoff is $\phi+\tau_R(1-\mathbb{1}_{E_1})+(1-\tau-\tau_R)(1-\mathbb{1}_{E_1\cup E_2}) \geq \phi$. Otherwise, $|\mathcal{E}_A| \geq 1$ and $U_A(\mathcal{E}_1,\mathcal{E}_2,\mathcal{E}_A) \leq \phi + (1-\tau-\tau_R)(1-\mathbb{1}_{E_1\setminus E_A\cup E_2}) - c_A + \tau_R(1-\mathbb{1}_{E_1\setminus E_A}) \leq \phi+1-\tau-c_A < \phi$. Thus, it is a best response for A to play $\mathcal{E}_A = \emptyset$. Similarly, if $c_D > \frac{1}{n-1}$, then if D plays $\mathcal{E}_1 = \mathcal{E}_2 = \emptyset$, its utility is 0. Otherwise, its utility is bounded above by $1-(n-1)c_D$ which corresponds to a connected tree network with the minimum number of links. □

In the following, we thus suppose that $c_A < 1-\tau$ and $c_D < \frac{1}{n-1}$.

Note that the SPE can correspond only to a set of situations summarized as follows.

Lemma 4.2. *Suppose that* $(\mathcal{E}_1, \mathcal{E}_A, \mathcal{E}_2)$ *is an SPE. Then, we are necessarily in one of the situations given in Table 4.1.*

Situation	$\mathbb{1}_{E_1}$	$\mathbb{1}_{E_1 \setminus E_A}$	$\mathbb{1}_{E_1 \setminus E_A \cup E_2}$
1	1	1	1
2	1	0	1
3	1	0	0
4	0	0	1
5	0	0	0

Table 4.1: Different potential combinations of values of $\mathbb{1}_{E_1}$, $\mathbb{1}_{E_1 \setminus E_A}$ and $\mathbb{1}_{E_1 \setminus E_A \cup E_2}$ at the SPE.

Proof. Note that, in total, 8 situations should be possible. However, if $\mathbb{1}_{E_1} = 0$, then it is impossible that $\mathbb{1}_{E_1 \setminus E_A} = 1$. Therefore, the situations where $(\mathbb{1}_{E_1}, \mathbb{1}_{E_1 \setminus E_A}, \mathbb{1}_{E_1 \setminus E_A \cup E_2})$ equaling to $(0, 1, 0)$ and $(0, 1, 1)$ are not possible. Further, if $\mathbb{1}_{E_1 \setminus E_A} = 1$, then it is impossible that $\mathbb{1}_{E_1 \setminus E_A \cup E_2} = 0$. Thus, the situation $(\mathbb{1}_{E_1}, \mathbb{1}_{E_1 \setminus E_A}, \mathbb{1}_{E_1 \setminus E_A \cup E_2}) = (1, 1, 0)$ is impossible. All other combinations are summarized in Table 4.1. □

In Situations 4 and 5, D does not create a connected network in the beginning, and thus A has no incentive to attack the network at phase τ. The structure of the SPE depends on the values of the parameters of the game. In particular, it depends on whether D has incentive to fully reconstruct (heal) the system after the attack of A. More precisely, if $1 - \tau - \tau_R > (n-1)c_D$, then D prefers to heal the network even if all links have been compromised by the attacker. Otherwise, there should be a minimum number of links remained after the attack for the D to heal the network at the SPE. We sequentially analyze these two cases in Sections 4.4.1 and 4.4.2, respectively.

4.4 SPE Analysis of the Dynamic Game

Depending on the parameters, we derive SPE of the dynamic game in two regimes: $1-\tau-\tau_R > (n-1)c_D$ and the otherwise in this section.

Before presenting the results, we first present the definition of Harary network [76] which plays an essential role in the SPE analysis. For a network containing n nodes being resistant to k link attacks, one necessary condition is that each node should have a degree of at least $k+1$, yielding the total number of links more than $\left\lceil \frac{(k+1)n}{2} \right\rceil$, where $\lceil \cdot \rceil$ denotes the ceiling operator. Harary network presented below can achieve this lower bound on the number of required links.

Definition 4.1 (Harary Network [76]). *In a network containing n nodes, Harary network is the optimal design that uses the minimum number of links equaling $\left\lceil \frac{(k+1)n}{2} \right\rceil$ for the network still being connected after removing any k links.*

The constructive method of general Harary network can be described with cycles as follows. It first creates the links between node i and node j such that $(|i-j| \mod n) = 1$, and then $(|i-j| \mod n) = 2$, etc. When the number of nodes is odd, then the last cycle of link creation is slightly different since $\frac{(k+1)n}{2}$ is not an integer. However, the bound $\left\lceil \frac{(k+1)n}{2} \right\rceil$ can be still be achieved.

Another critical network topology used in the analysis is the tree network defined as follows.

Definition 4.2 (Tree network [68]). *A tree is an undirected graph in which any two nodes are connected by exactly one path. Equivalently, the network is a tree if and only if it is connected and acyclic (contains no cycles).*

4.4.1 Regime 1: $1-\tau-\tau_R > (n-1)c_D$

In the case where $1-\tau-\tau_R > (n-1)c_D$, D always reconstructs the network to be connected after the attack. The potential SPE can occur in only three of the Situations in Table 4.1, and we summarize them in the following proposition.

Proposition 4.1. *Suppose that* $1-\tau-\tau_R > (n-1)c_D$ *and let* $k_A^R \equiv \left\lfloor \frac{\tau_R}{c_A} \right\rfloor$, *where* $\lfloor\cdot\rfloor$ *denotes the floor operator (resp. to the ceiling operator* $\lceil\cdot\rceil$*). Note that* k_A^R *is the largest number of links that* A *can compromise to have a nonnegative payoff. Then, the SPE of the game is unique and satisfies:*

(1) If $\tau_R < c_A$, *then* $U_D = 1-(n-1)c_D$ *and* $U_A = 0$ *(Situation 1).*

(2) Otherwise, i.e., $\tau_R \geq c_A$, *and*

(i) if $\tau > c_D$ *and* $\tau_R > c_D\left\lceil \frac{n(k_A^R-1)}{2} \right\rceil$ *or if* $\tau < c_D$ *and* $\tau+\tau_R > c_D\left\lceil \frac{n(k_A^R-1)}{2}+1 \right\rceil$, *then the SPE satisfies*

$$\begin{cases} U_D = 1-c_D\left\lceil \frac{n(k_A^R+1)}{2} \right\rceil \\ U_A = 0 \end{cases}$$ *(Situation 1).*

(ii) If $\tau > c_D$ *and* $\tau_R < c_D\left\lceil \frac{n(k_A^R-1)}{2} \right\rceil$, *then the SPE satisfies* $\begin{cases} U_D = 1-\tau_R-nc_D \\ U_A = \tau_R - c_A \end{cases}$ *(Situation 2).*

(iii) If $\tau < c_D$ *and* $\tau+\tau_R < c_D\left\lceil \frac{n(k_A^R-1)}{2}+1 \right\rceil$, *then the SPE satisfies*

$$\begin{cases} U_D = 1-\tau-\tau_R-(n-1)c_D \\ U_A = \tau+\tau_R \end{cases}$$ *(Situation 4).*

Proposition 4.1 is a direct consequence of the following lemma. Note that the conditions in Proposition 4.1 are obtained via comparing D's utility U_D at various SPEs in Table 4.2.

Lemma 4.3. *Suppose that* $1-\tau-\tau_R > (n-1)c_D$. *The potential SPEs have the properties given in Table 4.2.*

Situation	$\lvert\mathcal{E}_1\rvert$	$\lvert\mathcal{E}_A\rvert$	$\lvert\mathcal{E}_2\rvert$	U_D	U_A
$1\&k_A^R > 0$	$\left\lceil \frac{n(k_A^R+1)}{2} \right\rceil$	0	0	$1 - c_D \left\lceil \frac{n(k_A^R+1)}{2} \right\rceil$	0
$1\&k_A^R = 0$	$n-1$	0	0	$1-(n-1)c_D$	0
2	$n-1$	1	1	$1-\tau_R-nc_D$	$\tau_R - c_A$
4	0	0	$n-1$	$1-\tau-\tau_R-(n-1)c_D$	$\tau+\tau_R$

Table 4.2: Different potential SPEs when $1-\tau-\tau_R > (n-1)c_D$ (Note: $k_A^R = \left\lfloor \frac{\tau_R}{c_A} \right\rfloor$).

Proof. First note that any connected network contains at least $n-1$ links. Conversely, any set of nodes can be made connected by using exactly $n-1$ links (any spanning tree is a solution). We consider a situation where $\mathbb{1}_{E_1 \setminus E_A} = 0$. Then, either D decides not to heal the network and receives a utility of $U^* = \tau \mathbb{1}_{E_1} - c_D|\mathcal{E}_1|$, or it decides to heal it (by using at most $n-1$ links) and receives a utility of at least $\overline{U} = (1-\tau-\tau_R) + \tau\mathbb{1}_{E_1} - c_D(|\mathcal{E}_1| + n - 1)$. The difference is $\overline{U} - U^* = (1-\tau-\tau_R) - c_D(n-1) > 0$. Thus, D always prefers to heal the network after the attack of A. Therefore, Situations 3 and 5 contain no SPE.

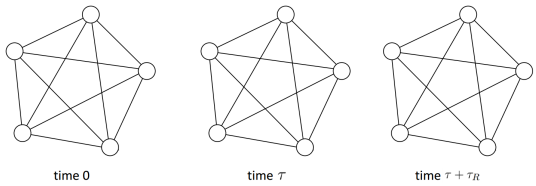
Next we consider Situation 4. Since $\mathbb{1}_{E_1 \setminus E_A \cup E_2} = 1$, then D needs to create in total at least $n-1$ links: $|\mathcal{E}_1| + |\mathcal{E}_2| \geq n-1$. Therefore, an optimal strategy is $\mathcal{E}_1 = \emptyset$ and $|\mathcal{E}_2| = n-1$. Since $\mathcal{E}_1 = \emptyset$, the optimal strategy of A is $\mathcal{E}_A = \emptyset$.

In Situation 2, $(\mathcal{N}, \mathcal{E}_1)$ is connected, and thus $|\mathcal{E}_1| \geq n-1$. Further, $\mathbb{1}_{E_1} = 1$ and $\mathbb{1}_{E_1 \setminus E_A} = 0$, and thus $|\mathcal{E}_A| \geq 1$. Since $1-\tau-\tau_R > (n-1)c_D$, then A should remove the minimum number of links to disconnect the network, and we obtain the result.

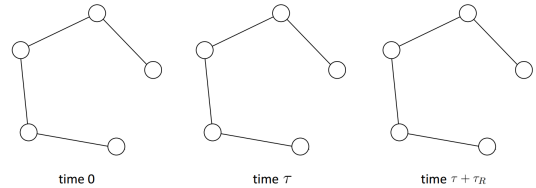
Finally, in Situation 1, since $\mathbb{1}_{E_1 \setminus E_A} = 1$, then D does not need to create any link during the healing phase: $\mathcal{E}_2 = \emptyset$. Since $1 - \tau - \tau_R > (n-1)c_D$, then A attacks at most k_A^R links if and only if it obtains a nonnegative reward, i.e., k_A^R is the largest integer such that $\tau_R - c_A k_A^R \geq 0$ which yields $k_A^R = \left\lfloor \frac{\tau_R}{c_A} \right\rfloor$. Thus, D designs a network that is resistant to an attack compromising up to k_A^R links. Such solution network is the $(|\mathcal{N}|, k_A^R + 1)$-Harary network [76]. □

Examples: For clarify, we depict the strategies of D and A at various SPEs using examples shown in Fig. 4.2. The network contains 5 nodes. Depending on the relationship between parameters shown in Proposition 4.1, the game admits various SPEs. Four possible SPEs with specific actions taken by D and A are presented. For example, when the SPE lies in Situation 1 with $k_A^R = 3$, then at least 10 links are necessary for the network being resistant to 3 attacks. Therefore, D creates a 4-Harary network initially in which each node has at least a degree of 4. In comparison, when $k_A^R = 0$ and the SPE is in Situation 1, then creating a connected tree network is sufficient for D since A is not capable to compromise any link. The SPEs corresponding to Situations 2 and 4 are shown in Figs. 4.2(c) and 4.2(d), respectively.

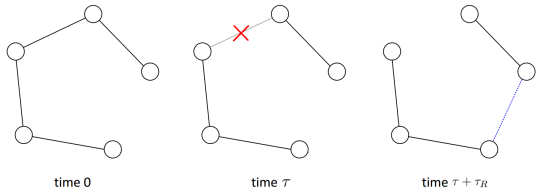
Based on Lemma 4.3, the stragies of two players at SPE in regime 1 are summarized as follows. Under Situation 1 and $k_A^R > 0$, A does not attack and D creates a connected $(|\mathcal{N}|, k_A^R + 1)$-Harary network at phase 0. Under Situation 1 and $k_A^R = 0$, D simply creates a connected network with the minimum number of $n-1$ links which can be achieved by any tree-structured network, and A admits a null strategy. In Situation 2, D initially constructs a tree network using $n-1$ links, and A attacks any one link at phase τ followed by D recovering the network at phase $\tau + \tau_R$. Finally, for Situation 4, A does not attack, and D constructs a



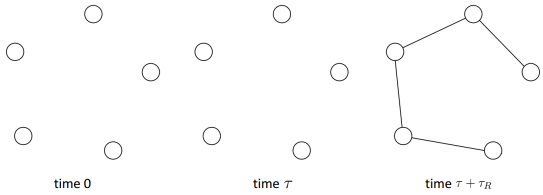
(a) Situation 1 and $k_A^R = 3$



(b) Situation 1 and $k_A^R = 0$



(c) Situation 2



(d) Situation 4

Figure 4.2: Strategies of D and A at different SPEs in regime 1. The network contains 5 nodes. In (a), the SPE is in Situation 1 and $k_A^R = 3$. Thus, at least 10 links are necessary for it being resistant to 3 attacks. In (b), when $k_A^R = 0$ and the SPE lies in Situation 1, a tree network is created by the defender following no actions of A and D. In (c), the SPE is in Situation 2, and A will compromise any one link at time τ and D will heal one link to reconnect the network. In (d), D will not protect the network at time 0 but will connect the network at time $\tau + \tau_R$ which shows SPE in Situation 4.

connected tree network only at phase $\tau + \tau_R$.

4.4.2 Regime 2: $1-\tau-\tau_R < (n-1)c_D$

We now consider the case where D has an incentive, at phase $\tau+\tau_R$, to heal the network if at most k links are required to reconnect it, where $k < n-1$ and

$$k \equiv \left\lfloor \frac{1-\tau-\tau_R}{c_D} \right\rfloor. \tag{4.1}$$

We sequentially study the potential SPE in Situations 3, 4 and 5 in Lemma 4.4, Situation 2 in Lemma 4.5, and Situation 1 in Lemma 4.6.

Lemma 4.4. *If $1-\tau-\tau_R < (n-1)c_D$, we have the following results:*

(i) Any SPE in Situation 3 satisfies $\mathcal{E}_2 = \emptyset$, $|\mathcal{E}_A| = k+1$ and $|\mathcal{E}_1| = n-1$, leading to utilities $U_D = \tau-(n-1)c_D$ and $U_A = 1-\tau-(k+1)c_A$ (occurs only if $\lfloor \frac{1-\tau}{c_A} \rfloor \geq k+1$);

(ii) There exists no SPE in Situation 4;

(iii) The only potential SPE in Situation 5 is the null strategy: $\mathcal{E}_1 = \mathcal{E}_2 = \mathcal{E}_A = \emptyset$, leading to utilities $U_D = 0$ and $U_A = 1$.

Proof. Suppose that an SPE occurs in Situation 5. Since the network is always disconnected, then $U_D = -c_D(|\mathcal{E}_1| + |\mathcal{E}_2|)$. The maximum utility is obtained when $\mathcal{E}_1 = \mathcal{E}_2 = \emptyset$. Thus, $\mathcal{E}_A = \emptyset$.

In Situation 4, since any connected network contains at least $n-1$ links, then the maximum utility of D is $U_D(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_A) = (1-\tau-\tau_R) - c_D(n-1) < 0$. Thus, D is better off with a null strategy (occurring in Situation 5).

In Situation 3, since $\mathbb{1}_{E_1} = 1$ then $|\mathcal{E}_1| \geq n-1$. D can achieves utility value $\tau-(n-1)c_D$ by playing a tree network. Since $\mathbb{1}_{E_1 \setminus E_A} \neq \mathbb{1}_{E_1}$ then $|\mathcal{E}_A| \geq 1$ and

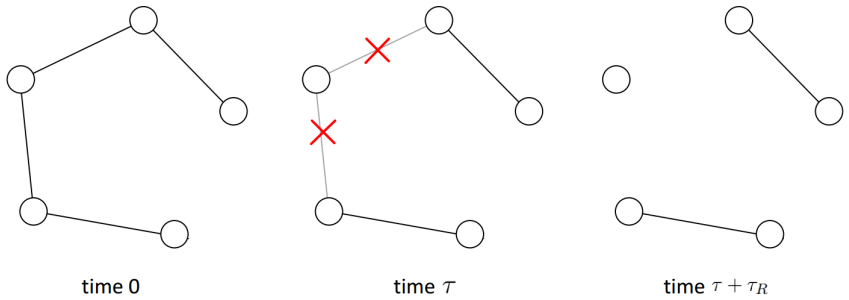


Figure 4.3: The SPE lies in Situation 3 with $k = 1$. Thus, D will only create a tree network followed by A compromising any 2 links to disconnect the network, and D does not recover at time $\tau + \tau_R$.

$U_A \leq 1 - \tau - c_A$. The bound is achieved by attacking any one link created by D. We further can show that A needs to attack $k + 1$ links such that D will not heal the network. □

Example: In regime 2, for SPEs in Situation 5, the network remains empty since D does not protect nor heal. An illustration of SPE in Situation 3 with $k = 1$ is depicted in Fig. 4.3. Specifically, D creates a connected network with tree structure initially. Then, A compromises any $k + 1 = 2$ links to disconnect the network. Since D is willing to recover at most $k = 1$ link, D does not heal the network at time $\tau + \tau_R$.

In the following, we focus on the SPEs in Situations 1 and 2. In both cases, $\mathbb{1}_{E_1} = 1$. Thus, D creates a connected network initially. For each node $i \in \mathcal{N}$, let d_i be its degree. To facilitate the analysis, we focus on the potential best response strategies of A to E_1 which are summarized in the following three distinct cases:

(i) A does not attack and obtains a utility of $U_A^{(1)} = 0$;

(ii) A attacks sufficiently many links so that the network admits 2 components, i.e., A attacks exactly $\min_{1 \leq i \leq n} d_i$ links to disconnect a node of minimal

degree. Then, D heals the network by constructing 1 link, and A receives utility

$$U_A^{(2)} = \tau_R - (\min_{1\leq i\leq n} d_i)c_A. \tag{4.2}$$

(iii) A attacks sufficiently many links so that the network admits $\ell+2$ components, for some sufficiently large ℓ (whose exact value is discussed in the following two lemmas). Then, D does not heal the network, and A receives utility

$$U_A^{(3)} = 1 - \tau - |\mathcal{E}_A|c_A. \tag{4.3}$$

Note that any intermediate value of components in the range $[\![2; \ell+2]\!]$ cannot happen at SPE since it amounts to a lower utility for A. The current case (iii) belongs to Situation 3 which eases the analysis in Lemmas 4.5 and 4.6.

The next lemma characterizes the SPEs for Situation 2.

Lemma 4.5. *The only SPEs in Situation 2 are such that* $|\mathcal{E}_1| = n-1$, $|\mathcal{E}_A| = 1$, $|\mathcal{E}_2| = 1$, $U_D = 1 - \tau_R - nc_D$, *and* $U_A = \tau_R - c_A$. *Furthermore, it occurs only if* $c_A \leq \tau_R$ *and* $\left\lfloor \frac{1-\tau-\tau_R}{c_D} \right\rfloor > \left\lfloor \frac{1-\tau-\tau_R}{c_A} \right\rfloor$.

Proof. At an SPE in Situation 2, the utility of D is of the form $1 - \tau_R - c_D(|\mathcal{E}_1| + |\mathcal{E}_2|)$. Then, it is a best strategy for D to heal the network at time $\tau + \tau_R$, i.e., $1 - \tau_R - (|\mathcal{E}_1| + |\mathcal{E}_2|)c_D \geq \tau - |\mathcal{E}_1|c_D$. Thus, $|\mathcal{E}_2| \leq \left\lfloor \frac{1-\tau-\tau_R}{c_D} \right\rfloor = k$, and k is the maximum number of links that D can create at time $\tau + \tau_R$ at an SPE. In addition, at this SPE, D receives a higher reward than by using its best strategy in Situation 3, i.e., $1 - \tau_R - (|\mathcal{E}_1| + |\mathcal{E}_2|)c_D \geq \tau - (n-1)c_D$. Thus, $|\mathcal{E}_1| + |\mathcal{E}_2| \leq \left\lfloor \frac{1-\tau-\tau_R}{c_D} \right\rfloor + (n-1) = k + (n-1)$. Since $k < n-1$, then altogether D can create at most $|\mathcal{E}_1| + |\mathcal{E}_2| \leq 2(n-1)$ links.

For any SPE in Situation 2, note that $|\mathcal{E}_1| \geq n-1$. Thus, we can write $|\mathcal{E}_1| = n-1+\alpha$ and $|\mathcal{E}_2| \leq k-\alpha$, for some $\alpha < k$. For Situation 2, we obtain $U_A^{(2)} \geq U_A^{(1)}$ which yields $(\min_{1\leq i\leq n} d_i) \leq \left\lfloor \frac{\tau_R}{c_A} \right\rfloor$. If $\tau_R < c_A$, then no SPE exists in Situation 2. Further, based on $0 \leq U_A^{(2)} - U_A^{(3)} = (|\mathcal{E}_A| - (\min_{1\leq i\leq n} d_i))c_A - (1-\tau-\tau_R)$, we obtain $|\mathcal{E}_A| \geq \left\lceil \frac{1-\tau-\tau_R}{c_A} \right\rceil + (\min_{1\leq i\leq n} d_i)$. Since at $\tau+\tau_R$, D can create at most $k-\alpha$ links, then the goal of A in case (iii) is to create at least $\ell = k-\alpha+2$ components in the network (i.e., to create a $k-\alpha+1$ cut). Hence, D constructs $\mathcal{E}_1$ in a way that at least $k_A + (\min_{1\leq i\leq n} d_i)$ links need to be removed so that the network consists of $k+2-\alpha$ components, where $k_A := \left\lceil \frac{1-\tau-\tau_R}{c_A} \right\rceil$.

Recall that $k = \left\lfloor \frac{1-\tau-\tau_R}{c_D} \right\rfloor$ is the maximal number of links that D can recover at phase $\tau+\tau_R$. Suppose that $k < k_A$ (i.e., $k \leq k_A - 1$). Then, for any E_1, consider the following attack: first remove α links so that the resulting network is a tree and then remove $k_2+1-\alpha$ links. Then, the resulting network has exactly $n-2-k+\alpha$ links, i.e., it has $n-(n-2-k+\alpha) = k-\alpha+2$ components and is obtained using $k+1 < k_A + (\min_{1\leq i\leq n} d_i)$ links. Thus, if $k < k_A$, no SPE in Situation 2 exists. If $k > k_A+1$ (i.e., $k \geq k_A$), then we consider the strategy that D creates a line network at time 0. Then to induce $k+2$ components, A needs to remove $k+1$ links. However, due to $k > k_A+1$, it is not of the best interest to A. Instead, the best response for A is to attack exactly one link (one being adjacent to one of the nodes with degree 1). Then, the best strategy for D is to re-create this compromised link at time $\tau+\tau_R$ which is an SPE. It is strategic as it minimizes the number of created links. □

In Lemma 4.5, the condition $c_A \leq \tau_R$ ensures that A has an incentive to compromise the network, and the condition $\left\lfloor \frac{1-\tau-\tau_R}{c_D} \right\rfloor > \left\lfloor \frac{1-\tau-\tau_R}{c_A} \right\rfloor$ guarantees that D is capable to heal the network after the attack. Note that when these two

conditions are satisfied, all other strategies that D creates a tree network at phase 0 and A attacks one link which is further reconnected by D also constitute SPEs of Situation 2.

To study the SPE in Situation 1, for convenience, we denote

$$k_A^R \equiv \left\lfloor \frac{\tau_R}{c_A} \right\rfloor \text{ and } k_A^H \equiv \left\lfloor \frac{1-\tau}{c_A} \right\rfloor,$$

where k_A^R (resp. k_A^H) corresponds to the maximal number of attacks that A is willing to deploy to disconnect the network during the phase interval $[\tau, \tau+\tau_R]$ (resp. $[\tau, 1]$) so that $U_A^{(2)}$ (resp. $U_A^{(3)}$) achieves a positive value.

The following lemma characterizes the possible SPEs in Situation 1.

Lemma 4.6. *If $\tau_R/c_A > n-1$ or $\left\lfloor \frac{1-\tau}{c_A} \right\rfloor > \left\lfloor \frac{1-\tau}{c_D} \right\rfloor$, then no SPE exists in Situation 1. Otherwise, let*

$$\delta = \begin{cases} \left\lceil \frac{n\left(k_A^R+1\right)}{2} \right\rceil & \text{if } k \geq 1 \text{ and } k_A^R > 1, \\ \left\lceil \frac{n\left(k_A^H+1\right)}{2} \right\rceil & \text{if } k = 0 \text{ and } k_A^R > 1, \\ n & \text{if } k_A^H = k+1 \text{ and } k_A^R = 1, \\ n + \left\lfloor \frac{n}{k} \right\rfloor + \left\lceil \frac{\left\lfloor \frac{n}{k} \right\rfloor}{2} \right\rceil & \text{if } k_A^H \neq k+1 \text{ and } k_A^R = 1, \\ n-1 & \text{if } k_A^H = k \text{ and } k_A^R = 0, \\ n & \text{if } k_A^H \neq k \text{ and } k_A^R = 0. \end{cases} \tag{4.4}$$

If $1 < \delta c_D$ or if $1-\tau < (\delta - n + 1)c_D$, then no SPE in Situation 1 exists. Otherwise, the unique SPE is such that $U_D = 1 - \delta c_D$ and $U_A = 0$.

Proof. When $\tau_R/c_A > n-1$, A always attacks the network at phase τ, and hence Situation 1 is not possible. The SPE in Situation 1 satisfies $U_A^{(1)} > U_A^{(2)}$ and

$U_A^{(1)} > U_A^{(3)}$. Thus, the goal of D is to create a network with the minimal cost such that all nodes have a degree of at least $\left\lfloor \frac{\tau_R}{c_A} \right\rfloor + 1 = k_A^R + 1$, and at least $\left\lfloor \frac{1-\tau}{c_A} \right\rfloor + 1 = k_A^H + 1$ links need to be removed to yield a network with $k+2$ components (i.e., the minimum $(k+1)$-cut requires at least $\left\lfloor \frac{1-\tau}{c_A} \right\rfloor + 1$ links). For $k_A^R \geq 1$, we consider the strategy of D that consists in creating an $(|\mathcal{N}|, k_A^R + 1)$-Harary network. Thus,

$$|\mathcal{E}_1| \geq \begin{cases} \left\lceil \frac{n\left(k_A^R+1\right)}{2} \right\rceil & \text{if } k_A^R \geq 2, \\ n & \text{if } k_A^R = 1, \\ n-1 & \text{otherwise.} \end{cases} \tag{4.5}$$

Let $k_D^H \equiv \left\lfloor \frac{1-\tau}{c_D} \right\rfloor$. First, suppose that $k_D^H < k_A^H$, and at phase 0, D constructs a network with $(n-1) + \overline{k}$ links for some $\overline{k} \leq k_D^H$. Consider the strategy for A that consists in attacking randomly k_A^H links. Since $k_A^H > k_D^H \geq \overline{k}$, then the resulting network has less than $n-1$ links and is thus disconnected. At phase $\tau + \tau_R$, D can reconstruct at most $(n-1) + k_D^H - (n-1) - \overline{k} = k_D^H - \overline{k}$ links. Then, the network at phase $\tau+\tau_R$ would contain at most $(n-1)+\overline{k}-k_A^H+k_D^H-\overline{k} = (n-1)+k_D^H-k_A^H < n-1$ links, and the network is disconnected. Therefore, no SPE exists in Situation 1 if $k_D^H < k_A^H$.

Conversely, suppose that $k_D^H \geq k_A^H$. Then, we have $k_A^R \leq \left\lfloor \frac{\tau_R}{c_D} \right\rfloor$. Furthermore, $k_A^H \leq k_D^H \Rightarrow \frac{1}{c_A} - \frac{1}{c_D} < \frac{1}{1-\tau} \Rightarrow \frac{1-\tau-\tau_R}{c_A} - \frac{1-\tau-\tau_R}{c_D} < \frac{1-\tau-\tau_R}{1-\tau} < 1$, which gives $\left\lfloor \frac{1-\tau-\tau_R}{c_A} \right\rfloor \leq k$. Then, by definition, $k_A^H = \left\lfloor \frac{1-\tau}{c_A} \right\rfloor = \left\lfloor \frac{1-\tau-\tau_R}{c_A} + \frac{\tau_R}{c_A} \right\rfloor \leq \left\lfloor \frac{1-\tau-\tau_R}{c_A} \right\rfloor + \left\lfloor \frac{\tau_R}{c_A} \right\rfloor + 1 \leq k + k_A^R + 1$. Hence, we obtain $k_A^H \leq k + k_A^R + 1$. Based on the obtained results, we next focus on four distinct cases and derive their corresponding SPEs.

Case 1 ($k > 0$ and $k_A^R > 1$): If $k_A^R \geq 3$, then $k_A^R + 1$ link removals are needed

to disconnect the network, and any further additional component creation requires to remove at least 2 links. Thus, at least $2k + k_A^R + 1$ link removals are necessary so that the network has $k + 2$ components. Then, based on $2k + k_A^R + 1 > k_A^H + 1$, A does not attack the network. If $k_A^R = 2$, and if $k \leq \lfloor \frac{n}{2} \rfloor$, then at least $k_A^R + 1 + 2k$ link removals are required, and otherwise (i.e., $k > \lfloor \frac{n}{2} \rfloor$) $k_A^R + 1 + k$ link removals are necessary. Thus, A does not attack the network.

Case 2 ($k = 0$ and $k_A^R > 1$): In this case, we have $k_A^H \leq k_A^R + 1$. A only needs to disconnect the network since D does not heal due to $k = 0$. Thus, if $k_A^R > 1$, D creates an $(|\mathcal{N}|, k_A^H + 1)$-Harary network at phase 0.

Case 3 ($k_A^R = 0$): In this case, if $k_A^H = k$, then D creates a tree network which is an optimal strategy. Otherwise, $k_A^H = k + 1$ in which case D creates a ring network.

Case 4 ($k_A^R = 1$): In this scenario, if $k_A^H = k + 1$, then the ring network, i.e., the $(|\mathcal{N}|, 2)$-Harary network, is optimal for D. Otherwise, if $k_A^H = k + 2$, then D needs to create a network of minimal cost such that no k cut exists with $k + 1$ links. To this end, we consider the following network. For each $i \in \mathcal{N}$, we create a link between nodes i and $(i + 1) \mod n$ (ring network). Then, we connect node k to node $2k$, and connect node $2k$ to node $3k$, and so on. If $\lfloor \frac{n}{k} \rfloor$ is even, then we connect node $k\lfloor \frac{n}{k} \rfloor$ to node 0. Otherwise, we connect node 0 to any node of the network excluding 1 and $n - 1$. Thus, the resulting network contains no k cut of size $k+1$ links and is minimal in terms of the number of links. The resulting utility for D is $U_D = 1 - (n + \lfloor \frac{n}{k} \rfloor + \left\lceil \frac{\lfloor \frac{n}{k} \rfloor}{2} \right\rceil) c_D$.

By defining δ as in (4.4), the condition $1 < \delta c_D$ ensures a positive utility for D at SPE of Situation 1. The condition $1 - \tau < (\delta - n + 1)c_D$ guarantees that the SPE is achieved in Situation 1 instead of in Situation 3. □

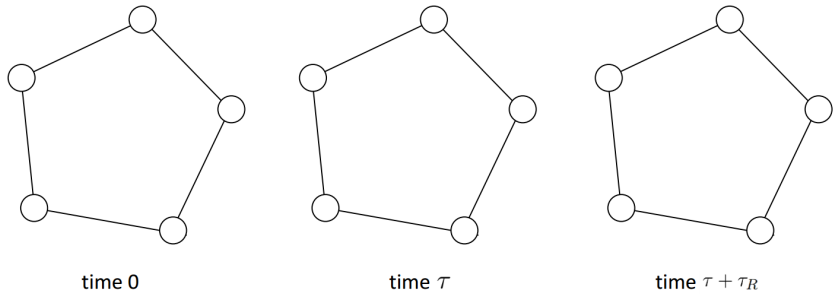


Figure 4.4: The SPE lies in Situation 1 with $\delta = 5$ ($k_A^H = 2$ and $k_A^R = 1$). Thus, D creates a 2-Harary network with the ring topology. A will not attack and thus D does not heal the network.

Example: For clarity, an illustration of SPE in Situation 1 with $\delta = 5$ is depicted in Fig. 4.4. There are 5 nodes in the network and the parameters are $k_A^H = 2$ and $k_A^R = 1$. Specifically, D creates a 2-Harary network with the ring topology initially. Then, A is not capable to attack. The network remains connected over the entire time period.

For convenience, the results of Lemmas 4.4, 4.5 and 4.6 are summarized in Table 4.3.

Situation	$\lvert\mathcal{E}_1\rvert$	$\lvert\mathcal{E}_A\rvert$	$\lvert\mathcal{E}_2\rvert$	U_D	U_A
1	δ	0	0	$1 - c_D\delta$	0
2	$n-1$	1	1	$1 - \tau_R - nc_D$	$\tau_R - c_A$
3	$n-1$	$k+1$	0	$\tau - (n-1)c_D$	$1 - \tau - (k+1)c_A$
5	0	0	0	0	1

Table 4.3: Different potential SPEs when $1 - \tau - \tau_R < (n-1)c_D$ (Note: δ is given by Eq. (4.4), and $k = \left\lfloor \frac{1-\tau-\tau_R}{c_D} \right\rfloor$).

We next comment on the strategies of D and A at SPEs. Specifically, the players' strategies in Situation 2 under regime 2 are the same as the corresponding

ones under regime 1. In Situation 3, D creates a tree network at time 0 and does not heal it after A compromising any $k+1$ links at phase τ. Depending on the system parameters, in Situation 1, D creates a connected network using δ links either in a tree, ring or Harary network topology, and A does not attack.

Remark: In the previous two Sections 4.4.1 and 4.4.2, we have not explicitly determined those SPEs satisfying the boundary conditions. Note that at boundaries where multiple SPEs could be feasible, the defender playing a leader role will first choose the one that yields the highest utility. Then, after fixing the defender's strategy, the attacker selects the SPE that maximizes its payoff.

4.4.3 Discussions on Constrained Action Set of A

In some scenarios, A may not be capable to attack a particular set of links due to constraints. Thus, some links initially created by D cannot be compromised by A, and they can be regarded as *secure links*. The major SPE analysis of this chapter is still valid for this constrained scenario with extra considerations on A's feasible action set. We present the results for this extension in regime 1 briefly as follows, and the results in regime 2 can be obtained using similar arguments.

First, we consider the case that every node can create at least one secure link with other nodes. Then the SPE in Situation 1 under $k_A^R > 0$ becomes as $|\mathcal{E}_1| = n-1$, $|\mathcal{E}_A| = 0$, and $|\mathcal{E}_2| = 0$. In this subcase, D can create a connected network with all secure links using a tree topology and thus Harary network, $|\mathcal{E}_1| = \left\lceil \frac{n(k_A^R+1)}{2} \right\rceil$, is not optimal to D. Furthermore, Situation 2 is not possible as the network created by D cannot be attacked. In addition, Situation 4 remains the same in this case. We next investigate cases in Situation 2. Indeed, SPE in Situation 2 occurs if there exists at least a single link in the tree network created by D at phase 0 which is

insecure. Then, A disconnects the network by compromising this vulnerable link. Finally, we analyze the case when a subset of nodes in the network can form secure links with others. In this scenario, the results of Situation 1 & $k_A^R = 0$, Situation 2, and Situation 4 in Table 4.2 still hold. For Situation 1 & $k_A^R > 0$, D does not need to create a Harary network at phase 0 as some created links are secure. To this end, we can leverage network contraction [37] to derive the SPE. Network contraction refers to the principle that if there is a secure link between two nodes, we can aggregate them together and see them as a single super node. In Situation 1 & $k_A^R > 0$, depending on the places where secure links can be formed, it leads to different policies for D at phase 0. We illustrate the design principle for Situation 1 & $k_A^R > 0$ in Fig. 4.5. In this example, $|\mathcal{E}_1| = 5$ is sufficient in the constrained scenario for D to construct a secure network at time 0, while it requires $|\mathcal{E}_1| = 6$ links in the unconstrained counterpart.

4.5 Network Resilience and Strategic Attack

In this section, we investigate the impact of network resilience on the SPE of the dynamic game and the attacker's behavior on the timing of attack.

4.5.1 Resilience Planning

The CPS network resilience is measured by the response and recovery time after the cyber attack which is τ_R in our scenario. Thus, instead of merely maximizing U_D, the network operator should also take resilience metric τ_R into account. Thus,

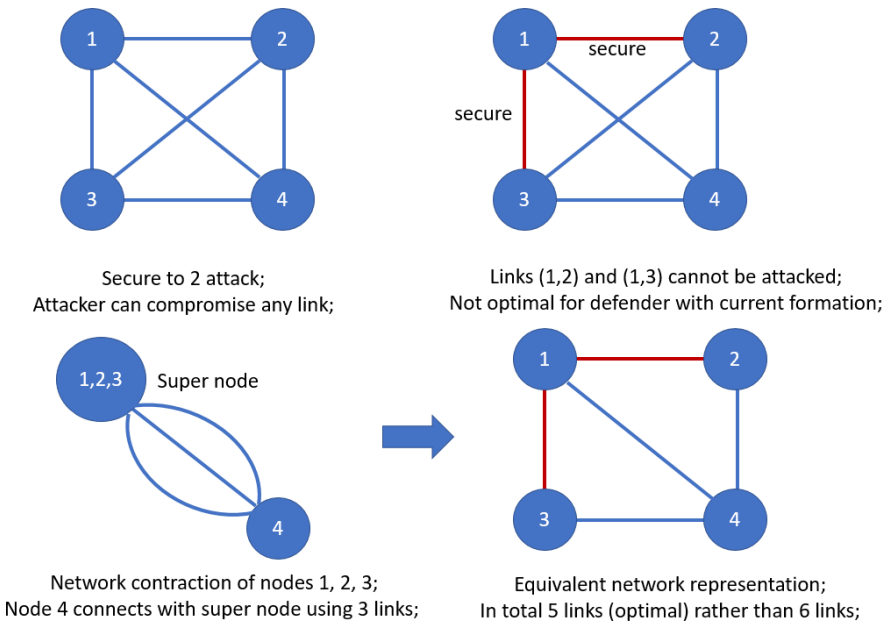


Figure 4.5: Illustration of network contraction for designing D's optimal strategy when a subset of nodes can form secure links with others. In the example, 6 links are required for the network being resistant to 2 link removals if A can compromise any link. When links (1,2) and (1,3) cannot be attacked, nodes 1, 2, and 3 can be aggregrated as a super node by network contraction. Then, node 4 connects with the super node using 3 links. In sum, 5 links are sufficient for this constrained scenario which is different from the unconstrained case.

the aggregated objective function of D can be formulated as follows:

$$F_D(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_A, \tau_R) = U_D(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_A) - R_D(\tau_R), \tag{4.6}$$

where $R_D : [0,1] \to [0,1]$ quantifies the normalized system resilience cost. Specifically, R_D is a monotonically decreasing function with respect to τ_R. By considering the SPE of the dynamic game, D chooses the best τ_R that results in an optimal utility F_D.

Based on Section 4.4, we obtain the following results. In regime 1 with agile resilience, i.e., $\tau_R < 1 - \tau - (n-1)c_D$, the utilities of D under various SPE are

summarized in Table 4.4.

Situation	F_D
$1\&k_A^R > 0$	$1 - c_D\left\lceil \frac{n(k_A^R+1)}{2} \right\rceil - R_D(\tau_R)$
$1\&k_A^R = 0$	$1 - (n-1)c_D - R_D(\tau_R)$
2	$1 - \tau_R - nc_D - R_D(\tau_R)$
4	$1 - \tau - \tau_R - (n-1)c_D - R_D(\tau_R)$

Table 4.4: Utilities of D under different potential SPE when $1-\tau-\tau_R > (n-1)c_D$ (Note: $k_A^R = \left\lfloor \frac{\tau_R}{c_A} \right\rfloor$).

Similarly, in regime 2 with $\tau_R > 1 - \tau - (n-1)c_D$, D's utilities with different scenarios are presented in Table 4.5.

Situation	F_D
1	$1 - c_D\delta - R_D(\tau_R)$
2	$1 - \tau_R - nc_D - R_D(\tau_R)$
3	$\tau - (n-1)c_D - R_D(\tau_R)$
5	0

Table 4.5: Utilities of D under different potential SPE when $1-\tau-\tau_R < (n-1)c_D$ (Note: δ is given by Eq. (4.4)).

Remark: Under different regimes and situations, the aggregated payoff F_D of D admits various forms. Comparing the values of F_D in Tables 4.4 and 4.5, the designer selects a τ_R that yields the largest F_D, and the corresponding SPE strategies can be determined based on Tables 4.2 and 4.3.

4.5.2 Strategic Timing of Attack

The attacker's behavior depends on the recovery ability of the network. When A decides to compromise the network, then choosing the attacking phase τ also becomes a critical issue. Specifically, for a given τ_R, A needs to decide the value of τ. As shown in Lemma 4.2, A compromises the network only if D creates a connected network initially. Thus, we focus on two Situations: 2 and 3. Proposition 4.1 indicates that when Situation 2 is an SPE, the corresponding utility of A is $U_A = \tau_R - c_A$ which does not depend on the attacking phase τ. In an SPE of Situation 3, D does not heal the network after attack, and the utility of A is $U_A = 1 - \tau - (k+1)c_A$. Hence, the timing of attack τ has an influence on A's payoff. In another case when SPE takes a form of Situation 4, A's utility is $\tau + \tau_R$ which is also influenced by the attacking phase. Despite that A does not attack, its action induces a threat to the network. We summarize the results in the following Lemma.

Lemma 4.7. *When SPE of the game admits a form of Situation 3, then the best timing of attack for A is to choose the smallest τ in the set $\{\tau | \tau \geq \frac{1-\tau_R}{(n-1)c_D},\ \left\lfloor \frac{1-\tau}{c_A} \right\rfloor \geq \left\lfloor \frac{1-\tau-\tau_R}{c_D} \right\rfloor + 1\}$. When SPE takes a form of Situation 4, then the best τ for A is choosing the largest value in the set $\{c_D, 1-\tau_R-(n-1)c_D, c_D\left\lceil \frac{n(k_A^R-1)}{2} + 1 \right\rceil - \tau_R\}$. When SPE of the game is of another form except for Situations 3 and 4, then τ does not affect the utility of A.*

Proof. The attacker chooses a τ to maximize its utility $1 - \tau - (\left\lfloor \frac{1-\tau-\tau_R}{c_D} \right\rfloor + 1)c_A$ while satisfying the conditions $\lfloor \frac{1-\tau}{c_A} \rfloor \geq \left\lfloor \frac{1-\tau-\tau_R}{c_D} \right\rfloor + 1$ and $1 - \tau - \tau_R < (n-1)c_D$. The objective function indicates that a smaller τ yields a higher payoff of A. Thus, the best timing of attack is the smallest τ resulting in an SPE of Situation 3.

We relax the strict inequality constraint by including the boundary, since when $\tau = \frac{1-\tau_R}{(n-1)c_D}$, D does not heal the network and Situation 3 is still an SPE. Similarly, in Situation 4, those boundary values of τ at the inequality constraint are feasible since D chooses not to create a connected network if the payoffs are the same. □

In Situation 3, A prefers to attack the network in an early phase which aligns with the fact that D does not recover the network, and hence A receives the total rewards after τ. In contrast, A chooses to compromise the network at a larger phase τ in Situation 4 (though he does not really attack since the network is not connected), which extracts all the utility from time 0 to $\tau + \tau_R$.

4.6 Case Studies

In this section, we use case studies of UAV-enabled communication networks to corroborate the obtained results. UAVs become an emerging technology to serve as communication relays, especially in disaster recovery scenarios in which the existing communication infrastructures are out of service [132]. In the following, we consider a team of $n = 10$ UAVs. The normalized unitary costs of creating and compromising a communication link between UAVs for the operator/defender and adversary are $c_D = 1/20$ and $c_A = 1/8$, respectively.

4.6.1 Illustrations of SPEs (Results in Section 4.4)

First, we illustrate SPE of the game when network resilience cost and timing of attack are not considered (results in Section 4.4). Specifically, the adversary attacks the network at phase $\tau = 0.3$, and the defender heals it after $\tau_R = 0.2$. The UAV-enabled communication network configuration at SPE is shown in Fig.

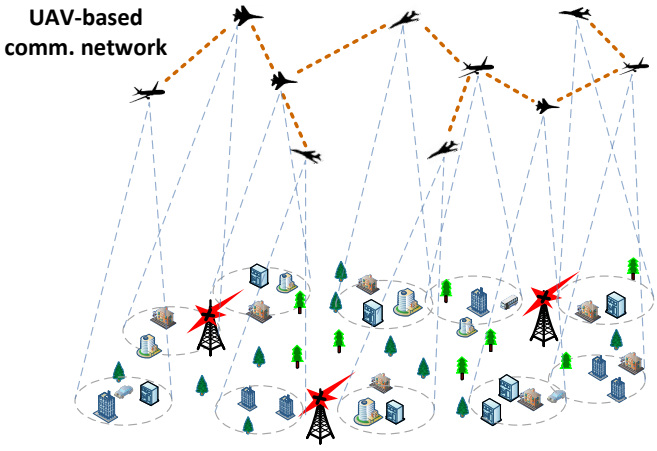


Figure 4.6: UAV-enabled communication networks for disaster recovery. The UAVs form a tree network at SPE ($\tau = 0.3$, $\tau_R = 0.2$).

4.6 which admits a tree structure, and A does not attack the network at SPE. In addition, the utilities for D and A at SPE with $\tau_R \in [0, 0.6]$ are shown in Fig. 4.7. The SPE encounters switching with different τ_R. As τ_R increases, the UAV network operator needs to allocate more link resources to secure the network. Otherwise, the attacker has an incentive to compromise the communication links with a positive payoff. Specifically, when $\tau_R < 0.375$, A does not attack the UAV network, and D obtains a positive utility by constructing a securely connected network. The secure network admits various structures depending on τ_R. As shown in Fig. 4.7, it can be in a tree network or a Harary network and the SPEs are in Situation 1. When $0.375 < \tau_R < 0.5$, the defender creates a connected network with the minimum effort, i.e., 9 links, at phase 0. In this interval, the attacker will successfully compromise the system during phase $[\tau, \tau + \tau_R]$, and the defender heals the network afterward. The initially connected network in this regime admits a tree structure, and it may not be the same as the one created in the regime of $\tau_R < 0.375$. When τ_R exceeds 0.5, the defender does not either protect or heal the network. The

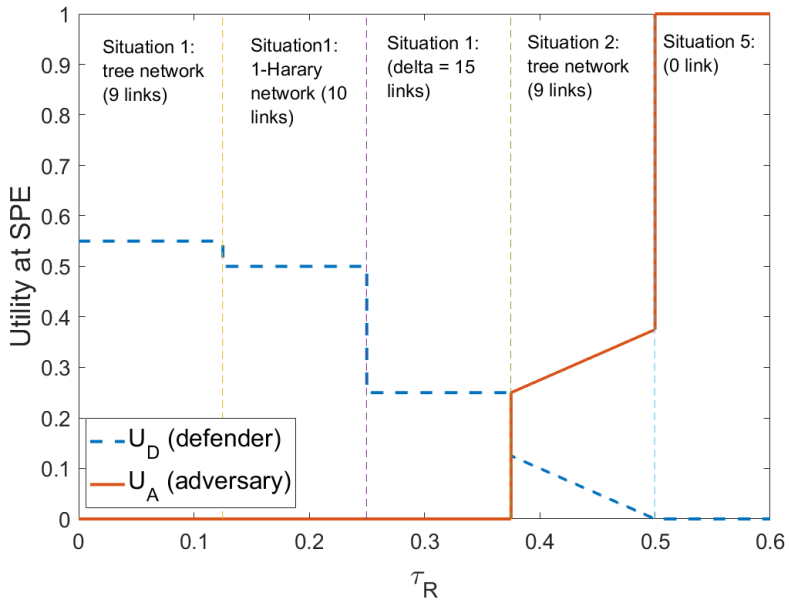


Figure 4.7: Utilities for D and A at SPE with varying τ_R. The SPEs and the strategies of D and A are different with the increase of τ_R.

reason is that a larger τ_R provides more incentives for the attacker to compromise the links and receive a higher payoff. Furthermore, the aggregated utility for the defender from two intervals, i.e., from the initial phase to the attacking phase and from the recovery phase to the terminal phase, is small, and hence it does not provide sufficient incentive for the defender to protect and recover the network. This also indicates that agile resilience is critical in mitigating cyber threats in the CPS networks.

4.6.2 Strategic Resilience Planning

Next, we take into account the cost of network resilience and study its impact on the SPE. The cost function of resilience is $R_D(\tau_R) = (\tau_R - 1)^4$. The convexity of R_D indicates that the marginal cost of resilience increases as τ_R decreases. The

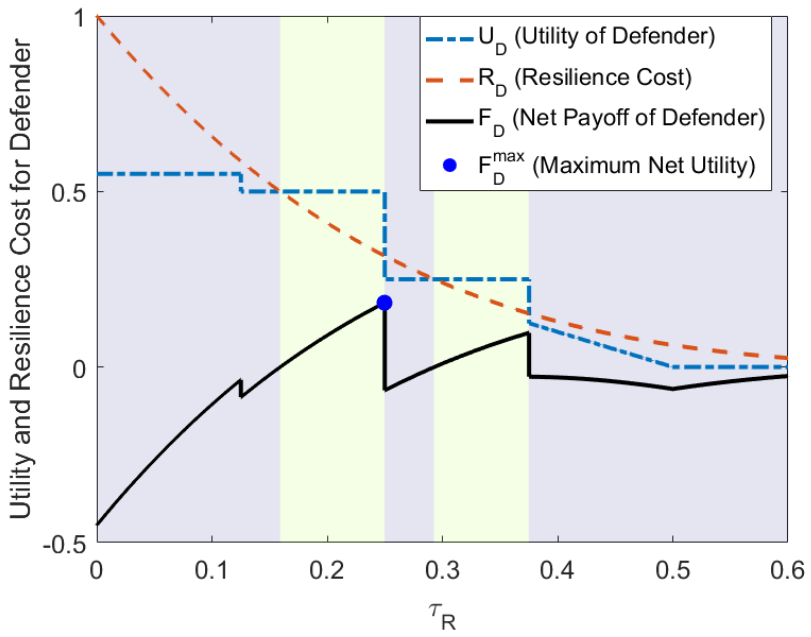
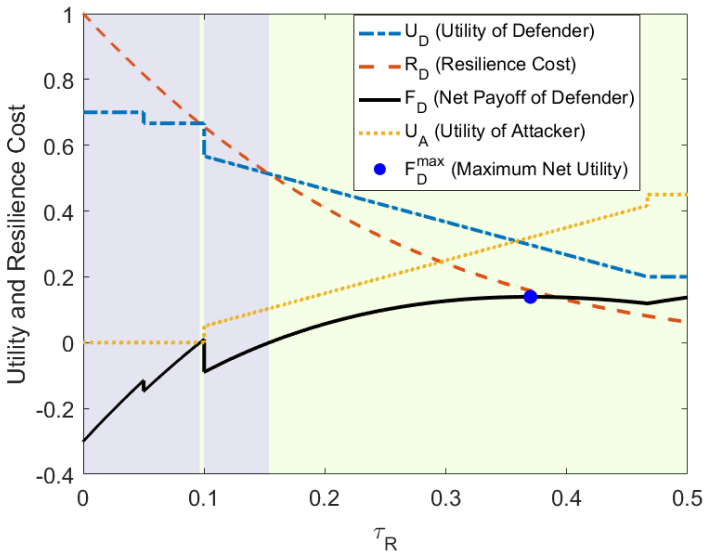
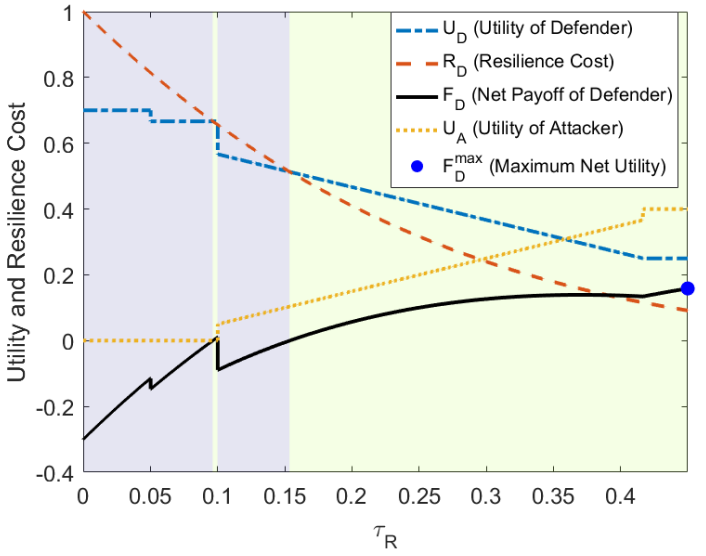


Figure 4.8: Defender's utility with varying τ_R by considering the resilience cost. The optimal resilience planning is achieved at $\tau_R = 0.25$. Values of τ_R in the interval $[0, 0.16] \cup [0.375, 0.6]$ are not feasible since F_D is negative.

timing of attack is fixed to $\tau = 0.3$ in this case study. The equilibrium strategies of both players under costly network resilience are illustrated in Fig. 4.8. Based on the analysis in Section 4.5.1, D chooses a τ_R that maximizes the net utility F_D. Though U_D is larger in a regime with smaller values of τ_R, the cost of agile network resilience is much higher for it being the best strategy of designer. In addition, the defender will not choose a τ_R in the intervals $[0, 0.16] \cup [0.375, 0.6]$ since F_D is negative. Hence, the optimal resilience planning of D is $\tau_R = 0.25$ which yields the optimal payoff $F_D = 0.183$. At this SPE, which falls into Situation 1, D creates a $(10, 1)$-Harary network using 10 links initially and A does not attack.



(a) $\tau = 0.5$



(b) $\tau = 0.55$

Figure 4.9: (a) and (b) illustrate the strategies of D and A with different τ. The SPE under optimal resilience planning switches from Situation 2 to Situation 3 as τ changes from 0.5 to 0.55. In both (a) and (b), the shaded grey areas, i.e., $\tau_R \in [0, 0.096] \cup [0.01, 0.154]$, are not feasible due to the negative value F_D.

4.6.3 Strategic Attacks and Resilience Planning

We finally investigate the strategic attack behavior of A. In the following, the costs of creating and compromising a communication link are selected as $c_D = 1/30$ and $c_A = 1/20$, respectively. The SPEs and the corresponding utilities with $\tau = 0.5$ and $\tau = 0.55$ are shown in Fig. 4.9. Specifically, Fig. 4.9(a) shows that the optimal resilience planning for D at $\tau = 0.5$ is $\tau_R = 0.37$, leading to $F_D = 0.14$. Note that this SPE, where D constructs a tree network at phase 0 and A attacks one link at τ with D healing the network afterward, belongs to Situation 2 in regime 2 as shown in Table 4.5. As $\tau = 0.55$, the best resilience planning of D is to adopt $\tau_R = 0.45$ as illustrated in Fig. 4.9(b). At this SPE, which is a case of Situation 3 in regime 2, D creates a tree network initially and A attacks one link at τ, and D does not recover the network. We can see that the SPE under optimal resilience planning switches from Situation 2 to Situation 3 as τ increases. In addition, the utility of A varies under different SPEs. Based on Lemma 4.7, for an SPE in Situation 3, the attacker can increase its utility by choosing an appropriate τ. Thus, we study the impact of attacking phase τ on the SPE of the game, and the result is depicted in Fig. 4.10. Note that the utility of D is optimal under each τ in the sense that the resilience cost R_D is considered. When $\tau \in [0.4, 0.515)$, the SPE belongs to Situation 2, and the optimal utilities of D and A remain as constants, where the resilience metric is given by $\tau_R = 0.37$. When $\tau \in [0.515, 0.6]$, the SPE switches to a case of Situation 3. In this interval, D does not recover after the attack and $\tau_R = 1 - \tau$. Furthermore, the optimal timing of attack is selected as $\tau = 0.515$, leading to $U_A = 0.435$, the largest utility of A. The result is in consistence with Lemma 4.7, indicating that a smaller τ yields a higher utility of A when SPE admits a form of Situation 3.

We next investigate the SPEs under the optimal resilience planning of D and

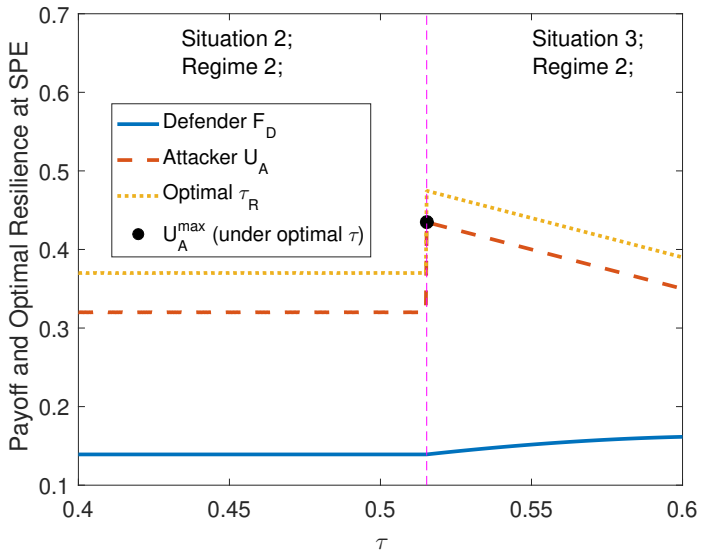


Figure 4.10: Players' utilities at SPE with varying τ under the optimal resilience planning. The best timing of attack is $\tau = 0.515$ with optimal $\tau_R = 0.37$.

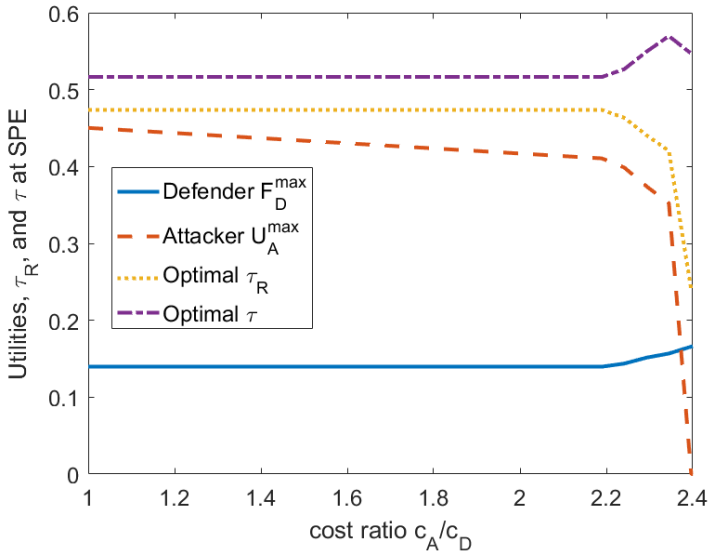


Figure 4.11: Players' utilities, optimal resilience planing τ_R, strategic timing of attack τ, at SPE with varying c_A/c_D.

the strategic timing of attack of A together over varying cost ratio c_A/c_D. We fix $c_D = 1/30$ and the ratio c_A/c_D varies. Figure 4.11 shows the obtained results.

As the cost ratio c_A/c_D increases, the utility of A decreases monotonically. When $c_A/c_D \in [1, 2.2]$, the strategies of D and A does not change and the SPE belongs to Situation 3. Since the optimal τ_R and τ stay the same in this interval, the utility of D remains unchanged. When $c_A/c_D \in [2.2, 2.4]$, the SPE switches to Situation 2 and D heals the network after the attack. Since the recovery is agile (τ_R becomes smaller), D's utility increases and A's utility decreases dramatically in this interval. Furthermore, the strategic timing of attack τ varies to account for the better recovery speed τ_R and the increasing cost of attack.

4.7 Summary

In this chapter, we have established a two-player three-stage dynamic game for the CPS network protection and recovery. We have characterized the strategic strategies of the network defender and the attacker by analyzing the subgame perfect equilibrium (SPE) of the game. With case studies on UAV-enabled communication networks for disaster recovery, we have observed that with an agile response to the attack, the defender can obtain a positive utility by creating a securely connected CPS network. Furthermore, a higher level resilience saves link resources for the defender and yields a better payoff. In addition, a longer duration between the attack and recovery phases induces a higher level of cyber threats to the infrastructures. Future work would investigate dynamic games with incomplete information of the defender on the attacking time and attack cost. Another direction is to design SPE strategies under the scenarios that the feasible action sets of both defender and attacker are constrained.

Part III

Trustworthy Decision Making over CPS Networks

Chapter 5

Cyber Risk Management under Bounded Rationality in IoT Networks

5.1 Introduction

Recent years have witnessed a significant growth of urban population. As the growth continues, cities need to become more efficient to serve the surging population. IoT plays a central role in supporting the development of smart city. There are several features of IoT devices need to be considered when they are deployed. First, IoT devices come from different manufacturers, and they have heterogeneous functionalities and security configurations and policies. No uniform security standards are used for IoT devices as they are developed using different system platforms for various functionalities. Moreover, due to the connections between IoT devices, the security of one device is also dependent on the security

of other devices to which it connects. Therefore, the heterogeneity and the interconnectivity of massive heterogeneous IoT have created significant challenges for security management. Fig. 1.4 depicts a highly connected smart community enabled by IoT devices. Each household needs to take into account the cyber risks coming from their connected neighbors when securing their devices.

The security management and practices of users are often viewed as the weakest link [137]. The lack of security awareness and expertise at the user's end creates human-induced vulnerabilities that can be easily exploited by an adversary. Therefore, each device owner needs to allocate resources (e.g. human resources, computing resources, investments or cognition) to secure his applications in a decentralized way. For example, the smart building operator can spend resources on upgrading the hardware, hiring staff members for network monitoring and forensics, and developing tailored security solutions to the smart building. A smart home user, on the other hand, can safely configure its network and regularly updates its software and password of the IoT devices.

The process of decentralized security decision-making can be modeled as a game problem. The users cannot be aware of the security policies taken by all its connected neighbors in the massive IoT network. This is consistent with the fact that humans with limited knowledge or cognitive resources are bounded rational, since they cannot pay attention to all the information [53, 66]. Thus, the game model needs to take into account the bounded rationality of players [62]. In the game framework, we use a cognition vector representing the observation structure of each IoT user. Specifically, a sparser cognition vector represents a user with weaker cognition ability, and he observes a smaller number of other users' behaviors when deciding his strategy. Thus, the limited attention nature of users creates a

bounded perception of cyber risks.

In the established bounded rational game model, the users need to make security management decisions as well as design their cognition networks jointly. In order to achieve this goal, we define a new solution concept called *Gestalt Nash equilibrium* (GNE) to capture the cognitive network formation and the security management under the bounded rationality simultaneously. The analysis of the GNE provides a quantitative method to understand the risk of massive IoTs and gives tractable security management policies. We further design a proximal-based iterative algorithm to compute the GNE of the game. The GNE resulting from the algorithm reveals several typical phenomena that match well with the real-world observations. For example, when the network contains two groups of users, then under the limited attention, all users will allocate their cognition resources to the same group which demonstrates *the law of partisanship*. Further, in a heterogeneous massive IoT, the equilibrium successfully identifies the set of agents that are invariably paid attention to by other users, demonstrating the phenomenon of *attraction of the mighty*. Since the framework predicts the high-level systemic risk of the IoT network, it also can be used to inform the design of security standards and incentive mechanisms, e.g., through contracts and cyber insurance.

5.1.1 Summary of Notations

For convenience, we summarize the notations used in this chapter in Table 5.1. Note that notations associated with $*$ refer to the value at equilibrium. Furthermore, notations with index k stands for its value at step k during the iterative updates.

Table 5.1: Nomenclature of Chapter 5

$\mathcal{N}$	$\mathcal{N} := \{1, 2, ..., N\}$, set of players/users
R_{ii}^i	security investment cost coefficient of player i
R_{ij}^i	security investment influence coefficient of player j on player i
r_i	unit return of security investment of player i
r	$r := [r_1, r_2, ..., r_N]$
u_i	security investment decision of player i
u	$u := [u_1, u_2, ..., u_N]$
u_{-i}	set of decisions of all players except i-th one
$\mathcal{U}$	set of decisions of all players
m^i	$m^i := [m_j^i]_{j \neq i, j \in \mathcal{N}}$, $m_j^i \in [0, 1]$, the attention network of player i
$u_j^{c_i}$	$u_j^{c_i} = m_j^i u_j$, decision of player j perceived by player i
J_i	cost function of player i
$\tilde{J}^i$	cost function of player i under bounded rationality
BR^i	best response of player i
Λ^i	$\Lambda^i := [\Lambda_{jk}^i]_{j \neq i, k \neq i, j \in \mathcal{N}, k \in \mathcal{N}}$, $\Lambda_{jk}^i := \frac{1}{R_{ii}^i} R_{ij}^i R_{ik}^i u_j u_k$
e_{N-1}	an $N-1$-dimensional column vector with all one entries
α_i	weighting factor quantifying the unit cost of player i's cognition
β_i	total number of links in the cognitive network of player i
$\|\| \cdot \|\|_1$	standard L-1 norm
$\|\| \cdot \|\|$	standard L-2 norm
ι_C	indicator function on set C
prox.	proximal operator

5.2 Problem Formulation

In this section, we formulate a problem involving strategic security decision making and cognitive network formation of players in the IoT networks.

5.2.1 Security Management Game over Networks

In an IoT user network including a set $\mathcal{N}$ of nodes[1], where $\mathcal{N} := \{1, 2, ..., N\}$, each node can be seen as a player that makes strategic decisions on the security management to secure their IoT devices. For instance, in Fig. 1.4, each smart home is a player securing their smart things to mitigate the cyber threats. We define $\mathcal{U} := \{u_1, ..., u_N\}$ by the decision profile of all the players. Specifically, u_i is a one-dimensional decision variable representing player i's security management effort. For convenience, we denote $u_{-i} := \mathcal{U} \setminus \{u_i\}$. The objective of player i, $i \in \mathcal{N}$, is to minimize his security risk strategically by taking the costly action u_i. We define by $F_1^i : \mathbb{R}_+ \to \mathbb{R}_+$ the cost of security management effort of player i which is an increasing function of u_i. The corresponding benefit of security management is captured by a function $F_2^i : \mathbb{R}_+ \to \mathbb{R}_+$. Intuitively, a larger u_i yields a higher return, and hence F_2^i is monotonically increasing. Due to the interconnections in the IoT, the risk of player i is also dependent on his connected users. Then, we use a function $F_3^i : \mathbb{R}_+ \times \mathbb{R}_+^{N-1} \to \mathbb{R}_+$ to represent the influence of player i's connected users on his security. The coupling between players in the IoT is in a strategic complement fashion with respect to the security decisions. More specifically, a larger security investment u_j of player j, a connected node of player i, decreases the cyber risks of player i as well. Therefore, the cost function of player i can be expressed as the following form:

$$J^i(u_i, u_{-i}) = F_1^i(u_i) - F_2^i(u_i) - F_3^i(u_i, u_{-i}), \tag{5.1}$$

[1]The terms of node, agent and player refer to the user in the IoT, and they are used interchangeably.

where $J^i : \mathbb{R}_+ \times \mathbb{R}_+^{N-1} \to \mathbb{R}$. To facilitate the analysis and design of security risk management strategies, we specify some appropriate forms of functions in (5.1). In the following, we focus on player i taking the quadratic form: $F_1^i(u_i) = \frac{1}{2}R_{ii}^i u_i^2$, $F_2^i(u_i) = r_i u_i$, and $F_3^i(u_i, u_{-i}) = \sum_{j\neq i, j\in\mathcal{N}} R_{ij}^i u_i u_j$. Thus, (5.1) can be detailed as

$$J^i(u_i, u_{-i}) = \frac{1}{2}R_{ii}^i u_i^2 - r_i u_i - \sum_{j\neq i, j\in\mathcal{N}} R_{ij}^i u_i u_j, \tag{5.2}$$

where $R_{ii}^i > 0,\ r_i > 0,\ \forall i$, and $R_{ij}^i \geq 0, \forall j \neq i, i \in \mathcal{N}$. Note that parameters R_{ij}^i, $i, j \in \mathcal{N}$, represent the risk dependence network of player i in the IoT, and the value of R_{ij}^i indicates the strength of risk influence of player j on player i which is given as a prior. The first term $\frac{1}{2}R_{ii}^i u_i^2$ in (5.2) is the cost of security management with an increasing marginal price. The second term $r_i u_i$ denotes the corresponding payoff of cyber risk reduction. Then, the first two terms capture the fact that increasing a certain level of cyber security becomes more difficult in a secure network than a less secure one. The last term $\sum_{j=1, j\neq i}^N R_{ij}^i u_i u_j$ is the aggregated security risk effect from connected users of player i. Specifically, the structure of F_3^i in u_i and u_j indicates that the risk measure J^i of player i decreases linearly with respect to user j's action. Hence, in the established model, larger investment from a user helps reduce cyber risk influence in a linear way. We have following assumption on the security influence parameters.

Assumption 5.1. $R_{ii}^i > \sum_{j\neq i, j\in\mathcal{N}} R_{ij}^i,\ \forall i \in \mathcal{N}$.

Assumption 5.1 has a natural interpretation which indicates that the security of a user is mainly determined by his own strategy rather than other users' decisions in the IoT network. Moreover, based on the heterogeneous influence networks characterized by Assumption 5.1, each node designs its own security investment

strategy which enables the decentralized decision-making. The strategies of nodes are interdependent due to the coupling between their cost functions shown in (5.2).

Through the first order optimality condition (FOC), we obtain

$$R_{ii}^i u_i - \sum_{j\neq i, j\in\mathcal{N}} R_{ij}^i u_j - r_i = 0,\ \forall i \in \mathcal{N}. \tag{5.3}$$

Putting (5.3) in a matrix form yields

$$\begin{bmatrix} R_{11}^1 & -R_{12}^1 & \cdots & -R_{1N}^1 \\ -R_{21}^2 & R_{22}^2 & \cdots & -R_{2N}^2 \\ \vdots & \vdots & \ddots & \vdots \\ -R_{N1}^N & -R_{N2}^N & \cdots & R_{NN}^N \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_N \end{bmatrix} = \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_N \end{bmatrix} \Leftrightarrow\ Ru = r, \tag{5.4}$$

where $r := [r_i]_{i\in\mathcal{N}}$, $u := [u_i]_{i\in\mathcal{N}}$.

For convenience, we denote this security management game by $\mathcal{G}$. One solution concept of game $\mathcal{G}$ is Nash equilibrium (NE) which is defined as follows.

Definition 5.1 (Nash Equilibrium of Game $\mathcal{G}$ [18]). *The strategy profile* $u^* = [u_i^*]_{i\in\mathcal{N}}$ *constitutes a Nash equilibrium of game* $\mathcal{G}$ *if* $J^i(u_i, u_{-i}^*) \geq J^i(u_i^*, u_{-i}^*),\ \forall i \in \mathcal{N},\ \forall u_i \in \mathcal{U}_i$.

The NE of game $\mathcal{G}$ yields strategic security management policies of players under the condition that they can perceive all the cyber risks in the IoT network.

5.2.2 Bounded Rational Security Management Game

In reality, the users in IoT are connected with numerous other agents. For example, a single household can be connected with a number of other houses in

terms of various types of IoT products in the smart communities. Therefore, when making security management strategies, each user may not be capable to observe all its connected neighbors. Instead, a user can only respond to a selected number of other players' decisions. Then, this bounded rational response mechanism creates a cognitive network formation process for the players in the network. Specifically, player i's irrationality is captured by a vector $m^i := [m^i_j]_{j\neq i, j\in\mathcal{N}}$, $m^i_j \in [0,1]$, which stands for the attention network that player i builds. When $m^i_j = 0$, user i pays no attention to user j's behavior; when $m^i_j = 1$, user i observes the true value of security management u_j of user j. The value that m^i_j admits between 0 and 1 can be interpreted as the trustfulness of user i on the perceived u_j. Another interpretation of m^i_j can be the probability that user i observes the behavior of user j at each time instance on the security investment over a long period. Hence, the decision of player j perceived by player i becomes $u^{c_i}_j = m^i_j u_j$. Then, player i minimizes the modified cost function with bounded rationality defined as:

$$\begin{aligned}\tilde{J}^i(u_i, u^{c_i}_{-i}, m^i) &= \frac{1}{2}R^i_{ii}u_i^2 - r_i u_i - \sum_{j\neq i, j\in\mathcal{N}} m^i_j R^i_{ij} u_i u_j \\ &= \frac{1}{2}R^i_{ii}u_i^2 - r_i u_i - \sum_{j\neq i, j\in\mathcal{N}} R^i_{ij} u_i u^{c_i}_j, \end{aligned} \tag{5.5}$$

where $\tilde{J}^i : \mathbb{R}_+ \times \mathbb{R}_+^{N-1} \times [0,1]^{N-1} \to \mathbb{R}$.

The FOC of (5.5) gives $R^i_{ii}u_i - \sum_{j\neq i, j\in\mathcal{N}} R^i_{ij}u^{c_i}_j - r_i = 0,\ \forall i \in \mathcal{N}$, which is

equivalent to

$$\begin{bmatrix} R_{11}^1 & -m_2^1 R_{12}^1 & \cdots & -m_N^1 R_{1N}^1 \\ -m_1^2 R_{21}^2 & R_{22}^2 & \cdots & -m_N^2 R_{2N}^2 \\ \vdots & \vdots & \ddots & \vdots \\ -m_1^N R_{N1}^N & -m_2^N R_{N2}^N & \cdots & R_{NN}^N \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_N \end{bmatrix} = \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_N \end{bmatrix} \Leftrightarrow \quad R^s u = r. \tag{5.6}$$

The bounded rational best-response of player i, $i \in \mathcal{N}$, then becomes

$$u_i = BR^i(u_{-i}^{c_i}) = \frac{1}{R_{ii}^i} \left(\sum_{j \neq i, j \in \mathcal{N}} R_{ij}^i u_j^{c_i} + r_i \right), \tag{5.7}$$

where $u_j^{c_i} = m_j^i u_j$.

We denote the security management game of players with limited attention by $\tilde{\mathcal{G}}$. Comparing with the solution concept NE of game $\mathcal{G}$, the one of game $\tilde{\mathcal{G}}$ is generalized to bounded rational Nash equilibrium (BRNE). The formal definition of BRNE is as follows.

Definition 5.2 (Bounded Rational Nash Equilibrium of Game $\tilde{\mathcal{G}}$)**.** *With given cognition vectors m^i, $\forall i \in \mathcal{N}$, the strategy profile $u^* = [u_i^*]_{i \in \mathcal{N}}$ constitutes a BRNE of game $\tilde{\mathcal{G}}$ if $\tilde{J}^i(u_i, u_{-i}^*, m^i) \geq \tilde{J}^i(u_i^*, u_{-i}^*, m^i),\ \forall i \in \mathcal{N},\ \forall u_i \in \mathcal{U}_i$.*

Note that the cognitive network each user built has an impact on the BRNE of game $\tilde{\mathcal{G}}$. Hence, how the users determine the cognition vector m^i, $i \in \mathcal{N}$, becomes a critical issue. In the ensuing section, we introduce the cognitive network formation of players in the IoT.

5.2.3 Cognitive Network Formation

Due to the massive connections in IoT, each user builds a sparse cognitive network containing the agents to observe. To this end, the real cost of user i by taking the bounded rationality into account becomes

$$\begin{aligned}
J^i(BR^i(u_{-i}^{c_i}), u_{-i}) &= \frac{1}{2R_{ii}^i}\left(\sum_{j\neq i, j\in\mathcal{N}} R_{ij}^i u_j^{c_i} + r_i\right)^2 \\
&- \sum_{k\neq i, k\in\mathcal{N}}\left[\frac{1}{R_{ii}^i}R_{ik}^i u_k\left(\sum_{j\neq i, j\in\mathcal{N}} R_{ij}^i u_j^{c_i} + r_i\right)\right] - \frac{r_i}{R_{ii}^i}\left(\sum_{j\neq i, j\in\mathcal{N}} R_{ij}^i u_j^{c_i} + r_i\right) \\
=&\frac{1}{2}\sum_{j\neq i, j\in\mathcal{N}}\sum_{k\neq i, k\in\mathcal{N}}\frac{1}{R_{ii}^i}R_{ij}^i R_{ik}^i u_j^{c_i} u_k^{c_i} - \frac{1}{2R_{ii}^i}(r_i)^2 \\
&- \sum_{k\neq i, k\in\mathcal{N}}\left(\sum_{j\neq i, j\in\mathcal{N}} u_j^{c_i} R_{ij}^i\right)\frac{1}{R_{ii}^i}R_{ik}^i u_k - \sum_{k\neq i, k\in\mathcal{N}}\frac{1}{R_{ii}^i} r_i R_{ik}^i u_k.
\end{aligned}$$

Incorporating the cognition vector m^i into the real cost of player i further yields

$$\begin{aligned}
J^i(BR^i(u_{-i}^{c_i}), u_{-i}) &= \frac{1}{2}\sum_{j\neq i, j\in\mathcal{N}}\sum_{k\neq i, k\in\mathcal{N}} m_j^i \frac{1}{R_{ii}^i}R_{ij}^i R_{ik}^i m_k^i u_j u_k - \frac{1}{2R_{ii}^i}(r_i)^2 \\
&- \sum_{k\neq i, k\in\mathcal{N}}\sum_{j\neq i, j\in\mathcal{N}} m_j^i \frac{1}{R_{ii}^i}R_{ij}^i R_{ik}^i u_j u_k - \sum_{k\neq i, k\in\mathcal{N}}\frac{1}{R_{ii}^i} r_i R_{ik}^i u_k. \qquad (5.8)
\end{aligned}$$

Recall that each user aims to minimize the security risk based on the risks he perceives. Thus, by considering the real cost induced by the bounded rationality constraint, the strategic cognitive network formation problem of player i can be

formulated as

$$\begin{aligned} m^{i*} &= \arg \min_{m^i_j, j\neq i, j\in\mathcal{N}} J^i(BR^i(u^{c_i}_{-i}), u_{-i}) + \alpha_i \|m^i\|_1 \\ &= \arg \min_{m^i_j, j\neq i, j\in\mathcal{N}} \frac{1}{2} \sum_{j\neq i, j\in\mathcal{N}} \sum_{k\neq i, k\in\mathcal{N}} \frac{1}{R^i_{ii}} R^i_{ij} R^i_{ik} u_j u_k m^i_j m^i_k \\ &\quad - \sum_{j\neq i, j\in\mathcal{N}} \sum_{k\neq i, k\in\mathcal{N}} \frac{1}{R^i_{ii}} R^i_{ij} R^i_{ik} u_k u_j m^i_j + \alpha_i \|m^i\|_1 \\ &= \arg \min_{m^i_j, j\neq i, j\in\mathcal{N}} \frac{1}{2} m^{iT} \Lambda^i m^i - e^T_{N-1} \Lambda^i m^i + \alpha_i \|m^i\|_1, \end{aligned}$$

where $\Lambda^i := [\Lambda^i_{jk}]_{j\neq i, k\neq i, j\in\mathcal{N}, k\in\mathcal{N}}$, $\Lambda^i_{jk} = \frac{1}{R^i_{ii}} R^i_{ij} R^i_{ik} u_j u_k$, e_{N-1} is an $N-1$-dimensional column vector with all one entries, and α_i is a weighting factor capturing the unit cost of cognition of player i and it can be tuned to match with experimental data. The term $\|m^i\|_1$ is a convex relaxed version of $\|m^i\|_0$ which approximately maintains the sparse property of player i's cognitive network [13, 28]. The integrated term $\alpha_i \|m^i\|_1$ can be interpreted as the *cognitive cost* of user i.

Therefore, for player i, we need to solve the following constrained optimization problem:

$$\begin{aligned} &\min_{m^i_j, j\neq i, j\in\mathcal{N}} \frac{1}{2} m^{i\mathsf{T}} \Lambda^i m^i - e^{\mathsf{T}}_{N-1} \Lambda^i m^i + \alpha_i \|m^i\|_1 \\ &\quad \text{s.t.} \quad 0 \leq m^i_j \leq 1, j \neq i, j \in \mathcal{N}, \text{ (Risk perception)}, \end{aligned} \tag{5.9}$$

where 'T' denotes the transpose operator; and the constraints $m^i_j \in [0, 1]$, $\forall j \neq i$, indicate the risk perception behavior of user i.

The number of cognitive links that player i can form is generally a positive integer, i.e., $\|m^i\|_1 = \beta_i \in \mathbb{N}^+$. Note that β_i here and α_i in (5.9) have the same interpretation which both quantify the cognition ability of player i. Then,

by choosing α_i strategically, the problem in (5.9) is equivalent to the following problem:

$$\begin{aligned}\min_{m^i_j, j\neq i, j\in\mathcal{N}} \ & \frac{1}{2} m^{i\mathsf{T}} \Lambda^i m^i - e_{N-1}^{\mathsf{T}} \Lambda^i m^i \\ \text{s.t.} \ \ & 0 \leq m^i_j \leq 1, j \neq i, j \in \mathcal{N}, \ \text{(Risk perception)}, \\ & \|m^i\|_1 = \beta_i, \ \text{(Limited attention)}, \end{aligned} \tag{5.10}$$

where $\beta_i \in \mathbb{N}^+ \leq N-1$ is the total number of links that player i can form in his cognitive network, quantifying his limited attention. Simulation studies in Section 5.5 reflect that considering $\|m^i\|_1 = \beta_i$ yields sparser cognitive networks. Note that we still solve (5.9) by selecting a proper α_i which yields equivalent (5.9) and (5.10).

5.2.4 Gestalt Nash Equilibrium

The formulated security management under bounded rationality problem boasts a games-of-games structure. The users make decisions strategically in the IoT network as well as form their cognitive networks selfishly. The security management game and cognitive network formation game are interdependent. Therefore, the cognitive and IoT user layers shown in Fig. 5.1 constitute a network-of-networks framework. In this chapter, we aim to design an integrated algorithm to design the cognitive networks and determine the security risk management decisions of users in a holistic manner.

To this end, we present the solution concept, Gestalt Nash equilibrium, of the bounded rational security risk management game as follows.

Definition 5.3 (Gestalt Nash Equilibrium)**.** *The Gestalt Nash equilibrium (GNE) of the security risk management game under bounded rationality is a profile* (m^{i*}, u_i^*),

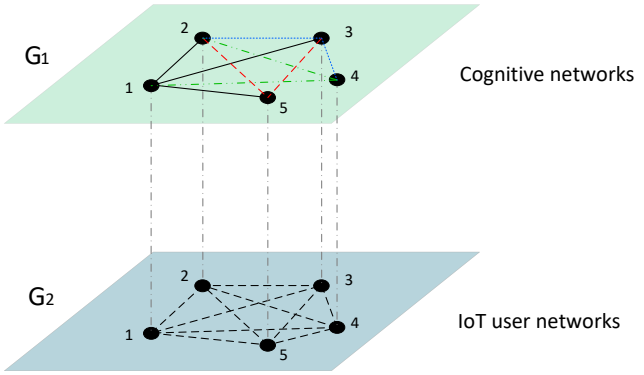


Figure 5.1: IoT user and cognitive network-of-networks. Users make strategic security management decisions in the IoT network as well as determine their cognitive networks. The security management game in layer G_2 and the cognitive network formation game in layer G_1 are interdependent which create a games-of-games framework.

$\forall i \in \mathcal{N}$, *that satisfies*

$$\tilde{J}^i(u_i^*, u_{-i}^*, m^{i*}) \leq \tilde{J}^i(u_i, u_{-i}^*, m^i),\ \forall u_i \in \mathcal{U}_i,\ \forall m^i \in [0,1]^{N-1}.$$

At the GNE, all the players in the network do not change their action u_i *and cognition vector* m^i, $\forall i \in \mathcal{N}$, *simultaneously.*

Remark: The strategic security management profile $u^* = [u_i^*]_{i\in\mathcal{N}}$ at GNE is also a BRNE.

In the following, we aim to analyze the GNE of the game and compute it by designing algorithms.

5.3 Problem Analysis

We first analyze the convergence of the bounded rational best-response dynamics of players in Section 5.2.2. Then, we quantify the risk of bounded perception due to

limited attention of players. We further reformulate the cognitive network formation problem presented in Section 5.2.3.

5.3.1 Bounded Rational Best Response Dynamics

Based on Section 5.2.2, the bounded rational best-response dynamics of player i under cognitive network m^i, $i \in \mathcal{N}$, can be written as

$$u_{i,k+1} = BR^i(u^{c_i}_{-i,k}) = \frac{1}{R^i_{ii}} \left(\sum_{j \neq i, j \in \mathcal{N}} R^i_{ij} u^{c_i}_{j,k} + r_i \right), \tag{5.11}$$

where $u^{c_i}_{j,k} = m^i_j u_{j,k}$ and k denotes the iteration index. Then, we obtain the following convergence result of security management strategy updates of users under given cognition networks.

Lemma 5.1. *Under Assumption 5.1, the sparse best-response dynamics (5.11) for all players converge to a unique BRNE.*

Proof. In the sparse cognition networks, $R^i_{ii} > \sum_{j \neq i, j \in \mathcal{N}} m^i_j R^i_{ij}$, $\forall i \in \mathcal{N}$, since $m^i_j \in [0, 1]$. Then, R^s defined in (5.6) is strictly diagonal dominant by rows, and u admits a unique solution. In addition, both Gauss-Seidel and Jacobi types of best-response dynamics (5.11) converges [122]. □

Note that Assumption 5.1 is a sufficient condition. In some cases, the best-response dynamics (5.11) may still converge when Assumption 5.1 does not hold. We focus on the scenarios under Assumption 5.1 which exhibit a natural security dependence interpretation.

5.3.2 Risk of Bounded Perception

When making security strategies in the IoT, the risk of bounded perception (RBP) of users due to irrationality/limited attention is defined as follows.

Definition 5.4 (RBP). *With the cognition vector m^i, the RBP of player i, $i \in \mathcal{N}$, is defined as*

$$L_i(m^i, u_{-i}) = J^i(BR^i(u_{-i}^{c_i}), u_{-i}) - J^i(BR^i(u_{-i}), u_{-i}), \tag{5.12}$$

where $L_i : \mathcal{M}_i \times \mathcal{U}_{-i} \to \mathbb{R}$.

Note that RBP is defined over the real-world cost functions (5.2), quantifying the security loss of the users due to limited attention. We further present the following lemma.

Lemma 5.2. *Under the bounded rational model, each user in the network has a degraded security level comparing with the one obtained from the model containing fully rational users. The RBP of player i, $i \in \mathcal{N}$, with bounded rationality is*

$$L_i(m^i, u_{-i}) = \frac{1}{2} \sum_{j \neq i, j \in \mathcal{N}} \sum_{k \neq i, k \in \mathcal{N}} (1 - m_j^i)(1 - m_k^i) \frac{1}{R_{ii}^i} R_{ji}^i R_{ik}^i u_j u_k.$$

Proof. Based on (5.8), we can compute the RBP of node i as

$$\begin{aligned}
&L_i(m^i, u_{-i}) = J^i(BR^i(u_{-i}^{c_i}), u_{-i}) - J^i(BR^i(u_{-i}), u_{-i}) \\
&= \frac{1}{2} \sum_{\substack{j \neq i \\ j \in \mathcal{N}}} \sum_{\substack{k \neq i \\ k \in \mathcal{N}}} \frac{m_j^i}{R_{ii}^i} R_{ji}^i R_{ik}^i m_k^i u_j u_k - \frac{1}{2} \sum_{\substack{k \neq i \\ k \in \mathcal{N}}} \sum_{\substack{j \neq i \\ j \in \mathcal{N}}} \frac{m_j^i}{R_{ii}^i} R_{ji}^i R_{ik}^i u_j u_k \\
&+ \frac{1}{2} \sum_{\substack{j \neq i \\ j \in \mathcal{N}}} \sum_{\substack{k \neq i \\ k \in \mathcal{N}}} \frac{1}{R_{ii}^i} R_{ji}^i R_{ik}^i u_j u_k - \frac{1}{2} \sum_{\substack{k \neq i \\ k \in \mathcal{N}}} \sum_{\substack{j \neq i \\ j \in \mathcal{N}}} \frac{m_j^i}{R_{ii}^i} R_{ji}^i R_{ik}^i u_j u_k.
\end{aligned}$$

Further, we can rewrite $\sum_{j\neq i,j\in\mathcal{N}}\sum_{k\neq i,k\in\mathcal{N}}\frac{1}{R^i_{ii}}R^i_{ji}R^i_{ik}u_ju_k=\sum_{j\neq i,j\in\mathcal{N}}\sum_{k\neq i,k\in\mathcal{N}}m^i_j$ $\frac{1}{R^i_{ii}}R^i_{ji}R^i_{ik}u_ju_k+\sum_{j\neq i,j\in\mathcal{N}}(1-m^i_j)\sum_{k\neq i,k\in\mathcal{N}}(1-m^i_k)\frac{1}{R^i_{ii}}R^i_{ji}R^i_{ik}u_ju_k+\sum_{j\neq i,j\in\mathcal{N}}(1-m^i_j)\sum_{k\neq i,k\in\mathcal{N}}m^i_k\frac{1}{R^i_{ii}}R^i_{ji}R^i_{ik}u_ju_k$. Therefore, we obtain

$$\begin{aligned}
L_i(m^i,u_{-i}) &= \frac{1}{2}\sum_{j\neq i,j\in\mathcal{N}}\sum_{k\neq i,k\in\mathcal{N}}m^i_j\frac{1}{R^i_{ii}}R^i_{ji}R^i_{ik}m^i_ku_ju_k\\
&+\frac{1}{2}\sum_{j\neq i,j\in\mathcal{N}}(1-m^i_j)\sum_{k\neq i,k\in\mathcal{N}}m^i_k\frac{1}{R^i_{ii}}R^i_{ji}R^i_{ik}u_ju_k\\
&-\frac{1}{2}\sum_{k\neq i,k\in\mathcal{N}}\sum_{j\neq i,j\in\mathcal{N}}m^i_j\frac{1}{R^i_{ii}}R^i_{ji}R^i_{ik}u_ju_k\\
&+\frac{1}{2}\sum_{j\neq i,j\in\mathcal{N}}(1-m^i_j)\sum_{k\neq i,k\in\mathcal{N}}(1-m^i_k)\frac{1}{R^i_{ii}}R^i_{ji}R^i_{ik}u_ju_k\\
&=\frac{1}{2}\sum_{j\neq i,j\in\mathcal{N}}\sum_{k\neq i,k\in\mathcal{N}}(1-m^i_j)(1-m^i_k)\frac{1}{R^i_{ii}}R^i_{ji}R^i_{ik}u_ju_k.
\end{aligned}$$

□

Remark: Note that the RBP of each player is nonnegative from Lemma 5.2, since the coefficients and security investments are nonnegative and the cognition variable admits a value between 0 and 1. Intuitively, if player i is able to perceive all the cyber risks in the network, i.e., $m^i_j=1,\ \forall j\neq i,\ j\in\mathcal{N}$, then the RBP is $L_i(m^i,u_{-i})=0$. In this scenario, the bounded rational model degenerates to the fully rational one. This indicates that, with more observations, the IoT users can design security management strategies better to lower their security risks. This fact also leads to the conclusion that more information (better cognitive ability) is beneficial for the users in our security management game. The result in Lemma 5.2 is further illustrated and corroborated through case studies in Section 5.5.

5.3.3 Problem Reformulation

We can rewrite the constrained optimization program (5.9) as

$$\min_{m_j^i, j\neq i, j\in\mathcal{N}} Q_i(m^i) := \frac{1}{2} m^{i\mathsf{T}} \Lambda^i m^i - e_{N-1}^{\mathsf{T}} \Lambda^i m^i + \alpha_i \|m^i\|_1 + \iota_C(m^i), \tag{5.13}$$

where $Q_i : [0,1]^{N-1} \to \mathbb{R} \cup \{+\infty\}$, $C := \{m^i | 0 \leq m_j^i \leq 1, j \neq i, j \in \mathcal{N}\}$, and ι_C is an indicator function, i.e.,

$$\iota_C(x) = \begin{cases} 0, & \text{if } x \in C, \\ +\infty, & \text{otherwise.} \end{cases} \tag{5.14}$$

For convenience, we decompose the function Q_i into three parts and define

$$\begin{aligned} f_1^i(m^i) &= \frac{1}{2} m^{i\mathsf{T}} \Lambda^i m^i - e_{N-1}^{\mathsf{T}} \Lambda^i m^i, \text{ (Security loss)}, \\ f_2^i(m^i) &= \alpha_i \|m^i\|_1, \text{ (Cognition cost)}, \\ f_3^i(m^i) &= \iota_C(m^i), \text{ (Feasible risk perception)}, \end{aligned} \tag{5.15}$$

where $f_1^i : \mathbb{R}^{N-1} \to \mathbb{R}$, $f_2^i : \mathbb{R}^{N-1} \to [0, +\infty)$ and $f_3^i : \mathbb{R}^{N-1} \to \{0, +\infty\}$. Specifically, for user $i \in \mathcal{N}$, f_1^i quantifies a modified security loss; f_2^i captures the cognition cost; and f_3^i ensures a feasible risk perception over the IoT.

The optimization problem (5.13) is quite challenging to solve. First, note that the convexity of f_1^i depends on the characteristics of matrix Λ^i. Specially, when Λ^i is positive definite, then f_1^i is convex in m^i. When Λ^i is not definite, then solving the quadratic program is an NP hard problem. Second, the l_1 norm-based function f_2^i and the indicator function f_3^i are nonsmooth and not differentiable, though they are convex. The traditional gradient-based optimization tools are not sufficient to

deal with this type of optimization problem in (5.13) [113]. To this end, we aim to design a proximal algorithm to solve this problem.

5.4 Algorithm for Computing GNE

In this section, our goal is to design an algorithm to solve problem (5.13). We further characterize the closed form solutions for a special case with homogeneous agents for comparison during case studies in Section 5.5. In addition, we present an integrated algorithm that computes the GNE of the bounded rational security management game.

5.4.1 Basics of Proximal Operator

To address (5.13), we leverage the tools from proximal operator theory. We first present the definition of proximal operator as follows.

Definition 5.5 (Proximal Operator [19]). *Let $g \in \Gamma_0$, where Γ_0 denotes the set of proper lower semicontinuous convex functions. The proximal mapping associated to g is defined as*

$$\text{prox}_{\lambda g}(x) = \arg\min_{l} \; g(l) + \frac{1}{2\lambda}\|l - x\|^2. \tag{5.16}$$

Note that the proximal mapping is unique, since the optimization problem in (5.16) is convex. Specifically, for function f_2^i in (5.15), we have

$$\left[\text{prox}_{\lambda f_2^i}(x)\right]_j = \begin{cases} x_j - \lambda\alpha_i, & x_j \geq \lambda\alpha_i, \\ 0, & |x_j| < \lambda\alpha_i, \\ x_j + \lambda\alpha_i, & x_j \leq -\lambda\alpha_i, \end{cases}$$

for $j \neq i,\ j \in \mathcal{N}$, which can be put in a compact form as [116]

$$\text{prox}_{\lambda f_2^i}(x) = (x - \lambda\alpha_i e_{N-1})_+ - (-x - \lambda\alpha_i e_{N-1})_+. \tag{5.17}$$

In addition, $\text{prox}_{\lambda f_3^i}(x) = \text{proj}_C(x),\ C = [0,1]^{N-1}$, which is equivalent to

$$\left[\text{prox}_{\lambda f_3^i}(x)\right]_j = [\text{proj}_C(x)]_j = \begin{cases} 1, & \text{if } x_j > 1, \\ x_j, & \text{if } 0 \leq x_j \leq 1, \\ 0, & \text{if } x_j < 0, \end{cases}$$

where "proj" denotes the *projection* operator.

The following lemma characterizes the aggregated proximal operator of functions f_2^i and f_3^i which is useful in designing the proximal algorithm.

Lemma 5.3. *Functions f_2^i and f_3^i defined in (5.15), $\forall i \in \mathcal{N}$, satisfy the property:* $\text{prox}_{\lambda(f_2^i + f_3^i)} = \text{proj}_C \circ \text{prox}_{\lambda f_2^i}$.

Proof. We proof for single dimensional case, i.e., $C = [0,1]$, and the analysis can be generalized for higher dimensional cases. By definition, we obtain $\text{prox}_{\lambda(f_2^i+f_3^i)}(x) = \arg\min_l\ f_2^i(l) + f_3^i(l) + \frac{1}{2\lambda}\|l - x\|^2 = \arg\min_{l\in C}\ f_2^i(l) + \frac{1}{2\lambda}\|l - x\|^2$. Let $l^* = \arg_l \left(\frac{\partial\left(f_2^i(l) + \frac{1}{2\lambda}\|l-x\|^2\right)}{\partial x} = 0\right) = \text{prox}_{\lambda f_2^i}(x)$. In addition, function $f_2^i(l) + \frac{1}{2\lambda}\|l - x\|^2$ is decreasing in $l < l^*$ and increasing in $l \geq l^*$. Remind that $C = [0,1]$ is a closed set. Hence, when $0 \leq l^* \leq 1$, $\text{prox}_{\lambda(f_2^i+f_3^i)}(x) = l^*$; when $l < l^*$, $\text{prox}_{\lambda(f_2^i+f_3^i)}(x) = 0$; and when $l > l^*$, $\text{prox}_{\lambda(f_2^i+f_3^i)}(x) = 1$. In all three cases, we obtain $\text{prox}_{\lambda(f_2^i+f_3^i)}(x) = \text{proj}_C(l^*) = \text{proj}_C(\text{prox}_{\lambda f_2^i}(x))$. □

Lemma 5.3 indicates that we can deal with the convex terms of cognitive cost and feasible risk perception jointly. The security loss term f_1^i is addressed in the

ensuing section.

5.4.2 Design of Proximal Algorithm

Recall that f_2^i and f_3^i, $\forall i \in \mathcal{N}$, are nonsmooth and not differentiable. To characterize the optimal cognition vector in f_2^i and f_3^i, we first present the definition of subdifferential of a function which can be nonconvex and nonsmooth as follows.

Definition 5.6 (Subdifferential [121]). *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a proper and lower semicontinuous function.*

1. *The domain of f is denoted by* $\text{dom } f := \{x \in \mathbb{R}^n : f(x) < +\infty\}$.

2. *For $x \in \text{dom } f$, the Fréchet subdifferential of f at x is the set of vectors $p \in \mathbb{R}^n$, denoted by $\hat{\partial} f(x)$, that satisfy*

$$\lim_{y \neq x, y \to x} \inf \frac{1}{\|y - x\|} \left[f(y) - f(x) - \langle p, y - x \rangle \right] \geq 0.$$

3. *The limiting-subdifferential (or subdifferential) of f at $x \in \text{dom } f$, denoted by $\partial f(x)$, is defined by*

$$\partial f(x) := \left\{ p \in \mathbb{R}^n : \exists x_n \to x, f(x_n) \to f(x),\ p_k \in \hat{\partial} f(x_n) \to p \right\}.$$

Remark: Based on the subifferential, a necessary condition for $x \in \mathbb{R}^n$ being a minimizer of f is

$$\partial f(x) \ni 0. \tag{5.18}$$

Note that the points satisfying (5.18) are called critical points of f. Our goal is to find a critical point $\bar{m}^i \in \text{dom } Q_i$ that can be characterized by the necessary FOC:

$0 \in \partial Q_i(\bar{m}^i)$.

Note that f_1^i is continuously differentialble with Lipschitz continuous gradient, i.e.,

$$\|\nabla f_1^i(x) - \nabla f_1^i(y)\| \leq L_i\|x-y\|,\ \forall x, y \in \mathbb{R}^{N-1},$$

where L_i is the Lipschitz constant of f_1^i. Specifically, $\nabla f_1^i(m^i) = \Lambda^i m^i - \Lambda^i e_{N-1}$, which further yields

$$\|\nabla f_1^i(x) - \nabla f_1^i(y)\| = \|\Lambda^i(x-y)\| \leq L_i\|x-y\|,\ \forall x, y \in \mathbb{R}^{N-1}. \tag{5.19}$$

The main steps in solving (5.13) for a general Λ^i of user i are designed as follows:

$$y_k^i = x_k^i + \frac{t_{k-1}^i}{t_k^i}(z_k^i - x_k^i) + \frac{t_{k-1}^i - 1}{t_k^i}(x_k^i - x_{k-1}^i), \tag{5.20}$$

$$z_{k+1}^i = \text{proj}_C\left(\text{prox}_{\lambda_y^i f_2^i}(y_k^i - \lambda_y^i \nabla f_1^i(y_k^i))\right), \tag{5.21}$$

$$v_{k+1}^i = \text{proj}_C\left(\text{prox}_{\lambda_x^i f_2^i}(x_k^i - \lambda_x^i \nabla f_1^i(x_k^i))\right), \tag{5.22}$$

$$t_{k+1}^i = \left(1 + \sqrt{4(t_k^i)^2 + 1}\right)/2, \tag{5.23}$$

$$x_{k+1}^i = \begin{cases} z_{k+1}^i, & \text{if } Q_i(z_{k+1}^i) \leq Q_i(v_{k+1}^i), \\ v_{k+1}^i, & \text{Otherwise}, \end{cases} \tag{5.24}$$

where the step constants λ_x^i and λ_y^i satisfy $0 < \lambda_x^i < 1/L_i$ and $0 < \lambda_y^i < 1/L_i$, respectively. If the algorithm converges, the values of x_k^i, y_k^i, z_k^i and v_k^i are the same which give the optimal cognition vector m^i.

Remark: Note that (5.22) serves as a monitor of the update in (5.21). Together with the condition in (5.24), each player updates their cognitive network when there is a sufficient decrease of the security management cost.

Before presenting the convergence results of the algorithm (5.20)-(5.24), we first characterize a critical property of function $Q_i(m^i)$ defined in (5.13).

Definition 5.7 (Kurdyka-Łojasiewicz (KL) Property [6]). *A function $f : \mathbb{R}^n \to (-\infty, +\infty]$ has the KL property at $x^* \in \text{dom } \partial f := \{x \in \mathbb{R}^n : \partial f(x) \neq \emptyset\}$ if there exists $\eta \in (0, +\infty]$, a neighborhood U of x^*, and a desingularising function $\phi \in \Phi_\eta$, such that $\forall x \in U \cap \{x \in \mathbb{R}^n : f(x^*) < f(x) < f(x^*) + \eta\}$, the following KL inequality holds,*

$$\phi'(f(x) - f(x^*))\text{dist}(0, \partial f(x)) \geq 1, \tag{5.25}$$

where Φ_η includes a class of function $\phi : [0, \eta) \to \mathbb{R}^+$ satisfying: (1) ϕ is concave and $\phi \in C^1((0, \eta))$; (2) ϕ is continuous at 0 with $\phi(0) = 0$; and (3) $\phi'(x) > 0$, $\forall x \in (0, \eta)$. In addition, $\text{dist}(0, \partial f(x)) := \inf \{\|z\| : z \in \partial f(x)\}$.

Note that a proper lower semicontinuous function f having the KL property at each point of dom ∂f is called a *KL function*. KL inequality (5.25) ensures that, by choosing a proper desingularising function ϕ, we can reparameterize the values of function f near its critical points to avoid flatness. Thus, ϕ has an impact on the convergence rate of the designed algorithm which will be presented in Theorem 5.1. KL property is general in functions. Notably, the semi-algebraic functions satisfy the KL property [6]. Some examples include real polynomial functions, indicator functions of semi-algebraic sets and $\|\cdot\|_p$ with $p \geq 0$. Furthermore, the semi-algebraic property preserves under composition, finite sums and products of semi-algebraic functions [23].

Lemma 5.4. *Functions f_1^i, f_2^i and f_3^i in (5.15) satisfy the KL property, and thus Q_i in (5.13) is a KL function. In addition, the desingularising function $\phi(u)$ can be chosen as $\phi(u) = \frac{\kappa}{\theta} u^\theta$ for some $\theta \in (0, \frac{1}{2}]$ and $\kappa > 0$.*

Proof. We know that f_1^i, f_2^i and f_3^i are semi-algebraic functions, and thus Q_i satisfies the KL property [6]. Remind that when $m^i \notin C := \{m^i | 0 \leq m_j^i \leq 1, j \neq i, j \in \mathcal{N}\}$, $Q_i(m^i) \to +\infty$. Based on Definition 5.6, we obtain dom $\partial Q_i = C$. Therefore, $Q_i(m^i)$ is analytic over dom ∂Q_i. In addition, the desingularising function of real-analytical functions satisfying inequality (5.25) can be chosen as $\phi(u) = u^{1-\delta}$, where $\delta \in [\frac{1}{2}, 1)$ [23]. □

Based on Lemma 5.4, we present the convergence result of the designed algorithm (5.20)-(5.24) in Theorem 5.1.

Theorem 5.1. *The algorithm given by* (5.20)-(5.24) *converges to a critical point with rates related to the parameters* κ *and* θ*, where* κ *and* θ *are defined in Lemma 5.4. Specifically, there exists a* k_0 *such that* $\forall k > k_0$*,*

$$Q_i(x_k) - Q_i^* \leq \left(\frac{\kappa}{(k - k_0)(1 - 2\theta) d_2} \right)^{\frac{1}{1-2\theta}},$$

where Q_i^* *is the function value achieved at critical points of* $\{x_k\}$*,* $d_2 = \min\{\frac{1}{2d_1\kappa}, \sigma(Q_i(v_0) - Q_i^*)^{2\theta-1}\}$*,* $d_1 = 2\alpha(\frac{1}{\lambda_x} + L)^2/(1 - 2\alpha)$*, and* $\sigma = \frac{\kappa}{1-2\theta}\left(2^{\frac{2\theta-1}{2\theta-2}} - 1\right)$.

Proof. The main idea of the proof follows [60] with several differences. Especially the imposed conditions for showing convergence in [60] are different. In addition, our algorithm contains projections and an auxiliary parameter v_{k+1} during updates. First, based on Definition 5.5, $v_{k+1} = \text{proj}_C\left(\text{prox}_{\lambda_x f_2^i}(x_k - \lambda_x \nabla f_1^i(x_k))\right) = \arg\min_{x \in C} \langle \nabla f_1^i(x_k), x - x_k \rangle + \frac{1}{2\lambda_x}\|x - x_k\|^2 + f_2^i(x)$. Then, $\langle \nabla f_1^i(x_k), v_{k+1} - x_k \rangle + \frac{1}{2\lambda_x}\|v_{k+1} - x_k\|^2 + f_2^i(v_{k+1}) \leq f_2^i(x_k)$. Based on the Lipschitz continuous condition

of f_1^i, we obtain

$$\begin{aligned} Q_i(v_{k+1}) &\leq f_2^i(v_{k+1}) + f_1^i(x_k) + f_3^i(x_k) + \langle \nabla f_1^i(x_k), v_{k+1} - x_k \rangle + \frac{L_i}{2}\|v_{k+1} - x_k\|^2 \\ &\leq f_2^i(x_k) - \langle \nabla f_1^i(x_k), v_{k+1} - x_k \rangle - \frac{1}{2\lambda_x}\|v_{k+1} - x_k\|^2 \\ &+ f_1^i(x_k) + f_3^i(x_k) + \langle \nabla f_1^i(x_k), v_{k+1} - x_k \rangle + \frac{L_i}{2}\|v_{k+1} - x_k\|^2 \\ &= Q(x_k) - \left(\frac{1}{2\lambda_x} - \frac{L_i}{2}\right)\|v_{k+1} - x_k\|^2. \end{aligned} \tag{5.26}$$

When $Q_i(z_{k+1}) \leq Q_i(v_{k+1})$, $x_{k+1} = z_{k+1}$, $Q_i(x_{k+1}) = Q_i(z_{k+1}) \leq Q_i(v_{k+1})$, and when $Q_i(z_{k+1}) > Q_i(v_{k+1})$, $x_{k+1} = v_{k+1}$, $Q_i(x_{k+1}) = Q_i(z_{k+1})$. Hence,

$$Q_i(x_{k+1}) \leq Q_i(v_{k+1}) \leq Q_i(x_k). \tag{5.27}$$

Based on (5.26) and (5.27),

$$Q_i(v_{k+1}) \leq Q_i(v_k) - \left(\frac{1}{2\lambda_x} - \frac{L_i}{2}\right)\|v_{k+1} - x_k\|^2. \tag{5.28}$$

In addition,

$$\mathrm{dist}(0, \partial \mathrm{Q_i}(\mathrm{v_{k+1}})) \leq \left(\frac{1}{\lambda_x} + L_i\right)\|v_{k+1} - x_k\|. \tag{5.29}$$

Furthermore, $\{x_k\}$ and $\{v_k\}$ have the same accumulation points. Let Ψ be the set containing all the accumulation points of $\{x_k\}$. Note that Q_i admits the same value Q_i^* at all accumulation points in Ψ due to the non-increasing $Q_i(v_k)$. Then, $Q_i(v_k) \geq Q_i^*$ and $Q_i(v_k) \to Q_i^*$. If there exists an n such that $Q_i(v_n) = Q_i^*$, the algorithm converges. If $Q_i(v_k) \geq Q_i^*$, $\forall k$, then there exists a $\tilde{k}_1$ such that $Q_i(v_k) < Q_i^* + \eta$ for $k > \tilde{k}_1$. Since $\mathrm{dist}(v_k, \Psi) \to 0$, there exists a $\tilde{k}_2$ such that

$\text{dist}(v_k, \Psi) < \epsilon$ for $k > \tilde{k}_2$. Thus, when $k > k_0 = \max\{\tilde{k}_1, \tilde{k}_2\}$, $v_k \in \{v, \text{dist}(v_k, \Psi) < \epsilon\} \cap \{Q_i^* < Q_i(v) < Q_i^* + \eta\}$. Based on the KL property in Definition 5.7, there exists a concave function ϕ such that

$$\phi'(Q_i(v_k) - Q_i^*)\text{dist}(0, \partial Q_i(v_k)) \geq 1. \tag{5.30}$$

Define $r_k := Q_i(v_k) - Q_i^*$, and we further assume that $r_k > 0,\ \forall k$. Otherwise, the algorithm converges in finite steps by definition. Then, $\forall k > k_0$,

$$\begin{aligned} 1 &\leq \phi'(Q_i(v_k) - Q_i^*)\text{dist}(0, \partial Q_i(v_k)) \leq \left(\phi'(r_k)\left(\frac{1}{\lambda_x} + L_i\right)\|v_k - x_{k-1}\|\right)^2 \\ &\leq (\phi'(r_k))^2\left(\frac{1}{\lambda_x} + L_i\right)^2 \frac{Q_i(v_{k-1}) - Q_i(v_k)}{\frac{1}{2\lambda_x} - \frac{L_i}{2}} = d_1(\phi'(r_k))^2(r_{k-1} - r_k), \end{aligned} \tag{5.31}$$

where $d_1 = 2\alpha(\frac{1}{\lambda_x} + L)^2/(1 - 2\alpha)$. Besides, ϕ admits the form $\phi(u) = \frac{\kappa}{\theta}u^\theta$. Then, (5.31) can be rewritten as

$$1 \leq d_1\kappa^2 r_k^{2(\theta-1)}(r_{k-1} - r_k). \tag{5.32}$$

Lemma 5.4 indicates that $0 < \theta \leq \frac{1}{2}$, then, we have $-1 \leq \theta - 1 < -\frac{1}{2}$ and $-1 < 2\theta - 1 < 0$. When $r_{k-1} > r_k$, we obtain $r_{k-1}^{2(\theta-1)} < r_k^{2(\theta-1)}$ and $r_0^{2\theta-1} < r_1^{2\theta-1} < \ldots < r_k^{2\theta-1}$. In addition, define $\zeta(u) = \frac{\kappa}{1-2\theta}u^{2\theta-1}$, and then $\zeta'(u) = -\kappa u^{2\theta-2}$. When $r_k^{2(\theta-1)} \leq 2r_{k-1}^{2(\theta-1)}$, then $\forall k > k_0$, $\zeta(r_k) - \zeta(r_{k-1}) = \kappa\int_{r_k}^{r_k} u^{2(\theta-1)}du \geq \kappa r_{k-1}^{2(\theta-1)}(r_{k-1} - r_k) \geq \frac{1}{2}\kappa r_{k-1}^{2(\theta-1)}(r_{k-1} - r_k) \geq \frac{1}{2\kappa d_1}$. When $r_k^{2(\theta-1)} > 2r_{k-1}^{2(\theta-1)}$, then $r_k^{2\theta-1} > 2^{\frac{2\theta-1}{2(\theta-1)}}r_{k-1}^{2\theta-1}$, and $\zeta(r_k) - \zeta(r_{k-1}) = \frac{\kappa}{1-2\theta}(r_k^{2\theta-1} - r_{k-1}^{2\theta-1}) > \frac{\kappa}{1-2\theta}(2^{\frac{2\theta-1}{2(\theta-1)}} - 1)r_{k-1}^{2\theta-1} > \frac{\kappa}{1-2\theta}(2^{\frac{2\theta-1}{2(\theta-1)}} - 1)r_0^{2\theta-1}$. Let $\sigma = \frac{\kappa}{1-2\theta}(2^{\frac{2\theta-1}{2(\theta-1)}} - 1)$ and $d_2 = \min\{\frac{1}{2\kappa d_1}, \sigma r_0^{2\theta-1}\}$, then $\forall k > k_0$, $\zeta(r_k) - \zeta(r_{k-1}) \geq d_2$, and $\zeta(r_k) \geq \zeta(r_k) - \zeta(r_{k_0}) \geq \sum_{t=k_0+1}^{k}\zeta(r_t) - \zeta(r_{t-1}) \geq (k - k_0)d_2$. Hence, $r_k^{2\theta-1} \geq \frac{d_2}{\kappa}(k - k_0)(1 - 2\theta)$, leading to $r_k \leq \frac{\kappa}{d_2(k-k_0)(1-2\theta)}^{\frac{1}{1-2\theta}}$.

Therefore, we obtain $Q_i(x_k) - Q_i^* \leq Q_i(v_k) - Q_i^* = r_k = \left(\frac{\kappa}{d_2(k-k_0)(1-2\theta)}\right)^{\frac{1}{1-2\theta}}$. □

For a special case where f_1^i is convex, the following simplified steps (5.33)-(5.36) can be adopted to accelerate the computation. The monitoring update step v_{k+1} is omited due to the convexity of f_1^i. This algorithm is slightly different with the one in [20] in terms of the projection step. Since Q_i is convex, then algorithm (5.33)-(5.36) converges to a unique optimal solution.

$$y_k^i = x_k^i + \frac{t_{k-1}^i}{t_k^i}(z_k^i - x_k^i) + \frac{t_{k-1}^i - 1}{t_k^i}(x_k^i - x_{k-1}^i), \tag{5.33}$$

$$z_{k+1}^i = \text{proj}_C\left(\text{prox}_{\lambda_y^i f_2^i}(y_k^i - \lambda_y^i \nabla f_1^i(y_k^i))\right), \tag{5.34}$$

$$t_{k+1}^i = \left(1 + \sqrt{4(t_k^i)^2 + 1}\right)/2, \tag{5.35}$$

$$x_{k+1}^i = \begin{cases} z_{k+1}^i, & \text{if } Q_i(z_{k+1}^i) \leq Q_i(x_k^i), \\ x_k^i, & \text{Otherwise.} \end{cases} \tag{5.36}$$

Similar to (5.20)-(5.24), when the algorithm (5.33)-(5.36) converges, the values of x_k^i, y_k^i and z_k^i are the same which give the optimal cognition vector m^i.

Homogeneous Users Case: When the agents in the IoT network are homogeneous, i.e., $R_{ii}^i = R_{jj}^j$, $R_{ij}^i = R_{ji}^j$, $r_i = r_j = r$, $\beta_i = \beta_j = \beta \leq N-1$, $\forall i, j \in \mathcal{N}$, we can characterize the closed form solutions of decisions u_i and m^i, $\forall i \in \mathcal{N}$. Specifically, we obtain, $\forall i \in \mathcal{N}$,

$$\begin{aligned} m_j^{i*} &= \frac{\beta}{N-1}, \ \forall j \neq i, j \in \mathcal{N}, \\ u_i^* &= \frac{r}{R_1 - \beta R_2}, \end{aligned} \tag{5.37}$$

where $R_1 = R_{ii}^i$ and $R_2 = R_{jk}^i$ for $j \neq i$ and $k \neq i$. The results indicate that, at

Algorithm 5.1 Cognitive Network Formation for Player i

1. Input f_1^i, f_2^i and $C = [0,1]^{N-1}$
2. Initialize parameters z_0^i, x_0^i, x_1^i, t_0^i, t_1^i, λ_x^i and λ_y^i
3. **for** $k = 1, 2, ...$ **do**
4. **if** f_1^i is convex
5. Update y_k^i, z_{k+1}^i, v_{k+1}^i, t_{k+1}^i and x_{k+1}^i through (5.33)-(5.36)
6. **else**
7. Update y_k^i, z_{k+1}^i, v_{k+1}^i, t_{k+1}^i and x_{k+1}^i through (5.20)-(5.24)
8. **end**
9. **end for**
10. **Return** $m^i = x_k^i$

GNE, the cognitive network that each user i forms, $i \in \mathcal{N}$, is symmetric, i.e., the allocated attention to other users $j \neq i$ by user i is the same. In addition, with a larger β, the users spend more effort on the security management at GNE. This can be interpreted as follows: with a better perception of cyber risks in the IoT, the users becomes better informed of the risks and make best effort to reduce the security loss.

5.4.3 Integrated Algorithm and Discussions

For clarity, we summarize the combined algorithm including the strategic security decision-makings of players in the IoT networks and their corresponding cognitive network formations together in Algorithm 5.2. The integrated algorithm exhibits an alternating pattern between the best-response of security management and the strategic cognitive network formation of IoT users.

Algorithm 5.2 Strategic Risk Management with Bounded Rationality

1. Initialize parameters in the game $\mathcal{G}$, cognition cost α_i, cognitive networks $m^i,\ \forall i \in \mathcal{N}$
2. **Do**
   Best response dynamics:
3. Based on m^i, $i \in \mathcal{N}$, player i determines their best-response strategy through (5.11) iteratively until reaching a BRNE
   Cognitive network formation:
4. Each player i, $i \in \mathcal{N}$, forms their cognitive network m^i through Algorithm 5.1
5. **Until** $[m^i]_{i\in\mathcal{N}}$ and $[u_i]_{i\in\mathcal{N}}$ converge
6. **Return** m^i and u_i, $\forall i \in \mathcal{N}$, which form a GNE

We next discuss some observations obtained from the algorithm. The steps z^i_{k+1} and v^i_{k+1} in (5.21) and (5.22) of the algorithm can be simplified further. Here, we only analyze z^i_{k+1}, and the procedure follows for v^i_{k+1}. First, we have $\nabla f^i_1(y^i_k) = \Lambda^i(y^i_k - e_{N-1})$. Then, $[y^i_k - \lambda^i_y \nabla f^i_1(y^i_k)]_j = [y^i_k - \lambda^i_y \Lambda^i(y^i_k - e_{N-1})]_j \geq 0$, $\forall j \neq i, j \in \mathcal{N}$. Thus, based on (5.17), we obtain

$$\begin{aligned} z^i_{k+1} &= \text{proj}_C \left(y^i_k - \lambda^i_y \Lambda^i (y^i_k - e_{N-1}) - \lambda^i_y \alpha_i e_{N-1} \right) \\ &= \text{proj}_C \left(y^i_k + \lambda^i_y (\Lambda^i (e_{N-1} - y^i_k) - \alpha_i e_{N-1}) \right). \end{aligned}$$

The update of player i's attention on player j at step $k+1$, $j \neq i$, can be expressed as

$$[z^i_{k+1}]_j = \text{proj}_{[0,1]} \left([y^i_k]_j + \lambda^i_y \left(\frac{R^i_{ij}}{R^i_{ii}} u_j \sum_{p\neq i, p\in\mathcal{N}} R^i_{ip} u_p \left(1 - [y^i_k]_p\right) - \alpha_i \right) \right).$$

When $\frac{R_{ij}^i}{R_{ii}^i} u_j \sum_{p\neq i, p\in\mathcal{N}} R_{ip}^i u_p \left(1 - [y_k^i]_p\right) \geq \alpha_i$ which is equivalent to $\sum_{p\neq i, p\in\mathcal{N}} R_{ip}^i u_p [y_k^i]_p \leq \sum_{p\neq i, p\in\mathcal{N}} R_{ip}^i u_p - \frac{R_{ii}^i}{R_{ij}^i u_j}\alpha_i$, we know that $[z_{k+1}^i]_j \geq [z_k^i]_j$. The player i's attention on player j increases at step $k+1$, since there remains extra cognition resources to be allocated which corresponds to a phenomenon called *filling the inattention*. In addition, a smaller cognition cost α_i yields a larger upper bound for $\sum_{p\neq i, p\in\mathcal{N}} R_{ip}^i u_p [y_k^i]_p$, and hence player i can pay more attention to other players which again leads to the observation of filling the inattention.

In the IoT network, user j's decision has an impact on the strategy of user i. To illustrate the discovery, we consider two groups of IoT users, and one group of users have more incentive to secure the devices, i.e., their security investment is larger. Then, from user i's perspective, his attention on user j is influenced by the term $R_{ii}^i/(R_{ij}^i u_j)$. When user j lies in the group of a higher investment u_j, then the upper bound $\sum_{p\neq i, p\in\mathcal{N}} R_{ip}^i u_p - \frac{R_{ii}^i}{R_{ij}^i u_j}\alpha_i$ is larger. Therefore, each IoT user will allocate more cognition resources to the users in the group with a higher security standard which exposes the phenomenon of *emergence of partisanship*.

In a heterogeneous IoT network, the system parameters R_{ij}^i, R_{ii}^i, and decisions u_i are generally different. Then, for player $i \in \mathcal{N}$, the term $\frac{R_{ij}^i}{R_{ii}^i} u_j \sum_{p\neq i, p\in\mathcal{N}} R_{ip}^i u_p$, $j \neq i,\ j \in \mathcal{N}$, identifies the most influential agents in the network. Moreover, the critical agents to pay attention to for each user almost overlap, resulting the phenomenon of *attraction of the mighty* during the cognitive network formation.

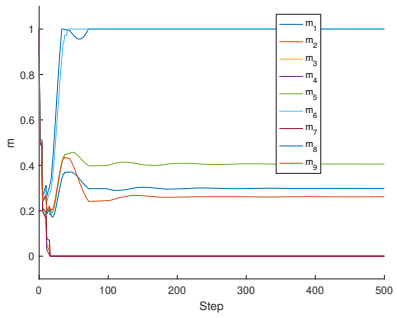
We illustrate the discovered phenomena in Section 5.5.

5.5 Case Studies

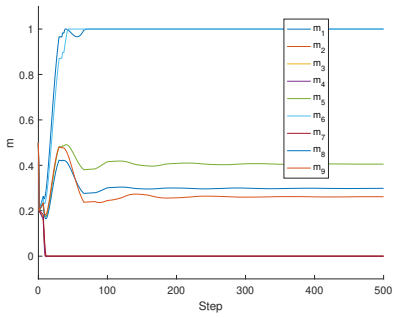
We use case studies of IoT-enabled smart communities shown in Fig. 1.4 to corroborate the designed algorithms and illustrate the security management of bounded rational agents in this section.

5.5.1 Effectiveness of Algorithm 5.1

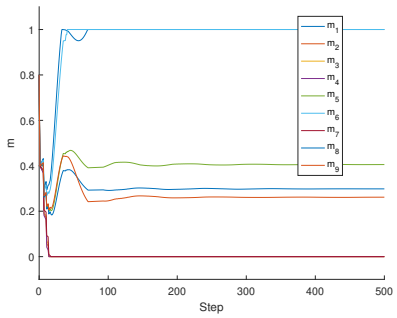
First, we verify the effectiveness of Algorithm 5.1. Specifically, we choose $N = 10$, $\alpha = 100$ and generate a 9×9 random matrix which is not definite for Λ^i. Thus, f_2^i in (5.15) is not convex. The iterative updates through the designed proximal algorithm are presented in Fig. 5.2 which reveal fast convergence to the steady state. In addition, the algorithm yields a sparse cognition vector $m = [1, 0, 0, 0, 0.41, 1, 0, 0.30, 0.26]$. To investigate the robustness of the algorithm, we study the same network as in Fig. 5.2(a) with different initial conditions. The results are shown in Figs. 5.2(b) and 5.2(c). We can verify that the steady states in Figs. 5.2(b) and 5.2(c) are the same as the ones in Fig. 5.2(a) which corroborate the robustness of the algorithm to initial conditions. To further verify the algorithm, we also investigate the network containing different numbers of agents. The results with 7 and 15 agents are presented in Figs. 5.2(d) and 5.2(e). Both results indicate that the designed algorithm is reliable in computing the sparse steady strategy. After conducting sufficient number of case studies, we conclude that the algorithm is effective with probability 1 under arbitrary number of agents.



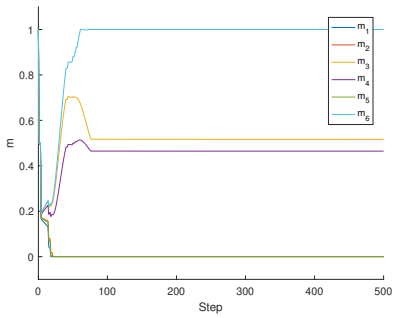
(a) $N = 10$, case 1



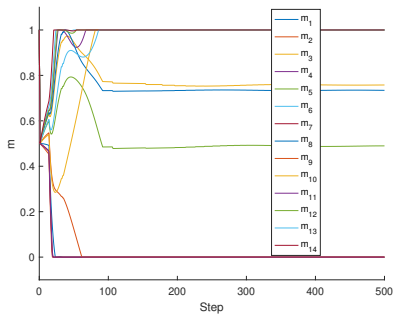
(b) $N = 10$, case 2



(c) $N = 10$, case 3



(d) $N = 7$



(e) $N = 15$

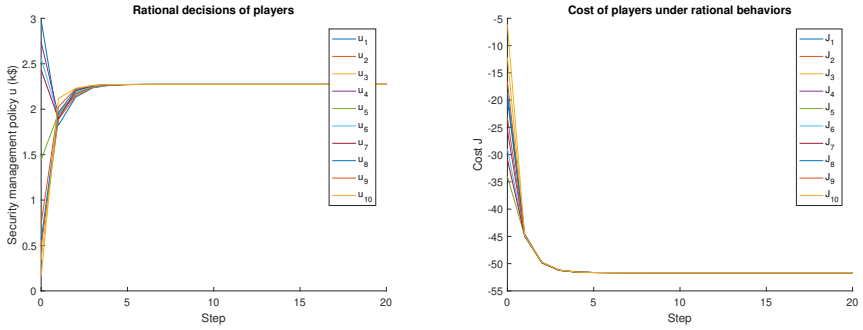
Figure 5.2: Performance of Algorithm 5.1 on a nonconvex f_2^i in (5.15). (a), (d), and (e) show the results with 10, 7 and 15 agents in the network, respectively. The network configurations in (a), (b), and (c) are the same, but their initial conditions are different. The algorithm yields the same result for cases in (a), (b), and (c) which shows the robustness of the algorithm.

5.5.2 Homogeneous Smart Homes

In this case study, we consider $N = 10$ homogeneous households in the smart community, i.e., all the parameters are the same for each agent. Specifically, the parameters are chosen as follows: $R^i_{jk} = 20$ unit/k\$^{2} if $j = k = i$, otherwise $R^i_{jk} = 1$ unit/k\$^{2}, $\forall i$; $r_i = 25$ unit/k\$, $\forall i \in \mathcal{N}$ and $\alpha^i = \alpha$, $\forall i$, is chosen to satisfy $\beta = \|m^i\|_1 = 3$. The selected parameters indicate that the security level of a household is mainly determined by its own security management policy rather than the ones of connected households. Recall that we have obtained the analytical solutions for homogeneous case in (5.37) which yield $m^i_j = \frac{1}{3},\ \forall j \neq i, j \in \mathcal{N}$ and $u_i = \frac{25}{17} = 1.47$k\$. Thus, each agent allocates attention resource equally to their connected neighbors. Fig. 5.3 presents the results by using Algorithm 5.2, where the step index represents an iteration between two components of cognitive network formation and security investment. We can conclude that the rational decision yields less cost for players compared with their irrational decision counterparts due to the bounded rationality. Furthermore, the algorithm gives the same cognitive network structure as the one obtained from the analytical results which corroborates the proposed integrated algorithm.

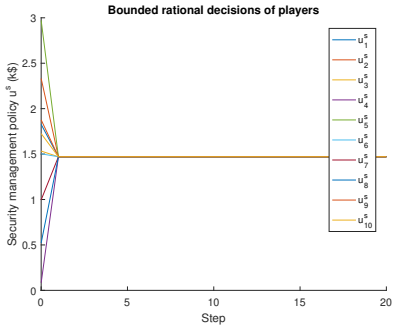
5.5.3 Emergence of Partisanship

We next investigate a smart community including two groups of agents denoted by $G1$ and $G2$, respectively. Specifically, $G1$ includes 5 agents, $G1 = \{1, ..., 5\}$, and $G2$ contains 10 agents, $G2 = \{6, ..., 15\}$. The parameters are the same as those in Section 5.5.2 except that for agents in $G1$, $r_i = 40$ unit/k\$, $\forall i \in G1$, to distinguish two groups of users. Thus, the agents in $G1$ have more incentives to secure their

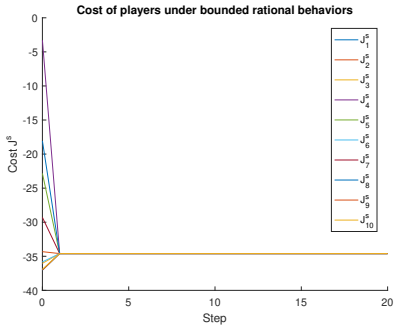


(a) rational strategy

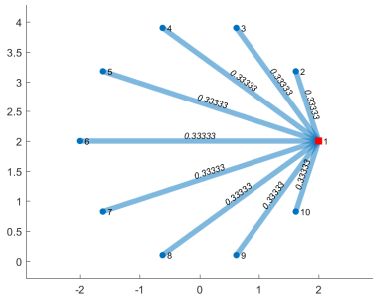
(b) cost under rational strategy



(c) bounded rational strategy



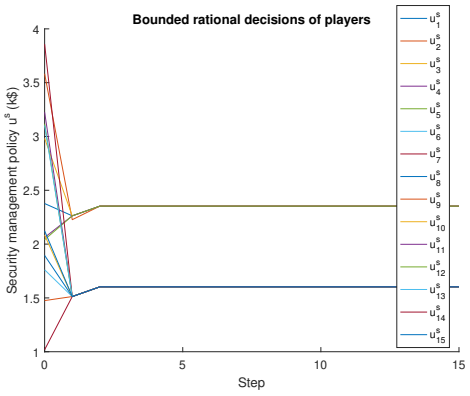
(d) cost under bounded rational strategy



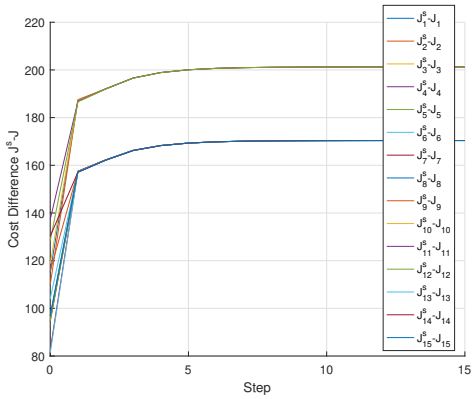
(e) cognitive network

Figure 5.3: (a) and (b) are the rational decision of players and the corresponding cost, respectively. (c) and (d) are the counterparts of (a) and (b) with bounded rationality. (e) illustrates the formed cognitive networks which is symmetric in this homogeneous case.

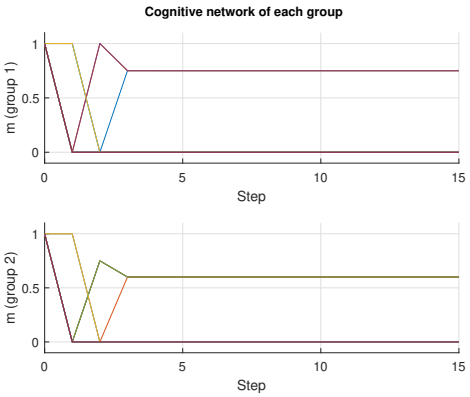
IoT products than those in $G2$. Fig. 5.4 shows the results. For agents in $G1$, the cognitive network is characterized by $m^i = [0.75, ..., 0.75, 0, ..., 0]$, $i \in G1$, and for



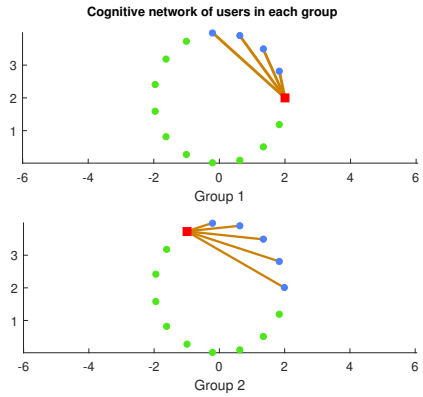
(a) bounded rational strategy



(b) RBP



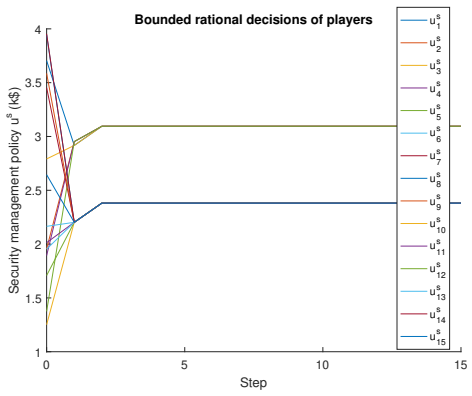
(c) cognition vector m



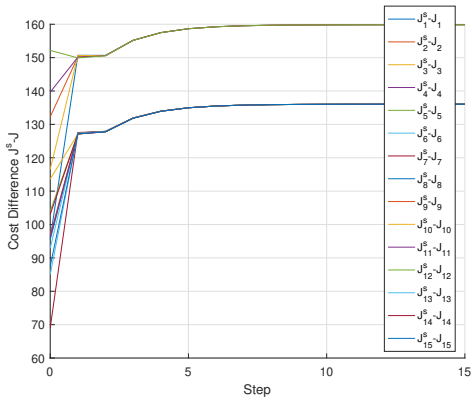
(d) cognitive network

Figure 5.4: (a) shows the bounded rational strategy of players, indicating that players in $G1$ have a lower cost. (b) depicts the RBP which corroborates that the security risk of users increases under the bounded rational model comparing with the fully rational one. (c) and (d) illustrate the formed sparse cognitive networks. In (d), blue and green dots are agents in $G1$ and $G2$, respectively, and the red ones are representatives in each group. In the network, all agents only allocate cognition resource to smart homes in $G1$ at GNE, leading to the emergence of partisanship.

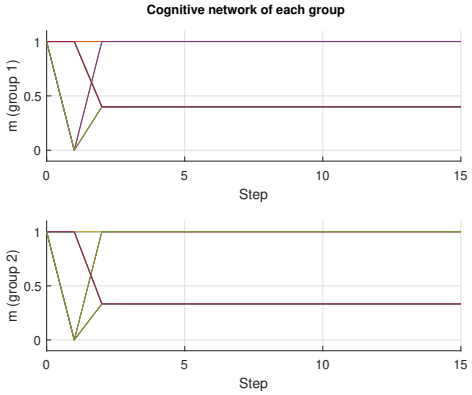
agents in $G2$, $m^j = [0.6, ..., 0.6, 0, ..., 0]$, $j \in G2$. Therefore, with limited cognition, all agents only pay attention to the security decisions made by smart homes in $G1$ which yields the phenomenon of partisanship. We also verify that the RBP increases due to the bounded rationality.



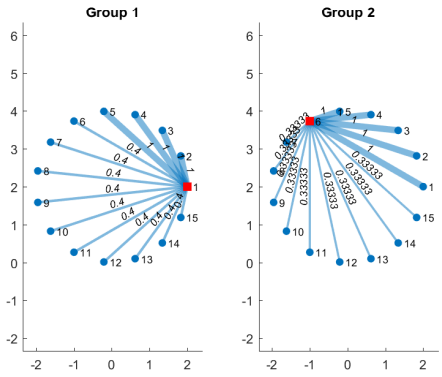
(a) bounded rational strategy



(b) RBP



(c) cognition vector m



(d) cognitive network

Figure 5.5: (a) shows the bounded rational decisions, and (b) presents the RBP which is positive. (c) and (d) illustrate the formed cognitive networks. This case study indicates that players in $G1$ are more critical that those in $G2$ in the cognitive networks. In addition, cognition resource is further allocated to the users in $G2$ which reveals the phenomenon of filling the inattention.

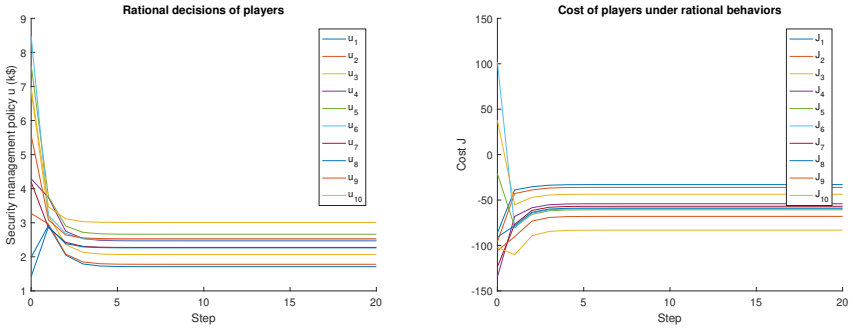
5.5.4 Filling the Inattention

Under the setting of Section 5.5.3, we further assume that the agents have better cognitive ability and can perceive more cyber risks in the smart community in a way that $\beta = \|m^i\|_1 = 8$. Other parameters are the same as those in Section 5.5.3. Fig. 5.5 presents the results. Specifically, we obtain $m^i = [1, ..., 1, 0.4, ..., 0.4]$

for $i \in G1$ and $m^j = [1, ..., 1, 0.33, ..., 0.33]$ for $j \in G2$, which show that the agents in $G1$ play a critical role in the security risk management of smart community. Furthermore, with more cognition resource, the agents in $G2$ that are not paid attention to previously in Section 5.5.3 are considered by other households. This phenomenon is termed as filling the inattention.

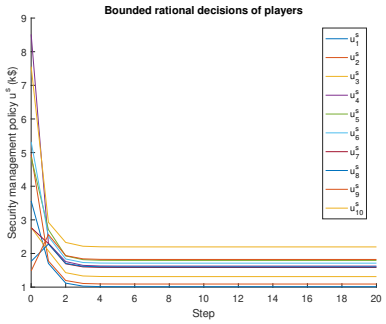
5.5.5 Attraction of the Mighty

The critical agents in the IoT-enabled smart community are those households whose security management policies will be taken into account by the other agents during their decision makings. Specifically, the nodes who often appear in the cognitive networks of other nodes can be regarded as critical agents. In the following case study, we aim to identify the critical agents in a smart community with $N = 10$ households using Algorithm 5.2. To model the heterogeneity of smart homes, we choose $R^i_{jk} = 3\sin(i) + 20$ unit/k\$^{2} for $j = k = i$. Otherwise, $R^i_{jk} = 1$ unit/k\$^{2}, $\forall i$; $r_i = 15 + 2i$ unit/k\$ for $i \in \mathcal{N}$; and other parameters are the same as those in Section 5.5.2. The results are shown in Fig. 5.6. Specifically, Fig. 5.6(e) shows the established cognitive network of each player. For example, during the cognitive network formation, player 1 chooses to observe the strategies of players 5, 9, and 10 in the network, and player 5's cognitive network includes players 6, 9, and 10. Furthermore, agents 5, 9 and 10 present in all agents' cognitive networks, and hence they constitute a critical community in this smart home network. In addition, agent 6 also plays a critical role in agents 5, 9 and 10's cognitive networks. Therefore, the behavior of agents paying attention to a specific set of households can be described by the attraction of mighty. This case study demonstrates that Algorithm 5.2 is able to identify the critical components in the smart communities.

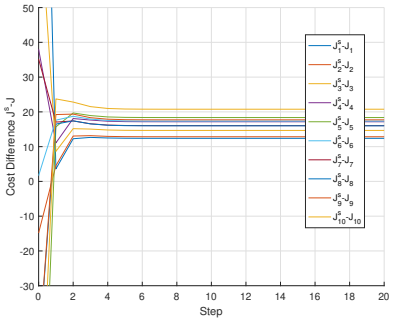


(a) rational strategy

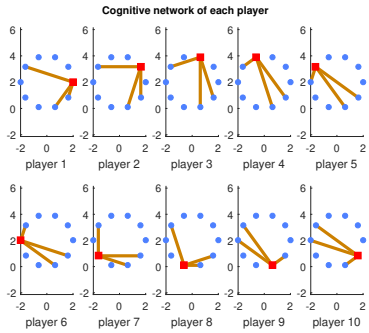
(b) cost under rational strategy



(c) bounded rational strategy



(d) RBP



(e) cognitive network

Figure 5.6: In this heterogeneous case with 10 users, the formed cognitive network shown in (e) is sparse for each smart home. Note that the red rectangular in each subplot of (e) denotes the user that forms his cognitive network with the lines standing for links. Under the bounded rational model, the algorithm can successfully detect the critical agents (attraction of the mighty) in the IoT network which are 5th, 9th and 10th users in this case.

5.6 Summary

In this chapter, we have investigated the security management of users with limited attention over IoT networks through a two-layer framework. The proposed Gestalt Nash equilibrium (GNE) has successfully characterized the bilevel decision makings, including the security management policies and the cognitive network formations of users. Under the security interdependencies, users with a better cognition ability can reduce their cyber risks by making mature decisions. Furthermore, the designed proximal-based algorithm for the computation of GNE has revealed some phenomena that match well with the real-life observations, including the emergence of partisanship and attraction of the mighty. The future work would be extending the framework to incorporate hidden information of unperceived cyber risks of IoT users and design mechanisms to mitigate security loss. Another interesting research direction is to extend the current model to scenarios when a set of users are not fully strategic in minimizing their own risks and analyze the impact of this class of users' misbehavior on the network security risk.

Chapter 6

Real-Time Security and Resilience for Networked Autonomous Systems

6.1 Introduction

This chapter shifts the focus from designing trustworthy decisions over static cyber-physical networks to secure and resilient control design for dynamic CPS.

Cooperative mobile autonomous system (MAS) has a wide range of applications, such as rescue and monitoring the crowd in mission critical scenarios. One of the challenges in designing the MAS network is to maintain the connectivity between agents/robots[1]. Connectivity control of the mobile robotic networks has been addressed in a number of previous works including [92]. They have successfully tackled a single network of cooperative robots. Recent advances in networked

[1]The "agent" refers to the robot in our MAS network. We also use the terms "MAS network" and "robotic network" interchangeably.

systems have witnessed emerging applications involving multi-layer networks or *network-of-networks*. Therefore, the current single network control paradigm is not yet sufficient to address the challenges related to the analysis and design of multi-layer MAS networks.

In the problem investigated, the operator of each layer MAS network aims to maximize the algebraic connectivity [57] of the global network. If the whole network is fully cooperative or governed by a single network operator, then the designed network is a *team-optimal* solution. However, in practice, different layers of robotic networks are often operated by different entities, which makes the coordination between separate entities difficult. This uncoordinated control design naturally leads to a *system-of-systems* (SoS) framework of the multi-layer MAS network. To address this problem, we establish a *Nash* game-theoretic model in which two players, i.e., network operators, control robots at their layer, to maximize the global connectivity independently. This model captures the lack of coordination between players and their decentralized decision making in optimizing the SoS performance. Furthermore, each network operator anticipates the jamming attacks and controls robots by anticipating that a set of critical links between agents can be compromised. This secure control design can be modeled by a *Stackelberg* game between each network operator and the attacker.

In this chapter, we integrate the modeled Nash game between two network operators as well as the Stackelberg game between the network operator and the attacker which further yields a *games-in-games* framework. This new type of game provides a holistic modeling that integrates the network-network interactions and the agent-adversary interactions together for the secure and decentralized control design of multi-layer MAS networks.

6.2 System Framework and Problem Formulation

In this section, we introduce the system framework which includes the wireless communication model and the strategic interdependent MAS network formation.

6.2.1 Wireless Communication Model

In the MAS, we consider a set V of robots in the network, and their positions at time k are defined by the vector $\mathbf{x}(k) = \big(x_1(k);\ x_2(k); ...; x_n(k)\big) \in \mathbb{R}^{3n}$. Robots in the same network can exchange data via wireless communications. Denote the communication link between robots i and j as (i, j). Then, the strength of the communication link (i, j) is similar to the weight of the link in a network. Thus, we associate a weight function $w : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}_+$ with every communication link (i, j), such that

$$w_{ij}(k) = w\big(x_i(k), x_j(k)\big) = f\left(\| x_{ij}(k) \|_2^2\right), \tag{6.1}$$

for some differentiable $f : \mathbb{R}_+ \to \mathbb{R}_+$, where $x_{ij}(k) := x_i(k) - x_j(k)$, and $\| x_{ij}(k) \|_2$ is the distance between robots i and j at time k. To capture the communication strength decay with the distance, f is a monotonically decreasing function. A typical choice of f is $f(d) = \delta^{(c_1-d)/(c_1-c_2)}$, where δ, c_1 and c_2 are positive constants. Note that different forms of f capture various decay rates of communication strength with distance [131]. Thus, the weight of the link between robots is positive if their distance is within a threshold and degenerates to zero otherwise. Fig. 6.1 shows an example of f with $\delta = 0.1$, $c_1 = 2$ and $c_2 = 6$.

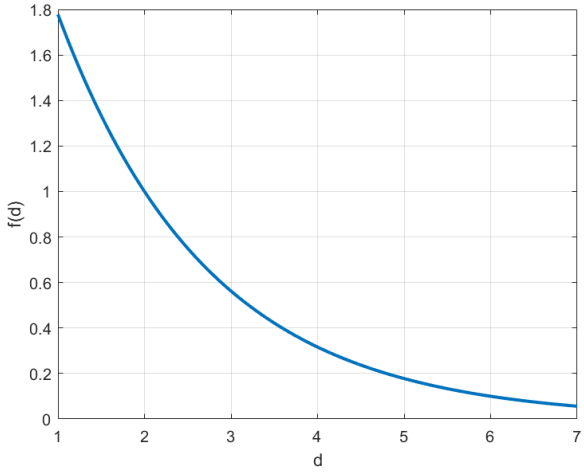


Figure 6.1: Communication strength under function $f(d) = \delta^{(c_1-d)/(c_1-c_2)}$ with $\delta = 0.1$, $c_1 = 2$ and $c_2 = 6$.

6.2.2 Secure Interdependent MAS Network Formation

A two-layer MAS network model is shown in Fig. 6.2, where networks G_1 and G_2 include n_1 and n_2 number of robots, respectively. More generally, we label robots in G_1 as $1, 2, ..., n_1$, and robots in G_2 as $n_1 + 1, n_1 + 2, ..., n_1 + n_2$, i.e., $V_1 := \{1, 2, ..., n_1\}$ and $V_2 := \{n_1 + 1, n_1 + 2, ..., n\}$. Note that $n = n_1 + n_2$. Robots in these two layers can also communicate, and this kind of communication link is called *intra-link* while the link inside of a network is known as *inter-link*. The agents at two layers are interdependent, and thus the integrated MAS network can be modeled as a *system-of-systems*.

6.2.2.1 Network Designer

We consider two players, player 1 (P_1) and player 2 (P_2), operating two interdependent MAS networks. P_1 controls robots in network G_1, and P_2 controls robots in G_2. Specifically, P_1 and P_2 update their own network with a fixed frequency

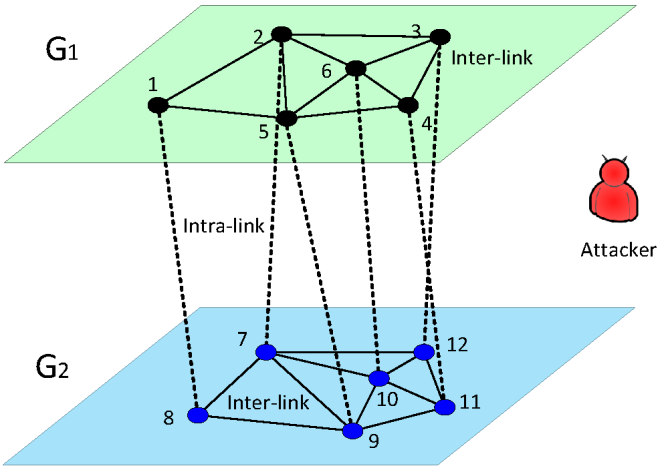


Figure 6.2: Multi-layer MAS network in an adversarial environment.

by controlling the positions of robots. After each update, the communication link strength between robots are modified due to the change of distance. For simplicity, define $-\gamma := \{1,2\} \setminus \gamma$, where $\gamma \in \{1,2\}$, and $\mathbf{x} := (\mathbf{x}_1, \mathbf{x}_2)$, where $\mathbf{x}_1 := (x_1; ...; x_{n_1}) \in \mathbb{R}^{3n_1}$ and $\mathbf{x}_2 := (x_{n_1+1}; ...; x_n) \in \mathbb{R}^{3n_2}$. Specifically, $\mathbf{x}_1$ and $\mathbf{x}_2$ are decision variables denoting the position of robots in G_1 and G_2, respectively. In addition, the action spaces of P_1 and P_2 are denoted by $\mathbf{X}_1$ and $\mathbf{X}_2$, respectively, which include all the possible network configurations. The set of pure strategy profiles $\mathbf{X} := \mathbf{X}_1 \times \mathbf{X}_2$ is the Cartesian product of the individual pure strategy sets. For each update, P_γ's strategy $\mathbf{x}_\gamma$ is based on the current configuration of network $G_{-\gamma}$. The goal of both players is to optimize the SoS performance, i.e., maximize the algebraic connectivity of the global network G. Hence, the utility function for both players is $\lambda_2\big(\mathbf{L}_G(\mathbf{x})\big)$: $\mathbf{X} \to \mathbb{R}_+$, where $\mathbf{L}_G(\mathbf{x})$ is the Laplacian matrix of network G when mobile robots have position $\mathbf{x}$.

In the adversarial network formation game, one of the constraints is the minimum distance between robots in each layer. Without this constraint, all robots at the

same layer will converge to one point finally which is not a reasonable solution. Thus, we assign a minimum distance ρ_1 and ρ_2 for robots in G_1 and G_2, respectively.

6.2.2.2 Cyber Attacker

In addition to the network players P_1 and P_2, our framework also includes a malicious jamming attacker as shown in Fig. 6.2. The attacker is able to disrupt communication links via injecting a large amount of spam into the channel which leads to the link breakdown eventually because of overload of the link. The attacker's objective is to minimize the algebraic connectivity of the network through compromising links. Generally, the behavior of attacker is unknown to the network operators. Therefore, it is difficult for the network designers to make optimal strategies that can achieve the best performances of the network. However, by knowing that attackers are strategic and are more prone to disrupt the critical communication links in the network, the network operators can design a secure MAS network resistant to cyberattacks. Specifically, network designers first anticipate that the attacker can compromise a number $\psi \in \mathbb{N}^+$ of links, and then design the MAS network by taking into account the worst-case attack that leads to the most decrease of the network algebraic connectivity. The resistant property of the network is reflected by the fact that the designers prepare for the potential attacks and respond to them with best strategies. Here, ψ quantifies the security level of the designed network.

Denote $\mathcal{A}$ by the action space of the attacker which is the set including all the possible single communication link removal in the network. For convenience, we denote $\mathbf{L}_G^e(\mathbf{x})$ by the Laplacian matrix of the network after removing a set of links $e \subseteq \mathcal{A}$, i.e., the network after attack is $G(V, E_1 \cup E_2 \cup E_{12} \setminus e)$, and the cardinality

of e is $|e| = \psi$ quantifying the ability of attacker, where $\psi \in \mathbb{N}^+$ is a positive integer. Denote the feasible set of e by $\mathcal{E}$. Then, the cost function of the attacker can be captured by $\Lambda(\mathbf{x}_1, \mathbf{x}_2, e) \triangleq \lambda_2\big(\mathbf{L}_G^e(\mathbf{x})\big)$, for $\Lambda : \mathbf{X}_1 \times \mathbf{X}_2 \times \mathcal{E} \to \mathbb{R}_+$.

6.2.3 Games-in-Games Formulation

During the MAS network formation, the interactions between two networks G_1 and G_2 can be modeled as a Nash game where both players aim to increase the global network connectivity. In addition, each network operator plays a Stackelberg game with the malicious jamming attacker. Therefore, the multi-layer MAS network formation in the adversarial environment can be characterized by a games-in-games framework which is shown in Fig. 6.3. In the following, we specifically formulate the attacker's and network operators' problems, respectively.

6.2.3.1 Stackelberg Game

In the Stackelberg game, network designer is the leader, and the jamming attacker is the follower. The objective of the attacker is to minimize the algebraic connectivity of network G. We can summarize the strategic behavior of the attacker into the following problem:

$$\mathcal{Q}_A^k : \quad \min_{e \subseteq \mathcal{A}, |e| = \psi} \lambda_2\big(\mathbf{L}_G^e(\mathbf{x}(k+1))\big). \tag{6.2}$$

On the leader side, network operator P_γ maximizes the algebraic connectivity of the network, where $\gamma \in \{1, 2\}$, and his decision can be obtained via solving the

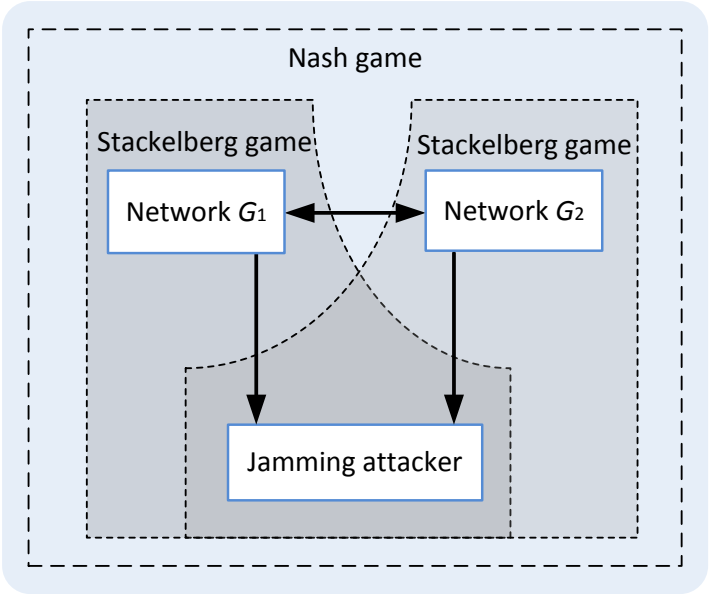


Figure 6.3: Games-in-Games framework which includes two network operators and one attacker. Both network operators prepare for the cyberattack which form a Stackelberg game with the attacker. In addition, two network operators are uncoordinated and aim to maximize the global network connectivity which create a Nash game.

optimization problem:

$$
\begin{aligned}
\mathcal{Q}_\gamma^k: \quad & \max_{\mathbf{x}_\gamma(k+c_\gamma)} \ \min_{e\subseteq\mathcal{A},|e|=\psi} \ \lambda_2\big(\mathbf{L}_G^e(\mathbf{x}(k+c_\gamma))\big) \\
\text{s.t.} \quad & ||x_{ij}(k+c_\gamma)||_2 \geq \rho_\gamma, \quad \forall (i,j)\in E_\gamma, \\
& ||x_{ij}(k+c_\gamma)||_2 \geq \rho_{12}, \quad \forall i\in V_\gamma,\ \forall j\in V_{-\gamma}, \\
& ||x_i(k+c_\gamma)-x_i(k)||_2 \leq d_\gamma, \quad \forall i\in V_\gamma, \\
& x_j(k+c_\gamma)=x_j(k),\ \forall j\in V_{-\gamma},
\end{aligned} \tag{6.3}
$$

where $c_\gamma \in \mathbb{N}^+$ is a positive integer indicating the update frequency; $\rho_\gamma \in \mathbb{R}_+$ is the safety distance between robots; $\rho_{12} \in \mathbb{R}_+$ is the minimum distance between robots in different layers; and $d_\gamma \in \mathbb{R}_+$ is the maximum distance that robots in network

G_γ can move at each update. The constraint $x_j(k + c_\gamma) = x_j(k),\ j \in V_{-\gamma}$ captures the uncoordinated nature that each network operator can only control the robots at his layer. Furthermore, this constraint preserves security consideration between agents in $V_{-\gamma}$ and also ensures consistent connectivity improvement when player γ updates his network.

The Stackelberg game between the attacker and network operator γ can be represented by $\Xi_\gamma := \{\mathcal{N}_\gamma, \mathbf{X}_\gamma, \mathcal{A}, \lambda_2\}$ for $\gamma \in \{1, 2\}$, where $\mathcal{N}_\gamma := \{P_\gamma, Attacker\}$ is the set of players, $\mathbf{X}_\gamma$ and $\mathcal{A}$ are action spaces and λ_2 is the objective function.

6.2.3.2 Nash Game

The interaction between two robotic networks in an adversarial environment can be characterized as a Nash game in which both players aim to increase the global network connectivity. We denote this strategic game by $\Xi_I := \{P_1, P_2, \mathbf{X}_1, \mathbf{X}_2, \lambda_2\}$.

Note that the MAS network formation game is played repeatedly over time, and its structure is the same only with different initial conditions in terms of the robots' position. This two-person interdependent MAS network formation game can be naturally generalized into an N-person game where each player controls a subset of robots in the multi-layer networks.

It is possible that the attacker could manipulate and exploit operator's anticipation for his own benefit. To capture this scenario, we need to propose an alternative model that extends the current framework. In this work, we assume that the network operators choose an action by anticipating credible adversarial behaviors. The attacker can manipulate the above defense mechanism by anticipating defender's strategy. One way to achieve this goal for the attacker is to make decisions over a time horizon instead of a single time step. When the time horizon contains two

steps, then the attacker address a three-stage game (attacker-defender-attacker) that he takes the lead first. A dynamic game of similar three-stage structure has been investigated in [3, 36]. Interested readers can refer to that for detailed description of the framework.

6.3 Problem Analysis and Solution Concepts

In this section, we first reformulated problems in Section 6.2, and then present the solution concept of the MAS network formation game.

6.3.1 Problem Reformulation

Note that each network designer updates the robotic network iteratively based on the current configuration. It is essential to obtain the relationship between the updated position and the current one due to the natural dynamics of robots. To achieve this goal, we define $\mathcal{Z}_{ij}(k) := ||x_{ij}(k)||_2^2$ for notational convenience. Analogous to applying Euler's first order method to continuous dynamics, we can obtain $\mathcal{Z}_{ij}(k+m)$ based on the current positions $x_i(k)$ and $x_j(k)$ as follows:

$$\mathcal{Z}_{ij}(k+m) + \mathcal{Z}_{ij}(k) = 2\{x_i(k+m) - x_j(k+m)\}^{\mathsf{T}}\{x_i(k) - x_j(k)\}, \tag{6.4}$$

where 'T' denotes the transpose operator. Similarly, by using the function f in (6.1), the updated weight $w_{ij}(k+m)$ can be expressed as:

$$w_{ij}(k+m) = w_{ij}(k) + \left.\frac{\partial f}{\partial ||x_{ij}||_2^2}\right|_k (\mathcal{Z}_{ij}(k+m) - \mathcal{Z}_{ij}(k)). \tag{6.5}$$

Therefore, we can obtain the Laplacian matrix $\mathbf{L}_G\big(\mathbf{x}(k+m)\big)$ by using (6.5) for the global network.

Each network designer needs to solve a *max min* problem which are not straightforward to deal with. We first present the following result.

Theorem 6.1. *For a network containing n nodes, the optimization problem*

$$\max_{\mathbf{x}} \min_{e\subseteq\mathcal{A},|e|=\psi} \lambda_2(\mathbf{L}_G^e(\mathbf{x})) \tag{6.6}$$

is equivalent to

$$\begin{aligned} &\max_{\mathbf{x},\beta} \quad \beta \\ &\text{s.t.} \quad \mathbf{L}_G^e(\mathbf{x}) \succeq \beta(\mathbf{I}_n - \frac{1}{n}\mathbf{1}\mathbf{1}^\mathsf{T}),\ \forall e \subseteq \mathcal{A},\ |e| = \psi, \end{aligned} \tag{6.7}$$

where β is a scalar, and $\mathbf{I}_n$ is an n-dimensional identity matrix. Note that the optimal $\mathbf{x}$ and the corresponding objective values in these two problems are equal.

Proof. Let v_i be the eigenvector associated with eigenvalue λ_i of the Laplacian matrix $\mathbf{L}_G^e(\mathbf{x})$, for $\forall i \in V$. Since $\mathbf{L}_G^e(\mathbf{x})$ is real and symmetric, its eigenvectors can be chosen such that they are real and orthonormal, i.e., $v_i^\mathsf{T} v_j = 0, \forall i \neq j \in V$ and $v_i^\mathsf{T} v_i = 1$. Specially, we define $v_1 := \frac{\mathbf{1}}{\sqrt{n}}$, which is actually the eigenvector corresponding to $\lambda_1 = 0$. For convenience, we denote $\mathbf{V} := [v_1, v_2, ..., v_n]$, and $\Upsilon = diag(\lambda_1, \lambda_2, ..., \lambda_n)$, where *diag* is the diagonal operator. Thus, Υ is a diagonal matrix with ith diagonal entry $\lambda_i(\mathbf{L}_G^e(\mathbf{x}))$. Furthermore, based on the orthonormal basis, we obtain $\mathbf{V}\mathbf{V}^\mathsf{T} = \sum_{i=1}^n v_i v_i^\mathsf{T} = \mathbf{I}_n$. The definition of eigenvalue yields

$\mathbf{L}_G^e(\mathbf{x})\mathbf{V} = \mathbf{V}\Upsilon$. Multiplying by $\mathbf{V}^\mathsf{T}$ on the right leads to eigen-decomposition:

$$\mathbf{L}_G^e(\mathbf{x}) = \mathbf{L}_G^e(\mathbf{x})\mathbf{V}\mathbf{V}^\mathsf{T} = \mathbf{V}\Upsilon\mathbf{V}^\mathsf{T} = \sum_{i=1}^{n} \lambda_i(\mathbf{L}_G^e(\mathbf{x}))v_i v_i^\mathsf{T}. \tag{6.8}$$

Since $\lambda_1 = 0$, equation (6.8) can be simplified as

$$\mathbf{L}_G^e(\mathbf{x}) = \sum_{i=2}^{n} \lambda_i(\mathbf{L}_G^e(\mathbf{x}))v_i v_i^\mathsf{T}. \tag{6.9}$$

Next, we add $\lambda_2(\mathbf{L}_G^e(\mathbf{x}))v_1 v_1^\mathsf{T}$ to both sides of (6.9) and obtain $\mathbf{L}_G^e(\mathbf{x}) + \lambda_2(\mathbf{L}_G^e(\mathbf{x}))v_1 v_1^\mathsf{T}$ $= \sum_{i=2}^{n} \lambda_i(\mathbf{L}_G^e(\mathbf{x}))v_i v_i^\mathsf{T} + \lambda_2(\mathbf{L}_G^e(\mathbf{x}))v_1 v_1^\mathsf{T}$. Note that similar to (6.8), $\sum_{i=2}^{n}(\lambda_i(\mathbf{L}_G^e(\mathbf{x})) - \lambda_2(\mathbf{L}_G^e(\mathbf{x})))v_i v_i^\mathsf{T} + 0 \cdot v_1 v_1^\mathsf{T} = \mathbf{V}(\Upsilon - diag(0, \lambda_2, \lambda_2, ..., \lambda_2))\mathbf{V}^\mathsf{T} = \mathbf{L}_G^e(\mathbf{x}) - diag(0, \lambda_2, \lambda_2, ..., \lambda_2)$, where we use λ_2 for clarity in the diagonal entries. The eigenvalues of matrix $\mathbf{L}_G^e(\mathbf{x}) - diag(0, \lambda_2, \lambda_2, ..., \lambda_2)$ can be obtained straightforwardly as $\{0, 0, \lambda_3 - \lambda_2, ..., \lambda_n - \lambda_2\}$ and thus $\mathbf{L}_G^e(\mathbf{x}) - diag(0, \lambda_2, \lambda_2, ..., \lambda_2) \succeq 0$ based on property (2.32), meaning that it is positive semidefinite. In sum, $\sum_{i=2}^{n}(\lambda_i(\mathbf{L}_G^e(\mathbf{x})) - \lambda_2(\mathbf{L}_G^e(\mathbf{x})))v_i v_i^\mathsf{T} \succeq 0$ which can be rewritten as $\mathbf{L}_G^e(\mathbf{x}) \succeq \sum_{i=2}^{n} \lambda_2(\mathbf{L}_G^e(\mathbf{x}))v_i v_i^\mathsf{T}$. Then,

$$\begin{aligned} \mathbf{L}_G^e(\mathbf{x}) + \lambda_2(\mathbf{L}_G^e(\mathbf{x}))v_1 v_1^\mathsf{T} &\succeq \sum_{i=2}^{n} \lambda_2(\mathbf{L}_G^e(\mathbf{x}))v_i v_i^\mathsf{T} \\ + \lambda_2(\mathbf{L}_G^e(\mathbf{x}))v_1 v_1^\mathsf{T} &= \lambda_2(\mathbf{L}_G^e(\mathbf{x})) \sum_{i=1}^{n} v_i v_i^\mathsf{T}. \end{aligned} \tag{6.10}$$

Thus, we obtain $\mathbf{L}_G^e(\mathbf{x}) \succeq \lambda_2(\mathbf{L}_G^e(\mathbf{x}))(\mathbf{I}_n - v_1 v_1^\mathsf{T})$, yielding

$$\mathbf{L}_G^e(\mathbf{x}) \succeq \lambda_2(\mathbf{L}_G^e(\mathbf{x}))(\mathbf{I}_n - \frac{1}{n}\mathbf{1}\mathbf{1}^\mathsf{T}). \tag{6.11}$$

The above analysis is for any given attacker's strategy $e \subseteq \mathcal{A}$. Next, we show that our modified algebraic connectivity maximization problem is equivalent to $\max_{\mathbf{x},\beta}\ \beta$

in (6.7), i.e., $\max_{\mathbf{x},\beta}\ \beta = \lambda_2(\mathbf{L}_G^{e^*}(\mathbf{x}^*))$, where $\mathbf{x}^*$ and e^* are the optimal decisions. For convenience, we denote $\beta^* = \max_{\mathbf{x},\beta}\ \beta$. The proof includes two parts. First, we show that $\beta^* \geq \lambda_2(\mathbf{L}_G^{e^*}(\mathbf{x}^*))$. We aim to maximize the algebraic connectivity $\lambda_2(\mathbf{L}_G^{e}(\mathbf{x}))$, and $(\mathbf{x}^*, e^*)$ is a feasible solution pair. Therefore, based on (6.11), $\beta^* \geq \lambda_2(\mathbf{L}_G^{e^*}(\mathbf{x}^*))$ should hold, since β is a free variable to optimize in the problem (6.7) while its counterpart in (6.11), $\lambda_2(\mathbf{L}_G^{e}(\mathbf{x}))$, is dependent on $\mathbf{x}$ and e. Second, we show that $\beta^* \leq \lambda_2(\mathbf{L}_G^{e^*}(\mathbf{x}^*))$. Since $\beta^*, e^*, \mathbf{x}^*$ are feasible, then, the constraints in (6.7) should be satisfied, i.e., $L_G^{e}(\mathbf{x}^*) \succeq \beta^*(\mathbf{I}_n - \frac{1}{n}\mathbf{1}\mathbf{1}^\mathsf{T})$, $\forall e \subseteq \mathcal{A},\ |e| = \psi$, which gives $L_G^{e^*}(\mathbf{x}^*) \succeq \beta^*(\mathbf{I}_n - \frac{1}{n}\mathbf{1}\mathbf{1}^\mathsf{T})$. Let μ be any unit vector that satisfies $\mu^\mathsf{T} v_1 = 0$. Then, we obtain $\mu^\mathsf{T}\mathbf{L}_G^{e^*}(\mathbf{x}^*)\mu \geq \mu^\mathsf{T}\beta^*(\mathbf{I}_n - \frac{1}{n}\mathbf{1}\mathbf{1}^\mathsf{T})\mu \rightarrow\ \mu^\mathsf{T}\mathbf{L}_G^{e^*}(\mathbf{x}^*)\mu \geq \beta^*\mu^\mathsf{T}\mathbf{I}_n\mu - \beta^*\mu^\mathsf{T}v_1v_1^\mathsf{T}\mu \rightarrow$ $\mu^\mathsf{T}\mathbf{L}_G^{e^*}(\mathbf{x}^*)\mu \geq \beta^*\mu^\mathsf{T}\mathbf{I}_n\mu = \beta^*$. Since vector μ is not fixed, and based on (2.33), we have $\lambda_2(\mathbf{L}_G^{e^*}(\mathbf{x}^*)) \geq \beta^*$. Therefore, $\max_{\mathbf{x},\beta}\beta = \lambda_2(\mathbf{L}_G^{e^*}(\mathbf{x}^*))$, and (6.6) is equivalent to (6.7). □

Next, we define a new Stackelberg game $\widetilde{\Xi}_\gamma := \{\mathcal{N}_\gamma, \mathbf{X}_\gamma, \mathcal{A}, \alpha_\gamma, \lambda_2\}$, for $\gamma \in \{1, 2\}$, where $\mathcal{N}_\gamma$, $\mathbf{X}_\gamma$ and $\mathcal{A}$ are the same as those defined in game Ξ_γ; α_γ and λ_2 are the objective functions of the network designer and attacker, respectively. Based on (6.4), (6.5) and Theorem 6.1, the network designer γ's problem is formulated as

follows, for $\gamma \in \{1, 2\}$:

$$
\begin{aligned}
\widetilde{\mathcal{Q}}_{\gamma}^{k}: \quad & \max_{\mathbf{x}_{\gamma}(k+c_{\gamma}), \alpha_{\gamma}(k+c_{\gamma})} \quad \alpha_{\gamma}(k+c_{\gamma}) \\
\text{s.t.} \quad & \mathbf{L}_{G}^{e}(k+c_{\gamma}) \succeq \alpha_{\gamma}(k+c_{\gamma})(\mathbf{I}_{n} - \frac{1}{n}\mathbf{1}\mathbf{1}^{\mathsf{T}}), \ \forall e \subseteq \mathcal{A}, \ |e| = \psi, \\
& 2\{x_{i}(k+c_{\gamma}) - x_{j}(k+c_{\gamma})\}^{\mathsf{T}}\{x_{i}(k) - x_{j}(k)\} \\
& \qquad = \mathcal{Z}_{ij}(k+c_{\gamma}) + \mathcal{Z}_{ij}(k), \quad \forall i, j \in V_{\gamma}, \\
& ||x_{ij}(k+c_{\gamma})||_{2} \geq \rho_{\gamma}, \qquad \forall (i,j) \in E_{\gamma}, \\
& ||x_{ij}(k+c_{\gamma})||_{2} \geq \rho_{12}, \quad \forall i \in V_{\gamma}, \ \forall j \in V_{-\gamma}, \\
& ||x_{i}(k+c_{\gamma}) - x_{i}(k)||_{2} \leq d_{\gamma}, \quad \forall i \in V_{\gamma}, \\
& x_{j}(k+c_{\gamma}) = x_{j}(k), \ \forall j \in V_{-\gamma}.
\end{aligned}
$$

Note that Laplacian matrices $\mathbf{L}_{G}^{e}(k+c_{\gamma})$, for $\gamma = 1, 2$, are constructed based on (6.5).

The above analysis leads to the following corollary.

Corollary 6.1. *The Stackelberg game $\widetilde{\Xi}_{\gamma}$ is strategically equivalent to the game Ξ_{γ} defined in Section 6.2.3, for $\gamma \in \{1, 2\}$. The interactions between two network operators can be captured by a strategic equivalent Nash game denoted by $\widetilde{\Xi}_{I}$, where $\widetilde{\Xi}_{I}$ includes α_{γ}, $\gamma = 1, \ 2$..*

6.3.2 Equilibrium Solution Concepts

6.3.2.1 Stackelberg Equilibrium of the Adversarial Game $\widetilde{\Xi}_{\gamma}$

In the Stackelberg game, the attacker's strategy is the best response to the action that network designer chooses. Recall that $\Lambda(\mathbf{x}_1, \mathbf{x}_2, e) = \lambda_2\big(\mathbf{L}_{G}^{e}(\mathbf{x})\big)$, and the formal definition of best response is as follows.

Definition 6.1 (Best Response)**.** *For a given strategy pair* $(\mathbf{x}_1, \mathbf{x}_2)$*, where* $\mathbf{x}_1 \in \mathbf{X}_1$ *and* $\mathbf{x}_2 \in \mathbf{X}_2$*, the best response of the attacker is defined by* $BR(\mathbf{x}_1, \mathbf{x}_2) := \{e' : \Lambda(\mathbf{x}_1, \mathbf{x}_2, e') \leq \Lambda(\mathbf{x}_1, \mathbf{x}_2, e), \forall e, e' \subseteq \mathcal{A},\ |e'| = |e| = \psi\}$.

Thus, we give the definition of the Stackelberg equilibrium of game $\widetilde{\Xi}_\gamma$, for $\gamma \in \{1, 2\}$.

Definition 6.2 (Stackelberg Equilibrium)**.** *For a given* $\mathbf{x}_{-\gamma} \in \mathbf{X}_{-\gamma}$*, the profile* $(\mathbf{x}^*_\gamma, e^*)$ *constitutes a Stackelberg equilibrium of the adversarial game* $\widetilde{\Xi}_\gamma$*, for* $\gamma \in \{1, 2\}$*, if the following conditions are satisfied:*

1. *Attacker's strategy* $e^* \subseteq \mathcal{A}$*, where* $|e^*| = \psi$*, is a best response to* $(\mathbf{x}^*_\gamma, \mathbf{x}_{-\gamma})$*, i.e.,* $e^* \in BR(\mathbf{x}^*_\gamma, \mathbf{x}_{-\gamma})$.

2. *Network designer* γ*'s strategy* $\mathbf{x}^*_\gamma \in \mathbf{X}_\gamma$ *satisfies*

$$\min_{e \in BR(\mathbf{x}^*_\gamma, \mathbf{x}_{-\gamma})} \Lambda(\mathbf{x}^*_\gamma, \mathbf{x}_{-\gamma}, e) = \max_{\mathbf{x}_\gamma \in \mathbf{X}_\gamma} \min_{e \in BR(\mathbf{x}_\gamma, \mathbf{x}_{-\gamma})} \Lambda(\mathbf{x}_\gamma, \mathbf{x}_{-\gamma}, e) \triangleq \Lambda^{\gamma *},$$

where $\Lambda^{\gamma *}$ *is the Stackelberg utility of the designer* γ.

6.3.2.2 Nash Equilibrium of the MAS Network Formation Game $\widetilde{\Xi}_I$

After P_1 takes his action at step k, G_1 and G_{12} are reconfigured, where G_{12} is the network between G_1 and G_2. We denote network G_1 and G_{12} at stage k as $G_{1,k}$ and $G_{12,k}$, respectively. For simplicity, we further define $\widetilde{G}_{12,k} := G_{1,k} \cup G_{12,k}$, which is a shorthand notation for the merged network. Then, network G_k can be expressed as $G_k = \widetilde{G}_{12,k} \cup G_{2,k}$. Similarly, after P_2 updates network G_2 at step k, the whole network G_k becomes $G_k = \widetilde{G}_{21,k} \cup G_{1,k}$, where $\widetilde{G}_{21,k} := G_{2,k} \cup G_{12,k}$. Then, the formal definition of Nash equilibrium (NE) which depends on the *position* of robots is as follows.

Definition 6.3 (Nash Equilibrium)**.** *The Nash equilibrium solution to game* $\widetilde{\Xi}_I$ *is a strategy profile* $\mathbf{x}^*$*, where* $\mathbf{x}^* = (\mathbf{x}_1^*, \mathbf{x}_2^*) \in \mathbf{X}$*, that satisfies*

$$\lambda_2\big(\mathbf{L}_{G_k}(\mathbf{x}_1^*, \mathbf{x}_2^*)\big) \geq \lambda_2\big(\mathbf{L}_{G_k}(\mathbf{x}_1, \mathbf{x}_2^*)\big),$$
$$\lambda_2\big(\mathbf{L}_{G_k}(\mathbf{x}_1^*, \mathbf{x}_2^*)\big) \geq \lambda_2\big(\mathbf{L}_{G_k}(\mathbf{x}_1^*, \mathbf{x}_2)\big),$$

for $\forall \mathbf{x}_1 \in \mathbf{X}_1$ *and* $\forall \mathbf{x}_2 \in \mathbf{X}_2$*, where* k *denotes the time step.*

Note that $\mathbf{L}_{G_k}$ in Definition 6.3 captures the network characteristic under all possible attacks instead of a particular one. At the NE point, no player can individually increase the global network connectivity by reconfiguring their MAS network.

6.3.2.3 Meta-Equilibrium of the Games-in-Games

To design a secure multi-layer MAS, each network operator should take into account the attacker's behavior and the other network operator's strategy. The Nash game and the Stackelberg game are inherently coupled, as the adversarial consideration naturally affects the operators' decisions in the Nash game. Furthermore, the NE (Definition 6.3) alone cannot fully capture all the required elements in the games-in-games framework, as the adversarial strategy is characterized by the Stackelberg equilibrium. Hence, a holistic solution concept is necessary for our composed game which is presented as follows.

Definition 6.4 (Meta-Equilibrium)**.** *The meta-equilibrium of the multi-layer MAS network formation game is captured by the profile* $(\mathbf{x}_1^*, \mathbf{x}_2^*, e^*)$ *which satisfies the following conditions:*

1. $(\mathbf{x}_\gamma^*, e^*)$ *constitutes a Stackelberg equilibrium of game* $\widetilde{\Xi}_\gamma$*, for* $\gamma = 1, 2$.

2. $\mathbf{x}^* = (\mathbf{x}_1^*, \mathbf{x}_2^*)$ *is an NE of game* $\widetilde{\Xi}_I$.

Note that the meta-equilibrium is a solution concept for the composed game (games-in-games), which captures the incoordination between two network operators (Nash game) and the security consideration of each network operator (Stackelberg game) simultaneously.

6.4 SDP-Based Approach and Iterative Algorithm

In this section, we reformulate the network designer's problem as a semidefinite programming (SDP) and design an algorithm to compute the meta-equilibrium of the MAS network formation game.

6.4.1 SDP Reformulation

Notice that in $\widetilde{\mathcal{Q}}_\gamma^k$, the minimum distance constraints $||x_{ij}(k+c_\gamma)||_2 \geq \rho_\gamma,\ \forall (i,j) \in E_\gamma$, are *nonconvex*. To address this issue, we regard $\mathcal{Z}_{ij}(k+c_\gamma)$ as a new decision variable. Based on the definition $\mathcal{Z}_{ij}(t) := ||x_{ij}(t)||_2^2$, we have $||x_{ij}(k+c_\gamma)||_2^2 = \mathcal{Z}_{ij}(k+c_\gamma)$. Note that the Laplacian matrix $\mathbf{L}_G^e(k+c_\gamma)$ depends linearly on $\mathcal{Z}_{ij}(k+c_\gamma)$, $i,j \in V$, based on (6.5). Then, we solve problems $\widetilde{\mathcal{Q}}_\gamma^k$ with respect to unknowns $\mathcal{Z}_{ij}(k+c_\gamma)$ and $\mathbf{x}(k+c_\gamma)$ jointly. In this way, $\widetilde{\mathcal{Q}}_\gamma^k$ becomes a convex problem. However, due to the coupling between the robots position and the distance vectors, solving $\widetilde{\mathcal{Q}}_\gamma^k$ via merely adding new variables yields inconsistency between the obtained solutions $\mathbf{x}(k+c_\gamma)$ and $\mathcal{Z}_{ij}(k+c_\gamma),\ \forall i,j \in V$. To address this issue, we first present the following definition.

Definition 6.5 (Euclidean Distance Matrix)**.** *Given the positions of a set of* n *points denoted by* $\{x_1, ..., x_n\}$*, the Euclidean distance matrix representing the points*

spacing is defined as

$$\mathbf{D} := [d_{ij}]_{i,j=1,...,n}, \text{ where } d_{ij} = ||x_i - x_j||_2^2.$$

A critical property of the Euclidean distance matrix is summarized in the following theorem.

Theorem 6.2 ([50]). *A matrix* $\mathbf{D} = [d_{ij}]_{i,j=1,...,n}$ *is an Euclidean distance matrix if and only if*

$$-\mathbf{CDC} \succeq 0, \text{ and } d_{ii} = 0, \ i = 1, ..., n, \tag{6.12}$$

where $\mathbf{C} := \mathbf{I}_n - \frac{1}{n}\mathbf{1}\mathbf{1}^\mathsf{T}$.

Note that (6.12) is a necessary and sufficient condition that ensures $\mathbf{D}$ an Euclidean distance matrix. In addition, the inequality and equality in (6.12) are both convex. Therefore, Theorem 6.2 provides an approach to avoid the inconsistency between the robots position and distance vectors when they are treated as independent variables. In specific, denote $\mathbf{Z} = [\mathcal{Z}_{ij}]_{i,j\in V}$, $\mathbf{C} = \mathbf{I}_n - \frac{1}{n}\mathbf{1}\mathbf{1}^\mathsf{T}$,

and we can further reformulate problems $\widetilde{\mathcal{Q}}_\gamma^k$, $\gamma \in \{1,2\}$, as

$$
\begin{aligned}
\overline{\mathcal{Q}}_\gamma^k: \quad & \max_{\mathbf{x}_\gamma(k+c_\gamma),\mathbf{Z}(k+c_\gamma),\alpha_\gamma(k+c_\gamma)} \quad \alpha_\gamma(k+c_\gamma) \\
\text{s.t.} \quad & \mathbf{L}_G^e(k+c_\gamma) \succeq \alpha_\gamma(k+c_\gamma)\mathbf{C}, \quad \forall e \subseteq \mathcal{A},\ |e| = \psi, \\
& 2\{x_i(k+c_\gamma) - x_j(k+c_\gamma)\}^\mathsf{T}\{x_i(k) - x_j(k)\} \\
& \qquad = \mathcal{Z}_{ij}(k+c_\gamma) + \mathcal{Z}_{ij}(k), \quad \forall i,j \in V_\gamma, \\
& \mathcal{Z}_{ij}(k+c_\gamma) \geq \rho_\gamma^2,\ \forall (i,j) \in E_\gamma, \\
& \mathcal{Z}_{ij}(k+c_\gamma) \geq \rho_{12}^2, \quad \forall i \in V_\gamma,\ \forall j \in V_{-\gamma}, \\
& -\mathbf{C}\mathbf{Z}(k+c_\gamma)\mathbf{C} \succeq 0,\ \mathcal{Z}_{ii}(k+c_\gamma) = 0,\ i \in V, \\
& ||x_i(k+c_\gamma) - x_i(k)||_2 \leq d_\gamma,\ \forall i \in V_\gamma, \\
& x_j(k+c_\gamma) = x_j(k),\ \forall j \in V_{-\gamma}. \qquad (6.13)
\end{aligned}
$$

Remark: In $\overline{\mathcal{Q}}_\gamma^k$, the relationship $||x_{ij}(k+c_\gamma)||_2^2 = \mathcal{Z}_{ij}(k+c_\gamma)$ is ensured by the constraint $2\{x_i(k+c_\gamma) - x_j(k+c_\gamma)\}^\mathsf{T}\{x_i(k) - x_j(k)\} = \mathcal{Z}_{ij}(k+c_\gamma) + \mathcal{Z}_{ij}(k)$. In this constraint, $\mathcal{Z}_{ij}(k)$ is known which can be calculated based on the current position $\mathbf{x}(k)$, i.e., $\mathcal{Z}_{ij}(k) = ||x_i(k) - x_j(k)||_2^2$. Furthermore, constraints $-\mathbf{C}\mathbf{Z}(k+c_\gamma)\mathbf{C} \succeq 0$ and $\mathcal{Z}_{ii}(k+c_\gamma) = 0$ guarantee that the elements in $\mathbf{Z}(k+c_\gamma)$ are equal to the distances between corresponding nodes.

Note that P_γ controls robots in G_γ and reconfigures the network by solving $\overline{\mathcal{Q}}_\gamma^k$ to obtain the new positions of robots for $\gamma \in \{1,2\}$. Furthermore, $\overline{\mathcal{Q}}_\gamma^k$ becomes convex and admits an SDP formulation which can be solved efficiently.

6.4.2 Iterative Algorithm

We have obtained the SDP formulations $\overline{Q}_{\gamma}^{k}$, $\gamma = 1, 2$, and next we aim to find the solution that results in a meta-equilibrium MAS configuration. In the MAS formation game, P_1 controls robots in G_1 and reconfigures the network by solving the optimization problem $\overline{Q}_{1}^{k}$ to obtain a new position of each robot. P_2 controls robots in network G_2 in a similar way by solving $\overline{Q}_{2}^{k}$. Note that the players' action at the current step can be seen as a best-response to the network at the previous step by taking the worst-case attack into account. Since both players maximize the global network connectivity at every update step, then one approach to find the meta-equilibrium solution is to address $\overline{Q}_{1}^{k}$ and $\overline{Q}_{2}^{k}$ iteratively by two players until the yielding MAS possesses the same secure topology, i.e., P_1 and P_2 cannot increase the network connectivity further through reallocating their robots. For clarity, Algorithm 6.1 shows the updating details. A typical example of the algorithm is *alternating update* in which P_1 and P_2 have the same update frequency but not update at the same time and reconfigure the MAS network sequentially.

6.4.3 Structural Results

Regarding the feasibility of the problems $\overline{\mathcal{Q}}_{\gamma}^{k}$ for $\gamma = 1, 2$, we have the following remark.

Remark: For a given multi-layer MAS network where the distance between robots satisfies the predefined minimum distance constraint, problems $\overline{\mathcal{Q}}_{1}^{k}$ and $\overline{\mathcal{Q}}_{2}^{k}$ are always feasible. The feasibility can be indeed achieved by the players' strategies that they do not update the position of robots at step k.

When $\overline{\mathcal{Q}}_{1}^{k}$ and $\overline{\mathcal{Q}}_{2}^{k}$ are feasible at each update step, another critical property is

Algorithm 6.1 Secure and resilient MAS network formation

Initialize mobile robots' position $x_i(0)$, $\forall i \in V$, $\mathbf{x}(1) = 2\mathbf{x}(1-c_1) = 2\mathbf{x}(1-c_2)$, c_1, c_2, $\kappa = 10^{-6}$.
for $k = 1, 2, 3, \ldots$ **do**
  if $k \mod c_1 = 0$ and $\|\mathbf{x}(k) - \mathbf{x}(k-c_1)\|_\infty > \kappa$ **then**
    P_1 obtains new strategy $\mathbf{x}_1(k+c_1)$ via solving $\overline{\mathcal{Q}}_1^k$
  else $\mathbf{x}_1(k) = \mathbf{x}_1(k-1)$
  end if
  if $k \mod c_2 = 0$ and $\|\mathbf{x}(k) - \mathbf{x}(k-c_2)\|_\infty > \kappa$ **then**
    P_2 obtains new strategy $\mathbf{x}_2(k+c_2)$ via solving $\overline{\mathcal{Q}}_2^k$
  else $\mathbf{x}_2(k) = \mathbf{x}_2(k-1)$
  end if
  Break if $\|\mathbf{x}(k) - \mathbf{x}(k-c_1)\|_\infty \leq \kappa$ and $\|\mathbf{x}(k) - \mathbf{x}(k-c_2)\|_\infty \leq \kappa$ and $k > \max(c_1, c_2)$
  $k \leftarrow k+1$
end for
return $\mathbf{x}(k)$

the convergence of the proposed iterative algorithm. The result is summarized in Theorem 6.3.

Theorem 6.3. *The proposed Algorithm 6.1 of the adversarial network formation game converges to a meta-equilibrium asymptotically.*

Proof. Note that at each stage of play, the game captured by $\bar{\mathcal{Q}}_1^k$ and $\bar{\mathcal{Q}}_2^k$ can be characterized as a constrained *potential game* due to the identical objective of two players [107]. The designed algorithm is based on the best response dynamics which yields a non-decreasing network connectivity sequence. Furthermore, for a network with n nodes, its algebraic connectivity is upper bounded by a value depending on $f(d_\gamma)$ [68]. Thus, based on the monotone convergence theorem [63], the algorithm converges to a meta-equilibrium asymptotically. □

We next show that designers' adversary-anticipation is beneficial to the network performance and the multi-layer MAS network is resistant to strategic attacks.

Lemma 6.1. *Under the established games-in-games model in Section 6.2.3, we obtain* $\lambda_2\big(\mathbf{L}_{G_k}^{e_k}(\mathbf{x}_1(k),\mathbf{x}_2(k))\big) \geq \lambda_2\big(\mathbf{L}_{G_k}^{\tilde{e}_k}(\tilde{\mathbf{x}}_1(k),\tilde{\mathbf{x}}_2(k))\big)$*, where* $(\mathbf{x}_1(k),\mathbf{x}_2(k))$ *is a strategy pair of network operators resulting from* (6.13) *with an appropriate time index;* $(\tilde{\mathbf{x}}_1(k),\tilde{\mathbf{x}}_2(k))$ *is a corresponding strategy pair without adversary-anticipation (ignoring the first constraint in* (6.13)*); and* e_k *and* $\tilde{e}_k$ *are the attacker's admissible strategies at step* k *satisfying* $e_k \in BR(\mathbf{x}_1(k),\mathbf{x}_2(k))$ *and* $\tilde{e}_k \in BR(\tilde{\mathbf{x}}_1(k),\tilde{\mathbf{x}}_2(k))$*. The inequality also holds at the meta-equilibrium* $(\mathbf{x}^*, e^*)$*.*

Proof. We prove the result consecutively in two parts, i.e., before and after the network reaching meta-equilibrium. For the first part, the network configuration at every time step k incorporates the consideration of $|e| = \psi$ link attacks and the physical constraints, i.e., the maximum distance that robot can move at one time step and the minimum distances between robots. Assume that designer γ, $\gamma \in \{1,2\}$, updates the configuration and the position of robots becomes $\mathbf{x}_\gamma(k)$ at time k. Then, the updated position $\mathbf{x}_\gamma(k)$ of player γ is a best response to $\mathbf{x}_{-\gamma}(k)$ with the consideration of constraints (ones in (6.13) with different time index), and $(\mathbf{x}_1(k),\mathbf{x}_2(k))$ is an optimal strategy maximizing the connectivity under any ψ link attacks. Therefore, the global MAS network is resistant to this type of strategic attacks during updates. We next proceed to show the second part. Through the designed algorithm, the network has been shown to converge to a meta-equilibrium. The network connectivity at the meta-equilibrium $(\mathbf{x}_1^*,\mathbf{x}_2^*)$ under attack $e^* \in BR(\mathbf{x}_1^*,\mathbf{x}_2^*)$ is $\lambda_2\big(\mathbf{L}_G^{e^*}(\mathbf{x}^*)\big)$. Since two designers have the same objective, at their equilibrium strategies $(\mathbf{x}_1^*,\mathbf{x}_2^*)$, both designers have a consistent anticipation on the set of link removals under the worst-case attack, i.e., e^*. By the definition of Stackelberg game, we know that $\mathbf{x}_\gamma^*$ is the optimal strategy under any ψ link removals for designer γ, and this fact holds simultaneously for both designers at

equilibrium. Therefore, $\lambda_2\big(\mathbf{L}_G^{e^*}(\mathbf{x}^*)\big)$ is the maximum network connectivity that designers can achieve under strategic attacks, showing the resistance of the network to adversary at equilibrium. □

We next investigate the uniqueness of the meta-equilibrium of the game, and the result is shown in the following theorem.

Theorem 6.4. *The meta-equilibrium of the game is not unique, i.e., different equilibrium profiles* $(\mathbf{x}_1^*, \mathbf{x}_2^*, e^*)$ *are possible.*

Proof. To show the nonuniqueness of the meta-equilibrium, one possible way is to find a different position pair $(\tilde{\mathbf{x}}_1^*, \tilde{\mathbf{x}}_2^*)$ but the network configuration is the same with a one under the meta-equilibrium, say $(\mathbf{x}_1^*, \mathbf{x}_2^*)$. This can be achieved by the simultaneous offset or rotation in $\mathbf{x}_1^*$ and $\mathbf{x}_2^*$. For example, under the meta-equilibrium $(\mathbf{x}_1^*, \mathbf{x}_2^*, e^*)$, the profile $(\mathbf{x}_1^* + \zeta, \mathbf{x}_2^* + \zeta, e^*)$ is also a meta-equilibrium, where $\zeta \in \mathbb{R}^3$, and this shows the nonuniqueness of the equilibrium. □

The network configuration at meta-equilibrium can also be different at which the network exhibits various levels of network connectivity. This phenomenon is further demonstrated through case studies in Section 6.6.

Remark: Due to nonuniqueness of meta-equilibrium, it is important for the network designers to achieve an equilibrium state with a higher connectivity. We need to deal with a mechanism design or an equilibrium selection problem. One general method to address this type of problem is through a top-down approach. Specifically, we first need to know the complete set of equilibria and then decentralize the solution for two network designers to drive the system to a desired equilibrium state. Hence, in addition to two network operators, we need to include an additional central planner who has perfect information of the system and guides

the decentralized network configuration updates of two designers to achieve a particular equilibrium solution.

Another result is on the effectiveness of our proposed strategy comparing with simpler ones without attack anticipation for the network designers. In the proposed model considering adversary, if the attack does not occur, then the network connectivity achieved at the meta-equilibrium is no better than the one obtained by the model without considering adversaries. However, when the attack is successfully launched, the network performance under the established framework is no worse than the one without considering adversaries. Characterizing the conditions under which these two classes of strategies coincide is not trivial and it is also related to the system parameters of multi-layer MAS.

In Section 6.6, we use a case study to show the advantage of our proposed framework over the traditional optimal design when the adversary is ignored. In the case study, the equilibrium network is still connected under the strategic attack while the optimal network counterpart is disconnected. Therefore, preparation for and reacting to attacks can yield significant benefits for the MAS network under adversarial environment.

6.5 Adversarial Analysis

In this section, we first analyze the security of MAS network by deriving a closed form solution of the jamming attacker, and then present another type of cyberattacks for further resiliency quantification of the proposed iterative algorithm. Finally, we discuss the benefits of anticipating and reacting to the adversary for the network designers during control design.

6.5.1 Adversarial Analysis

Denote the network as $\widetilde{G}(i,j) = (V, E \setminus (i,j))$ after removing a link $(i,j) \in E$ from network G, then, we have $\widetilde{\mathbf{L}} = \mathbf{L} - \Delta\mathbf{L}$ and $\Delta\mathbf{L} = \Delta\mathbf{D} - \Delta\mathbf{A}$, where $\Delta\mathbf{D}$ and $\Delta\mathbf{A}$ are the decreased degree and adjacency matrices, respectively. By using equation (2.31), we obtain $\Delta\mathbf{D}$ and $\Delta\mathbf{A}$ as follows: $\Delta\mathbf{D} = \mathbf{e}_i\tilde{\mathbf{e}}_{i,j}^{\mathsf{T}} + \mathbf{e}_j\tilde{\mathbf{e}}_{j,i}^{\mathsf{T}}, \Delta\mathbf{A} = \mathbf{e}_i\tilde{\mathbf{e}}_{j,i}^{\mathsf{T}} + \mathbf{e}_j\tilde{\mathbf{e}}_{i,j}^{\mathsf{T}}$, where $\mathbf{e}_i$ and $\tilde{\mathbf{e}}_{i,j}$ are n-dimensional zero vectors except the i-th element equaling to 1 and w_{ij}, respectively, and similar for $\mathbf{e}_j$ and $\tilde{\mathbf{e}}_{j,i}$. Denote the Laplacian matrix of $\widetilde{G}(i,j)$ as $\widetilde{\mathbf{L}}(i,j)$, and by using $\Delta\mathbf{D}$ and $\Delta\mathbf{A}$, we have

$$\widetilde{\mathbf{L}}(i,j) = \mathbf{L} - \big(\mathbf{e}_i - \mathbf{e}_j\big)\big(\tilde{\mathbf{e}}_{i,j} - \tilde{\mathbf{e}}_{j,i}\big)^{\mathsf{T}}. \tag{6.14}$$

When link (i,j) is attacked, the resulting Laplacian is given by (6.14). Denote the Fiedler vector of $\mathbf{L}$ as $\mathbf{u}$, and thus $\mathbf{u}^{\mathsf{T}}\mathbf{L}\mathbf{u} = \lambda_2(\mathbf{L})$ based on the definition. By using Courant-Fisher Theorem in (2.33), we obtain the following:

$$\begin{aligned}
\lambda_2\big(\widetilde{\mathbf{L}}(i,j)\big) &\leq \mathbf{u}^{\mathsf{T}}\widetilde{\mathbf{L}}(i,j)\mathbf{u} \\
&= \mathbf{u}^{\mathsf{T}}\big(\mathbf{L} - \big(\mathbf{e}_i - \mathbf{e}_j\big)\big(\tilde{\mathbf{e}}_{i,j} - \tilde{\mathbf{e}}_{j,i}\big)^{\mathsf{T}}\big)\mathbf{u} \\
&= \mathbf{u}^{\mathsf{T}}\mathbf{L}\mathbf{u} - (u_i - u_j)(w_{ij}u_i - w_{ji}u_j) \\
&= \lambda_2(\mathbf{L}) - w_{ij}(u_i - u_j)^2.
\end{aligned} \tag{6.15}$$

Therefore, by removing the link $(i,j)^*$, where

$$(i,j)^* \in \arg\max_{(i,j)\in E} \; w_{ij}(u_i - u_j)^2, \tag{6.16}$$

the upper bound of $\lambda_2\big(\widetilde{\mathbf{L}}(i,j)\big)$ is the smallest. The strategy in (6.16) can be seen as a greedy heuristic for the attacker to compromise the network G. Specifically,

the attacker can apply the above procedure iteratively to find a set of critical links to accommodate the attacker's ability. To this end, the jamming attacker's strategy is to compromise those links with top ψ largest value of $w_{ij}(u_i - u_j)^2$, $i, j \in V$. Therefore, the network operators designs secure strategies by anticipating that these ψ critical links could be compromised by the attacker.

6.5.2 Another Type of Cyberattack

In order to assess the resilience of designed iterative algorithm in Section 6.4.2, we introduce another type of adversarial attacks to the MAS network called global positioning system (GPS) spoofing attack.

GPS Spoofing Attack: A GPS spoofing attack aims to deceive a GPS receiver in terms of the object's position, velocity and time by generating counterfeit GPS signals [2]. In [89], the authors have demonstrated that UAVs can be controlled by the attackers and go to a wrong position through the GPS spoofing attack. We consider the scenario that the compromised robot is spoofed which can be realized by adding a disruptive position signal to the robot's real control command. Therefore, through the GPS spoofing attack, the mobile robot is controlled by the adversary, but it still maintains communications with other robots in the network. In addition, we assume that the attack cannot last forever but for a period of g_a in the discrete time measure, since the resource of an attacker is limited, and the abnormal/unexpected behavior of the other unattacked robots resulting from the spoofing attack can be detected by the network operator.

Specifically, if robot i, $i \in V$, is compromised by the spoofing attack at time step k_1, and the attack lasts for g_a time steps, then this scenario can be captured by adding the following constraint to $\overline{\mathcal{Q}}_\gamma^k$: $x_i(k+1) = x_i(k) + \epsilon(k),\ k = k_1, ..., k_1 + g_a - 1,$

where $\epsilon(k)$ is the disruptive signal added by the attacker. The attacked robot is usually randomly chosen. To evaluate the impact of attack, we choose the robot that has the maximum degree denoted by i_{max} and satisfies

$$i_{max} \in \arg \max_{i \in V} \sum_{j \in \mathcal{N}_i} w_{ij}, \tag{6.17}$$

where $\mathcal{N}_i$ is the set of nodes connected to robot i.

The GPS spoofing attack decreases the network connectivity. The resilience of the designed algorithm can be quantified by the increased network performance by the network operators' responses to the cyberattacks.

6.5.3 Benefits of Anticipating and Reacting to Adversary

We comment on the benefits of the established approach that enhances the network resistance to attacks. First, the Stackelberg modeling incorporates the security consideration of network designers. This anticipative behavior of the defender ensures the resistance of network under successful worst-case attacks. The security consideration is critical and also practical for the network operators in devising proactive defense strategies, and its significance is demonstrated through case studies in Section 6.6. Second, besides the inherent security modeling, reacting to the adversary also helps in improving the system performance if the attack is unanticipated. Then, the operator can respond to the unanticipated attack in the next round which enhances network resilience. Thus, the proposed method guides the secure and resilient decentralized control design of MAS networks.

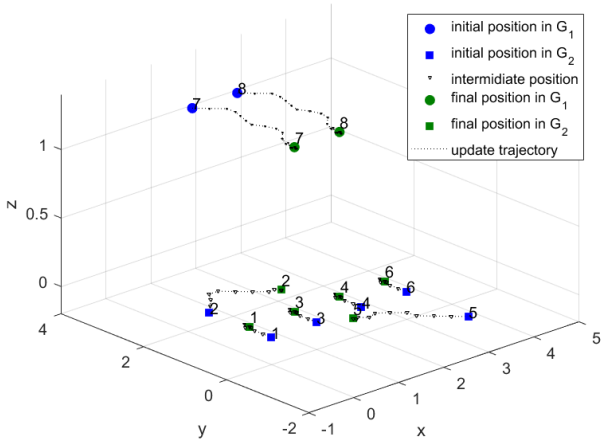
6.6 Case Studies

In this section, we use case studies to quantify the security and resiliency of the designed algorithm, and identify the interdependency in the multi-layer MAS networks. We adopt YALMIP [101] to solve the corresponding SDP problems. Specifically, we consider a two-layer MAS network in which G_1 contains 2 nodes and G_2 contains 6 nodes. To illustrate that the designed framework can be applied to cases where the robots at one layer can further be operated in a decentralized way, we assume that the robots in G_2 are divided into 2 equal-size groups connected by a secure link between nodes 3 and 4. The investigated scenario is applicable when the agents in MAS are sparsely distributed in geometric clusters.

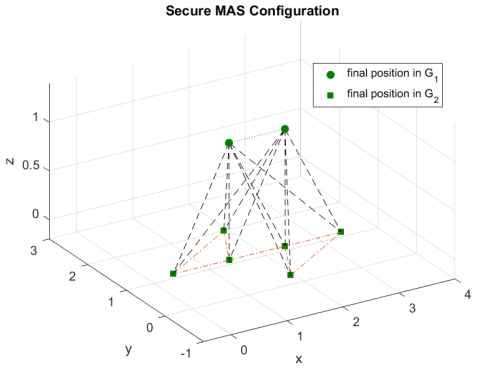
The communication strength between agents follows the one in Fig. 6.1. Further, two layers of MAS are operated in two planes where the third dimension of their position is fixed satisfying the minimum distance ρ_{12}. The initial positions of robots in G_1 (upper layer) are (1,3,1.2), (2,3,1.2), and robots in G_2 (lower layer) are (0,0,0), (0,1.5,0), (1,0,0), (2,0,0), (3,-1.5,0), (3,0,0). The safety distance between robots in G_1 and G_2 is $\rho_1 = \rho_2 = 1$, and the maximum distance that robots at each layer can move at each update step is $d_1 = d_2 = 0.2$. The update frequency of network operator P_1 is two times faster than network operator P_2, i.e., $2c_1 = c_2$. In addition, both network designers prepare for the worst-case single link removal of jamming attack, i.e., $|e| = \psi = 1$, during the MAS network formation.

6.6.1 Secure Design of MAS Networks

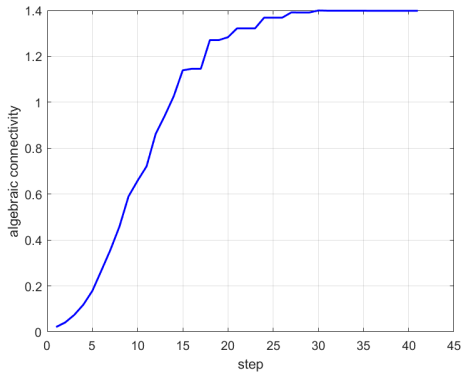
First, we illustrate the secure design of two-layer MAS network under the jamming attack using Algorithm 6.1. Fig. 6.4 shows the results. The final positions



(a)



(b)



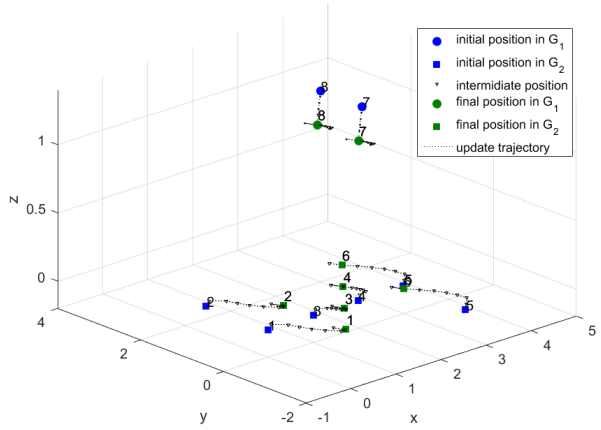
(c)

Figure 6.4: (a) shows the evolutionary configuration of secure MAS network at each step. (b) depicts the final network configuration. (c) shows the network connectivity under attack with $\psi = 1$.

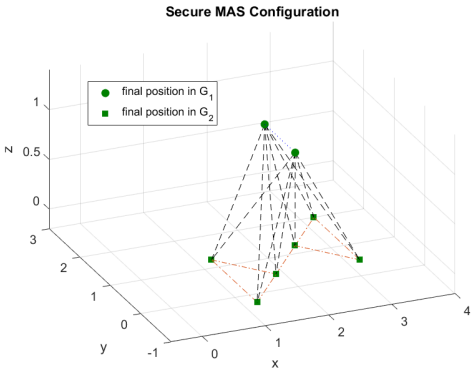
of agents in G_1 are (1.88,-0.13,1.2), (1.88,0.87,1.2), and those in G_2 are (0.94,-0.85,0), (0.94,0.65,0), (1.60,-0.10,0), (2.26,0.65, 0), (1.55,-0.29,0), (2.92,1.40,0). The connectivity of the integrated MAS network is iteratively improved, and converges to a steady value 1.4 after approximate 40 steps. During the updates, each network operator anticipates of the strategic jamming attack that compromises the most critical communication link. Hence, the network shown in Fig. 6.4(b)

is a meta-equilibrium configuration. This example shows the effectiveness of the proposed method in designing secure multi-layer MAS network. To show the nonuniqueness of the equilibrium solutions, we modify the initial positions of agents where the robots in G_1 (upper layer) start with (3,1,1.2) and (3,2,1.2). The results are shown in Fig. 6.5. We can see that the final positions of agents in G_1 are (1.06,0.59,1.2), (2.06,0.59,1.2), and those in G_2 are (0.05,0.58,0), (1.55,1.45,0), (1.05,0.58,0), (2.05,0.58, 0), (1.55,-0.29,0), (3.05,0.58,0). Further, the final network configuration as well as network connectivity are different with the ones shown in Fig. 6.4 which corroborate the meta-equilibrium of the proposed game is not unique.

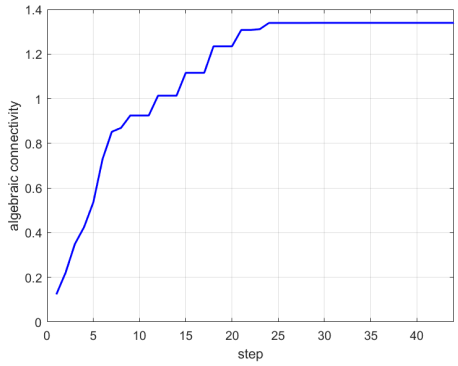
Another critical question is to compare the quality of the solution at meta-equilibrium with the one obtained without considering attacks. To better illustrate the results, we select another set of parameters for communication channels: $\delta = 0.1$, $c_1 = 1$, and $c_2 = 1.2$, where agents have a lower range of communication than the one in Fig. 6.4. In addition, the number of agents in the upper layer G_1 is reduced to 1 and the number of attacks is equal to $\psi = 2$. The adversary's action set $\mathcal{A}$ includes the links between two layers, i.e., inter-links. Other settings are the same as those in previous case studies. The results of network configurations with and without considering attacks are shown in Fig. 6.6. In Fig. 6.6(a), since no adversary is present in this scenario, the network connectivity remains around 0.48. To demonstrate the difference of the optimal solution without considering attack and the equilibrium solution, we introduce two attacks by removing two most critical inter-links using the strategy in Section 6.5.1 to the optimal network (removing links (3,7) and (4,7)) at step 50, and the result is shown in Fig. 6.6(b). Comparing with the secure MAS configuration using the proposed control with



(a)



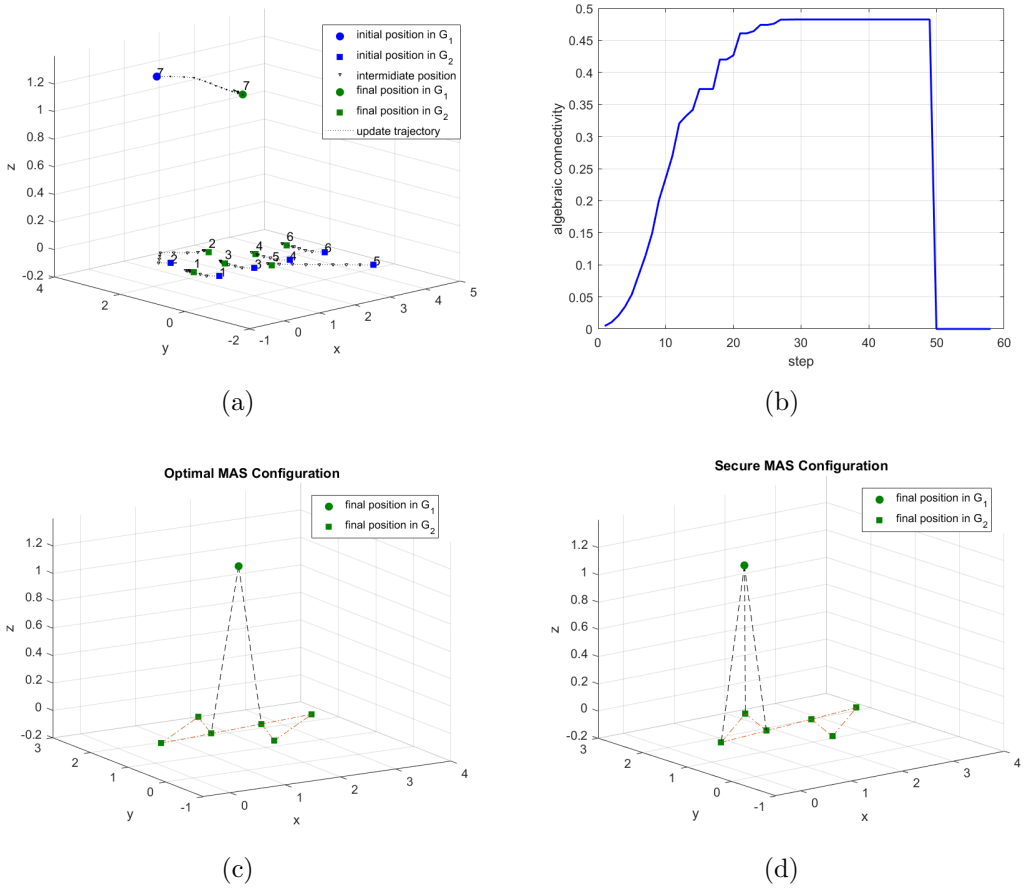
(b)



(c)

Figure 6.5: (a), (b), and (c) show the results of the ones in Fig. 6.4. The initial conditions of agents are modified and the final equilibrium network is different with the one in Fig. 6.4 which shows the nonuniqueness of the equilibrium.

connectivity 0.17 shown in Fig. 6.6(d), the originally optimal network is completely disconnected after the attack which makes the isolated agent 7 in an unanticipated condition. This result shows the advantage of our proposed framework over the traditional optimal design, since our approach integrates the security aspects in the MAS control design.



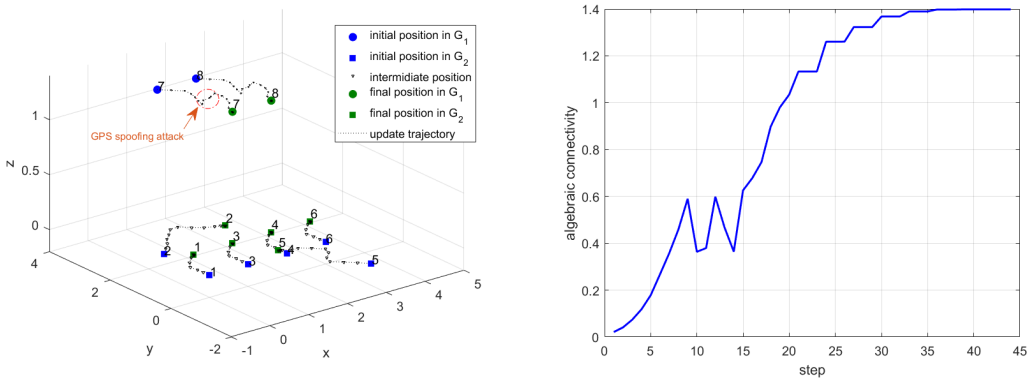
(a) (b)

(c) (d)

Figure 6.6: (a), (b), and (c) show the results when the network designers do not anticipate attacks. (d) is the equilibrium network when designers considers two link attacks. The final network configurations in (c) and (d) are different. After introducing the worst-case attacks to the optimal network (compromising the inter-links (3,7) and (4,7)), the optimal network in (c) is disconnected and the connectivity becomes 0. However, the meta-equilibrium network in (d) is still connected after 2 inter-links attacks with a connectivity of 0.17 which demonstrates the enhanced security of MAS networks.

6.6.2 Resilience of the Network to Cyberattacks

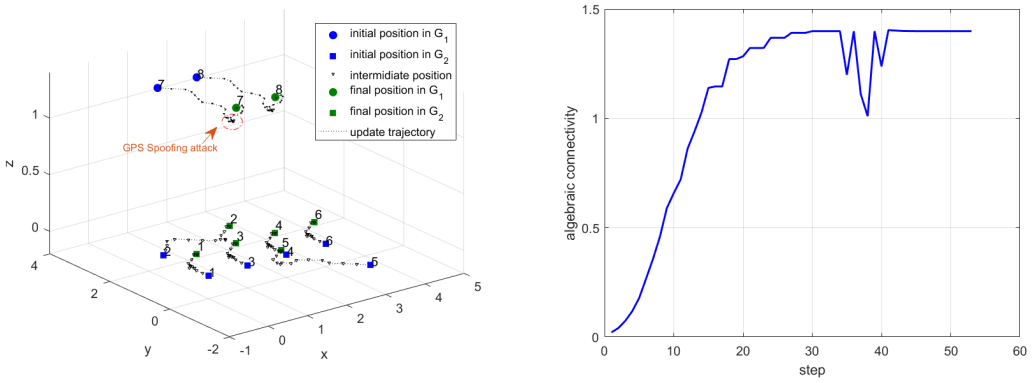
Second, we investigate the resilience of the designed MAS network to cyberattacks presented in Section 6.5.2. The metric used for quantifying the resilience is the recovery ability of network connectivity after the adversarial attack.



(a) (b)

Figure 6.7: (a) shows the evolutionary configuration of secure MAS network at each step. The GPS spoofing attack is introduced at time step 9, and it lasts for 5 steps. The attack duration depends on the detection ability of the network designer. (b) shows the corresponding network connectivity.

For the GPS spoofing attack, we assume that it lasts for 5 time steps from step 9 to 14 before the detection of abnormal movement of MAS by the network operator. Note that the attack duration depends on the detection ability of the network designer. After the identification of attack, the network designer can reboot the compromised agent for it returning to the normal state. Moreover, the horizontal axis in attacker's disruptive command $\epsilon(k)$, $k = 9, ..., 14$, is drawn uniformly from $[0, 0.2]$. Fig. 6.7 shows the obtained results where agent 7 is compromised. Specifically, the network connectivity encounters a sudden drop at step 9, from 0.58 to 0.37, as shown in Fig. 6.7(b) due to the spoofing attack. At step 12 which is still in the attacking window, the connectivity, however, has an increase which is a result from the updates of agents at the lower layer G_2. When the spoofing attack is removed, the network recovers quickly after step 14 which shows agile resilience of the proposed control algorithm. Note that the final MAS network configuration is the same as the one in Section 6.6.1.



(a) (b)

Figure 6.8: (a) shows the evolutionary configuration of secure MAS network at each step. (b) shows the corresponding network connectivity. The spoofing attack launches at step 35 and it lasts for 6 steps. The network recovers and reaches a meta-equilibrium quickly after the removal of attack.

We next investigate a scenario in which the spoofing attack is introduced after the network reaching an equilibrium. Specifically, the attack launches at step 35 and it lasts for 6 steps. The results are shown in Fig. 6.8. Similar to the previous case, the network can response to the attack in a fast fashion and tries to recover the network connectivity with its best effort during the attacking window. After the detection and removal of the attack, the network performance is improved and the equilibrium network configuration is achieved which is the same as the previous one before attack. Thus, the designed two-layer MAS network using Algorithm 6.1 is resilient to spoofing cyberattacks.

6.7 Summary

In this chapter, we have investigated the secure control of multi-layer MAS networks under the adversarial environment by establishing a games-in-games framework. The newly proposed meta-equilibrium solution concept has successfully

captured the secure and uncoordinated design of each layer of MAS network through integrative Stackelberg and Nash games. The developed iterative algorithm has been shown effective in maximizing the network algebraic connectivity under adversaries, yielding a meta-equilibrium network configuration. Case studies have shown that the designed multi-layer MAS network is of agile resilience to various kinds of cyberattacks. As for future work, we can consider the network operators having different estimations of severity of attacks, and design the multi-layer MAS network with heterogeneous security requirements. Another research direction is to design mechanisms and decentralized algorithms to drive the multi-layer MAS to a desired meta-equilibrium if multiple equilibria exist. We can also investigate other games-in-games frameworks where the attacker's behavior is more sophisticated, e.g., the attacker makes decisions over a time horizon.

Part IV

Mechanism Design for CPS

Network Economics

Chapter 7

Security as a Service in the Cloud-Enabled Internet of Controlled Things

7.1 Introduction

A cloud-enabled *Internet of Controlled Things* (IoCT) allows heterogeneous components to provide services in an integrated system. For example, cloud resources can provide data aggregation, storage and processing for the physical systems. Fig. 7.1 shows a framework of the cloud-enabled IoCT. The sensors associated with devices[1] can send data to the remote controllers through up-links, and the control commands can be sent back to the actuator via down-links. Both directions of information transmission are enabled by the cloud layer. The cloud-enabled IoCT can be divided into two layers including the cyber and physical

[1]The term of devices in this chapter refers to things and physical systems in cloud-enabled IoCT, and they are used interchangeably.

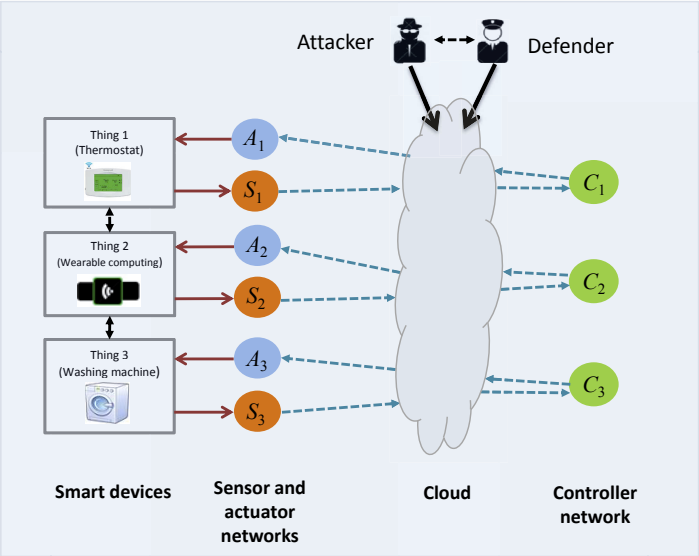


Figure 7.1: Cloud-enabled IoCT framework. The sensor data associated with physical devices can be stored and aggregated in the cloud. The remote controllers use these collected information to compute the control commands with cloud resources and sent them back to the actuators. The integration of cloud layer enhances the performance of IoCT. Note that the vulnerability of cloud directly influences the physical layer performance.

components. Generally, the devices at the physical layer and the cloud at the cyber layer belong to two different entities, e.g., the physical devices may not own the cyber infrastructure to communicate the controller or sensor information.

The cloud layer in Fig. 7.1 can be insecure, since it faces cyber threats, e.g., *advanced persistent threats* (APTs) [129] where malicious attackers can steal keys used to authenticate devices in the cloud-enabled IoCT, leading to a complete system compromise. Thus, to ensure a trustworthy cyberspace, we use a contract-based `FlipCloud` (`CB-FlipCloud`) game-theoretic framework to model APTs of the cloud. In `CB-FlipCloud`, the attacker and the defender compete to control the cloud resources for a larger fraction of time through paying a cost. The strategic outcome of the `CB-FlipCloud` game determines the vulnerability of cloud layer in

IoCT.

At the physical layer, the devices use optimal control to minimize the operational cost. As shown in Fig. 7.1, the performance of the physical system is closely related to the security of the cloud. To use the cloud services, the device needs to plan and buy services from the cloud to fulfill its control task. Specifically, the device should provide economic incentives to the service provider (SP) at the cyber layer to secure the cloud resources. The quality of services (QoS) of different SPs in terms of the cloud security are not identical. The device has no knowledge about the type of the cloud which is private information of the SP. By leveraging techniques from *contract theory*, we capture the service relationships between the device and cloud SP which further create a new paradigm of *security as a service* (SaaS) in cloud-enabled IoCT. The challenge of the contract design lies in the design of an incentive compatible and efficient mechanism for the integrated system in spite of the incomplete information.

7.1.1 Notations and Conventions

To enhance the readability of this chapter, we summarize the adopted notations as follows. Matrices A, B and C correspond to the state space model of the physical system. Matrices Q and R related to the costs of state deviation and control effort of the physical system. $\rho_{\mathcal{M}}$ captures the quality of security service of $\mathcal{M}$-type cloud, which corresponds to the proportion of time that the defender controls the cloud resources denoted by $z_{\mathcal{M}}$. Note that the types of the contract lie in the set $\mathcal{M} \in \{H, L\}$. Some other key notations are summarized in Table 7.1.

Table 7.1: Nomenclature of Chapter 7

$\bar{p}_{\mathcal{M}}$	transfer payment in $\mathcal{M}$-type contract, $\mathcal{M} \in \{H, L\}$
$p_{\mathcal{M}}$	unit payment in $\mathcal{M}$-type contract
$q_{\mathcal{M}}$	targeted cloud quality in $\mathcal{M}$-type contract
$v_{\mathcal{M}}$	unit penalty of degraded service in $\mathcal{M}$-type contract
f	the renewal frequency of cloud defender
g	the attacking frequency of cloud attacker
z	the proportion of time of the defender controlling the cloud
$q_{\mathcal{M},\max}$	the upper bound of required QoS in $\mathcal{M}$-type contract
$q_{\mathcal{M},\min}$	the lower bound of required QoS in $\mathcal{M}$-type contract
$\epsilon_{\mathcal{M}}$	the minimum required profit of $\mathcal{M}$-type cloud
$\psi_{\mathcal{D}}^{\mathcal{M}}$	the unit defending cost of $\mathcal{M}$-cloud
$u_{\mathcal{A}}^{\mathcal{M}}$	the unit payoff of controlling the cloud of the attacker
$\phi_{\mathcal{M}}$	weighting parameter of the physical system performance
ζ	the spectral radius of matrix A
α_k	vulnerability of the controller to actuator link in IoCT
β_k	vulnerability of the sensor to controller link in IoCT
x_k	state of the device
y_k	output of the device
w_k	exogenous disturbance of the device
u_k	control input of the device
U^o	the best performance of device in IoCT without APTs

7.2 System Model

In this section, we first introduce a bi-level system model that captures the features of the contract design for cloud-enabled IoCT. Then, we present the service flows and timing in the contract design.

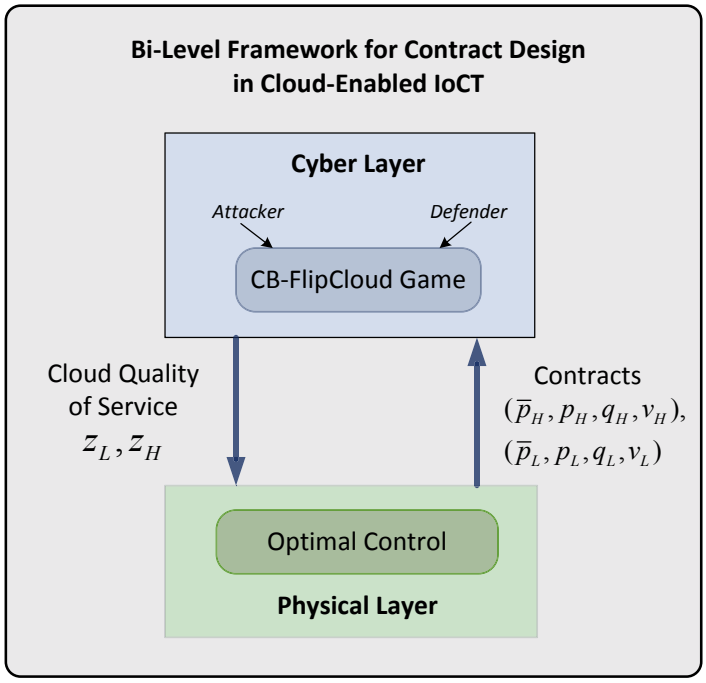


Figure 7.2: Bi-level framework for the optimal contract design in the cloud-enabled IoCT. The cyber layer uses a `CB-FlipCloud` game to capture the competitions between the defender and attacker with actions f and g, respectively, and then determines the cloud service z to the device based on the offered contract $(\bar{p}, p, q, v)$ from the physical layer. The physical system at the lower layer uses optimal control computed by the cloud, and its performance is dependent on the cloud QoS z. The interdependent structure makes the decision-makings of two layers correlated.

7.2.1 Bi-Level System Framework

The proposed bi-level system framework is shown in Fig. 7.2 including the cyber and physical layers. We introduce these two layers and state their couplings.

7.2.1.1 Cyber Layer

The cyber layer of the framework in Fig. 7.2 is concerned with cloud security under APTs. We adopt a two-person `CB-FlipCloud` game-theoretic framework to capture the interactions between the cloud defender and attacker. Specifically,

the two players, the defender and the attacker, at the cyber layer compete to control the cloud resources for a larger fraction of time. We denote by f and g the strategies of the defender and the attacker, respectively. When the cyber layer is under the control of the defender, then the cloud services can be reliably delivered to the devices at the physical layer. Otherwise, the cloud services will be degraded. Knowing that securing and attacking the cloud resources are costly for the defender and the attacker, respectively, both players choose their actions in a strategic manner. The outcome of the `CB-FlipCloud` game determines the cloud QoS provided to the device, denoted by z. We consider without loss of generality two types of QoS, high-type (H-type) and low-type (L-type). The type of QoS is private information of the cloud SPs which is unknown to the devices. Due to the asymmetric information, the devices at physical layer need to design a menu of two contracts. We present the details of `CB-FlipCloud` game in Section 7.3.2.

7.2.1.2 Physical Layer

At the physical layer shown in Fig. 7.2, the systems use optimal control computed by the cloud to operate the system. The role of cloud computing for the physical systems and the dynamic models of physical systems are discussed in Section 7.3.1. Note that the performance of the physical system is closely related to the security of cloud. A better cloud QoS z ensures that the physical system receives control commands more reliably. In order to receive cloud service, the device needs to design a contract with the SP to guarantee the reliability of the cloud. Since the physical system has no knowledge about the security of cloud, he needs to design two types of contracts including H-type and L-type: $(\bar{p}_H, p_H, q_H, v_H)$ and $(\bar{p}_L, p_L, q_L, v_L)$, where $\bar{p}_i \in \mathbb{R}_+$ is the transfer payment from the physical system;

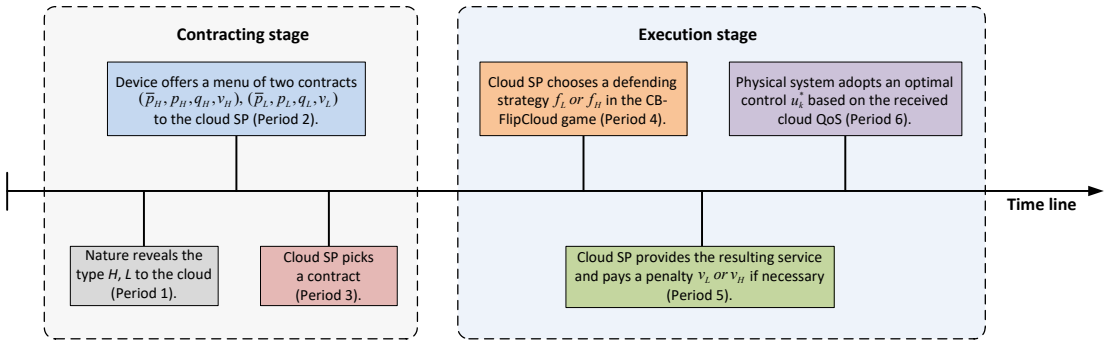


Figure 7.3: The timing of events in the contract design problem which include the contracting and execution stages.

$p_i \in \mathbb{R}_+$ is the unit payment of service; $q_i \in \mathbb{R}_+$ is the targeted cloud quality; and $v_i \in \mathbb{R}_+$ is a parameter corresponding to the penalty of degraded service, for $i \in \{H, L\}$. The detailed contract design problem for cloud-enabled IoCT is introduced in Section 7.3.3. The contract design investigated in this chapter is a hidden-type problem in contract theory. A more thorough introduction of the contract mechanism design can be found in Chapter 2.2.

7.2.1.3 Couplings between Cyber and Physical Layers

The cyber layer and the physical layer in Fig. 7.2 are interdependent. At the cyber layer, the cloud SP designs a cyber defense strategy f based on the received contract from devices, and the resulting *Nash equilibrium* of `CB-FlipCloud` game (f^*, g^*) determines the delivered cloud QoS z. The device at the physical layer designs the contracts by taking into account the received cloud QoS z. Here, we drop the type index H and L for clarity. Due to the reliance of optimal control of devices on the cloud services, the design of contract needs to take into account the requirement of physical system performance. This coupling between cyber physical layers makes the decision-makings of the cloud SP and the device interdependent.

7.2.2 Timing of Contract Design

To better clarify the coupled `CB-FlipCloud` game and the contract design, we present the detailed service flow in the bi-level framework in the following. The contract design can be divided into two main stages including the contracting and execution as shown in Fig. 7.3. The timing of the events are summarized as follows. First, the nature reveals the type to the cloud but not to the physical device which introduces an *asymmetric information* structure. Then, the device designs and offers two contracts in terms of the type of cloud SP. The cloud picks one of the contracts which completes the contracting stage. In the execution stage, based on the accepted contract, the cloud SP makes a defending strategy against the cyber attacker to achieve a certain level of security of the cloud resources. Then, the remote control of the physical system is enabled by the resulting cloud service. If the provided cloud quality does not meet the required one in the contract, then the cloud SP pays a penalty.

In summary, the proposed mechanism starts with devices designing a menu of contracts followed by the cloud SP providing agreed services. A penalty is paid to the devices if the QoS is violated. This constitutes the service flow in the cloud-enabled IoCT.

7.3 Problem Formulation

In this section, we first present the physical-layer optimal control of physical systems in Section 7.3.1 and then establish a cyber-layer two-player nonzero-sum `CB-FlipCloud` game for the cloud security in Section 7.3.2. The modular solutions are used to formulate the contract design problem between the physical device and

the cloud SP in Section 7.3.3.

7.3.1 Optimal Control of the Physical System

The devices in the cloud-enabled IoCT perform various tasks. To measure the performance of IoCT, we need to consider the dynamics of physical systems, e.g., unmanned vehicles, intelligent lighting and autonomous personal robots. Specifically, a device with discrete-time dynamics under the unreliable cloud can be captured by

$$\begin{aligned} x_{k+1} &= Ax_k + \alpha_k Bu_k + w_k, \\ y_k &= \beta_k Cx_k, \end{aligned} \tag{7.1}$$

for $k = 0, 1, ...$, where $x_k \in \mathbb{R}^n$ is the state; $u_k \in \mathbb{R}^m$ is the control input; $w_k \in \mathbb{R}^n$ is the exogenous disturbance with mean zero; $y_k \in \mathbb{R}^l$ is the sensor output; and A, B, C are time-invariant matrices with appropriate dimensions. Note that w_k, $\forall k$, are independent. The stochastic processes $\{\alpha_k\}$ and $\{\beta_k\}$ model the vulnerability nature of the cloud, and they capture the successful information transmission from the controller to the actuator (downlink) and from the sensor to the controller (uplink), respectively.

Role of cloud computing for the devices in IoCT: The cloud-enabled IoCT device is empowered with a high capacity of computational resources and data storage. The device maintains a constant communication with the cloud to collect and store sensor data, process information and compute optimal control outputs. Due to its reliance on the cloud, the device needs to be assured of the trustworthiness of the cloud. Note that $\{\alpha_k\}$ and $\{\beta_k\}$ model the physical impact of the unreliability of the cloud due to the APTs. Specifically, the disruption of

data collection and storage services of the cloud will make the sensor measurements unavailable, i.e., $\beta_k = 0$. In addition, the disruption of computational services will make the control outputs unavailable, i.e., $\alpha_k = 0$.

Note that the communications between the cloud and devices are secure in our model. The degraded performance of the physical system is due to the loss of sensing and control information at the cloud layer caused by APTs. Let α_k and β_k be two Bernoulli random variables with the same probability mass function. Since the provided cloud services are divided into two types including the H-type and the L-type, then each type of service has

$$\alpha_k^i,\ \beta_k^i = \begin{cases} 1, & \text{with probability } \rho_i, \\ 0, & \text{with probability } 1-\rho_i, \end{cases} \tag{7.2}$$

for $i \in \{H, L\}$. In addition, we have $1 \geq \rho_H > \rho_L > 0$ to distinguish two types of cloud.

Remark: The value of ρ_i, $i \in \{H, L\}$, which represents the cloud quality has a direct influence on the physical system performance given by (7.3). In the cloud-enabled IoCT, the real provided QoS by the cyber layer is determined by the offered contracts of the device.

We consider the optimal control of the physical system in an infinite horizon, and define the control policy as $\Pi = \{\mu_0, \mu_1, ..., \mu_{N-1}\}$, where N is the decision horizon, and function μ_k maps the information I_k to some control space, i.e., $u_k = \mu_k(I_k)$. The information set I_k includes $(\alpha_0, ..., \alpha_{k-1})$, $(\beta_0, ..., \beta_k)$, $(y_0, ..., y_k)$, and $(u_0, ..., u_{k-1})$, for $k = 1, 2, ...$, and specially for $k = 0$, $I_0 = (y_0, \beta_0)$. With a given cloud quality parameter ρ_i, the device aims to find an optimal control policy

that minimizes the quadratic cost function

$$J(\Pi^*|\rho_i) = \limsup_{N\to\infty} \frac{1}{N}\mathbb{E}\left\{\sum_{k=0}^{N-1}\left(x_k^T Q x_k + \alpha_k^i u_k^T R u_k\right)\right\}, \tag{7.3}$$

while considering the system dynamics (7.1), where $i \in \{H, L\}$, $R \succ 0$ and $Q \succeq 0$. Note that R and Q are two matrices that capture the costs of state deviation and control effort, respectively. *For notational brevity, we drop the type index H and L when the context is clear.*

7.3.2 `CB-FlipCloud` Game for the Cloud Security

The cloud layer in IoCT faces APTs, and the traditional cryptography approaches may fail to secure the integrated system. To mitigate the cyber risks, we use a `CB-FlipCloud` game to model the interactions between the defender ($\mathcal{D}$) and attacker ($\mathcal{A}$) in the cloud. Specifically, the strategies of $\mathcal{D}$ and $\mathcal{A}$ are to choose $f \in \mathbb{R}_+$ and $g \in \mathbb{R}_+$, the renewal and attacking frequencies with which they claim control of the cloud resources, respectively. Note that f and g are chosen by prior commitment such that neither $\mathcal{D}$ nor $\mathcal{A}$ knows the opponent's action when making choices. In addition, we focus the `CB-FlipCloud` game analysis on periodic strategies, in which the moves of $\mathcal{D}$ and $\mathcal{A}$ are both spaced equally apart, and their phases are chosen randomly from a uniform distribution [133].

Based on f and g, we can compute the expected proportions of time that $\mathcal{D}$ and $\mathcal{A}$ control the cloud. The main analysis follows from Section 4.1 in [133]. When $g = 0$, i.e., no $\mathcal{A}$ exists in the game, then $\mathcal{D}$ controls the cloud for all time which is a trivial case. When $\mathcal{A}$ exists and $\mathcal{D}$ moves no slower than $\mathcal{A}$, i.e., $f \geq g > 0$, and for a given $\mathcal{D}'$s move interval τ, the probability that $\mathcal{A}$ moves over his phase

selection which lies in τ is $\frac{g}{f}$. In addition, $\mathcal{A}$ only moves once in τ since $f \geq g$, and the move is uniformly distributed over τ. Therefore, the expected proportions of time that $\mathcal{A}$ and $\mathcal{D}$ control the cloud in this interval are $\frac{g}{2f}$ and $1 - \frac{g}{2f}$, respectively. Similar analysis applies to the case when $g > f > 0$. Denote the proportions of time by $z \in [0, 1]$ and $1 - z$ for $\mathcal{D}$ and $\mathcal{A}$ controlling the cloud, respectively, and we obtain

$$z = \begin{cases} 1, & \text{if } g = 0, \\ \frac{f}{2g}, & \text{if } g > f \geq 0, \\ 1 - \frac{g}{2f}, & \text{if } f \geq g > 0. \end{cases} \tag{7.4}$$

Notice that when $g > f \geq 0$, i.e., the attacking frequency of $\mathcal{A}$ is larger than the renewal frequency of $\mathcal{D}$, then the proportion of time that the cloud is secure is $z < \frac{1}{2}$; and when $f \geq g > 0$, we obtain $z \geq \frac{1}{2}$.

Remark: When the defender controls the cloud, then the information is successfully transmitted through the cloud. In addition, in the `CB-FlipCloud` game, when the interval between consecutive moves is small which results in high move frequencies of $\mathcal{D}$ and $\mathcal{A}$, then z can be interpreted as the probability of random variables α_k and β_k being 1 in (7.1). Therefore, the `CB-FlipCloud` game outcome z determines the cloud quality measure ρ in (7.2). We use z to represent the provided cloud QoS in the following.

Then, the optimization problem for the cloud SP under the H-type contract $(\bar{p}_H, p_H, q_H, v_H)$ can be formulated as

$$\pi_H(\bar{p}_H, p_H, q_H, v_H) = \max_{f_H} \{\bar{p}_H + \min\{p_H z_H, p_H q_H\} - C_H(f_H) - V_H(q_H, z_H, v_H)\},$$

where $\bar{p}_H$, p_H, q_H and v_H have been introduced in Section 7.2.1; f_H is the defense strategy of the cloud SP; and z_H is obtained through (7.4) based on f_H and g_H, where g_H denotes the attacker's strategy. C_H and V_H are defense cost and penalty functions which have mappings $C_H : \mathbb{R}_+ \to \mathbb{R}_+$ and $V_H : (0,1] \times (0,1] \times \mathbb{R}_+ \to \mathbb{R}_+$, respectively. The term $\min\left\{p_H z_H, p_H q_H\right\}$ indicates that the physical system will not pay more to the cloud SP for receiving better cloud service as requested in the contract. Similarly, for the L-type contract $(\bar{p}_L, p_L, q_L, v_L)$, the problem of the cloud SP becomes $\pi_L(\bar{p}_L, p_L, q_L, v_L) = \max_{f_L}\{\bar{p}_L + \min\{p_L z_L, p_L q_L\} - C_L(f_L) - V_L(q_L, z_L, v_L)\}$.

Based on the accepted contract, the attacker and defender in the `CB-FlipCloud` game yield a Nash equilibrium strategy pair (f^*, g^*) which has a unique mapping to z^* through (7.4). Hence, the `CB-FlipCloud` game equilibrium determines the risk of a chosen cloud service for the device subject to APTs. More details of the `CB-FlipCloud` game analysis including the equilibrium are presented in Section 7.4.1.

7.3.3 Contract Design for the Physical Layer

The type of the cloud is private information. The device designs a menu of two contracts, $(\bar{p}_H, p_H, q_H, v_H)$ and $(\bar{p}_L, p_L, q_L, v_L)$, based on the prior probability $\sigma \in [0,1]$ of the cloud being H-type.

Due to this asymmetric information structure, we find the optimal contracts for the device by formulating it as a mechanism design problem. Specifically, by using the *revelation principle* [110], we address the contract design by focusing on the incentive compatible and *direct revelation* mechanisms. Therefore, the contract

design problem (CDP) for the physical device is formulated as follows:

$$\begin{aligned}
\text{CDP}: \min_{(\bar{p}_H, p_H, q_H, v_H),\ (\bar{p}_L, p_L, q_L, v_L)} \quad & \\
\sigma \left(\bar{p}_H + p_H z_H^* + \phi_H \frac{U^o - U(z_H^*)}{|U^o|} - V_H\left(q_H, z_H^*, v_H\right) \right) & \\
+ (1-\sigma) \left(\bar{p}_L + p_L z_L^* + \phi_L \frac{U^o - U(z_L^*)}{|U^o|} - V_L(q_L, z_L^*, v_L) \right) & \quad (7.5) \\
\text{s.t.} \quad \pi_H(\bar{p}_H, p_H, q_H, v_H) \geq \pi_H(\bar{p}_L, p_L, q_L, v_L), & \quad (7.6a) \\
\pi_L(\bar{p}_L, p_L, q_L, v_L) \geq \pi_L(\bar{p}_H, p_H, q_H, v_H), & \quad (7.6b) \\
\pi_H(\bar{p}_H, p_H, q_H, v_H) \geq \epsilon_H, & \quad (7.6c) \\
\pi_L(\bar{p}_L, p_L, q_L, v_L) \geq \epsilon_L, & \quad (7.6d) \\
p_H > 0,\ p_L > 0, & \quad (7.6e) \\
q_{H,\min} \leq q_H \leq q_{H,\max} < 1, & \quad (7.6f) \\
q_{L,\min} \leq q_L \leq q_{L,\max} < 1, & \quad (7.6g)
\end{aligned}$$

where ϕ_H and ϕ_L are positive weighting parameters; $U : (0, 1] \to \mathbb{R}$ is a utility function of the physical device; and $U^o \in \mathbb{R}$ denotes the optimal utility of the device under $z = 1$ which is a known constant for each device. ϵ_H and ϵ_L are the minimum required profits of H-type and L-type cloud, respectively. $q_{H,\min}$, $q_{H,\max}$, $q_{L,\min}$ and $q_{L,\max}$ are bounds of the required cloud quality in each contract.

Note that (7.6a) and (7.6b) in CDP are *incentive compatibility* (IC) constraints which ensure that a cloud does not benefit from lying about its type to the physical system. In addition, (7.6c) and (7.6d) are called *individual rationality* (IR) constraints which indicate that a cloud accepts the contract only when its minimum profit is met. By focusing on the IC and IR constraints yielded by the revelation principle [110], the device at the physical layer designs such contracts that give an

optimal tradeoff between the payment to the cloud SP and the received cloud QoS.

7.4 Analysis of the Cloud Security and Physical Systems

In this section, we first analyze the `CB-FlipCloud` game that captures the cloud layer security, and then present the optimal control results of the physical systems. In addition, we discuss the impact of cloud quality on the performance of devices.

7.4.1 Security Analysis of the Cloud Layer

In order to design a strategy for the cloud defender, we first need to analyze the `CB-FlipCloud` game under each type of contract. The defense cost function $C_{\mathcal{M}} : \mathbb{R}_+ \to \mathbb{R}_+$ can be defined as

$$C_{\mathcal{M}}(f_{\mathcal{M}}) := \psi_{\mathcal{D}}^{\mathcal{M}} f_{\mathcal{M}} \tag{7.7}$$

which comes from the `CB-FlipCloud` game, where $\mathcal{M} \in \{H, L\}$, and $\psi_{\mathcal{D}}^{\mathcal{M}} > 0$ is the unit defending cost of the cloud. The cloud SP provides different types of services in terms of the QoS captured by z. The penalty function $V_{\mathcal{M}} : (0,1] \times (0,1] \times \mathbb{R}_+ \to \mathbb{R}_+$ admits the form

$$V_{\mathcal{M}}(q_{\mathcal{M}}, z_{\mathcal{M}}, v_{\mathcal{M}}) = v_{\mathcal{M}}(q_{\mathcal{M}} - z_{\mathcal{M}})\mathbf{1}_{\{q_{\mathcal{M}} > z_{\mathcal{M}}\}}, \tag{7.8}$$

where $z_{\mathcal{M}}$ is obtained through (7.4), and $\mathbf{1}_{\{\bullet\}}$ is an indicator function. Recall that $v_{\mathcal{M}}$ is a term in the $\mathcal{M}$-type contract.

Some natural assumptions on the parameters are as follows.

Assumption 7.1. *For the penalty and payment parameters, we have*

$$0 < p_L < p_H, \tag{7.9}$$

$$0 < v_L < v_H, \tag{7.10}$$

$$p_H < v_H \leq v_{H,\max}, \tag{7.11}$$

$$p_L < v_L \leq v_{L,\max}, \tag{7.12}$$

where $v_{H,\max}$ and $v_{L,\max}$ are the maximum unit penalty in the H-type and L-type contracts, respectively.

Note that the inequalities (7.9) and (7.10) differentiate the unit payment and penalty in the H-type and L-type contracts. In addition, (7.11) and (7.12) indicate that the unit penalty in both contracts is larger than the unit payment and bounded above.

Based on (7.4), we need to discuss two cases of the `CB-FlipCloud` game. Specifically, when $f_H \geq g_H > 0$ which yields $z_H = 1 - \frac{g_H}{2f_H}$, the `CB-FlipCloud` game for the cloud under the H-type contract can be formulated as

$$\begin{aligned}
\max_{f_H} F^H_{\mathcal{D}}(f_H, g_H|\bar{p}_H, p_H, q_H, v_H) = \max_{f_H} \Bigg\{ & \bar{p}_H + \min\left\{ p_H\left(1 - \frac{g_H}{2f_H}\right), p_H q_H \right\} \\
& - \psi^H_{\mathcal{D}} f_H - v_H \left(q_H + \frac{g_H}{2f_H} - 1\right) \mathbf{1}_{\left\{q_H > 1 - \frac{g_H}{2f_H}\right\}} \Bigg\}, \\
\min_{g_H} F^H_{\mathcal{A}}(f_H, g_H|\bar{p}_H, p_H, q_H, v_H) = \min_{g_H} & \left\{ \psi^H_{\mathcal{A}} g_H - u^H_{\mathcal{A}} \frac{g_H}{2f_H} \right\},
\end{aligned} \tag{7.13}$$

where $F^H_{\mathcal{D}} : \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}$ and $F^H_{\mathcal{A}} : \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}$ are objective functions of the

cloud defender and attacker, respectively, and $\psi_{\mathcal{A}}^{H} > 0$ and $u_{\mathcal{A}}^{H} > 0$ are the unit costs of attacking the cloud and unit payoff of controlling the cloud, respectively. In $F_{\mathcal{D}}^{H}$, recall that $\bar{p}_H + \min\left\{p_H\left(1-\frac{g_H}{2f_H}\right), p_H q_H\right\}$ denotes the payment from the physical system; $\psi_{\mathcal{D}}^{H} f_H$ captures the cloud defense cost; and $v_H\left(q_H + \frac{g_H}{2f_H} - 1\right)\mathbf{1}_{\left\{q_H > 1-\frac{g_H}{2f_H}\right\}}$ is the penalty of degraded service. In $F_{\mathcal{A}}^{H}$, the attacker's objective is to minimize the attacking cost $\psi_{\mathcal{A}}^{H} g_H$ while maximize the utility of controlling the cloud resources given by $u_{\mathcal{A}}^{H}\frac{g_H}{2f_H}$. For $f_L \geq g_L > 0$, the `CB-FlipCloud` game under the L-type contract can be formulated similarly.

Another non-trivial case of the `CB-FlipCloud` game is when $g_{\mathcal{M}} > f_{\mathcal{M}} > 0$, for $\mathcal{M} \in \{H, L\}$. In this scenario, the proportions of time that the cloud defender and attacker controlling the cloud resources are equal to $\frac{f_{\mathcal{M}}}{2g_{\mathcal{M}}}$ and $1 - \frac{f_{\mathcal{M}}}{2g_{\mathcal{M}}}$, respectively. Then, the `CB-FlipCloud` game can be formulated as

$$\begin{aligned}
\max_{f_{\mathcal{M}}\in\mathbb{R}_+} F_{\mathcal{D}}^{\mathcal{M}}(f_{\mathcal{M}}, g_{\mathcal{M}}|\bar{p}_{\mathcal{M}}, p_{\mathcal{M}}, q_{\mathcal{M}}, v_{\mathcal{M}}) = \max_{f_{\mathcal{M}}\in\mathbb{R}_+} \Bigg\{ & \bar{p}_{\mathcal{M}} + \min\left\{p_{\mathcal{M}}\frac{f_{\mathcal{M}}}{2g_{\mathcal{M}}}, p_{\mathcal{M}} q_{\mathcal{M}}\right\} \\
& - \psi_{\mathcal{D}}^{\mathcal{M}} f_{\mathcal{M}} - v_{\mathcal{M}}\left(q_{\mathcal{M}} - \frac{f_{\mathcal{M}}}{2g_{\mathcal{M}}}\right)\mathbf{1}_{\left\{q_{\mathcal{M}} > \frac{f_{\mathcal{M}}}{2g_{\mathcal{M}}}\right\}}\Bigg\}, \\
\min_{g_{\mathcal{M}}\in\mathbb{R}_+} F_{\mathcal{A}}^{\mathcal{M}}(f_{\mathcal{M}}, g_{\mathcal{M}}|\bar{p}_{\mathcal{M}}, p_{\mathcal{M}}, q_{\mathcal{M}}, v_{\mathcal{M}}) = \min_{g_{\mathcal{M}}\in\mathbb{R}_+} & \left\{\psi_{\mathcal{A}}^{\mathcal{M}} g_{\mathcal{M}} - u_{\mathcal{A}}^{\mathcal{M}}\left(1 - \frac{f_{\mathcal{M}}}{2g_{\mathcal{M}}}\right)\right\}.
\end{aligned}$$

The interpretations of each term in $F_{\mathcal{D}}^{\mathcal{M}}$ and $F_{\mathcal{A}}^{\mathcal{M}}$ are the same as the corresponding one in (7.13). Denote the nonzero-sum `CB-FlipCloud` security game under $\mathcal{M}$-type cloud by $\mathcal{G}_{\mathcal{M}}$, $\mathcal{M} \in \{H, L\}$, for convenience. Then, the solution concept of $\mathcal{G}_{\mathcal{M}}$ is defined as follows.

Definition 7.1 (Nash Equilibrium of $\mathcal{G}_{\mathcal{M}}$)**.** *A Nash equilibrium of the* ***`CB-FlipCloud`*** *game* $\mathcal{G}_{\mathcal{M}}$ *is a strategy profile* $(f_{\mathcal{M}}^{*}, g_{\mathcal{M}}^{*})$ *such that*

$$\begin{aligned}
F_{\mathcal{D}}^{\mathcal{M}}(f_{\mathcal{M}}^{*}, g_{\mathcal{M}}^{*}|\bar{p}_{\mathcal{M}}, p_{\mathcal{M}}, q_{\mathcal{M}}, v_{\mathcal{M}}) &= \max_{f_{\mathcal{M}}\in\mathbb{R}_+} F_{\mathcal{D}}^{\mathcal{M}}(f_{\mathcal{M}}, g_{\mathcal{M}}^{*}|\bar{p}_{\mathcal{M}}, p_{\mathcal{M}}, q_{\mathcal{M}}, v_{\mathcal{M}}), \\
F_{\mathcal{A}}^{\mathcal{M}}(f_{\mathcal{M}}^{*}, g_{\mathcal{M}}^{*}|\bar{p}_{\mathcal{M}}, p_{\mathcal{M}}, q_{\mathcal{M}}, v_{\mathcal{M}}) &= \min_{g_{\mathcal{M}}\in\mathbb{R}_+} F_{\mathcal{A}}^{\mathcal{M}}(f_{\mathcal{M}}^{*}, g_{\mathcal{M}}|\bar{p}_{\mathcal{M}}, p_{\mathcal{M}}, q_{\mathcal{M}}, v_{\mathcal{M}}).
\end{aligned}$$

game $\mathcal{G}_{\mathcal{M}}$ *is a strategy profile* $(f^*_{\mathcal{M}}, g^*_{\mathcal{M}})$ *such that*

$$f^*_{\mathcal{M}} \in \arg\max_{f_{\mathcal{M}} \in \mathbb{R}_+} F^{\mathcal{M}}_{\mathcal{D}}\left(f_{\mathcal{M}}, g^*_{\mathcal{M}} | \bar{p}_{\mathcal{M}}, p_{\mathcal{M}}, q_{\mathcal{M}}, v_{\mathcal{M}}\right), \tag{7.14}$$

$$g^*_{\mathcal{M}} \in \arg\min_{g_{\mathcal{M}} \in \mathbb{R}_+} F^{\mathcal{M}}_{\mathcal{A}}\left(f^*_{\mathcal{M}}, g_{\mathcal{M}} | \bar{p}_{\mathcal{M}}, p_{\mathcal{M}}, q_{\mathcal{M}}, v_{\mathcal{M}}\right), \tag{7.15}$$

for $\mathcal{M} \in \{H, L\}$.

Based on the Nash equilibrium of the `CB-FlipCloud` game $\mathcal{G}_{\mathcal{M}}$, we obtain

$$\pi_{\mathcal{M}}(\bar{p}_{\mathcal{M}}, p_{\mathcal{M}}, q_{\mathcal{M}}, v_{\mathcal{M}}) = F^{\mathcal{M}}_{\mathcal{D}}(f^*_{\mathcal{M}}, g^*_{\mathcal{M}} | \bar{p}_{\mathcal{M}}, p_{\mathcal{M}}, q_{\mathcal{M}}, v_{\mathcal{M}}). \tag{7.16}$$

Next, we analyze the cloud defender's strategy for a given contract $(\bar{p}, p, q, v)$. We first have the following proposition.

Proposition 7.1. *Given a contract* $(\bar{p}, p, q, v)$*, the Nash equilibrium strategy of the* ***`CB-FlipCloud`*** *game leads to* $q + \frac{g^*}{2f^*} - 1 \geq 0$ *for* $f^* \geq g^* > 0$*, and* $q - \frac{f^*}{2g^*} \geq 0$ *for* $g^* > f^* > 0$.

Proof. In the regime of $f^* \geq g^* > 0$, assume that $q + \frac{g^*}{2f^*} - 1 < 0$, then $p(1 - \frac{g^*}{2f^*}) > pq$ and $\min\{p(1 - \frac{g^*}{2f^*}), pq\} = pq$. By focusing on $F^{\mathcal{M}}_{\mathcal{D}}$ in the `CB-FlipCloud` game, there exists at least one pair (f', g') such that $f' < f^*$ and $1 - \frac{g'}{2f'} = q$. Then, $F^{\mathcal{M}}_{\mathcal{D}}(f', g' | \bar{p}, p, q, v) < F^{\mathcal{M}}_{\mathcal{D}}(f^*, g^* | \bar{p}, p, q, v)$ which indicates that (f^*, g^*) is not a `CB-FlipCloud` game equilibrium. Hence, $q + \frac{g^*}{2f^*} - 1 < 0$ does not hold. Similar analysis applies to the regime of $g^* > f^* > 0$, and we can obtain $q - \frac{f^*}{2g^*} \geq 0$. □

Proposition 7.1 indicates that the cloud will not provide better QoS than the one required in the contract to achieve more profits. Based on Proposition 7.1, we

can simplify the CB-FlipCloud game $\mathcal{G}_{\mathcal{M}}$ and obtain its Nash equilibrium solution as follows.

Theorem 7.1. *The Nash equilibria of the CB-FlipCloud game are summarized as follows:*

(i) when $\frac{\psi_{\mathcal{D}}}{v+p} < \frac{\psi_{\mathcal{A}}}{u_{\mathcal{A}}}$, *then* $f^* = \frac{u_{\mathcal{A}}}{2\psi_{\mathcal{A}}}$ and $g^* = \frac{\psi_{\mathcal{D}}}{2\psi_{\mathcal{A}}^2} \cdot \frac{u_{\mathcal{A}}^2}{v+p}$;

(ii) when $\frac{\psi_{\mathcal{D}}}{v+p} > \frac{\psi_{\mathcal{A}}}{u_{\mathcal{A}}}$, *then* $f^* = \frac{\psi_{\mathcal{A}}}{2\psi_{\mathcal{D}}^2} \cdot \frac{(v+p)^2}{u_{\mathcal{A}}}$ and $g^* = \frac{v+p}{2\psi_{\mathcal{D}}}$;

(iii) when $\frac{\psi_{\mathcal{D}}}{v+p} = \frac{\psi_{\mathcal{A}}}{u_{\mathcal{A}}}$, *then* $f^* = \frac{u_{\mathcal{A}}}{2\psi_{\mathcal{A}}}$ and $g^* = \frac{v+p}{2\psi_{\mathcal{D}}}$.

Proof. For $f \geq g > 0$, the cloud defender's problem is $\max_f \left\{\bar{p} + p(1 - \frac{g}{2f}) - \psi_{\mathcal{D}} f - v(q + \frac{g}{2f} - 1)\right\}$, which can be rewritten as $\max_f \left\{\bar{p} + (p+v)(1 - \frac{g}{2f}) - \psi_{\mathcal{D}} f - vq\right\}$. In addition, the attacker is solving $\min_g \left\{\psi_{\mathcal{A}} g - u_{\mathcal{A}} \frac{g}{2f}\right\}$. Then, the above CB-FlipCloud game is strategically equivalent to the game that the defender solves $\max_f \left\{(1 - \frac{g}{2f}) - \frac{\psi_{\mathcal{D}}}{p+v} f\right\}$, and the attacker solves $\max_g \left\{\frac{g}{2f} - \frac{\psi_{\mathcal{A}}}{u_{\mathcal{A}}} g\right\}$, which reduces the cloud security game to the form in [133] and can be solved accordingly. The analysis is similar for the case when $g > f > 0$. □

For clarity, a pictorial illustration of the obtained Nash equilibria of CB-FlipCloud game is shown in Fig. 7.4. Under the Nash equilibrium, the utility of the cloud SP can be expressed as

$$\pi(\bar{p}, p, q, v) = \bar{p} + p - \frac{u_{\mathcal{A}} \psi_{\mathcal{D}}}{\psi_{\mathcal{A}}} - v(q-1), \text{ for } \frac{\psi_{\mathcal{D}}}{v+p} < \frac{\psi_{\mathcal{A}}}{u_{\mathcal{A}}}, \tag{7.17}$$

$$\pi(\bar{p}, p, q, v) = \bar{p} - vq, \text{ for } \frac{\psi_{\mathcal{D}}}{v+p} \geq \frac{\psi_{\mathcal{A}}}{u_{\mathcal{A}}}. \tag{7.18}$$

Remark: From Proposition 7.1 and Theorem 7.1, we obtain that when $\frac{\psi_{\mathcal{D}}}{v+p} < \frac{\psi_{\mathcal{A}}}{u_{\mathcal{A}}}$, the required cloud quality q in the contract needs to satisfy $q \geq 1 - \frac{\psi_{\mathcal{D}} u_{\mathcal{A}}}{2\psi_{\mathcal{A}}(v+p)} > \frac{1}{2}$;

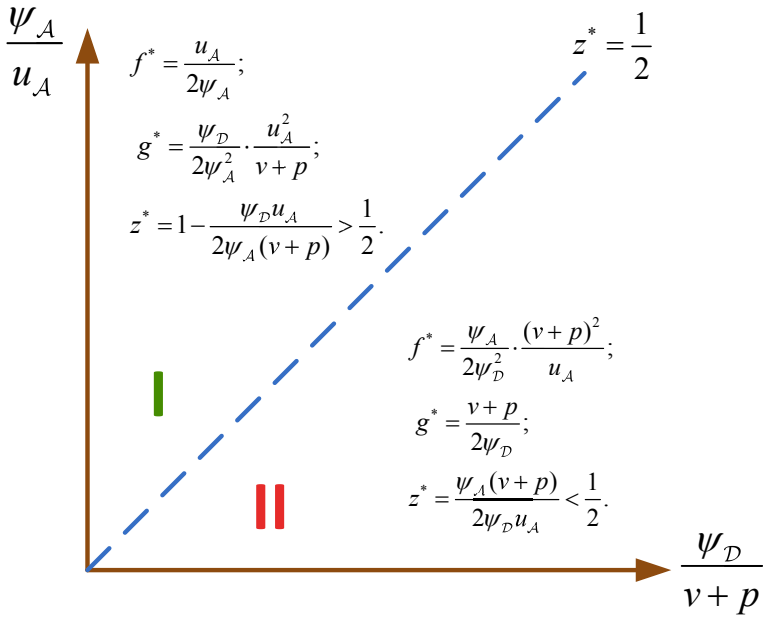


Figure 7.4: Illustration of the Nash equilibria of `CB-FlipCloud` game in terms of the relationship between $\frac{\psi_{\mathcal{D}}}{v+p}$ and $\frac{\psi_{\mathcal{A}}}{u_{\mathcal{A}}}$.

when $\frac{\psi_{\mathcal{D}}}{v+p} > \frac{\psi_{\mathcal{A}}}{u_{\mathcal{A}}}$, $q \geq \frac{\psi_{\mathcal{A}}(v+p)}{2\psi_{\mathcal{D}} u_{\mathcal{A}}}$; and when $\frac{\psi_{\mathcal{D}}}{v+p} = \frac{\psi_{\mathcal{A}}}{u_{\mathcal{A}}}$, $q \geq \frac{1}{2}$. In addition, two different regimes in Fig. 7.4 have various physical interpretations. Specifically, the contracts that result in a Nash equilibrium of `CB-FlipCloud` game in regime I correspond to the devices receiving a higher cloud QoS and hence a better physical system performance. Further, the cloud QoS in regime I means that more than half of the total packets are successfully transmitted over the cloud, since the proportion of time that the cloud is secure is $z^* > \frac{1}{2}$. In contrast, the security service in regime II with $z^* < \frac{1}{2}$ corresponds to the scenario that more than half of packets are lost during the transmission resulting in a worse cloud QoS than that in regime I.

The difference between the H-type and L-type cloud's profit under a certain contract is critical in designing the optimal contracts in Section 7.5, and we define it as follows.

Definition 7.2. *For a given contract* $(\bar{p}, p, q, v)$*, the benefit of being an* H*-type cloud over an* L*-type cloud is defined as* $\delta := \pi_H(\bar{p}, p, q, v) - \pi_L(\bar{p}, p, q, v)$.

Note that δ is not a function of contract terms, since $\bar{p}, p, q, v$ are not coupled with other parameters of the cloud attacker and defender as seen from equations (7.17) and (7.18). To facilitate the optimal contract design, without loss of generality, we make the following assumption on the parameters at cyber layer.

Assumption 7.2. *Several cyber layer parameters satisfy* $\frac{\psi_{\mathcal{D}}^H}{\psi_{\mathcal{A}}^H} < \frac{\psi_{\mathcal{D}}^L}{\psi_{\mathcal{A}}^L}$ and $u_{\mathcal{A}}^H = u_{\mathcal{A}}^L$.

In Assumption 7.2, the inequality $\frac{\psi_{\mathcal{D}}^H}{\psi_{\mathcal{A}}^H} < \frac{\psi_{\mathcal{D}}^L}{\psi_{\mathcal{A}}^L}$ indicates that the H-type cloud is more resistant to malicious attacks, and the equality $u_{\mathcal{A}}^H = u_{\mathcal{A}}^L$ represents that the unit payoff of compromising two types of cloud are the same. Note that Assumption 7.2 is *not strict*, and we use it to determine the sign of δ. Based on (7.17), (7.18) and Assumption 7.2, we obtain $\delta \geq 0$. Thus, the profit of the H-type cloud is no less than the L-type cloud for a given contract $(\bar{p}, p, q, v)$.

Remark: The parameter δ is not necessary non-negative, and Assumption 7.2 is not strict. To be practical, we choose δ to be non-negative. The results obtained in this section can be easily extended to the case with negative values of δ.

7.4.2 Physical System Analysis

The cloud defense strategy at the cyber layer and the contract design of device are interdependent. At the physical layer, one critical problem is the stability of the device. First, we present the following lemma.

Lemma 7.1 (Lemma 1, [85])**.** *Let* $(A, \sqrt{Q})$ *be observable and* B *invertible. Then, under the cloud quality* z*, the condition ensuring the mean-square stability of the*

physical device with the optimal control in Theorem 7.2 is

$$\zeta := \max |\lambda(A)| < \frac{1}{\sqrt{1-z}}, \tag{7.19}$$

where ζ and $\lambda(A)$ denote the spectral radius and the eigenvalue of system matrix A, respectively.

We choose the utility function of the physical system as

$$U(z) = -J(\Pi^*|z), \tag{7.20}$$

where $J(\Pi^*|z)$ is the optimal control cost under z.

Remark: The physical system is unstable when (7.19) is not satisfied, and $U(z) \to -\infty$ under which the contract design problem is infeasible. Hence, the contract should be designed in a way such that if it is picked by the cloud SP, the provided cloud QoS can stabilize the physical system.

Obtaining the optimal cost $J(\Pi^*|z)$ for the device is critical. We state the solution to the optimal controller design over insecure cloud as follows.

Theorem 7.2 (Theorem 3, [85]). *For the physical system with insecure cloud in IoCT, the optimal control law is*

$$u_k^* = G_k \hat{x}_k, \tag{7.21}$$

where the matrix $G_k = -(R + B^T K_{k+1} B)^{-1} B^T K_{k+1} A$, with K_k recursively given

by the Riccati equation

$$P_k = zA^T B(R + B^T K_{k+1} B)^{-1} B^T K_{k+1} A,$$
$$K_k = A^T K_{k+1} A - P_k + Q.$$

The estimator $\hat{x}_k$ *takes the form*

$$\hat{x}_k = \begin{cases} A\hat{x}_{k-1} + \alpha_{k-1} B u_{k-1}, & \beta_k = 0, \\ x_k, & \beta_k = 1. \end{cases}$$

In addition, when $k \to \infty$, $\lim_{k\to\infty} G_k = G$, *and the controller takes the form of* $u_k = G\hat{x}_k$ *and*

$$\begin{aligned} G =& -(R + B^T K B)^{-1} B^T K A, \\ K =& A^T K A + Q - zA^T K B(R + B^T K B)^{-1} B^T K A. \end{aligned} \tag{7.22}$$

Note that the parameter K in (7.22) corresponds to the cloud quality z, and the controller is computed using services in the cloud. Under condition (7.19), the system is stable in mean square sense at the steady state as $k \to \infty$. Therefore, the average physical system cost in an infinite horizon as shown in (7.3) will converge asymptotically to the expected system cost at the steady state (see Chapter 7, [21]). Based on (7.3) and (7.21), we obtain

$$\begin{aligned} J(\Pi^*|z) &= \limsup_{N\to\infty} \frac{1}{N} \mathbb{E}\left\{ \sum_{k=0}^{N-1} \left(x_k^T Q x_k + z u_k^T R u_k \right) \right\} \\ &= \mathbb{E}\{ x_{N-1}^T Q x_{N-1} + z u_{N-1}^T R u_{N-1} \} \\ &= \mathbb{E}\{ x_{N-1}^T Q x_{N-1} + z \hat{x}_{N-1}^T G^T R G \hat{x}_{N-1} \}. \end{aligned} \tag{7.23}$$

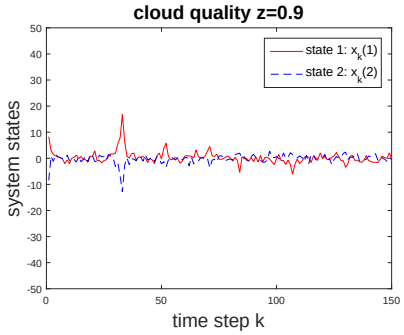
The relationship between z and $J(\Pi^*|z)$ is critical for the contract design. Specifically, we have the following lemma.

Lemma 7.2. *Under the condition* $\zeta < \frac{1}{\sqrt{1-z}}$*, the cost* $J(\Pi^*|z)$ *of the physical system is monotonically decreasing with the increase of cloud quality* z*.*

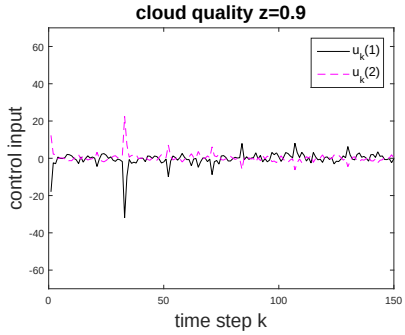
Remark: Lemma 7.2 can be interpreted as follows. With smaller z, i.e., the probability of loss of information over the cloud is large, then the physical system states and the control inputs will encounter large deviations from the nominal ones frequently. Therefore, the control cost $J(\Pi^*|z)$ increases. The following example is used to corroborate the monotonicity of $J(\Pi^*|z)$ with respect to z.

Example: The physical system matrices are given by $A = \begin{bmatrix} 1.25 & -1.3 \\ -1 & 0.5 \end{bmatrix}$, $B = C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Then the spectral radius of matrix A is equal to $\zeta = 2.08$. From Lemma 7.1, the worst-case cloud quality is $z = 0.77$ to stabilize the system. In addition, the exogenous disturbance is with zero mean and unit variance. By designing the optimal controller as in Theorem 7.2, Fig. 7.5 shows the system performance under various cloud qualities with an initial system state $x_0 = [10, -10]^T$. The results show that a better cloud quality leads to a lower system cost which corroborates Lemma 7.2.

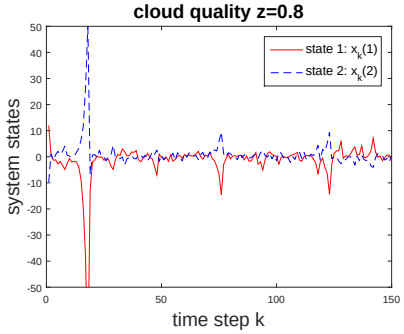
In the previous works [56, 85], the cyber security measurement z is fixed, and the physical systems design the optimal control strategy based on z. In our work, the physical layer plays an active role in the cloud-enabled IoCT and transfers the risks to the cyber layer by adopting a contract design approach to enable an on-demand service provision of security.



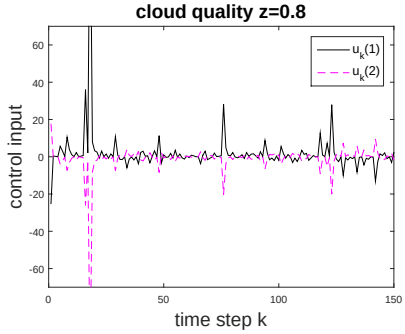
(a) system state ($z = 0.9$)



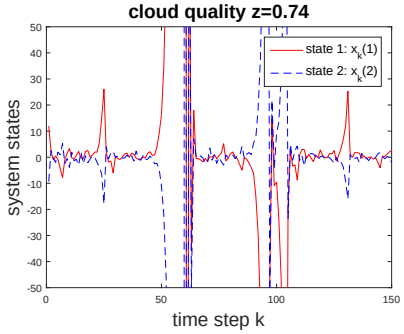
(b) control input ($z = 0.9$)



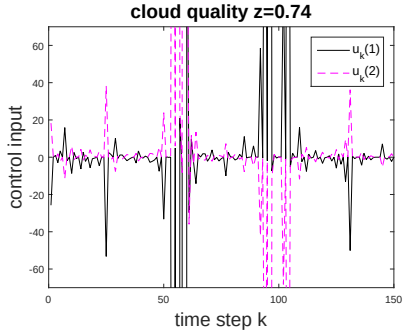
(c) system state ($z = 0.8$)



(d) control input ($z = 0.8$)



(e) system state ($z = 0.74$)



(f) control input ($z = 0.74$)

Figure 7.5: (a), (c) and (e) show the system states under the cloud quality $z = 0.9$, 0.8 and 0.74, respectively. (b), (d) and (f) are the corresponding control inputs. The physical system under $z = 0.74$ is unstable since $z < 0.77$. The results corroborate that higher cloud quality yields a better system performance.

7.5 Optimal Contracts Design under Asymmetric Information

We have analyzed the `CB-FlipCloud` game at the cyber layer and the optimal control of the physical system over insecure cloud in Section 7.4. In this section, we design the optimal H-type and L-type contracts for the device under the asymmetric information in both regimes shown in Fig. 7.4.

7.5.1 Optimal Contracts Design over Regime I

In regime I, the devices require a cloud QoS that more than half of the total packets are successfully transmitted over the cloud to stabilize the system. To design optimal contracts over regime I, we first simplify the constrained contract design problem formulated in Section 7.3.3 as follows.

Proposition 7.2. *The CDP in Section 7.3.3 is equivalent to*

$$\begin{aligned}
\text{CDP}': \quad & \min_{(\bar{p}_H, p_H, q_H, v_H)} Q_H(\bar{p}_H, p_H, q_H, v_H) + \min_{(\bar{p}_L, p_L, q_L, v_L)} Q_L(\bar{p}_L, p_L, q_L, v_L) \\
\text{s.t.} \quad & p_H > 0, \ p_L > 0, \\
& q_{H,\min} \leq q_H \leq q_{H,\max} < 1, \\
& q_{L,\min} \leq q_L \leq q_{L,\max} < 1,
\end{aligned}$$

where $Q_H(\bar{p}_H, p_H, q_H, v_H) := \sigma(\delta + \epsilon_L + \psi_{\mathcal{D}}^H f_H^* + \phi_H \frac{U^o - U(z_H^*)}{|U^o|})$ *and* $Q_L(\bar{p}_L, p_L, q_L, v_L) := (1-\sigma)(\epsilon_L + \psi_{\mathcal{D}}^L f_L^* + \phi_L \frac{U^o - U(z_L^*)}{|U^o|})$.

Proof. Based on (7.16), the objective function in CDP can be rewritten as

$$\min_{(\bar{p}_H,p_H,q_H,v_H),\ (\bar{p}_L,p_L,q_L,v_L)} \sigma\left(\pi_H(\bar{p}_H,p_H,q_H,v_H)+\psi_{\mathcal{D}}^{H}f_H^*+\phi_H\frac{U^o-U(z_H^*)}{|U^o|}\right)$$
$$+(1-\sigma)\left(\pi_L(\bar{p}_L,p_L,q_L,v_L)+\psi_{\mathcal{D}}^{L}f_L^*+\phi_L\frac{U^o-U(z_L^*)}{|U^o|}\right). \tag{7.24}$$

Furthermore, based on Definition 7.2, we have

$$\begin{aligned}\pi_H(\bar{p}_L,p_L,q_L,v_L)&=\pi_L(\bar{p}_L,p_L,q_L,v_L)+\delta,\\ \pi_L(\bar{p}_H,p_H,q_H,v_H)&=\pi_H(\bar{p}_H,p_H,q_H,v_H)-\delta.\end{aligned} \tag{7.25}$$

Then, plugging (7.25) into the IC constraints (7.6a) and (7.6b) yields

$$\begin{aligned}&\delta\geq\pi_H(\bar{p}_H,p_H,q_H,v_H)-\pi_L(\bar{p}_L,p_L,q_L,v_L)\geq\delta,\\ \Rightarrow\ &\pi_H(\bar{p}_H,p_H,q_H,v_H)-\pi_L(\bar{p}_L,p_L,q_L,v_L)=\delta.\end{aligned} \tag{7.26}$$

The constraints (7.6a)-(7.6d) can be equivalently captured by (7.26) together with $\pi_L(\bar{p}_L,p_L,q_L,v_L)\geq\epsilon_L$ since $\delta\geq 0$. On the other hand, notice that for given $p_{\mathcal{M}}$ and $v_{\mathcal{M}}$, the objective function (7.24) is minimized if $\pi_{\mathcal{M}}(\bar{p}_{\mathcal{M}},p_{\mathcal{M}},q_{\mathcal{M}},v_{\mathcal{M}})$ achieves the minimum. The underlying interpretation is that a lower utility of the cloud leads to a higher cloud QoS which is beneficial for the physical system. Therefore, based on (7.26) and the IR constraint $\pi_L(\bar{p}_L,p_L,q_L,v_L)\geq\epsilon_L$, we obtain $\pi_H(\bar{p}_H,p_H,q_H,v_H)-\pi_L(p_L,q_L,v_L)=\delta$ and $\pi_L(\bar{p}_L,p_L,q_L,v_L)=\epsilon_L$. Therefore, the constraints (7.6a)-(7.6d) further become

$$\pi_H(\bar{p}_H,p_H,q_H,v_H)=\delta+\epsilon_L, \tag{7.27}$$

$$\pi_L(\bar{p}_L,p_L,q_L,v_L)=\epsilon_L, \tag{7.28}$$

which result in CDP$'$. □

Remark: Note that in CDP$'$, IC and IR constraints are incorporated into the objective function. In addition, two separate minimization terms in CDP$'$ are *decoupled* in the decision variables, and thus can be solved independently.

First, we focus on $\min_{(\bar{p}_H,p_H,q_H,v_H)} Q_H(\bar{p}_H,p_H,q_H,v_H)$ in CDP$'$. In regime I, $f_H^* = \frac{u_{\mathcal{A}}^H}{2\psi_{\mathcal{A}}^H}$ and $z_H^* = 1 - \frac{\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}{2\psi_{\mathcal{A}}^H(v_H+p_H)}$. In addition, three underlying constraints are $\frac{\psi_{\mathcal{D}}^H}{v_H+p_H} < \frac{\psi_{\mathcal{A}}^H}{u_{\mathcal{A}}^H}$, $q_H \geq z_H^*$ and $\zeta < \sqrt{\frac{2\psi_{\mathcal{A}}^H(v_H+p_H)}{\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}}$. Then, we obtain the following lemma.

Lemma 7.3. *The H-type contract design in regime I is only dependent on the system performance at physical layer, and a larger value of $v_H + p_H$ leads to a better contract.*

Proof. Notice that $\underset{(\bar{p}_H,p_H,q_H,v_H)}{\arg\min}\ Q_H(\bar{p}_H,p_H,q_H,v_H) \iff \underset{(\bar{p}_H,p_H,q_H,v_H)}{\arg\max}\ U(z_H^*)$, since $f_H^* = \frac{u_{\mathcal{A}}^H}{2\psi_{\mathcal{A}}^H}$ is irrelevant to the contract parameters. Thus, the contract design only relates to the physical system performance. In addition, Lemma 7.2 indicates that $U(z_H^*)$ is monotonically increasing with respect to z_H^*. Since $z_H^* = 1 - \frac{\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}{2\psi_{\mathcal{A}}^H(v_H+p_H)}$, larger $v_H + p_H$ yields a better contract. □

Next, through analyzing the impact of contract on the physical systems, we obtain the optimal H-type contract in regime I as follows.

Theorem 7.3. *Under Assumptions 7.1 and 7.2, the optimal H-type contract*

$(\bar{p}_H, p_H, q_H, v_H)$ in regime I is designed as

$$\bar{p}_H = 0, \tag{7.29}$$

$$q_H = q_{H,\max}, \tag{7.30}$$

$$v_H = \min\left\{v_{H,\max}, \frac{\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}{2\psi_{\mathcal{A}}^H(1-q_{H,\max})} - p_H\right\}, \tag{7.31}$$

$$p_H = \frac{u_{\mathcal{A}}^L \psi_{\mathcal{D}}^L}{\psi_{\mathcal{A}}^L} + (q_{H,\max}-1)v_H + \epsilon_L. \tag{7.32}$$

Proof. From (7.27), we obtain $\pi_H(\bar{p}_H, p_H, q_H, v_H) = \bar{p}_H + p_H - \frac{u_{\mathcal{A}}^H \psi_{\mathcal{D}}^H}{\psi_{\mathcal{A}}^H} - v_H(q_H - 1) = \delta + \epsilon_L = \frac{u_{\mathcal{A}}^L \psi_{\mathcal{D}}^L}{\psi_{\mathcal{A}}^L} - \frac{u_{\mathcal{A}}^H \psi_{\mathcal{D}}^H}{\psi_{\mathcal{A}}^H} + \epsilon_L$, which yields $\bar{p}_H + p_H - v_H(q_H - 1) = \frac{u_{\mathcal{A}}^L \psi_{\mathcal{D}}^L}{\psi_{\mathcal{A}}^L} + \epsilon_L$. Therefore, $p_H + v_H = \frac{u_{\mathcal{A}}^L \psi_{\mathcal{D}}^L}{\psi_{\mathcal{A}}^L} + v_H q_H - \bar{p}_H + \epsilon_L$. To maximize $p_H + v_H$, we obtain $\bar{p}_H = 0$ and $q_H = q_{H,\max}$. We can also verify $q_H = q_{H,\max}$ from the constraint $q_H \geq z_H^*$. In addition, $q_H \geq 1 - \frac{\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}{2\psi_{\mathcal{A}}^H(v_H + p_H)}$ yields $v_H \leq \frac{\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}{2\psi_{\mathcal{A}}^H(1-q_H)} - p_H$. Therefore, together with the bound, the penalty parameter v_H takes $v_H = \min\{v_{H,\max}, \frac{\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}{2\psi_{\mathcal{A}}^H(1-q_{H,\max})} - p_H\}$, and then the unit payment p_H is equal to $p_H = \frac{u_{\mathcal{A}}^L \psi_{\mathcal{D}}^L}{\psi_{\mathcal{A}}^L} + (q_{H,\max} - 1)v_H + \epsilon_L$. □

Note that when $v_H + p_H \leq \frac{\zeta^2 \psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}{2\psi_{\mathcal{A}}^H}$, then *no contract* is placed to the H-type cloud, since the provided cloud QoS cannot stabilize the physical device.

It can be seen that problem $\min_{(\bar{p}_L, p_L, q_L, v_L)} Q_L(\bar{p}_L, p_L, q_L, v_L)$ in CDP′ is equivalent the problem $\max_{(\bar{p}_L, p_L, q_L, v_L)} U(z_L^*)$. Based on (7.28), we obtain $p_L + v_L = \frac{u_{\mathcal{A}}^L \psi_{\mathcal{D}}^L}{\psi_{\mathcal{A}}^L} + v_L q_L - \bar{p}_L + \epsilon_L$. Then, the L-type contract $(\bar{p}_L, p_L, q_L, v_L)$ immediately follows with a similar analysis in Theorem 7.3.

Theorem 7.4. *Under Assumptions 7.1 and 7.2, the optimal L-type contract*

$(\bar{p}_L, p_L, q_L, v_L)$ in regime I is given by

$$\begin{aligned}
\bar{p}_L &= 0, \\
q_L &= q_{L,\max}, \\
v_L &= \min\left\{v_{L,\max}, \frac{\psi_{\mathcal{D}}^L u_{\mathcal{A}}^L}{2\psi_{\mathcal{A}}^L(1-q_{L,\max})} - p_L\right\}, \\
p_L &= \frac{u_{\mathcal{A}}^L \psi_{\mathcal{D}}^L}{\psi_{\mathcal{A}}^L} + (q_{L,\max}-1)v_L + \epsilon_L.
\end{aligned} \tag{7.33}$$

Similarly, when the optimal contract in Theorem 7.4 satisfies $v_L + p_L \leq \frac{\zeta^2 \psi_{\mathcal{D}}^L u_{\mathcal{A}}^L}{2\psi_{\mathcal{A}}^L}$, then the device will not place the contract due to the instability of the physical system.

Remark: We summarize the features of the optimal H-type and L-type contracts design in regime I as follows. First, the complex contract design is simplified to a physical system cost minimization problem. Second, *no contract* will be offered to the cloud SP if the resulting QoS cannot stabilize the physical system. One possible reason is that the unit defending cost of cloud SP is relatively large, and thus the cloud defender prefers not to spend enough effort on protecting the cloud resources. Third, the transfer payment is equal to zero, and the requested cloud quality achieves the upper bound. Fourth, the payoffs of the H-type and L-type clouds are $\delta + \epsilon_L$ and ϵ_L, respectively, which are constants in this scenario.

7.5.2 Optimal Contracts Design over Regime II

In regime II, the physical system can be stabilized even under the condition that half of packets are lost during the transmission, and this characteristic indicates that the physical system is quite robust inherently. Via a similar analysis as in

regime I, the H-type and L-type optimal contracts over regime II can be designed independently. We first investigate the H-type contract design through solving $\min_{(\bar{p}_H,p_H,q_H,v_H)} Q_H(\bar{p}_H,p_H,q_H,v_H)$, where $f_H^* = \frac{\psi_{\mathcal{A}}^H(v_H+p_H)^2}{2(\psi_{\mathcal{D}}^H)^2 u_{\mathcal{A}}^H}$ and $z_H^* = \frac{\psi_{\mathcal{A}}^H(v_H+p_H)}{2\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}$. In addition, three underlying constraints are $\frac{\psi_{\mathcal{D}}^H}{v_H+p_H} \geq \frac{\psi_{\mathcal{A}}^H}{u_{\mathcal{A}}^H}$, $q_H \geq z_H^*$ and $\zeta \leq \sqrt{\frac{2\psi_{\mathcal{A}}^H u_{\mathcal{A}}^H}{2\psi_{\mathcal{A}}^H u_{\mathcal{A}}^H - \psi_{\mathcal{D}}^H(v_H+p_H)}}$.

On one hand, $f_H^* = \frac{\psi_{\mathcal{A}}^H(v_H+p_H)^2}{2(\psi_{\mathcal{D}}^H)^2 u_{\mathcal{A}}^H}$ indicates that small $v_H + p_H$ is desirable to minimize the objective. On the other hand, $U(z_H^*)$ is monotonically increasing with respect to z_H^*. Since $z_H^* = \frac{\psi_{\mathcal{A}}^H(v_H+p_H)}{2\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}$, then larger value of $v_H + p_H$ leads to a smaller objective value. Thus, we need to consider the tradeoff between two opposite terms in the objective. The optimization problem for the H-type contract design in regime II is

$$\begin{aligned}
\min_{(\bar{p}_H,p_H,q_H,v_H)} \quad & \frac{\psi_{\mathcal{A}}^H(v_H+p_H)^2}{2\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H} + \phi_H \frac{U^o - U(z_H^*)}{|U^o|} \\
\text{s.t.} \quad & p_H > 0,\ q_{H,\min} \leq q_H \leq q_{H,\max} < 1, \\
& q_H \geq z_H^*,\ z_H^* \leq \frac{1}{2},\ \frac{\psi_{\mathcal{D}}^H}{v_H+p_H} \geq \frac{\psi_{\mathcal{A}}^H}{u_{\mathcal{A}}^H}, \\
& \zeta \leq \sqrt{\frac{2\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}{2\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H - \psi_{\mathcal{A}}^H(v_H+p_H)}}.
\end{aligned}$$

Recall that ζ is a constant smaller than $\frac{1}{2}$. In addition, note that for the above optimization problem, the same value of $v_H + p_H$ leads to the same objective only if the constraints are satisfied. Thus, the optimal contract in regime II is not unique. We first focus on obtaining the optimal $v_H + p_H$.

Note that the constraints related to v_H+p_H can be captured by $\frac{\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}{\psi_{\mathcal{A}}^H}\left(1-\frac{1}{\zeta^2}\right) \leq v_H + p_H \leq \frac{\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}{\psi_{\mathcal{A}}^H}$. Next, define $T(x) := \frac{\psi_{\mathcal{A}}^H x^2}{2\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H} + \phi_H \frac{U^o - U(z_H^*)}{|U^o|}$, where $z_H^* = \frac{\psi_{\mathcal{A}}^H x}{2\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}$. In addition, the performance function $U(z_H^*)$ is approximated by an analytical function

Algorithm 7.1

1: Initialize feasible $x^{(0)} \in [\underline{x}, \bar{x}]$, ϵ, $w \in [0, 0.1]$, $n = 0$, $T(x^{(-1)}) = T(x^{(0)}) + 2\epsilon$
2: **while** $|T(x^{(n)}) - T(x^{(n-1)})| > \epsilon$ **do**
3: $\quad x^{(n+1)} = x^{(n)} - w \left(\frac{dT(x^{(n)})}{dx^{(n)}} \right)^{-1} T(x^{(n)})$
4: $\quad x^* = x^{(n+1)}$
5: $\quad$ **if** $x^{(n+1)} \in [\underline{x}, \bar{x}]$ **then**
6: $\quad\quad$ go to step 11
7: $\quad$ **else**
8: $\quad\quad$ project $x^{(n+1)}$ to the nearest feasible bound as x^*
9: $\quad\quad$ go to step 13
10: $\quad$ **end if**
11: $\quad n = n + 1$
12: **end while**
13: **return** x^*

according to the specific characteristics of the device. Then, $T(x)$ is continuously differentiable, and the gradient descent method can be used to find the optimal x^* that minimizes $T(x)$ over $x \in \left[\frac{\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}{\psi_{\mathcal{A}}^H} \left(1 - \frac{1}{\zeta^2} \right), \frac{\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}{\psi_{\mathcal{A}}^H} \right]$. Denote the feasible interval by $x \in [\underline{x}, \bar{x}]$ for convenience, and the iterative method to find the optimal x^* is summarized in Algorithm 7.1.

Based on Algorithm 7.1, the designed optimal H-type contract in regime II is summarized in the following theorem.

Theorem 7.5. *Under Assumptions 7.1 and 7.2, an optimal H-type contract $(\bar{p}_H, p_H, q_H, v_H)$ in regime II is*

$$\bar{p}_H = v_H q_H + \frac{u_{\mathcal{A}}^L \psi_{\mathcal{D}}^L}{\psi_{\mathcal{A}}^L} - \frac{u_{\mathcal{A}}^H \psi_{\mathcal{D}}^H}{\psi_{\mathcal{A}}^H} + \epsilon_L, \tag{7.34}$$

$$q_H = \max \left\{ q_{H,\min}, \frac{\psi_{\mathcal{A}}^H x^*}{2\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H} \right\}, \tag{7.35}$$

$$v_H = \min \left\{ x^*, v_{H,\max} \right\}, \tag{7.36}$$

$$p_H = x^* - v_H, \tag{7.37}$$

where x^* is obtained through Algorithm 7.1.

Proof. The outcome $x^* = p_H + v_H$ of Algorithm 7.1 yields an optimal value of the contract design problem in regime II. To design an optimal contract, we choose the maximum possible unit penalty as $v_H = \min\{x^*, v_{H,\max}\}$. Based on x^*, we obtain $p_H = x^* - v_H$. The least required cloud QoS in regime II is $q_H = \max\{q_{H,\min}, \frac{\psi_{\mathcal{A}}^H x^*}{2\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}\}$. In addition, based on $\pi_H(\bar{p}_H, p_H, q_H, v_H) = \bar{p}_H + p_H \frac{\psi_{\mathcal{A}}^H(v_H+p_H)}{2\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H} - \frac{\psi_{\mathcal{A}}^H(v_H+p_H)^2}{2\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H} - v_H(q_H - \frac{\psi_{\mathcal{A}}^H(v_H+p_H)}{2\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}) = \bar{p}_H - v_H q_H + \frac{\psi_{\mathcal{A}}^H(v_H+p_H)}{2\psi_{\mathcal{D}}^H u_{\mathcal{A}}^H}(p_H - (v_H + p_H) + v_H) = \bar{p}_H - v_H q_H$ and $\pi_H(\bar{p}_H, p_H, q_H, v_H) = \frac{u_{\mathcal{A}}^L \psi_{\mathcal{D}}^L}{\psi_{\mathcal{A}}^L} - \frac{u_{\mathcal{A}}^H \psi_{\mathcal{D}}^H}{\psi_{\mathcal{A}}^H} + \epsilon_L$, we obtain the transfer payment as $\bar{p}_H = v_H q_H + \frac{u_{\mathcal{A}}^L \psi_{\mathcal{D}}^L}{\psi_{\mathcal{A}}^L} - \frac{u_{\mathcal{A}}^H \psi_{\mathcal{D}}^H}{\psi_{\mathcal{A}}^H} + \epsilon_L$. □

To design the L-type contract in regime II, the function $T(x)$ in Algorithm 7.1 admits the form $T(x) := \frac{\psi_{\mathcal{A}}^L x^2}{2\psi_{\mathcal{D}}^L u_{\mathcal{A}}^L} + \phi_L \frac{U^o - U(z_L^*)}{|U^o|}$, where $z_L^* = \frac{\psi_{\mathcal{A}}^L x}{2\psi_{\mathcal{D}}^L u_{\mathcal{A}}^L}$ and $x \in \left[\frac{\psi_{\mathcal{D}}^L u_{\mathcal{A}}^L}{\psi_{\mathcal{A}}^L}\left(1 - \frac{1}{\zeta^2}\right), \frac{\psi_{\mathcal{D}}^L u_{\mathcal{A}}^L}{\psi_{\mathcal{A}}^L}\right]$. Through similar analysis as that in Theorem 7.5, we obtain the optimal L-type contract over regime II as follows.

Theorem 7.6. *Under Assumptions 7.1 and 7.2, an optimal L-type contract $(\bar{p}_L, p_L, q_L, v_L)$ in regime II is*

$$\begin{aligned}
\bar{p}_L &= v_L q_L + \epsilon_L, \\
q_L &= \max\left\{q_{L,\min}, \frac{\psi_{\mathcal{A}}^L x^*}{2\psi_{\mathcal{D}}^L u_{\mathcal{A}}^L}\right\}, \\
v_L &= \min\left\{x^*, v_{L,\max}\right\}, \\
p_L &= x^* - v_L,
\end{aligned} \tag{7.38}$$

where x^* is obtained through Algorithm 7.1.

Remark: The designed optimal contracts in Theorems 7.5 and 7.6 incorporate the nature that the device only requires the level of cloud QoS that can stabilize

the system. It is reasonable since the devices that propose contracts in regime II are less critical as those making contracts over regime I who always request the best possible cloud QoS. Different from the contracts in regime I, the transfer payment in the contracts over regime II is not zero, because the physical system aims to propose less unit payment while with a larger penalty in the contract. In addition, this type of contract, i.e., with a high transfer payment, also aligns with the fact that the cloud SP with worse QoS tends to receive payment ahead of time before delivering services.

7.6 Case Studies

In this section, we illustrate the designed optimal contracts via case studies. Specifically, we investigate the cloud security as a service for heterogeneous IoCTs with an application to smart home design.

7.6.1 Smart Home Framework

A smart home (SH) is an intelligent system that incorporates advanced automation technologies to provide inhabitants with sophisticated monitoring and control over the building function [77]. A general smart home illustration is shown in Fig. 7.6 which includes various physical systems and the cloud. Therefore, the SH can be seen as a small-scale cloud-enabled IoCT. Without loss of generality, we mainly focus on three devices: a smart lighting system, a heating, ventilation and air conditioning (HVAC) system and a pacemaker (Fig. 7.6). The smart lighting system is designed to be energy-saving while guaranteeing the necessary brightness of the room [104]. The HVAC system in the smart home controls the

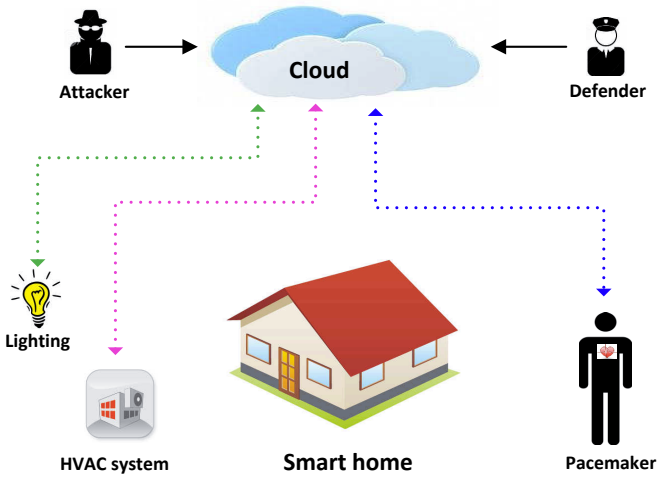


Figure 7.6: Cloud security as a service in SH design. The cloud-enabled SH includes various physical systems and cloud resources. The SH owner makes a contract with the cloud SP to enhance the system performance.

room temperature by optimally adjusting the air mass flow through the ducts into the room [102]. The pacemaker device is to maintain a normal heart rhythm of the patient through a controlled electrical pulse to the heart [51]. The various importance of each system and their different unit control cost can be captured by the matrices Q and R in the performance objective (7.3).

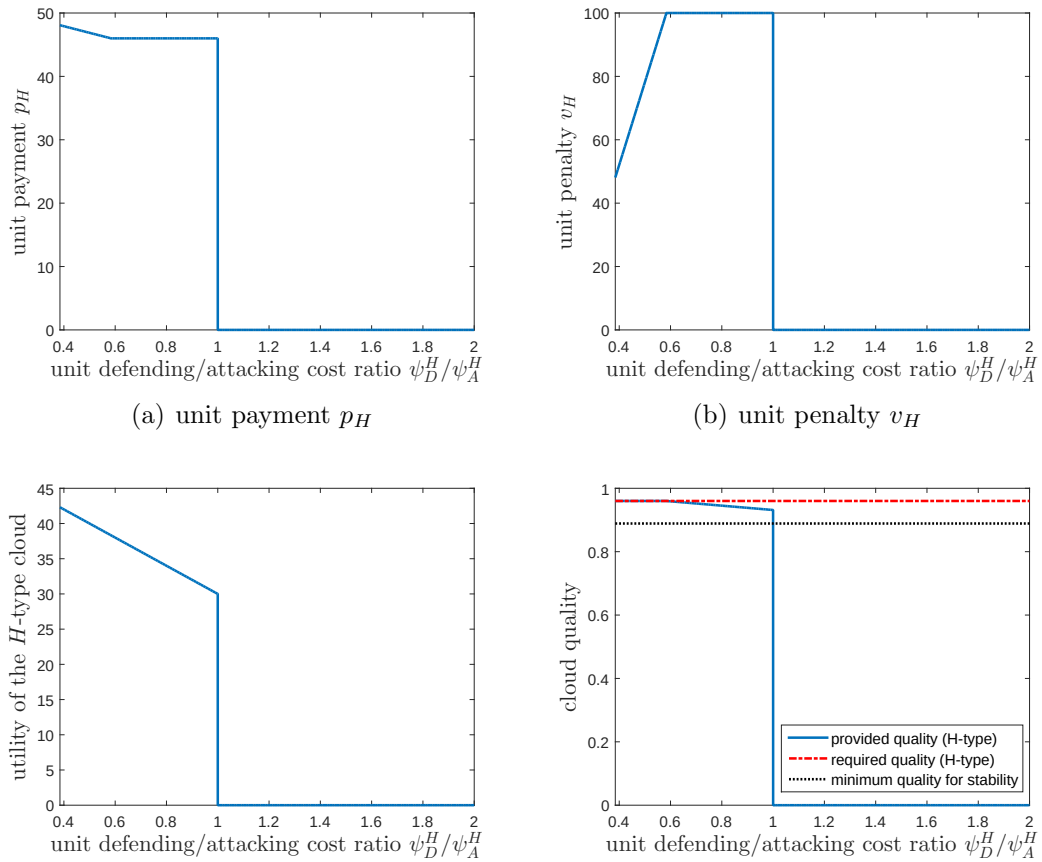
7.6.2 Regime I Study: Optimal Contracts for Pacemaker

We design the optimal contracts for the pacemaker device in this section. The system states include the heart rhythm and its adjustment speed [51, 123]. The objective is to maintain the patient's heart rhythm at a nominal value with small bounded state deviations. Due to the significant importance of the device, the required cloud quality should be high. Through the eigenvalue analysis of the adopted system model, the minimum cloud QoS is $z = 0.889$, above which the state deviations are within an acceptable interval. Since $z > 0.5$, the contract design for

pacemaker naturally falls into the regime I in Fig. 7.4.

Several other parameters in the contract design are summarized as follows: $\psi_{\mathcal{A}}^{H} = \$10\text{K}$, $\psi_{\mathcal{A}}^{L} = \$4\text{K}$, $u_{\mathcal{A}}^{H} = u_{\mathcal{A}}^{L} = \$20\text{K}$, $v_{H,\max} = \$100\text{K}$, $v_{L,\max} = \$90\text{K}$, $\epsilon_L = \$10\text{K}$, $\epsilon_H = \$30\text{K}$, $q_{L,\min} = 0.89$, $q_{L,\max} = 0.91$, $q_{H,\min} = 0.89$ and $q_{H,\max} = 0.96$. Note that the cloud defense and attack costs include the expenditures on facilities and labors, etc. The minimum profit for delivering the service varies with cloud service providers, e.g., Google and Microsoft [70]. In addition, the H-type and L-type contracts refer to different levels of provided cloud security services.

First, we illustrate the case of H-type contract design. Specifically, the unit defending cost of the L-type cloud is chosen as $\psi_{\mathcal{D}}^{L} = \$8\text{K}$, and we design the H-type contract in the reasonable regime of $\psi_{\mathcal{D}}^{H}$ that satisfies the conditions in Assumption 7.2. The corresponding results are shown in Fig. 7.7. In the contractable regime of Fig. 7.7(a), with the increasing of $\psi_{\mathcal{D}}^{H}$, the unit payment p_H decreases first and then keeps as a constant. In contrast, in Fig. 7.7(b), the unit penalty v_H increases first and then becomes unchanged. The unchanging regime of $\psi_{\mathcal{D}}^{H}$ is due to the fact that v_H achieves the maximum. The utility of the H-type cloud is decreasing as the defending cost becomes larger as depicted in Fig. 7.7(c), and this property can be verified by equation (7.27). Note that when $\psi_{\mathcal{D}}^{H}/\psi_{\mathcal{A}}^{H} \geq 1.01$, no H-type contract is accepted by the cloud since the cloud's minimum utility ϵ_H cannot be met by providing the service. The required and real provided cloud quality are presented in Fig. 7.7(d). As shown in Proposition 7.1, the provided cloud QoS z_H will never be greater than the required one q_H. In addition, in the middle regime, z_H decreases as the defending cost increases. The reason is that the penalty v_H and the payment p_H are constants, and then the cloud SP can earn more profit by spending less effort on protecting the cloud resources which results in worse QoS.



(a) unit payment p_H

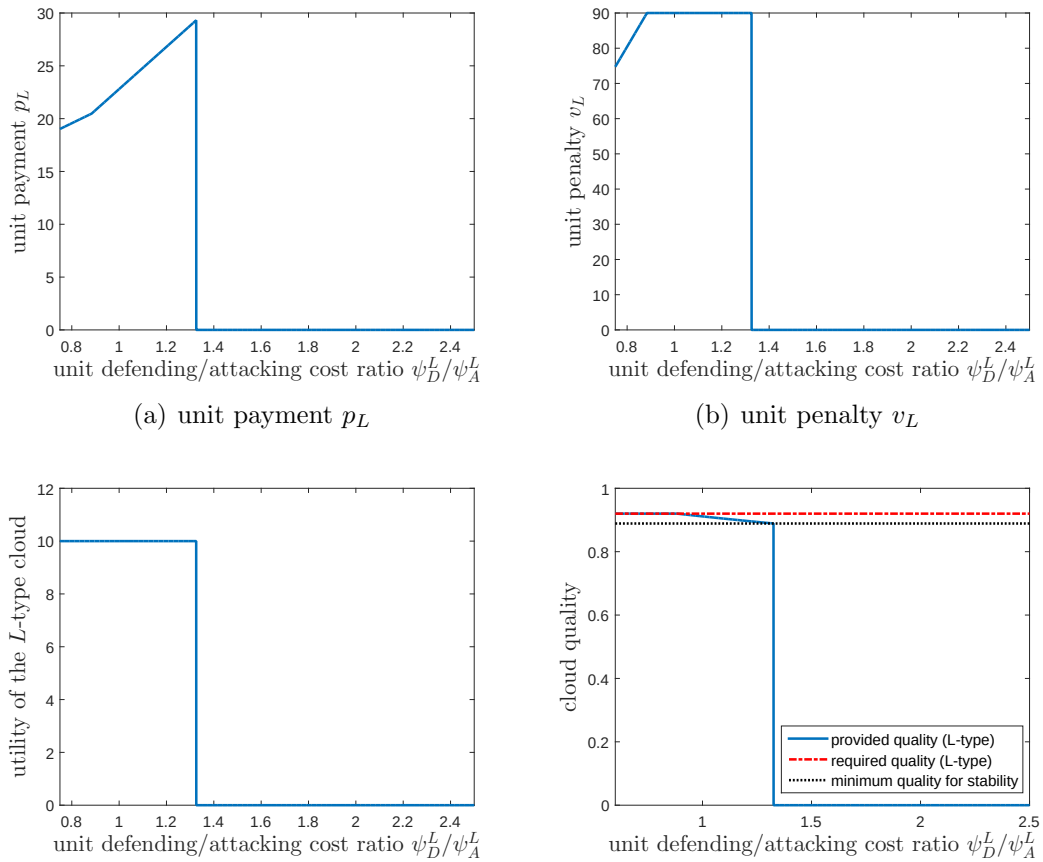
(b) unit penalty v_H

(c) H-type cloud utility

(d) required and provided QoS

Figure 7.7: (a) and (b) show the unit payment p_H and the unit penalty v_H in the designed H-type contract over regime I. (c) and (d) represent the utility of the H-type cloud and the provided cloud QoS z_H, respectively.

In the L-type contract, we fix the unit defending cost of the H-type cloud as $\psi_{\mathcal{D}}^H = \$6\text{K}$, and study the optimal contract design with varying parameter $\psi_{\mathcal{D}}^L$. Fig. 7.8 presents the results of the L-type contract. From Fig. 7.8(a), the unit payment p_L is increasing with larger unit defending cost $\psi_{\mathcal{D}}^L$ which is different with that in the H-type contract. The unit penalty v_L in Fig. 7.8(a) has the same trend as that in Fig. 7.7(a). The utility of the L-type cloud is a constant in the contractable regime as shown in Fig. 7.8(c) which verifies equation (7.28). The provided cloud



(a) unit payment p_L

(b) unit penalty v_L

(c) L-type cloud utility

(d) required and provided QoS

Figure 7.8: (a) and (b) show the unit payment p_L and the unit penalty v_L in the designed L-type contract over regime I. (c) and (d) represent the utility of the L-type cloud and the provided QoS z_L, respectively.

quality z_L first keeps the same as the requested one q_L in the contract, and then decreases as the defending cost $\psi_{\mathcal{D}}^L$ becomes larger, and finally jumps to zero since no contract is agreed. The reason for the uncontractable regime in this case differs from that in H-type contract design (the minimum profit is not met for the H-type cloud). When $\psi_{\mathcal{D}}^L/\psi_{\mathcal{A}}^L > 1.32$, the provided service z_L is smaller than the minimum required one $q_{L,\min} = 0.89$ which yields the uncontractable situation.

7.6.3 Regime II Study: Optimal Contracts for HVAC System

The HVAC system in SH adjusts the interior room temperature by controlling the air mass flow through the ducts into the house. Two critical states of the HVAC system are the room temperature and its changing rate [102]. The HVAC physical system is inherently robust, and it can be stabilized when the cloud quality satisfies $z > 0.28$. When $z < 0.28$, the control cost is extremely high and thus makes the control effort infeasible. Some parameters in the following case studies are as follows: $q_{H,\min} = 0.32$, $q_{H,\max} = 0.5$ and $\phi_H = 0.13$. Other parameters related to the cloud layer are the same as those in Section 7.6.2.

The contract design for HVAC system lies in regime II, since the provided cloud QoS will not exceed the required one which is upper bounded by $q_{H,\max} = 0.5$. To design the optimal contracts over regime II, knowing the relationship between the cloud QoS and the physical system performance is critical. The control cost of HVAC system with respect to cloud quality is depicted in Fig. 7.9. To enable the algorithmic design of contracts, the control cost of HVAC system can be approximated by an exponential function, and hence yields a continuously twice differentiable function $T(x)$ in algorithm 7.1. Together with the results in Theorem 7.5, we can design the optimal H-type contract for HVAC system.

The results corresponding to different cloud defending costs $\psi_{\mathcal{D}}^H$ are shown in Fig. 7.10. The obtained optimal contracts in the contractable regime is nonlinear with respect to $\psi_{\mathcal{D}}^H$. In addition, the cloud SP can provide the exactly required service as in the contract when $\psi_{\mathcal{D}}^H$ is small, and hence does not suffer penalty despite the unit penalty term v_H is increasing. However, the profit of the cloud

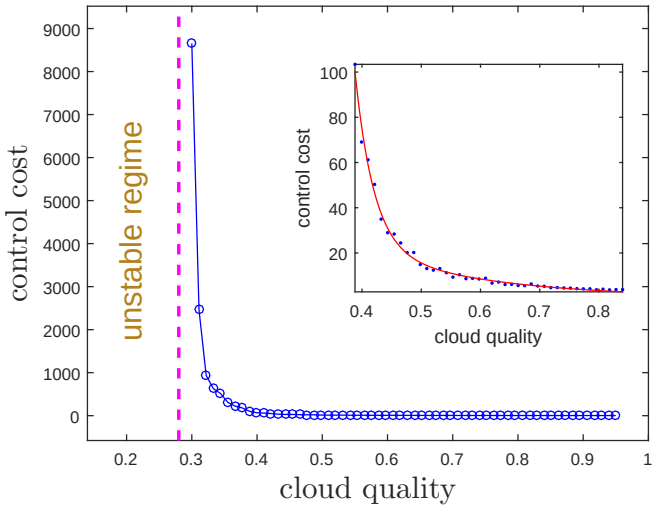
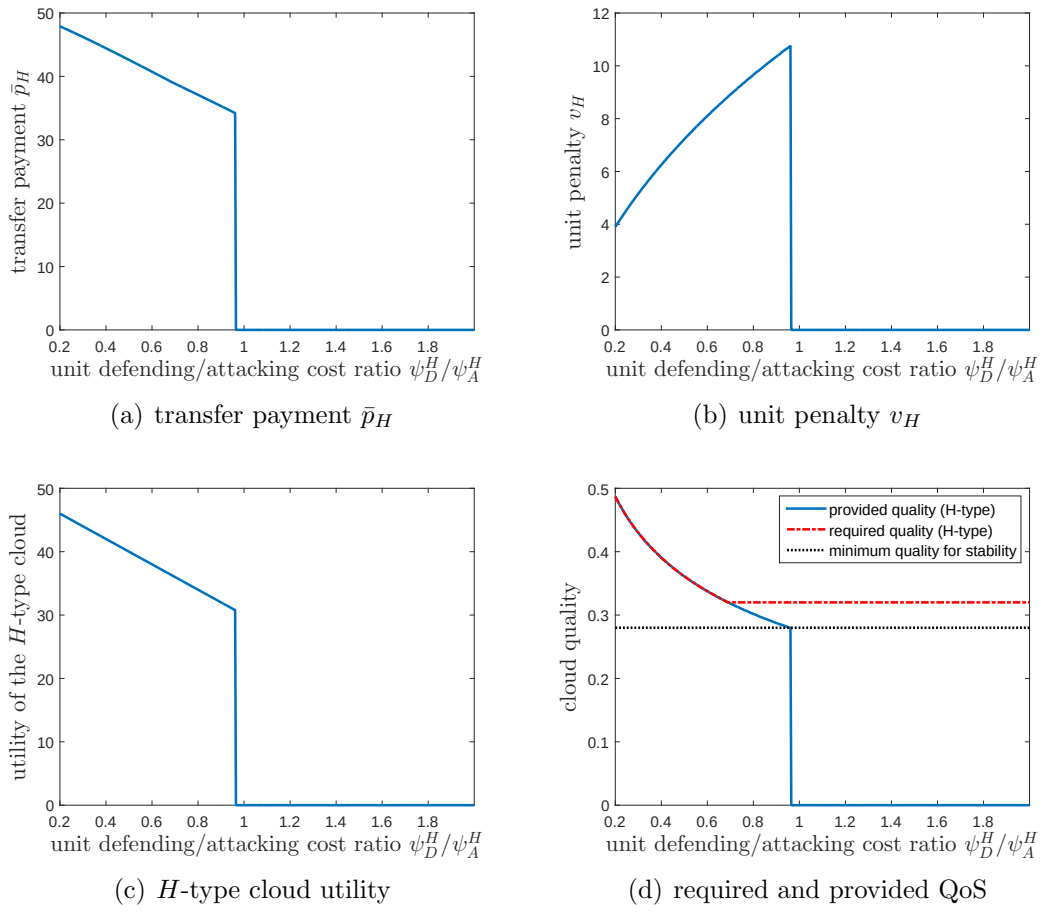


Figure 7.9: Performance of HVAC system. When $z < 0.28$, the system is unstable. In acceptable cloud quality regime, the system performance can be approximated by an exponential function.

SP is decreasing due to the increase of defending cost and the decrease of transfer payment. When the provided cloud QoS is worse than the required one, the device can still make a contract with the cloud SP until the received service incurs a huge control cost. The optimal L-type contract for HVAC system can be designed similarly according to the results in Theorem 7.6.

7.6.4 Joint Contracts Design for Heterogeneous Devices

In this section, we present the integrated contacts design for all devices shown in Fig. 7.6. The characteristics of the pacemaker device and HVAC system have been introduced in Sections 7.6.2 and 7.6.3, respectively. For the smart lighting system, better cloud QoS ensures the continuously smooth adjustment of the brightness in SH. Through the spectrum analysis on the modeled system matrices, the lighting system operates normally under the optimal control when cloud quality $z > 0.44$.



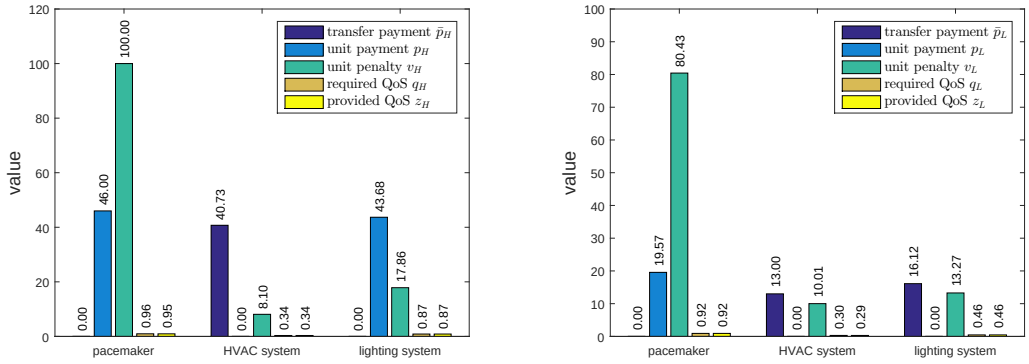
(a) transfer payment $\bar{p}_H$ (b) unit penalty v_H

(c) H-type cloud utility (d) required and provided QoS

Figure 7.10: (a) and (b) show the transfer payment $\bar{p}_H$ and the unit penalty v_H in the designed H-type contract over regime II. (c) and (d) represent the utility of the H-type cloud and the provided QoS z_H, respectively.

Next, we design the optimal contracts under given unit defending cost of cloud for all devices. Specifically, we set $\psi_{\mathcal{D}}^H = \$8\text{K}$ and $\psi_{\mathcal{D}}^L = \$3.2\text{K}$ for the H-type and L-type cloud, respectively. Other parameters are the same as those in Sections 7.6.2 and 7.6.3.

Based on the analytical results in Section 7.5, Fig. 7.11 presents the designed contracts for all three devices. Naturally, the terms in H-type contracts are all no less than their counterparts in L-type contracts. The contracts of pacemaker



(a) optimal H-type contracts

(b) optimal L-type contracts

Figure 7.11: (a) and (b) illustrate the optimal contracts design for the pacemaker, HVAC system and lighting system in SH under both the H-type and L-type cloud service providers, respectively.

device have the highest unit payment and penalty due to its demanding request of cloud quality. Both H-type and L-type contracts of HVAC system are in regime II, since the provided cloud QoS is less than 0.5 but is still able to stabilize the system. The H-type contract of smart lighting system belongs to regime I while its L-type contract lies in regime II. Though the transfer payment is 0 in its H-type contract comparing with \$16.12K in the L-type one, the lighting system needs to pay more to the H-type cloud SP due to the corresponding larger unit payment. The established SH framework is flexible, and the user can design globally optimal contracts by taking the preferences of different devices into account.

7.7 Summary

We have studied the optimal contract design for the cloud-enabled Internet of Controlled Things (IoCT) through the paradigm of security as a service. In terms of the cloud security quality of service (QoS), the contract design has been

divided into two regimes (regimes I and II). The inherently robust devices can design optimal contracts in regime I of which the required cloud QoS stabilizes the physical system; while those devices whose optimal contacts lie in regime II always ask for the best cloud QoS. In addition, payoffs of the considered two types of cloud service providers (SPs) are constants based on the accepted incentive compatible and individual rational contract from the device. The cloud-enabled smart home design has shown that for critical devices, the user should require a high-level cloud security and assign a large penalty if receiving a degraded service in the contract. For the devices with lower priority, the user makes a transfer payment to the cloud SP ahead of time for the security service to optimize his utility. The future work would include the extension of the current framework by considering the continuous type of cloud service provider and quantifying the value of asymmetric information. Another future direction would take the communication security between the cyber and physical layers into account, and design contracts for trustworthy communication services.

Chapter 8

Dynamic Contract Design for Systemic Cyber Risk Management

8.1 Introduction

Due to the interconnections between nodes in the network, the cyber risk can propagate and escalate into systemic risks, which have been a major contributor to massive spreading of Mirai botnets, phishing messages, and ransomware, causing information breaches and financial losses. In addition, systemic risks are highly dynamic by nature as the network faces a continuous flow of cybersecurity incidents. Hence, it becomes critical for the network and asset owner to protect resources from cyber attacks.

Due to the complex interdependencies between nodes and fast evolution nature of threats, it is challenging to mitigate systemic risks of enterprise network. The

asset owners need to delegate tasks of risk management to security professionals. The owner can be viewed as a principal who employs a security professional to fulfill security tasks. The security professionals can be viewed as an agent whose efforts are remunerated by the principal.

In the cyber risk management of enterprise network, one distinction is the lack of knowledge of the principal about the effort spent by the agent. This leads to a dynamic principal-agent problem under asymmetric information in which the risk manager determines his effort over time, while this effort is hidden to or unobservable by the asset owner. This information structure makes the contract design a challenging decision making problem. Conventional methods to address problems of incomplete information include information state based separation principle [86, 87] and belief update scheme [48]. However, these methods cannot be directly applied to design an optimal contract for the players. To address this challenge, we develop a systematic solution methodology which includes an estimation phase, a verification phase, and a control phase. Specifically, we first anticipate the risk manager's optimal effort based on the systemic risk outcome by designing an estimator for the principal. Then, we show that the principal has *rational controllability* of the systemic risk by verifying that the estimated effort is incentive compatible. Finally, we transform the problem using decision variables that adapt to the principal's information set and obtain the solution by solving a reformulated standard stochastic control program.

8.2 Problem Formulation

This section formulates the dynamic systemic cyber risk management problem of enterprise networks under asymmetric information using a principal-agent framework, and presents an overview of the adopted methodology.

8.2.1 Systemic Cyber Risk Management

An enterprise network is comprised of a set $\mathcal{N}$ of nodes, where $\mathcal{N} = \{1, 2, ..., N\}$. Due to the interdependencies among different nodes and fast changing nature of the threats, mitigating the systemic cyber risk is a challenging task which requires expertise from cybersecurity professionals. For example, to reduce the enterprise network vulnerability, it requires a constant monitoring of the Internet traffic into and out of the system, regular patching and updating of the device software, and continuous traffic scanning for intrusion detection. The principal[1] can delegate the risk management tasks over a time period $[0, T]$ to a professional manager.

The cyber risk of each node depends on the level of compliance with security criteria, the number of vulnerabilities of the software and hardware assets, the system configurations, the intrusion detection system alerts, and the concerned threat models [120]. The risk also evolves over time as the enterprise node constantly updates its software, introduces new functionalities, and interconnects with other nodes. We let $Y_t^i \in \mathbb{R}$ be the state of node $i \in \mathcal{N}$ to capture the risk of each node that maps the system configurations at time t and the threat models to the associated risk. Determining the value of Y_t can be a sophisticated task, depending on the system's complexity. To measure the risk, the cyber professional needs to identify

[1]The principal refers to the network/asset owner, and the agent refers to the risk manager or security professional which are used interchangeably.

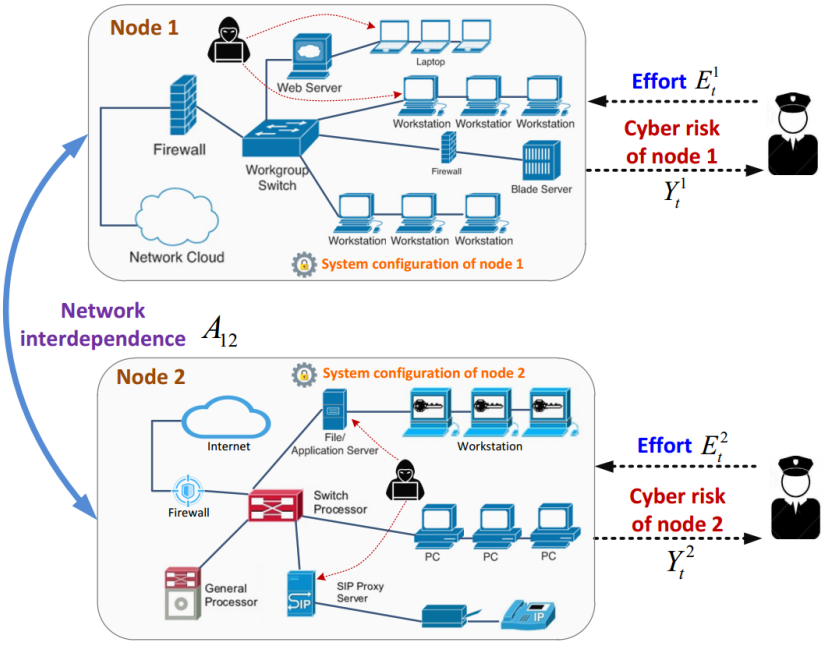


Figure 8.1: Systemic cyber risk management of an enterprise network containing two nodes. The cyber risk at node i is denoted by Y_t^i and the applied risk manager's effort is E_t^i, $i \in \{1, 2\}$. The cyber risk at each node depends on its system configuration, the attack model, and the risk manager's effort. Note that the cyber risk can propagate due to the connections between nodes.

the attack graph comprised of paths that the adversary can exploit to penetrate the network. Interested readers can refer to Chapter 5 in [120] for detailed steps of cyber risk assessment, such as identification of risk sources, risk consolidation, risk evaluation, aggregation and grouping. Game-theoretic frameworks can also be adopted to quantify risks. For example, under the advanced persistent threat (APT) type of cyber attacks, one can assess the node's risk using FlipIt game model in which the defender strategically configures the system by reclaiming the control of the node with some frequencies [133]. The FlipIt game outcome yields node's risk, which is the expected proportion of time that the node may be compromised by the adversary. As the nodes in the enterprise network are connected, their risks become interdependent, and this leads to systemic risk [59, 78]. We use an

$N \times N$-dimensional real matrix A with non-negative entries to model the influence of node i on node j, $i, j \in \mathcal{N}$. The diagonal entries in A represent the strength of internal risk evolution, and the off-diagonal entries capture the risk influence magnitude between nodes [106, 112]. For convenience, the risk profile of the network is denoted by $Y_t = [Y_t^1, Y_t^2, \cdots, Y_t^N]$. The dynamics of the risk profile describes the evolution of the systemic risk of the whole network.

To manage the risk profile, the risk manager can apply effort continuously over the time period $[0, T]$. Specifically, at every time t, $t \in [0, T]$, the risk manager can spend effort $E_t \in \mathcal{E} \subseteq \mathbb{R}_+^N$ on the nodes that mitigates the systemic cyber risk, where $\mathcal{E}$ is a compact set. As fore-mentioned, the effort can be measured by the amount of time and effectiveness of the risk manager spent on monitoring the cyberspace of the enterprise network. The amount of reduced risk is monotonically increasing with the allocated effort E_t [106]. This fact is reflected by many security practices, e.g., frequent scanning and analyzing the log files as well as timely patching the software can reduce the probability of successful cyber compromise by the adversary. Another critical factor to be considered is that the cyber risk quantification faces uncertainties due to the randomness in the cyber network. For instance, the risk uncertainty can be due to lack of knowledge as to whether the vulnerabilities in question actually exist, and if so, how easily they can be exploited by the attacker, or the risk source (malware, botnet) and attack graph are not fully identified by the cyber risk assessor, which introduce the underestimation of random cyber threats [58, 99]. Similar to [32], we use an N-dimensional standard Brownian motion B_t which is defined on the complete probability space $(\Omega, \mathcal{F}, \mathbb{P})$ to model the risk uncertainties on nodes. For clarity, Fig. 8.1 depicts an example of cyber risk management of the enterprise network containing two interdependent

nodes. Each node stands for a subnetwork with its own system configuration, and the adversary can target different assets, e.g., application servers and workstations. The risk manager applies efforts E_t^1 and E_t^2 to node 1 and node 2 continuously to reduce the cyber risks Y_t^1 and Y_t^2, respectively. The interdependency between two nodes is captured by the factor $A_{12} = A_{21}$.

In sum, we focus on a model of systemic cyber risk evolution described by the following stochastic differential equation (SDE):

$$\begin{aligned} dY_t &= AY_t dt - E_t dt + \Sigma_t(Y_t) dB_t, \\ Y_0 &= y_0, \end{aligned} \tag{8.1}$$

where $y_0 \in \mathbb{R}_+^N$ is a known positive vector denoting the initial systemic risk. Let $\mathbb{D}_+^{N\times N}$ denote the space of diagonal real matrices with positive elements. Then, $\Sigma_t : \mathbb{R}^N \to \mathbb{D}_+^{N\times N}$ captures the volatility of cyber risks in the network. Here, the diffusion coefficient $\Sigma_t(Y_t)$ indicates that the magnitude of uncertainty can be related to the dynamic risk of each node. We assume that the entries in $\Sigma_t(Y_t)$ are bounded, satisfying $\int_0^T \|\Sigma_t(Y_t)\mathbf{1}_N\|^2 dt \le C_1$ almost surely, where C_1 is a positive constant, $\|\cdot\|$ denotes the standard Euclidean norm, and $\mathbf{1}_N$ is an N-dimensional vector with all ones. Furthermore, the risk manager's effort E_t satisfies the condition $\int_0^T |E_t| dt \le C_2$ almost surely, where C_2 is a positive constant. Since the manager can apply effort to every node through E_t, the systemic risk level Y_t is fully manageable in the sense that more effort on each node reduces its cyber risk more significantly. Note that the model in (8.1) captures the characteristics of systemic cyber risks of enterprise network, and it is also adopted in various others' risk management scenarios including cyber-physical industrial control systems [146] and financial networks [59, 64]. Furthermore, [11] has leveraged a similar stochastic model as in

(8.1) with additional jumps to model the contagion of cyber security attacks, and the authors have provided empirical justifications for the model using real-world data of cyber attacks to various related components of a firm's information system.

The dynamic contract design for cyber risk management can be broken into two stages, namely the contracting stage and the execution stage. In the contracting stage, the principal first provides a dynamic contract that specifies the payment rules for the risk management to the agent and suggested/anticipated effort. Then, the agent chooses to accept the contract or not based on the provided benefits. If the agent accepts, then at the execution stage he needs to determine the adopted effort E_t to reduce the systemic cyber risk. During the task, the principal observes the dynamic risk outcome Y_t and pays $p_t \in \mathcal{P} \subseteq \mathbb{R}_+$ compensation to the agent according to the agreed contract, where $\mathcal{P}$ is a compact set. After completing the task, the agent also receives a terminal payment $c_T \in \mathbb{R}_+$ which finalizes the contract. Note that the claimed dynamic aspect of contract design lies in the fact that the systemic risk, applied effort, and payments evolve over time. However, the contract rule is fixed once the agent chooses to accept it, i.e., after the contracting stage.

Therefore, the principal needs to decide on the payment process $\{p_t\}_{0\leq t\leq T}$ as well as the final compensation c_T by observing the systemic risks. Note that the effort level E_t, $t \in [0, T]$, is hidden information of the agent, which corresponds to the hidden-action scenario, or moral hazard, in contract theory. This feature a reflection of the fact that the principal (asset owner) of the enterprise network cares about the cyber risk outcome Y_t rather than the implicit effort E_t adopted by the risk manager. Furthermore, we denote the principal's information set by $\mathcal{Y}_t$, representing the augmented filtration generated by $\{Y_s\}_{0\leq s\leq t}$. The agent's

information set is denoted by $\mathcal{A}_t$, including $\{Y_s\}_{0\leq s\leq t}$ and $\{B_s\}_{0\leq s\leq t}$. Note that for the agent, knowing $\{Y_s\}_{0\leq s\leq t}$ or $\{B_s\}_{0\leq s\leq t}$ is equivalent as he can determine one based on the other using also his effort process $\{E_s\}_{0\leq s\leq t}$. Specifically, at time t, the principal's knowledge includes only the path of Y_s, $0 \leq s \leq t$. In comparison, the agent can observe every term in the system, including the principal's information as well as the path of B_s, $0 \leq s \leq t$. The principal observes risk outcome Y_t, and his goal is to reduce the systemic risk by providing incentives to the manager. Therefore, the principal has no direct control of the systemic risk, and the difficulty he faces is in designing an efficient remuneration scheme based only on the limited observable information.

Next, we rewrite the $\mathcal{Y}_T$-measurable terminal payment as $c_T = \int_0^T dc_t + c_0$, to facilitate the contract analysis, where c_t has an interpretation of cumulative payment during $[0, t]$, and c_0 is a constant to be determined. Note that c_0 is a virtual initial payment and the agent receives it not at initial time 0, but rather at the terminal time T which is captured by the term c_T. The evolution of the aggregated equivalent $\mathcal{Y}_t$-measurable financial income process M_t of the cyber risk manager can be described by

$$dM_t = dc_t + p_t dt. \tag{8.2}$$

The cyber risk manager's cost function is:

$$J_A\left(\{E_t\}_{0\leq t\leq T}; \{p_t\}_{0\leq t\leq T}, c_T\right) = \mathbb{E}\int_0^T e^{-rt} f_A(t, p_t, E_t)dt + e^{-rT} h_A(M_T), \tag{8.3}$$

where $\mathbb{E}$ is the expectation operator, $r \in \mathbb{R}_+$ is a discount factor, $f_A : [0, T] \times \mathbb{R}_+ \times \mathcal{E} \to \mathbb{R}$ is the running cost, and $h_A : \mathbb{R}_+ \to \mathbb{R}_-$ is the terminal cost. The function

f_A is (implicitly) composed of two terms: the cost of spending effort E_t in risk management, and the received compensation p_t from the principal. Note that the final compensation c_T is incorporated into $h_A(M_T)$. Assumptions we make on the two additive terms of the cost functions are as follows.

Assumption 8.1. *The running cost function $f_A(t, p_t, E_t)$ is uniformly continuous and differentiable in p_t and E_t. Further, it is monotonically decreasing in p_t, and monotonically increasing and strictly convex in E_t. The terminal cost function $h_A(M_T)$ is a continuously differentiable, convex, and monotonic decreasing function.*

The principal's cost function, on the other hand, is specified as:

$$J_P(\{p_t\}_{0\le t\le T}, c_T) = \mathbb{E}\int_0^T e^{-rt} f_P(t, Y_t, p_t)dt + e^{-rT}\left(c_T + h_P(Y_T)\right), \tag{8.4}$$

where $f_P : [0,T] \times \mathbb{R}^N \times \mathcal{P} \to \mathbb{R}$ is the running cost, and $h_P : \mathbb{R}^N \to \mathbb{R}$ denotes the terminal cost. The function f_P captures the instantaneous cost of dynamic systemic risk and the payment to the agent.

Assumption 8.2. *The running cost for the principal, $f_P(t, Y_t, p_t)$, is uniformly continuous and differentiable in Y_t and p_t. Further, it is monotonically increasing in p_t and Y_t. The terminal cost for the principal, $h_P(Y_T)$, is a continuously differentiable and monotonic increasing function.*

It is worth pointing out that the focused contract in this chapter does not include renegotiation option for the participants, and it is assumed that both the principal and the agent fully commit to the contracted rules. It would be interesting to extend the current framework to the one where either the principal or the agent can choose to renegotiate the rules during the execution of the contract, and this requires to

include an extra variable in the contract capturing the cost of renegotiation. In such cases, the designed optimal contracts should be renegotiation-proof.

Another point relates the continuous observation of dynamic risks by the principal. This setup is different from the one in [90], where the authors have investigated a single-period (one-time observation) contract design for cyber insurance to mitigate the cyber risks. In our framework, instead of only focusing on the risk at a particular instant, the principal cares about the macroscopic level of risk mitigation of owned networked system over a period of time. To achieve this goal, the principal can leverage professional software, such as UpGuard [1], to continuously observe and monitor the dynamic cyber risks. We note that extension to contract design under controlled observation (similar to [84]) by the principal is also worth investigating, i.e., the principal needs to strategically determine when to observe the cyber risk instead of having continuous access to the variable Y_t.

8.2.2 Dynamic Principal-Agent Model

In cyber risk management, the principal contracts with the agent over $[0, T]$. For a given contract, the risk manager is strategic in minimizing the net cost. This rational behavior can be captured by the following definition.

Definition 8.1 (Incentive Compatibility)**.** *Under a given payment process* $\{p_t\}_{0\le t\le T}$ *and terminal compensation* c_T *of the principal, the effort trajectory* $\{E_t^*\}_{0\le t\le T}$ *of the agent is incentive compatible (IC) if it optimizes the cost function* (8.3)*, i.e.,*

$$\begin{aligned} &J_A\left(\{E_t^*\}_{0\le t\le T}; \{p_t\}_{0\le t\le T}, c_T\right) \\ &\le J_A\left(\{E_t\}_{0\le t\le T}; \{p_t\}_{0\le t\le T}, c_T\right), \forall E_t \in \mathcal{E},\ t \in [0, T]. \end{aligned} \tag{8.5}$$

The asset owner needs to provide sufficient incentives for the agent to fulfill the task of risk management, and this fact is captured through individual rationality as follows.

Definition 8.2 (Individual Rationality)**.** *The agent's policy is individually rational (IR) if the effort trajectory* $\{E_t^*\}_{0\le t\le T}$ *leads to satisfaction of*

$$J_A\left(\{E_t^*\}_{0\le t\le T};\{p_t\}_{0\le t\le T},c_T\right)=\inf_{E_t\in\mathcal{E}} J_A\left(\{E_t\}_{0\le t\le T};\{p_t\}_{0\le t\le T},c_T\right)\le \underline{J}_A, \quad (8.6)$$

where $\underline{J}_A$ *is a predetermined non-positive constant.*

Note that the non-positiveness of $\underline{J}_A$ ensures the profitability of risk manager by fulfilling the risk management tasks.

We next provide precise formulations of the problems faced by the agent and the principal. Under a contract $\{\{p_t\}_{0\le t\le T},c_T\}$, the agent minimizes his total cost by solving the following problem:

$$(\mathrm{O}-\mathrm{A}): \quad \min_{E_t\in\mathcal{E},\ t\in[0,T]} J_A\left(\{E_t\}_{0\le t\le T};\{p_t\}_{0\le t\le T},c_T\right)$$

subject to the stochastic dynamics (8.1), and the payment process (8.2).

By taking into account the IC and IR constraints, the principal addresses the following optimization problem:

$$(\mathrm{O}-\mathrm{P}): \quad \min_{p_t\in\mathcal{P},\ t\in[0,T],\ c_T} J_P(\{p_t\}_{0\le t\le T},c_T)$$

subject to the stochastic dynamics (8.1), IC (8.5), and IR (8.6).

Note that the designed contract terms $\{p_t\}_{0\le t\le T}$ and c_T should adapt to the infor-

mation available to the principal in view of the underlying incomplete information. Denote the solution to $(\mathrm{O}-\mathrm{P})$ by $\{p_t^*\}_{0\leq t\leq T}$ and c_T^*. We present the solution concept of the formulated problem as follows.

Definition 8.3 (Optimal Dynamic Mechanism Design (ODMD))**.** *The ODMD consists of the contract* $\{\{p_t^*\}_{0\leq t\leq T}, c_T^*\}$ *as well as the effort process* $\{E_t^*\}_{0\leq t\leq T}$ *that solve the problems* $(\mathrm{O}-\mathrm{P})$ *and* $(\mathrm{O}-\mathrm{A})$*, respectively. In addition, the compensation processes* p_t^* *and* c_T^* *are adapted to* $\mathcal{Y}_t$ *and* $\mathcal{Y}_T$*, respectively, and the risk manager's effort* E_t^* *is adapted to* $\mathcal{A}_t$*.*

Remark: ODMD captures the bi-level interdependent decision making of the principal and the agent, which is a Stackelberg differential game with a nonstandard information structure. Since the principal (leader) delegates the control task to the agent (follower) but cannot observe his adopted action, ODMD features the limited nature of the principal's information. For those readers interested in the introduction of differential games, they can refer to Chapter 2.1.4 for more details.

Due to the hidden effort of the risk manager, $(\mathrm{O}-\mathrm{P})$ is not a classical stochastic optimal control problem. Specifically, the principal only observes the cyber risk outcome rather than the effort which has to be incentivized. To address this challenge brought about by the presence of asymmetric information, we adopt a systematic approach to design an incentive compatible and optimal mechanism.

Comment on the Principal-Agent Model: In reality, there may exist multiple risk managers executing tasks for the asset owner. In such cases, it would be possible to extend the current single-principal single-agent framework to a single-principal multi-agent one. To design the optimal contracts in this case, we need to analyze a noncooperative game between the agents, as they compete for larger payments for the work done. The solution concept for the agents' problem would be the Nash

equilibrium. The existence of this equilibrium depends on the contract designed by the principal, and hence is not guaranteed under arbitrary contracts. It may also be possible that the networked system components are owned by different parties, and are managed by a number of risk managers. Then, we need to establish a multi-principal multi-agent framework to capture this scenario. In addition to analyzing the game between agents, we should also study, in this case, the strategic behaviors of principals. Similar to the single-principal multi-agent case, the existence of equilibrium between agents depends on the contracts designed by the principals. Therefore, the contract design not only needs to consider the interactions between principals, but also the rational responses of agents. These practical extensions require a systematic investigation in the future.

8.2.3 Overview of the Methodology

We present an overview of the steps involved in our derivation, with details worked out in the following sections.

The principal first estimates the risk manager's effort based on the systemic risk output (estimation phase), and then verifies that the estimated effort is incentive compatible (verification phase), and finally designs an optimal compensation scheme under the incentive compatible estimator (control phase). To address the challenge, our goal is to transform the problem using variables that adapt to the principal's information set. To this end, the principal first assumes that the agent behaves optimally with effort level E_t^* (even though the principal does not know the exact value) and calculates the corresponding cost of the agent. Another interpretation for this step would be that the principal anticipates the agent implementing E_t^* which satisfies the IC constraint. Then, the principal designs the terminal payment

form using the estimated agent's cost (Section 8.3.1). The agent responds to the contract strategically through his best effort E_t^o. When the anticipated E_t^* coincides with E_t^o, E_t^* is an incentive compatible estimator and the principal facilitates the agent implementing E_t^* successfully (Section 8.3.2). Therefore, the principal can determine the optimal payment p_t^* based on E_t^* by solving a standard stochastic optimal control problem (Section 8.4.2).

8.3 Analysis of Risk Manager's Incentives

We first provide a form of the terminal payment contract term and then focus on deriving an incentive compatible estimator of the cyber risk manager's effort.

8.3.1 Terminal Payment Analysis

We first present the following result on the IR constraint.

Lemma 8.1. *The IR constraint holds as an equality, i.e.,*

$$J_A\left(\{E_t^*\}_{0\le t\le T};\{p_t\}_{0\le t\le T},c_T\right)=\underline{J}_A. \tag{8.7}$$

Proof. If $J_A\left(\{E_t^*\}_{0\le t\le T};\{p_t\}_{0\le t\le T},c_T\right)<\underline{J}_A$, the designed contract is not optimal as the principal can further reduce his cost by paying less to the agent. □

Next, we first express the agent's cost under the principal's information set $\mathcal{Y}_t$ as well as using the property that the agent chooses an optimal E_t^*, and then use the principal's estimation about the agent's cost to characterize the cumulative payment process. We introduce a new variable W_t representing the expected future

cost of the agent anticipated by the principal as follows:

$$W_t = \mathbb{E}\left[\int_t^T e^{-r(s-t)} f_A\big(s, p_s, E_s^*\big) ds + e^{-r(T-t)} h_A(M_T) \big| \mathcal{Y}_t\right]. \tag{8.8}$$

Note that W_t is evaluated under the information available to the principal at time t. Thus, the total expected cost of the agent under the information $\mathcal{Y}_t$ can be expressed as

$$\begin{aligned} U_t &= \mathbb{E}\left[\int_0^T e^{-rt} f_A\big(t, p_t, E_t\big) dt + e^{-rT} h_A(M_T) \big| \mathcal{Y}_t, E_t = E_t^*\right] \\ &= \int_0^t e^{-rs} f_A\big(s, p_s, E_s^*\big) ds + e^{-rt} W_t. \end{aligned} \tag{8.9}$$

We further have conditions $U_0 = W_0 = \underline{J}_A$ and $W_T = h_A(M_T)$. The effort $E_t = E_t^*$ indicates that the agent behaves optimally under a given contract.

Proposition 8.1. *The total expected cost of the agent, U_t, is a martingale under $\mathcal{Y}_t$. In addition, there exists an N-dimensional progressively measureable process ζ_t such that*

$$dU_t = e^{-rt} \zeta_t^{\mathsf{T}} \left(dY_t - AY_t dt + E_t^* dt\right), \tag{8.10}$$

where T denotes the transpose operator.

Proof. First, we have

$$\begin{aligned} \mathbb{E}[U_t | \mathcal{Y}_\tau] =& \mathbb{E}\left[\int_0^\tau e^{-rs} f_A(s, p_s, E_s^*) ds + e^{-r\tau} W_\tau \big| \mathcal{Y}_\tau\right] \\ &+ \mathbb{E}\left[\int_\tau^t e^{-rs} f_A(s, p_s, E_s^*) ds + e^{-rt} W_t - e^{-r\tau} W_\tau \big| \mathcal{Y}_\tau\right] \\ =& U_\tau + \mathbb{E}\left[\int_\tau^t e^{-rs} f_A(s, p_s, E_s^*) ds + e^{-rt} W_t \big| \mathcal{Y}_\tau\right] - e^{-r\tau} W_\tau. \end{aligned} \tag{8.11}$$

Then, using (8.8), we obtain

$$\begin{aligned}&\mathbb{E}\left[\int_\tau^t e^{-rs}f_A(s,p_s,E_s^*)ds + e^{-rt}W_t\big|\mathcal{Y}_\tau\right]\\&\quad=\mathbb{E}\left[\int_\tau^T e^{-rs}f_A(s,p_s,E_s^*)ds + e^{-rT}h_A(M_T)\big|\mathcal{Y}_\tau\right] = e^{-r\tau}W_\tau.\end{aligned}\tag{8.12}$$

Hence, $\mathbb{E}[U_t|\mathcal{Y}_\tau] = U_\tau$, and U_t is a $\mathcal{Y}_t$-measurable martingale. Using martingale representation theorem [88] yields (8.10). □

Based on Proposition 8.1, we can subsequently obtain the following lemma which facilitates design of the terminal payment term design in the optimal contract.

Lemma 8.2. *The aggregate equivalent income process M_t evolves according to:*

$$\begin{aligned}dM_t =&\frac{rh_A(M_t)}{h_A'(M_t)}dt - \frac{f_A(t,p_t,E_t^*)}{h_A'(M_t)}dt + \frac{1}{h_A'(M_t)}\zeta_t^\mathsf{T}(dY_t - AY_tdt + E_t^*dt)\\&-\frac{1}{2}\frac{h_A''(M_t)}{h_A'(M_t)}\frac{\zeta_t^\mathsf{T}\Sigma_t(Y_t)\Sigma_t(Y_t)^\mathsf{T}\zeta_t}{h_A'^2(M_t)}dt.\end{aligned}\tag{8.13}$$

Proof. By substituting (8.10) into (8.9), we obtain

$$\begin{aligned}&dU_t = e^{-rt}f_A\big(t,p_t,E_t^*\big)dt - re^{-rt}W_tdt + e^{-rt}dW_t,\\\Rightarrow\quad&dW_t = rW_tdt - f_A\big(t,p_t,E_t^*\big)dt + \zeta_t^\mathsf{T}\left(dY_t - AY_tdt + E_t^*dt\right).\end{aligned}\tag{8.14}$$

Since $W_T = h_A(M_T)$, we adopt the form $W_t = h_A(M_t)$ and aim to characterize the contract that yields this form. Then, we have $\underline{J}_A = h_A(M_0) = h_A(c_0)$. Further, (8.14) indicates that

$$\begin{aligned}h_A'(M_t)dM_t + \frac{1}{2}h_A''(M_t)\chi_t^2dt =&rh_A(M_t)dt - f_A\big(t,p_t,E_t^*\big)dt\\&+\zeta_t^\mathsf{T}\left(dY_t - AY_tdt + E_t^*dt\right),\end{aligned}\tag{8.15}$$

where χ_t is the volatility of process M_t. Matching the volatility terms in (8.15) gives $h_A'^2(M_t)\chi_t^2 = \zeta_t^\mathsf{T}\Sigma_t(Y_t)\Sigma_t(Y_t)^\mathsf{T}\zeta_t$. Then, (8.15) yields the result. □

Remark: Note that (8.10) includes information on the cyber risk dynamics (8.1). Thus, (8.13) can be seen as a modified stochastic dynamic system of the agent with M_t as a new state variable. In addition, ζ_t can be interpreted as the principal's control over the agent's revenue.

Another point to be highlighted is the role of p_t in (8.13). Here, p_t is not optimal yet and its value needs to be further determined by the principal. Currently, we can view p_t as an exogenous variable that enters the constructed dynamic contract form (8.13). In addition, the feedback structure of the dynamic contract on Y_t is reflected by the cumulative payment term c_t shown later in Lemma 8.3.

Interpretation of Dynamic Contract: The dynamic contract determines the risk manager's revenue in (8.13), which includes four separate terms. The first term, $\frac{rh_A(M_t)}{h_A'(M_t)}dt$, indicates that the risk manager's payoff should be increased to compensate the discounted future revenue. The second term, $-\frac{f_A(t,p_t,E_t^*)}{h_A'(M_t)}dt$, is an offset of the *direct cost* of agent's effort. The third part, $\frac{1}{h_A'(M_t)}\zeta_t^\mathsf{T}\left(dY_t - AY_tdt + E_t^*dt\right)$, is an *incentive* term, which captures the agent's benefit from spending effort in risk management. Here, the agent's real effort enters into the Y_t term. The last one, $-\frac{1}{2}\frac{h_A''(M_t)}{h_A'(M_t)}\frac{\zeta_t^\mathsf{T}\Sigma_t(Y_t)\Sigma_t(Y_t)^\mathsf{T}\zeta_t}{h_A'^2(M_t)}dt$, is a *risk compensation* term (the manager is risk-averse), capturing the fact that the risk manager faces uncertainties in the performance outcome due to the Brownian motion.

For completeness, we present the cumulative payment process c_t in the following lemma.

Lemma 8.3. *The cumulative payment process c_t evolves according to:*

$$\begin{aligned} dc_t =& \frac{rh_A(M_t)}{h'_A(M_t)}dt - \frac{f_A(t,p_t,E^*_t)}{h'_A(M_t)}dt + \frac{1}{h'_A(M_t)}\zeta_t^{\mathsf{T}}(dY_t - AY_t dt + E^*_t dt) \\ & - \frac{1}{2}\frac{h''_A(M_t)}{h'_A(M_t)}\frac{\zeta_t^{\mathsf{T}}\Sigma_t(Y_t)\Sigma_t(Y_t)^{\mathsf{T}}\zeta_t}{h'^2_A(M_t)}dt - p_t dt. \end{aligned} \tag{8.16}$$

Proof. The result can be directly obtained from (8.2) and Lemma 8.2. □

Lemma 8.3 characterizes the cumulative payment process c_t with initial value c_0 given by $h_A(c_0) = \underline{J}_A$. We focus on the class of contracts in (8.16), and aim to determine the optimal variables (ζ_t and p_t) to minimize the principal's cost. Note that (8.16) is adapted to the principal's information set $\mathcal{Y}_t$, since the principal observes M_t and Y_t, determines p_t, ζ_t, and anticipates E^*_t. In addition, this payment process is directly related to the actual effort that the agent adopts, captured by dY_t. The variable ζ_t can be further interpreted as the sensitivity (or gain) of contract payment to the risk difference under the agent's optimal and actual efforts. In addition, since $W_t = h_A(M_t)$, based on (8.8), we obtain

$$\begin{aligned} U_t &= \mathbb{E}\left[\int_0^T e^{-rt} f_A\big(t,p_t,E_t\big)dt + e^{-rT}h_A(M_T)\big|\mathcal{A}_t\right] \\ &= \int_0^t e^{-rs} f_A\big(s,p_s,E^*_s\big)ds + e^{-rt}h_A(M_t), \end{aligned} \tag{8.17}$$

where the conditional expectation on $\mathcal{A}_t$ admits the same value as that on $\mathcal{Y}_t$. Proposition 8.1 indicates that U_t is a martingale. Then, the expected value of $e^{-rt}h_A(M_t)$ in (8.17) is zero which confirms the zero expected future cost of the agent.

8.3.2 Incentive Analysis of Cyber Risk Manager

Recall that the principal suggests an optimal effort process E_t^* by assuming that the agent behaves optimally. However, the agent can determine his actual effort E_t that minimizes the cost J_A based on $\mathcal{A}_t$ which might not be the same as E_t^* that the principal suggests. Thus, the next important problem for the principal is to determine an incentive compatible contract. To achieve this goal, the principal determines the process ζ_t and the payment p_t strategically to control the agent's actual effort E_t.

Denote by $V_a(t, M_t)$ the agent's value function with terminal condition $V_a(T, M_T) = h_A(M_T)$. The property of value function ensures that the risk management effort is optimal if it satisfies the following dynamic programming equation: $e^{-rt}V_a(t, M_t) = \min_{E_t} \mathbb{E}\left\{\int_t^s e^{-ru} f_A(u, p_u, E_u)du + e^{-rs}V_a(s, M_s)\right\}$. Then, using (8.1), (8.2), and (8.16), the cyber risk manager's revenue can be expressed as:

$$\begin{aligned} dM_t =& \frac{rh_A(M_t)}{h'_A(M_t)}dt - \frac{f_A\big(t, p_t, E_t^*\big)}{h'_A(M_t)}dt + \frac{1}{h'_A(M_t)}\zeta_t^{\mathsf{T}}\left(E_t^* - E_t\right)dt \\ & - \frac{1}{2}\frac{h''_A(M_t)}{h'_A(M_t)}\frac{\zeta_t^{\mathsf{T}}\Sigma_t(Y_t)\Sigma_t(Y_t)^{\mathsf{T}}\zeta_t}{h'^2_A(M_t)}dt + \frac{1}{h'_A(M_t)}\zeta_t^{\mathsf{T}}\Sigma_t(Y_t)dB_t. \end{aligned} \tag{8.18}$$

We rewrite the risk manager's problem as follows:

$$(\mathrm{O}-\mathrm{A}'): \quad \min_{E_t\in\mathcal{E},\ t\in[0,T]} J_A\left(\{E_t\}_{0\le t\le T}; \{p_t\}_{0\le t\le T}, c_T\right)$$

subject to the stochastic dynamics (8.18), and the payment process (8.2).

The Hamilton-Jacobi-Bellman (HJB) equation associated with the stochastic opti-

mal control problem $(\mathrm{O}-\mathrm{A}')$ is

$$\min_{E_t}\left[\frac{1}{2}\frac{\partial^2 V_a}{\partial M_t^2}\left(\frac{1}{h_A'^2(M_t)}\zeta_t^{\mathsf{T}}\Sigma_t(Y_t)\Sigma_t(Y_t)^{\mathsf{T}}\zeta_t\right)+\frac{\partial V_a}{\partial M_t}\left(\frac{rh_A(M_t)}{h_A'(M_t)}-\frac{f_A\big(t,p_t,E_t^*\big)}{h_A'(M_t)}\right.\right.$$
$$\left.\left.+\frac{1}{h_A'(M_t)}\zeta_t^{\mathsf{T}}\left(E_t^*-E_t\right)-\frac{1}{2}\frac{h_A''(M_t)}{h_A'(M_t)}\frac{\zeta_t^{\mathsf{T}}\Sigma_t(Y_t)\Sigma_t(Y_t)^{\mathsf{T}}\zeta_t}{h_A'^2(M_t)}\right)+f_A(t,p_t,E_t)\right]+\frac{\partial V_a}{\partial t}=rV_a,$$
$$V_a(T,M_T)=h_A(M_T). \tag{8.19}$$

Based on the candidate value function $V_a(t,M_t)=h_A(M_t)$, the second-order condition of (8.19) is satisfied. Then, the optimal solution to $(\mathrm{O}-\mathrm{A}')$ is

$$\begin{aligned}E_t^o&=\arg\max_{E_t}\ \frac{\partial V_a}{\partial M_t}\frac{1}{h_A'(M_t)}\zeta_t^{\mathsf{T}}E_t-f_A(t,p_t,E_t)\\&=\arg\max_{E_t}\ \zeta_t^{\mathsf{T}}E_t-f_A(t,p_t,E_t).\end{aligned} \tag{8.20}$$

For a given contract, E_t^o is the optimal effort of the agent. Then, when the anticipated effort E_t^* of the principal coincides with E_t^o, i.e., $E_t^*=E_t^o$, the provided contract is IC and E_t^* is implemented. The following theorem captures this result.

Theorem 8.1. *When the compensation process in the contract is specified by (8.16), then the IC constraint is satisfied, i.e., E_t^* is implemented as expected by the principal, if and only if the following condition holds:*

$$E_t^*=\arg\max_{E_t}\ \zeta_t^{\mathsf{T}}E_t-f_A(t,p_t,E_t), \tag{8.21}$$

where ζ_t is adapted to the information $\mathcal{Y}_t$ available to the principal.

Proof. We verify that E_t^* is implemented by the agent.

For an arbitrary process $\{E_t\}_{0\leq t\leq T}$, we define a variable

$$\tilde{U}_t = \int_0^t e^{-rs} f_A\big(s, p_s, E_s\big) ds + e^{-rt} h_A(M_t),$$

where M_t is given by (8.18). Note that the HJB equation associated with $(\mathrm{O}-\mathrm{A}')$ can also be written as $0 = \min_{E_t} \ \mathbb{E}\left[d\tilde{U}_t | \mathcal{A}_t\right]$. Then, we know that when $E_t \neq E_t^*$, the drift term of $\tilde{U}_t$ is positive and yields $\tilde{U}_t < \mathbb{E}[\tilde{U}_T|\mathcal{A}_t]$. Hence, at time t, the expected total cost of the risk manager is greater than $\tilde{U}_t$. When $E_t = E_t^*$, we have $\mathbb{E}\left[d\tilde{U}_t|\mathcal{A}_t\right] = 0$, and thus $\tilde{U}_t = \mathbb{E}[\tilde{U}_T|\mathcal{A}_t]$. This verifies that E_t^* is the incentive compatible optimal decision of the risk manager such that his total expected cost is achieved at the lower bound. □

Based on Theorem 8.1, the principal can indirectly manipulate the implemented effort of the agent by determining the variables ζ_t and p_t jointly. Hence, under (8.21), the suggested effort E_t^* is incentive compatible. From (8.21), we can see that the risk manager's behavior is *strategically neutral*. Specifically, at time t, the risk manager decides on the optimal effort E_t^* based only on the current cost (term $f_A(t, p_t, E_t)$) and benefit (term $\zeta_t^\mathsf{T} E_t$) instead of future-looking variables. This neutral behavior is consistent with the fact that a larger current effort does not induce a higher payoff for the agent after time t, since as shown in (8.17), the expected future cost over time $(t, T]$ is zero due to the martingale property.

Remark: When addressing the agent's problem as shown in $(\mathrm{O}-\mathrm{A}')$, we adopt the current aggregated income process M_t as a state variable. Though the form of this process is not as succinct as W_t which is generally used (e.g., [124]), it facilitates the characterization of the cumulative payment c_t in Lemma 8.3. It also shows that leveraging M_t can also yield the result.

8.4 The Principal's Problem: Optimal Dynamic Systemic Cyber Risk Management

Our next goal is to characterize the dynamic contracts designed by the principal. Furthermore, we present a separation principle and explicit solutions to an LQ case in this section.

8.4.1 Rational Controllability

The controllability of the cyber risk is critical to the principal. To account for the incentives in the management of risk, we have the following definition.

Definition 8.4 (Rational Controllability)**.** *The dynamic systemic cyber risk is rationally controllable if the principal can provide incentives* $\{p_t\}_{0\leq t\leq T}$ *and* c_T *such that the risk manager's effort* $\{E_t\}_{0\leq t\leq T}$ *coincides with the one suggested by the principal.*

In ODMD, the rational controllability indicates that under $\{\{p_t^*\}_{0\leq t\leq T}, c_T^*\}$, the best-response behavior $\{E_t^*\}_{0\leq t\leq T}$ of the agent is the same as the principal's predicted effort. The unique feature of rational controllability is that the principal cannot control the cyber risk directly but can rely on other terms to infer the rational behavior of the agent, which further influences the applied effort in risk management. Corollary 8.1 later captures this result.

8.4.2 Stochastic Optimal Control Reformulation

Knowing that the cyber risk manager behaves strategically, the principal aims to implement E_t^* and thus (8.16) becomes

$$\begin{aligned} dc_t =& \frac{rh_A(M_t)}{h'_A(M_t)}dt - \frac{f_A\big(t,p_t,E_t^*\big)}{h'_A(M_t)}dt - \frac{1}{2}\frac{h''_A(M_t)}{h'_A(M_t)}\frac{\zeta_t^\intercal \Sigma_t(Y_t)\Sigma_t(Y_t)^\intercal \zeta_t}{h'^2_A(M_t)}dt \\ & - p_t dt + \frac{1}{h'_A(M_t)}\zeta_t^\intercal \Sigma_t(Y_t)dB_t. \end{aligned} \tag{8.22}$$

Instead of dealing with the complex revenue dynamics (8.18) of the principal, we deal with its equivalent counterpart dW_t shown in Theorem 8.2 below, which is much simpler. We reformulate the principal's problem as a standard stochastic optimal control problem as follows.

Theorem 8.2. *The principal's problem is reformulated as a stochastic optimal control problem as follows:*

$$\begin{aligned} (\mathrm{O}-\mathrm{P}'): \min_{p_t\in\mathcal{P},\ \zeta_t} \ & \mathbb{E}\int_0^T e^{-rt}\left(f_P(t,Y_t,p_t) - e^{-r(T-t)}p_t\right)dt + e^{-rT}\left(h_P(Y_T) + h_A^{-1}(W_T)\right) \\ \text{such that} \quad & dY_t = AY_t dt - E_t^* dt + \Sigma_t(Y_t)dB_t,\ Y_0 = y_0, \\ & dW_t = rW_t dt - f_A(t,p_t,E_t^*)dt + \zeta_t^\intercal \Sigma_t(Y_t)dB_t,\ W_0 = \underline{J}_A, \\ & E_t^* = \arg\max_{E_t}\ \zeta_t^\intercal E_t - f_A(t,p_t,E_t). \end{aligned}$$

Proof. Recall that the expected cost of the cyber risk manager is equal to $W_t = h_A(M_t)$. Then, under the optimal risk management effort, we obtain

$$dW_t = rW_t dt - f_A(t,p_t,E_t^*)dt + \zeta_t^\intercal \Sigma_t(Y_t)dB_t,\ W_0 = \underline{J}_A.$$

In addition, based on $dc_t = dM_t - p_t dt$, we have $c_T = M_T - \int_0^T p_t dt$. Since

$M_T = h_A^{-1}(W_T)$, we have $e^{-rT}c_T = e^{-rT}h_A^{-1}(W_T) - e^{-rt}\int_0^T e^{-r(T-t)}p_t dt$. Thus, the cost function of the principal can be rewritten as

$$\mathbb{E}\int_0^T e^{-rt}\left(f_P(t,Y_t,p_t) - e^{-r(T-t)}p_t\right)dt + e^{-rT}\left(h_P\big(Y_T\big) + h_A^{-1}(W_T)\big)\right),$$

which yields the result. □

In the investigated incomplete information situations, the principal preserves the indirect controllability of systemic risk Y_t by estimating the agent's effort E_t^* as well as specifying the contract terms p_t, c_T and process ζ_t.

Corollary 8.1. *By providing incentives* $\{\{p_t\}_{0\le t\le T}, c_T\}$ *and specifying process* $\{\zeta_t\}_{0\le t\le T}$*, the dynamic systemic cyber risk is rationally controllable, and the incentive compatible effort follows* (8.21)*. The optimal* $\{p_t^*\}_{0\le t\le T}$ *and* $\{\zeta_t^*\}_{0\le t\le T}$ *can be obtained from Theorem 8.2.*

Proof. The result directly follows from Theorems 8.1 and 8.2. □

Remark: Theorem 8.2 presents solution to a standard optimal control problem for the principal, whose the existence and uniqueness have been well studied [140]. With f_P, h_P, f_A, and h_A satisfying the conditions in Assumptions 8.1 and 8.2, and the corresponding coefficients in the functions well selected ensuring the feasibility of (O − P′), the control problem can be solved efficiently by numerical methods [95]. Therefore, the ODMD for the systemic risk management problem, i.e., E_t^*, p_t^*, and c_T^*, can be determined from (8.21), (8.22) and Theorem 8.2, respectively.

8.4.3 Separation Principle

We next present a separation principle for the asset owner in determining the compensation p_t and the auxiliary parameter ζ_t. First, we make assumptions on the separability of the cost functions.

(S1): The agent's running cost can generally be separated into two parts, including the effort and payment. Accordingly, we take $f_A(t, p_t, E_t)$ to be in the form

$$f_A(t, p_t, E_t) = f_{A,E}(E_t) - f_{A,p}(p_t), \tag{8.23}$$

where $f_{A,E} : \mathcal{E} \to \mathbb{R}_+$ is monotonically increasing, continuously differentiable and strictly convex, i.e., $f'_{A,E}(E_t) > 0$ and $f''_{A,E}(E_t) > 0$, and $f_{A,p} : \mathcal{P} \to \mathbb{R}_+$. Then, the constraint $E_t^* = \arg\max_{E_t} \zeta_t^\mathsf{T} E_t - f_A(t, p_t, E_t)$ can be simplified to

$$E_t^* = f'^{-1}_{A,E}(\zeta_t). \tag{8.24}$$

(S2): We also assume that the principal's running cost takes the form

$$f_P(t, Y_t, p_t) = f_{P,Y}(Y_t) + f_{P,p}(p_t), \tag{8.25}$$

where $f_{P,Y} : \mathbb{R}^N \to \mathbb{R}$ and $f_{P,p} : \mathcal{P} \to \mathbb{R}_+$ are monotonically increasing and continuously differentiable.

The inverse function h_A^{-1} plays a role in the principal's objective. We further have the following assumption.

(L1): The agent's terminal cost function h_A is linear, i.e., $h_A(M_T) = \gamma M_T$, where $\gamma < 0$.

Then, we have the following *separation principle*.

Theorem 8.3. *Under conditions* ***(S1)***, ***(S2)***, *and* ***(L1)***, *the principal's problem* $(\mathrm{O}-\mathrm{P}')$ *can be separated into two subproblems with respect to the decision variables* ζ_t *and* p_t *as:*

$$
\begin{aligned}
(SP1):\ \min_{\zeta_t}\ \mathbb{E}\ & \int_0^T e^{-rt}\left(f_{P,Y}(Y_t)-\frac{1}{\gamma}f_{A,E}\left(f_{A,E}'^{-1}(\zeta_t)\right)\right)dt \\
& + e^{-rT}h_P(Y_T)+\frac{1}{\gamma}\int_0^T e^{-rt}\zeta_t^{\mathsf{T}}\Sigma_t(Y_t)dB_t \\
\text{such that}\quad & dY_t = AY_t dt - f_{A,E}'^{-1}(\zeta_t)dt+\Sigma_t(Y_t)dB_t,\ Y_0=y_0. \\
(SP2):\ \min_{p_t\in\mathcal{P}}\ & \int_0^T e^{-rt}\left(f_{P,p}(p_t)-e^{-r(T-t)}p_t+\frac{1}{\gamma}f_{A,p}(p_t)\right)dt.
\end{aligned}
$$

Proof. For the constraint $dW_t = rW_t dt - f_{A,E}(f_{A,E}'^{-1}(\zeta_t))dt + f_{A,p}(p_t)dt + \zeta_t^{\mathsf{T}}\Sigma_t(Y_t)dB_t$, we obtain $W_t = e^{rt}W_0 - \int_0^t e^{r(t-s)}[f_{A,E}\big(f_{A,E}'^{-1}(\zeta_s)\big) - f_{A,p}(p_s)]ds + \int_0^t e^{r(t-s)}\zeta_s^{\mathsf{T}}\Sigma_s(Y_s)dB_s$. Thus, the principal's problem can be rewritten as

$$
\begin{aligned}
\min_{p_t\in\mathcal{P},\zeta_t}\ \mathbb{E}\int_0^T & e^{-rt}\left(f_{P,Y}(Y_t)+f_{P,p}(p_t)-e^{-r(T-t)}p_t\right)dt \\
& + e^{-rT}\Big[h_P(Y_T)+h_A^{-1}\big(e^{rT}\underline{J}_A - \int_0^T e^{r(T-s)}f_{A,E}\big(f_{A,E}'^{-1}(\zeta_s)\big)ds \\
& + \int_0^T e^{r(T-s)}f_{A,p}(p_s)ds + \int_0^T e^{r(T-s)}\zeta_s^{\mathsf{T}}\Sigma_s(Y_s)dB_s\big)\Big] \\
\text{such that}\quad & dY_t = AY_t dt - f_{A,E}'^{-1}(\zeta_t)dt+\Sigma_t(Y_t)dB_t,\ Y_0=y_0.
\end{aligned}
$$

Then, the decomposition of the problem follows naturally. □

Remark: ζ_t can be regarded as an *estimation variable* since it determines the anticipated effort E_t^*. The payment p_t is a *control variable* that manipulates the risk manager's incentives and is determined at the control phase. Under appropriate conditions, these two estimation and control variables can be designed in a separate

manner, yielding a separation principle in dynamic contract design for systemic risk management. The separation principle offers convenience and accelerates the computation of contract terms for the asset owner. That is, instead of solving a complicated stochastic control program, the asset owner can address two simpler problems to design the optimal contract.

To obtain more insights, we next focus on a class of models where the value function of the principal and the ODMD can be explicitly characterized.

8.4.4 ODMD in LQ Setting

In the LQ setting, the cost functions take forms as $f_{A,E}(E_t) = \frac{1}{2}E_t^{\mathsf{T}} R_t E_t$, and $f_{A,p}(p_t) = \delta_A p_t$, where R_t is a positive-definite $N \times N$-dimensional symmetric matrix and δ_A is a positive constant. Then we obtain

$$E_t^* = f_{A,E}'^{-1}(\zeta_t) = R_t^{-1}\zeta_t. \tag{8.26}$$

Further, we consider $h_P(Y_T) = \rho^{\mathsf{T}} Y_T$, where $\rho \in \mathbb{R}_+^N$ maps the cyber risks to monetary loss, and $f_P(t, Y_t, p_t) = \rho^{\mathsf{T}} Y_t + \delta_P p_t$, where δ_P is a positive constant. In addition, $h_A(M_T) = -M_T$ and $\Sigma_t(Y_t) = D_t \cdot diag(Y_t)$, where $D_t \in \mathbb{R}^{N\times N}$ and '$diag$' is a diagonal operator. The principal's problem becomes:

$$\begin{aligned}
&\min_{p_t\in\mathcal{P},\zeta_t} \ \mathbb{E}\int_0^T e^{-rt}(\rho^{\mathsf{T}} Y_t + \delta_P p_t - e^{-r(T-t)}p_t)dt + e^{-rT}(\rho^{\mathsf{T}} Y_T - W_T) \\
&\text{such that} \quad dY_t = (AY_t - R_t^{-1}\zeta_t)dt + D_t \cdot diag(Y_t)dB_t,\ Y_0 = y_0, \\
&\qquad\qquad dW_t = \left(rW_t - \frac{1}{2}\zeta_t^{\mathsf{T}} R_t^{-1}\zeta_t + \delta_A p_t\right)dt + \zeta_t^{\mathsf{T}}\Sigma_t(Y_t)dB_t,\ W_0 = \underline{J}_A.
\end{aligned}$$

The principal aims to maximize W_T, which is equivalent to minimizing the

agent's total revenue based on the relationship $W_T = -M_T$. The principal also considers the agent's participation constraint by setting $W_0 = W_0 = \underline{J}_A$, ensuring that the cyber risk manager has sufficient incentive to fulfill the task.

Since $e^{-rT}W_T = W_0 - \int_0^T e^{-rs}\left(\frac{1}{2}\zeta_s^\mathsf{T} R_s^{-1}\zeta_t - \delta_A p_s\right)ds + \int_0^T e^{-rs}\zeta_s^\mathsf{T} D_s \cdot diag(Y_s)dB_s$, the principal's problem can be rewritten as:

$$\min_{p_t\in\mathcal{P},\zeta_t} \mathbb{E}\int_0^T e^{-rt}\Big(\rho^\mathsf{T} Y_t + (\delta_P - \delta_A)p_t - e^{-r(T-t)}p_t + \frac{1}{2}\zeta_t^\mathsf{T} R_t^{-1}\zeta_t\Big)dt + e^{-rT}\rho^\mathsf{T} Y_T - \underline{J}_A$$

$$\text{such that} \quad dY_t = (AY_t - R_t^{-1}\zeta_t)dt + D_t \cdot diag(Y_t)dB_t,\ Y_0 = y_0.$$

According to Theorem 8.3, the separation principle holds in the LQ case. To determine the optimal p_t, we solve the following unconstrained optimization problem:

$$\min_{p_t\in\mathcal{P}} \int_0^T e^{-rt}(\delta_P - \delta_A - e^{-r(T-t)})p_t dt.$$

Depending on the values of parameters δ_P and δ_A, we obtain the following results. If $\delta_P - \delta_A \geq 1$, there is no intermediate payment, i.e., $p_t = 0$, $\forall t \in [0, T]$. In this regime, the principal has a higher valuation on the monetary payment than the agent does. In other words, the agent is relatively hard to be incentivized to do the risk management. When $\delta_P - \delta_A \leq 0$, i.e., the principal focuses more on the cyber risk deduction rather than the expenditure on incentivizing the agent, the optimal p_t is positively unbounded. However, in this regime, the terminal payment c_T is negatively unbounded based on (8.22). This contract corresponds to the scenario where the risk manager receives a large amount of intermediate payment during the task while returning it to the principal after finishing the task which is not

practical. Under $0 < \delta_P - \delta_A < 1$, the intermediate compensation is either 0 or unbounded depending on the time index. Hence, to design a practical contract, we focus on the regime in which the intermediate payment is zero, and the risk manager receives a positive terminal payment c_T.

To obtain the optimal $\{\zeta_t^*\}_{0\le t\le T}$, we assume that the process ζ_t, $t \in [0, T]$, is non-anticipative, which can be verified later after obtaining the solution ζ_t^*. Then, the problem can be further simplified to:

$$\begin{aligned} \min_{\zeta_t} \ & \mathbb{E}\int_0^T e^{-rt}\left(\rho^\mathsf{T} Y_t + \frac{1}{2}\zeta_t^\mathsf{T} R_t^{-1}\zeta_t\right)dt + e^{-rT}\rho^\mathsf{T} Y_T - \underline{J}_A \\ \text{such that} \quad & dY_t = (AY_t - R_t^{-1}\zeta_t)dt + D_t \cdot diag(Y_t)dB_t,\ Y_0 = y_0. \end{aligned}$$

The following theorem provides the optimal solution ζ_t^*.

Theorem 8.4. *In the LQ case, the optimal solution to the principal's problem is given by*

$$\zeta_t^* = K_t, \tag{8.27}$$

where K_t satisfies, and is the unique solution to

$$\dot{K}_t + (A - rI)^\mathsf{T} K_t + \rho = 0,\ K_T = \rho. \tag{8.28}$$

Furthermore, the minimum cost of the principal is given by

$$J_p^* = K_0^\mathsf{T} y_0 + m_0 - \underline{J}_A, \tag{8.29}$$

where m_0 is obtained uniquely from

$$\dot{m}_t - rm_t - \frac{1}{2}K_t^{\mathsf{T}} R_t^{-1} K_t = 0, \;\; m_T = 0. \tag{8.30}$$

Proof. Without loss of generality, we solve the optimal control problem by ignoring the constant term $\underline{J}_A$ in the cost function. The HJB equation

$$\begin{aligned} \min_{\zeta_t} \Big[\frac{1}{2} tr \left(\frac{\partial^2 V_p}{\partial Y_t^2} D_t \cdot diag(Y_t) \cdot diag(Y_t) D_t^{\mathsf{T}} \right) + \frac{\partial V_p}{\partial Y_t} \left(AY_t - R_t^{-1}\zeta_t \right) \\ + \rho^{\mathsf{T}} Y_t + \frac{1}{2}\zeta_t^{\mathsf{T}} R_t^{-1} \zeta_t \Big] + \frac{\partial V_p}{\partial t} = rV_p, \\ V_p(T, Y_T) = \rho^{\mathsf{T}} Y_T, \end{aligned} \tag{8.31}$$

yields the first-order condition $\zeta_t^* = \frac{\partial V_p}{\partial Y_t}$. Assume that the value function takes the form: $V_p(t, Y) = \frac{1}{2} Y^{\mathsf{T}} S_t Y + K_t^{\mathsf{T}} Y + m_t$, where S_t is an $N \times N$ symmetric matrix with continuously differentiable entries, K_t is a continuously differentiable N-dimensional vector, and m_t is a continuously differentiable function. Then, we obtain $\zeta_t^* = S_t Y_t + K_t$. Substituting ζ_t^* into the HJB equation yields

$$\begin{aligned} \frac{1}{2} tr \left(S_t D_t \cdot diag(Y_t) \cdot diag(Y_t) D_t^{\mathsf{T}} \right) + (S_t Y_t + K_t)^{\mathsf{T}} (AY_t - R_t^{-1} S_t Y_t - R_t^{-1} K_t) \\ + \rho^{\mathsf{T}} Y_t + \frac{1}{2}(S_t Y_t + K_t)^{\mathsf{T}} R_t^{-1} (S_t Y_t + K_t) \\ = r \left(\frac{1}{2} Y_t^{\mathsf{T}} S_t Y_t + K_t^{\mathsf{T}} Y_t + m_t \right) - \frac{1}{2} Y_t^{\mathsf{T}} \dot{S}_t Y_t - \dot{K}_t^{\mathsf{T}} Y_t - \dot{m}_t, \\ V_p(T, Y_T) = \rho^{\mathsf{T}} Y_T. \end{aligned} \tag{8.32}$$

Denote by I the N-dimensional identity matrix and by e_i the N-dimensional vector whose i-th element is 1 and the others are zero. Matching the coefficients in (8.32)

further yields the following coupled ordinary differential equations (ODEs):

$$\dot{S}_t + S_t A + A^\intercal S_t - rS_t - S_t R_t^{-1} S_t + \frac{1}{2}\sum_{i=1}^{N}\left(e_i e_i^\intercal D_t^\intercal S_t D_t\right) = 0,\ S_T = 0, \tag{8.33}$$

$$\dot{K}_t + (A - R_t^{-1}S_t - rI)^\intercal K_t + \rho = 0,\ K_T = \rho, \tag{8.34}$$

$$\dot{m}_t - rm_t - \frac{1}{2}K_t^\intercal R_t^{-1} K_t = 0,\ m_T = 0. \tag{8.35}$$

Here, (8.33) is a matrix Riccati equation. However, based on the terminal condition $S_T = 0$, we see that the unique solution to (8.33) is $S_t = 0$, $\forall t$. Therefore, a linear value function $V_p(t, Y) = K_t^\intercal Y + m_t$ is sufficient. Then, the ODEs (8.34) and (8.35) can be rewritten as (8.28) and (8.30), respectively, which being linear admit unique solutions. □

We then obtain the explicit form of optimal dynamic contract in the subsequent lemma.

Lemma 8.4. *In the LQ case, the optimal dynamic contract designed by the principal is given by*

$$\begin{aligned} dc_t &= \left(rc_t + \frac{1}{2}K_t^\intercal R_t^{-1} K_t\right)dt - K_t^\intercal\left(dY_t - AY_t dt + R_t^{-1}K_t dt\right) \\ &= \left(rc_t - \frac{1}{2}K_t^\intercal R_t^{-1} K_t\right)dt - K_t^\intercal\left(dY_t - AY_t dt\right), \end{aligned} \tag{8.36}$$

with $c_0 = -\underline{J}_A > 0$, and K_t is given by (8.28). The intermediate payment p_t degenerates to zero, and the anticipated effort of the agent under the optimal contract is $E_t^* = R_t^{-1}K_t$.

Proof. The result follows from Theorems 8.1, 8.4, and (8.22). □

Remark: As shown in Lemma 8.4, the cyber risk volatility $\Sigma_t(Y_t)$ does not

impact the optimal dynamic contract design, since the principal's expected cost is linear in the systemic risk Y_t. When one of the functions f_p, h_A and h_p is not linear, the volatility $\Sigma_t(Y_t)$ will play a role in the contract design in solving the problem presented in Theorem 8.2.

Even though the optimal dynamic contract does not depend on the cyber risk volatility in the LQ case, the risk volatility influences the real compensation during contract implementation.

Corollary 8.2. *The terminal compensation of risk manager has a larger variance when there are more complex interdependencies of risk uncertainties between nodes.*

Corollary 8.2 will further be illustrated through case studies in Section 8.6.

8.5 Benchmark Scenario: Systemic Cyber Risk Management under Full Information

In the full-information case, the principal observes the efforts that the cyber risk manager implements. We first solve the team problem in which the agent cooperates with the principal. To that end, the principal's cost under the team optimal solution is the best that he can achieve. Then, we aim to design a dynamic contract mechanism under which the agent will adopt the same policy as the team optimal one. In the cooperative case, the contract only needs to guarantee the participation constraint. Then, the principal's problem can be formulated as

follows:

$$
\begin{aligned}
(\mathrm{O}-\mathrm{B}): \quad & \min_{p_t\in\mathcal{P},c_T,E_t\in\mathcal{E}} \mathbb{E}\int_0^T e^{-rt} f_P(t,Y_t,p_t)dt + e^{-rT}\left(c_T + h_P(Y_T)\right) \\
& \text{such that} \quad dY_t = AY_t dt - E_t dt + \Sigma_t(Y_t)dB_t,\ Y_0 = y_0, \\
& \qquad\qquad J_A\left(\{E_t^*\}_{0\le t\le T}; \{p_t\}_{0\le t\le T}, c_T\right) = \underline{J}_A.
\end{aligned}
$$

As in the asymmetric information scenario, it is more convenient to deal with the dynamics of the cyber risk manager's expected cost. By designing the contract, the principal only needs to ensure the participation of the agent. Then, the principal's problem can be rewritten as follows:

$$
\begin{aligned}
(\mathrm{O}-\mathrm{B}'): \quad & \min_{p_t\in\mathcal{P},\zeta_t,E_t\in\mathcal{E}} \mathbb{E}\int_0^T e^{-rt}\Big(f_P(t,Y_t,p_t) - e^{-r(T-t)}p_t\Big)dt \\
& \qquad\qquad + e^{-rT}\left(h_P\big(Y_T\big) + h_A^{-1}(W_T)\right) \\
& \text{such that} \quad dY_t = AY_t dt - E_t dt + \Sigma_t(Y_t)dB_t,\ Y_0 = y_0, \\
& \qquad\qquad dW_t = rW_t dt - f_A\big(t,p_t,E_t\big)dt + \zeta_t^{\mathsf{T}}\Sigma_t(Y_t)dB_t,\ W_0 = \underline{J}_A.
\end{aligned}
$$

With the full observation of Y_t and E_t, ζ_t can be chosen freely, and E_t can be seen as a control variable of the principal. Note that the IC constraint (8.21) does not enter into $(\mathrm{O}-\mathrm{B}')$. In addition, the equivalent terminal payment process c_t admits the same form as (8.22). $(\mathrm{O}-\mathrm{B}')$ is a standard stochastic optimal control problem which can be solved efficiently.

To quantify the efficiency of dynamic contract designed in Section 8.4, we have the following definition.

Definition 8.5 (Information Rent)**.** *Denote the solutions to* $(\mathrm{O}-\mathrm{A})$ *and* $(\mathrm{O}-\mathrm{P})$ *by* $\{E_t^*\}_{0\le t\le T}$ *and* $\{\{p_t^*\}_{0\le t\le T}, c_T^*\}$*, respectively. Further, denote the solution to*

$(\mathrm{O}-\mathrm{B})$ *by* $\{\{p_t^b\}_{0\le t\le T}, c_T^b, \{E_t^b\}_{0\le t\le T}\}$. *Then, the information rent is given by*

$$I_R = J_P(\{p_t^*\}_{0\le t\le T}, c_T^*) - J_P(\{p_t^b\}_{0\le t\le T}, c_T^b). \tag{8.37}$$

Intuitively, information rent quantifies the difference between the principal's costs with optimal mechanisms designed under incomplete and full information.

We have following result on information rent.

Corollary 8.3. *The optimal cost of the principal under full information is no larger than the one under asymmetric information. Hence,* $I_R \ge 0$.

Proof. Comparing with the optimal $\{E_t^*\}_{0\le t\le T}$ in $(\mathrm{O}-\mathrm{P}')$, the implemented effort $\{E_t^b\}_{0\le t\le T}$ in $(\mathrm{O}-\mathrm{B}')$ does not depend on the variables ζ_t and p_t. Thus, $(\mathrm{O}-\mathrm{B}')$ admits a larger feasible solution space, which yields the result. □

8.5.1 LQ Setting: Certainty Equivalence Principle

To further characterize the optimal contracts under full information and quantify the information rent, we investigate a class of special scenarios. Specifically, we take the functions to have the same forms as in Section 8.4.4. The principal's problem can then be written as

$$\begin{aligned}\min_{p_t\in\mathcal{P}, E_t\in\mathcal{E}} \quad & \mathbb{E}\int_0^T e^{-rt}\Big(\rho^\intercal Y_t + (\delta_P-\delta_A)p_t - e^{-r(T-t)}p_t + \frac{1}{2}E_t^\intercal R_t E_t\Big)dt \\ & \qquad + e^{-rT}\rho^\intercal Y_T - \underline{J}_A \\ \text{such that} \quad & dY_t = (AY_t - E_t)dt + D_t\cdot diag(Y_t)dB_t,\ Y_0 = y_0.\end{aligned}$$

Note that ζ_t does not appear in the optimization problem. However, ζ_t enters the designed contract (8.22) through the term $-\zeta_t^\intercal \Sigma_t(Y_t)dB_t$. In the long term

contracting when T is relatively large, the expected value of $-\zeta_t^\intercal \Sigma_t(Y_t) dB_t$ is zero which is irrelevant with ζ_t. Hence, the principal can set $\zeta_t = 0$ to reduce the contract complexity.

Similar to the analysis in Section 8.4.4, we focus on the regime where the intermediate payment flow p_t is zero, to avoid the unrealistic situation of negative terminal payment. We obtain the following lemma characterizing the *certainty equivalence principle*.

Lemma 8.5. *In the LQ settings, $I_R = 0$ which reveals the certainty equivalence principle, i.e., the designed optimal contracts under the incomplete information are as efficient as those designed under complete information.*

Proof. By regarding E_t as the role of $R_t^{-1}\zeta_t$, we see that the problem is reduced to the one in Section 8.4.4. Hence, the minimum cost of the principal in the full information case is the same as that under the incomplete information. □

Remark: When the agent's terminal cost function h_A is not linear, $h_A^{-1}(W_T)$ will not be linear in W_T. Thus, the decision variable ζ_t remains in the principal's objective function. Then, the contract design under full information becomes more efficient as there is no dependency between ζ_t and E_t introduced by the IC constraint.

In the LQ case, the team optimal contract is summarized as follows.

Lemma 8.6. *In the LQ setting, the team optimal dynamic contract is*

$$\begin{aligned} dc_t^b &= \left(r c_t^b + \frac{1}{2} K_t^\intercal R_t^{-1} K_t \right) dt, \\ E_t^b &= R_t^{-1} K_t, \end{aligned} \tag{8.38}$$

with $c_0^b = -\underline{J}_A > 0$, and K_t is given by (8.28). The intermediate payment is zero.

Proof. The result follows immediately from Theorem 8.4 and (8.22) with $\zeta_t = 0$. □

The following lemma provides a mechanism that leads to implementation of the team optimal solution presented in Lemma 8.6 without forcing the agent to follow E_t^b.

Lemma 8.7. *In the LQ setting, the implementable optimal dynamic contract designed by the principal under full information is*

$$dc_t = \left(rc_t - \frac{1}{2} K_t^\intercal R_t^{-1} K_t + K_t^\intercal E_t \right) dt, \tag{8.39}$$

with $c_0 = -\underline{J}_A > 0$ *and* K_t *given by* (8.28). *The intermediate payment is zero, and the agent's best response is* $E_t = R_t^{-1} K_t$.

Proof. Similar to the methodologies proposed in [14, 15, 29], we let the contract take the following form:

$$dc_t = \left(rc_t + \frac{1}{2} K_t^\intercal R_t^{-1} K_t \right) dt + \Gamma_t^\intercal (E_t - R_t^{-1} K_t) dt, \tag{8.40}$$

where Γ_t is an N-dimensional vector to be determined. The second term $\Gamma_t^\intercal (E_t - R_t^{-1} K_t) dt$ is introduced to penalize the agent when his action deviates from $R_t^{-1} K_t$. The agent solves his problem by responding to this announced contract from the principal. Similar to (O − A′) and using $V_a(t, c_t) = h_A(c_t) = -c_t$, we obtain the corresponding HJB equations as

$$\min_{E_t} \left[\frac{\partial V_a}{\partial c_t} \left(rc_t + \frac{1}{2} K_t^\intercal R_t^{-1} K_t + \Gamma_t^\intercal (E_t - R_t^{-1} K_t) \right) + f_A(t, p_t, E_t) \right] + \frac{\partial V_a}{\partial t} = rV_a,$$

$$V_a(T, c_T) = -c_T.$$

The optimal solution of the agent is achieved at

$$E_t^o = \arg\min_{E_t} -\Gamma_t^\intercal E_t + \frac{1}{2} E_t^\intercal R_t E_t,$$

which yields $E_t^o = R_t^{-1}\Gamma_t$. Based on Lemma 8.6, we choose $\Gamma_t = K_t$, and thus the agent implements the team optimal solution E_t^b. Further, (8.40) degenerates to the one in (8.38). □

Remark: In the LQ setting under full information and incomplete information, the optimal contract and the manager's behavior do not relate to the risk volatility $\Sigma_t(Y_t)$ of the network. The reason is that the cost function of the principal is linear in the systemic risk Y_t. Hence, the expectation of the risk volatility term is zero, and $\Sigma_t(Y_t)$ does not play a role in the optimal dynamic contract. This fact in turn corroborates the zero information rent in the LQ setting due to the removal of risk uncertainty.

A more general class of scenarios satisfying the certainty equivalence principle that leads to zero information rent is summarized as follows.

Corollary 8.4. *When $f_P(t, \phi, p_t)$, $h_p(\phi)$ and $h_A(\phi)$ are linear in the argument ϕ, then $I_R = 0$, where the optimal contracts under the full information and incomplete information coincide.*

Proof. The linearity of functions removes the effects of risk uncertainties on the performance of the principal and the agent which leads to a zero information rent. □

Note that the certainty equivalence principle provides guidelines and insights for the asset owner when outsourcing the cyber risk management tasks to the

agent. Specifically, when proposing contracts, if the conditions in Corollary 8.4 are satisfied, the asset owner is confident that having access to the risk manager's hidden effort does not matter (due to certainty equivalence). Furthermore, in the LQ setting, the asset owner can directly leverage the closed-form solution shown in Lemma 8.7, which offers great convenience in contract design for systemic cyber risk management.

8.6 Case Studies

We demonstrate, in this section, the optimal design principles of dynamic contracts for systemic cyber risk management of enterprise networks through examples. Specifically, we first utilize a case study with one node to show that the dynamic contracts can successfully mitigate the systemic risk in a long period of time. Then, we investigate an enterprise network with a set of interconnected nodes to reveal the network effects in systemic risk management through dynamic contracts and discover a distributed way of mitigating the systemic risks.

8.6.1 One-Node System Case

First, we consider a one-dimensional case in which the enterprise network contains only one node, i.e., Y_t is a scalar. Therefore, the risk manager protects the system by directing the security resources to this node. Note that for the LQ setting, the coupled ODEs in Theorem 8.4 admit the unique solutions:

$$K_t = \frac{\rho}{A-r}\left((A-r+1)e^{(A-r)(T-t)}-1\right),\ m_t = \frac{K_t^2}{2rR_t}\left(e^{-r(T-t)}-1\right). \tag{8.41}$$

Therefore, based on Lemma 8.4, the optimal effort of the risk manager is

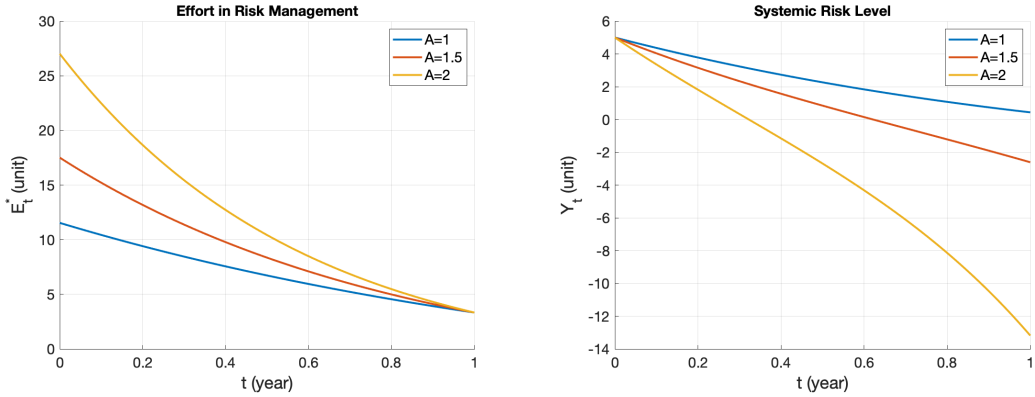
$$E_t^* = R_t^{-1}\zeta_t^* = \frac{\rho}{R_t(A-r)}\left((A-r+1)e^{(A-r)(T-t)}-1\right), \tag{8.42}$$

and the optimal compensation becomes

$$dc_t = \left(rc_t - \frac{K_t^2}{2R_t} + AK_tY_t\right)dt - K_tdY_t,\ c_0 = -\underline{J}_A. \tag{8.43}$$

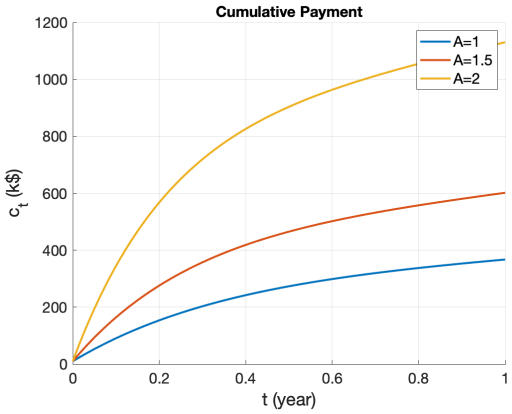
If the risk manager accepts this optimal contract, then the principal's excepted minimum cost is equal to $J_P^* = K_0^\intercal y_0 + m_0 - \underline{J}_A$.

To illustrate the optimal mechanism design, we choose specific values for the parameters in Section 8.4.4: $\rho = 5$ k\$/unit, $r = 0.3$, $R_t = 1.5$ k\$/unit^2, $T = 1$ year, $y_0 = 5$ unit, and $\underline{J}_A = -10$ k\$. Here, notation 1 k\$/unit represents \$1000 per unit. Figure 8.2 shows the results for varying values of the parameter A. Note that a single node system with a larger A indicates that it is more vulnerable and harder to mitigate the cyber risk. From Fig. 8.2, we find that with a larger A, the system requires more effort from the risk manager to bring the cyber risk down to a relatively low level. In all cases, the effort decreases as time increases, and finally converges to a positive constant $\frac{\rho}{R_t}$. This phenomenon indicates that when the system risk is high, the agent should spend more effort in risk management. When the risk is reduced to a relatively low level and the system becomes secure, then less effort is preferable as the risk will not grow. In addition, the corresponding terminal compensation c_T increases with the amount of effort spent.



(a) Effort

(b) Systemic cyber risk

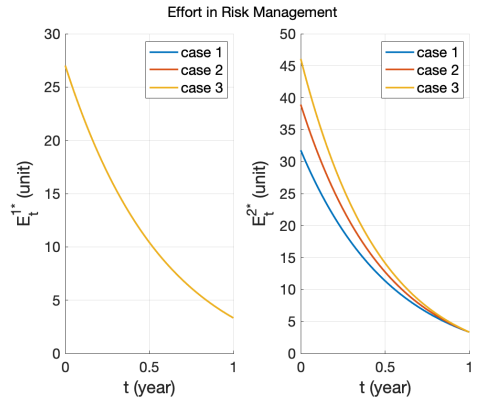


(c) Cumulative payment

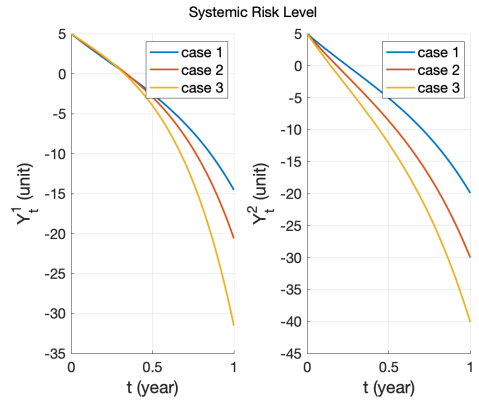
Figure 8.2: (a), (b), and (c) show the effort, the cyber risk, and the terminal payment under the optimal contract. The terminal compensation c_T increases with the spent effort of the risk manager.

8.6.2 Network Case

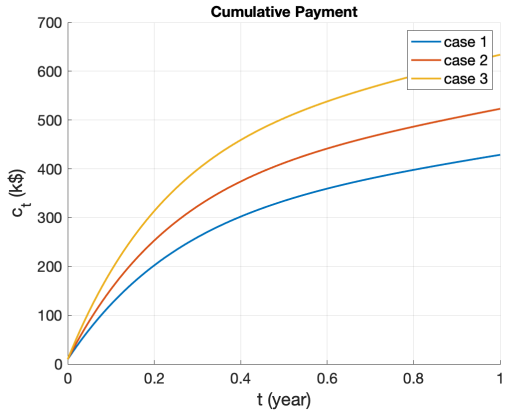
We next investigate cyber risk management over enterprise networks and characterize the interdependencies between nodes. The unique solutions to the ODEs



(a) Effort



(b) Systemic cyber risk



(c) Cumulative payment

Figure 8.3: (a), (b), and (c) show the effort, the systemic risk, and the terminal payment under the optimal contract. Case 1: $A = [2, 0.2; 0, 2]$; Case 2: $A = [2, 0.5; 0, 2]$; Case 3: $A = [2, 0.8; 0, 2]$. A higher network connectivity requires more effort to mitigate the systemic cyber risk.

in Theorem 8.4 are then as follows:

$$K_t = \rho \left[(A - rI)^\intercal\right]^{-1} \left(\left((A - rI)^\intercal + I\right) e^{(A-rI)^\intercal (T-t)} - I\right), \tag{8.44}$$

$$m_t = \frac{K_t^\intercal R_t^{-1} K_t}{2r} \left(e^{-r(T-t)} - 1\right), \tag{8.45}$$

The optimal effort of the risk manager is

$$E_t^* = R_t^{-1}\rho\left[(A-rI)^\mathsf{T}\right]^{-1}\left(\left((A-rI)^\mathsf{T}+I\right)e^{(A-rI)^\mathsf{T}(T-t)}-I\right),$$

and the optimal compensation follows (8.36).

We first consider a cyber network containing two connected nodes. For convenience, we adopt the form $[\mathsf{a},\mathsf{b},\mathsf{c};\mathsf{d},\mathsf{e},\mathsf{f}]$ to represent the matrix $\begin{bmatrix}\mathsf{a} & \mathsf{b} & \mathsf{c}\\ \mathsf{d} & \mathsf{e} & \mathsf{f}\end{bmatrix}$ throughout the following examples. The system parameters are chosen as $\rho = [5;5]$ k\$/unit, $r = 0.3$, $R_t = [1.5, 0; 0, 1.5]$ k\$/unit^2, $T = 1$ year, $y_0 = [5;5]$ unit, and $\underline{J}_A = -10$ k\$. Moreover, we compare three scenarios in terms of network interdependencies. Specifically, we have case 1: $A = [2, 0.2; 0, 2]$, case 2: $A = [2, 0.5; 0, 2]$, and case 3: $A = [2, 0.8; 0, 2]$. Figure 8.3 shows the results, where we denote by E_t^{i*} and Y_t^i the effort and the corresponding risk of node i, $i = 1, 2$, respectively. Similar to the single-node case, both the effort and systemic risk decrease over time. Specifically, the dynamic effort converges to $R_t^{-1}\rho$ which can be verified directly by the analytical expression. Comparing E_t^{1*} with E_t^{2*}, we find that the risk manager should spend more effort on the nodes which can heavily influence other nodes. Even though there is no risk influence from node 1 to node 2, the optimal effort E_t^{2*} increases as the influence strength becomes larger from node 2 to node 1. This phenomenon is consistent with the idea of *controlling the origin* to constrain the propagation of cyber risks. Furthermore, the value of E_t^{2*} indicates that a higher network connectivity requires more effort to mitigate the systemic cyber risk.

We next investigate a 4-node system where the network structures are shown in Fig. 8.4. The system parameters are the same as those in the 2-node case except for the matrix A. The diagonal entries in A are all equal to 2 and the off-diagonal

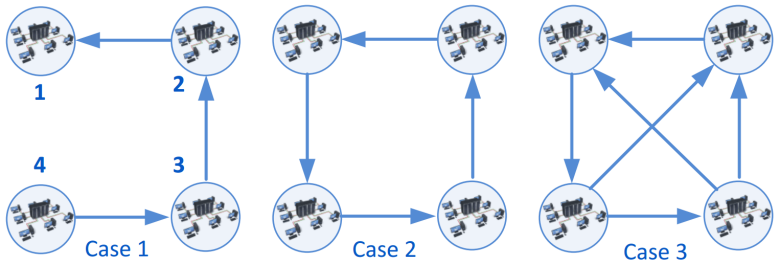
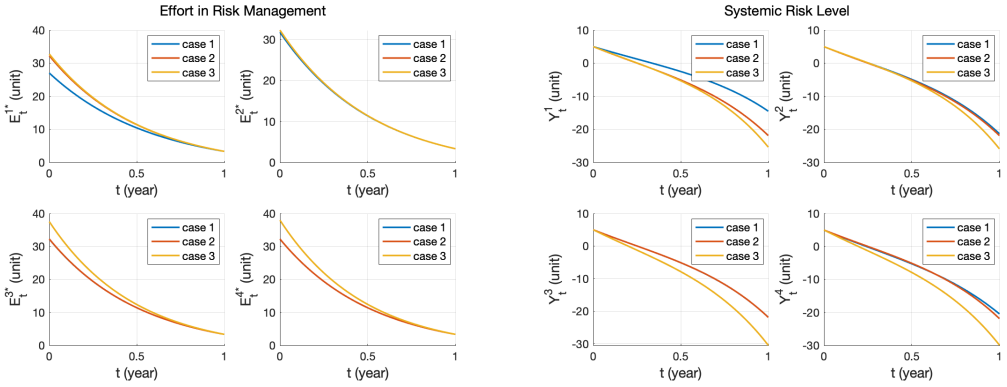
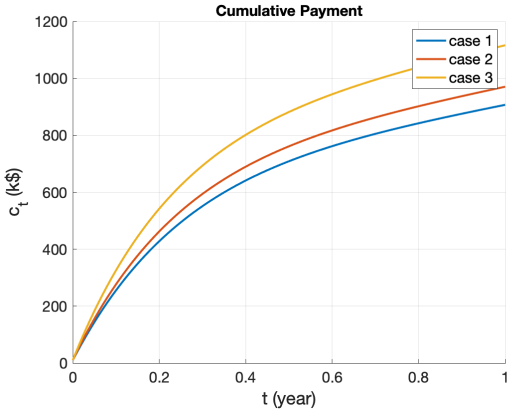


Figure 8.4: Three different structures of enterprise network. The risk influence strengths are the same, admitting a value of 0.2 in matrix A.



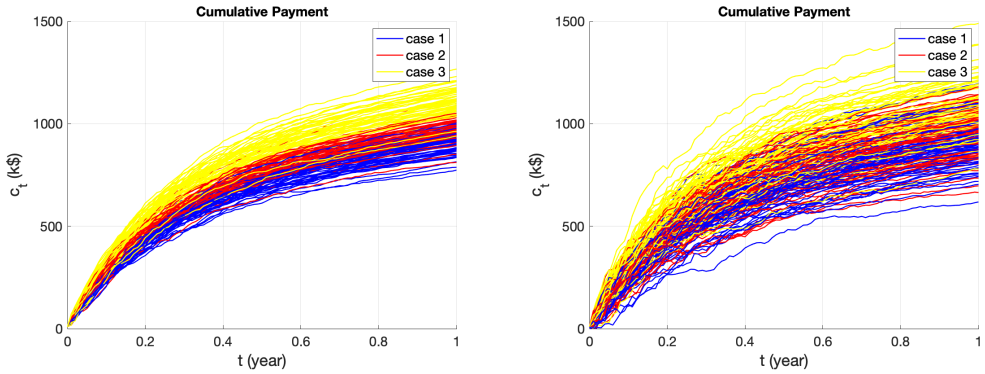
(a) Effort

(b) Systemic cyber risk



(c) Cumulative payment

Figure 8.5: (a), (b), and (c) show the effort, the systemic risk and the terminal payment under the optimal contract. Each node is self-accountable for its risk influence on others.



(a) (b)

Figure 8.6: (a) and (b) depict the optimal terminal payment under different risk volatility structure. The risk volatility of nodes is independent in (a), while the influence of risk volatility in (b) admits a cycle structure as case 2 in Fig. 8.4. The results indicate that a larger interdependency of cyber risk volatility yields compensation schemes with a larger variance.

entries that correspond to a link are all equal to 0.2. Figure 8.5 shows the results under the optimal mechanism. The risk manager spends more effort on node 1 in cases 2 and 3 than in case 1, as the risk of node 1 can propagate to node 4 in the former two cases. Another key observation is that the amount of allocated effort on each node mainly depends on its risk influences on other nodes rather than on the exogenous risks (node's outer degree), yielding a *self-accountable* risk mitigation scheme. For example, even though node 4 impacts node 2 in case 3, the risk management efforts on node 2 are close in cases 2 and 3. A similar pattern can be seen on node 4 in cases 1 and 2. This observation provides a distributed method of risk management which reduces the complexity of decision-making by simplifying the network structures and classifying the nodes based on their outer degrees. By comparing three cases, we also conclude that more complex cyber interdependencies induce higher cost on the principal in the security investment.

Note that in the above case studies, all variables were evaluated under the

expectation with respect to the cyber risk uncertainty. As shown in Corollary 8.2, even though the expected compensation is independent of the network risk uncertainty, the actual compensation during contract implementation is influenced by the volatility term $\Sigma_t(Y_t)$. We present two scenarios in Fig. 8.6, where Fig. 8.6(a) and Fig. 8.6(b) are the compensation realizations under $\Sigma_t(Y_t) = I$ and $\Sigma_t(Y_t) = [1, 1, 0, 0; 0, 1, 1, 0; 0, 0, 1, 1; 1, 0, 0, 1]$, respectively. When the nodes' risks face more sources of uncertainties in Fig. 8.6(b), the corresponding payment exhibits a larger variance comparing with the one in Fig. 8.6(a), which is consistent with the result of Corollary 8.2.

8.7 Summary

In this chapter, we have addressed the problem of dynamic systemic cyber risk management of enterprise networks, where the principal provides contractual incentives to the manager, which include the compensations of direct cost of effort and indirect cost from risk uncertainties. This has involved a stochastic Stackelberg differential game with asymmetric information in a principal-agent setting. Under the optimal incentive compatible scheme we have designed, the principal has rational controllability of the systemic risk where the suggested and adopted efforts coincide, and the risk manager's behavior is strategically neutral, depending only on the current net cost. Under mild conditions, we have obtained a separation principle where the effort estimation and the remuneration design can be separately achieved. We further have revealed a certainty equivalence principle for a class of dynamic mechanism design problems where the information rent is equal to zero. Through case studies, we have identified the network effects in the systemic risk management

where the connectivity and node's outer degree play an important role in the decision making. Future work on this topic would consider cyber risk management of enterprise networks under Markov jump risk dynamics. Another interesting direction of future work would be to incorporate the renegotiation option in the contract, which is a practical consideration in the risk management application.

Chapter 9

Conclusion and Future Work

9.1 Conclusion

In this dissertation, I have investigated in detail the secure and resilient design of high-confidence CPS networks from a cross-disciplinary perspective. Figure 9.1 depicts an overview of my research on the theme of CPS security and resilience. To achieve the goal, I have focused on three critical aspects including network design, trustworthy decision making, and network economics. The distinct challenges arising from CPS, including large-scale networks, massive connectivity, and complex interdependencies have been addressed. This dissertation has analyzed trustworthy CPS network design across different dimensions: from single-layer network to multi-layer networks, from static networks to dynamic systems, from fully rational decision making to bounded rational strategies, and from risk self-mitigation scheme to delegated risk transfer. We summarize this dissertation as follows.

Chapters 3 and 4 have been devoted to the strategic CPS network design. In Chapter 3, we have proposed a two-layer heterogeneous framework for IoT networks

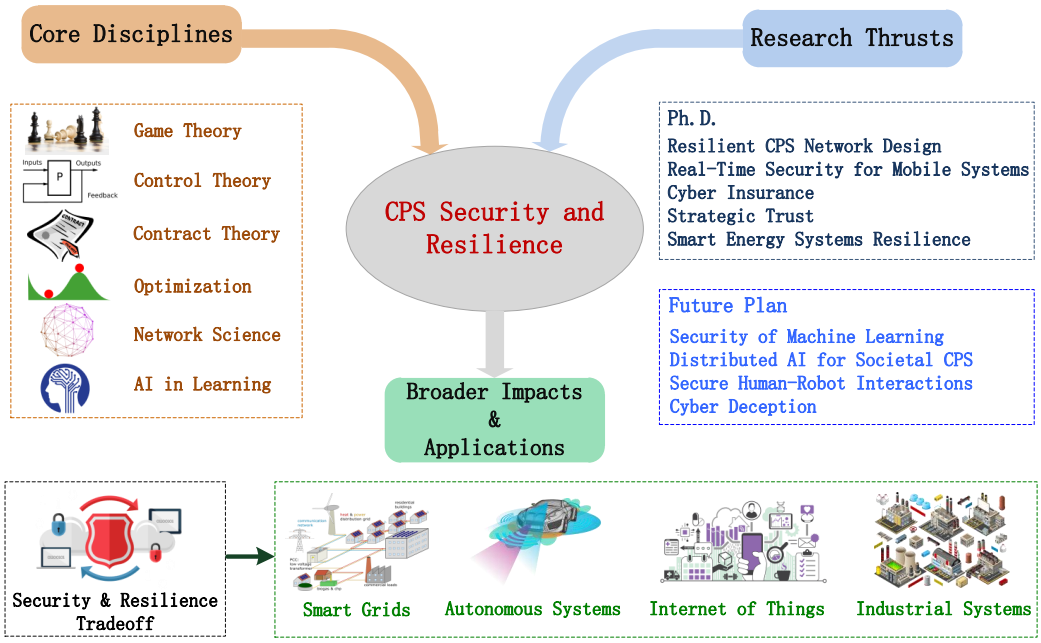


Figure 9.1: Overview of my Ph.D. research on the theme of CPS security and resilience.

consisting of various devices, where each layer network faces different levels of cyber threats. By utilizing the tools from graph theory and optimization, we have analyzed the lower bounds of the number of required links for the IoT network being connected. We have also derived optimal strategies for creating secure two-layer IoT networks with heterogeneous security requirements and provided their constructive algorithms. In Chapter 4, we have focused on analyzing the dynamic interplay between the network defender and attacker over infrastructure networks. We have proposed a two-player three-stage dynamic game framework to study the infrastructure network security and resiliency. Furthermore, we have provided a complete analysis of the subgame perfect Nash equilibrium of the dynamic game which includes the defense and recovery strategies of the network defender and the

attacking strategy of the adversary.

Chapters 5 and 6 have been focused on the trustworthy decision making in CPS networked systems. Specifically, Chapter 5's goal is to investigate the human's irrational behavior during security investment. To that end, we have proposed a holistic framework to study the security management of users with bounded rationality in the IoT networks, where the limited cognition of users has been modeled through a sparse vector. We also have designed a proximal-based algorithm to compute the solution which contains security management strategy and cognitive network of agents. The algorithm has discovered several phenomena including emergence of partisanship, filling the inattention, and attraction of the mighty. Our focus in Chapter 6 has been shifted from static CPS networks to dynamic networked systems. Specifically, we have established a games-in-games framework that enables uncoordinated and secure control of multi-layer autonomous systems under cyberattacks. Furthermore, we have proposed a meta-equilibrium solution concept to capture the interdependent decision makings of network players in a holistic fashion, and characterized the strategic behavior of the attacker explicitly. A resilient and decentralized iterative algorithm has been proposed that can maximize the connectivity of the networked autonomous systems.

Chapters 7 and 8 have been devoted to enhancing CPS security using a mechanism design approach. In Chapter 7, we have used contract design principles to propose an integrative cyber-physical framework to develop a holistic incentive-compatible and cost-efficient security as a service mechanism for real-time operation of cloud-enabled Internet of controlled things under advanced persistent threats. We have composed a game modeling cloud security with the contract design through a bi-level game model to capture the strategic interactions between the service

provider, the service requester, and the adversary. Further, we have proposed iterative algorithms to compute the optimal cyber-physical contract. In Chapter 8, we have focused on dynamic mechanism design for systemic cyber risk management of enterprise networks under the hidden-action type of incomplete information. To characterize the solution, we have provided a systematic methodology by transforming the problem into a stochastic optimal control problem with compatible information structures. We have also identified several important rules, including a separation principle and a certainty equivalence principle for a class of dynamic mechanism design problems. The proposed approach has been corroborated to be effective in the cyber risks transfer.

9.2 Future Work

There are many exciting research directions that can be explored further beyond the focuses of this dissertation. An important one is the design of intelligent and high-confidence next-generation large-scale CPS networks, as they will pervade more facets of our life in the coming decades. It is also critical to expedite CPS realizations with built-in security, resilience, and intelligence in a wide range of applications including robotic operations, transportation systems, manufacturing systems, and smart grids. To achieve these goals, there are a number of new areas to be explored, including *security of learning algorithms* for complex CPS, *distributed AI* for large-scale societal CPS, and *cyber deception* for proactive CPS security.

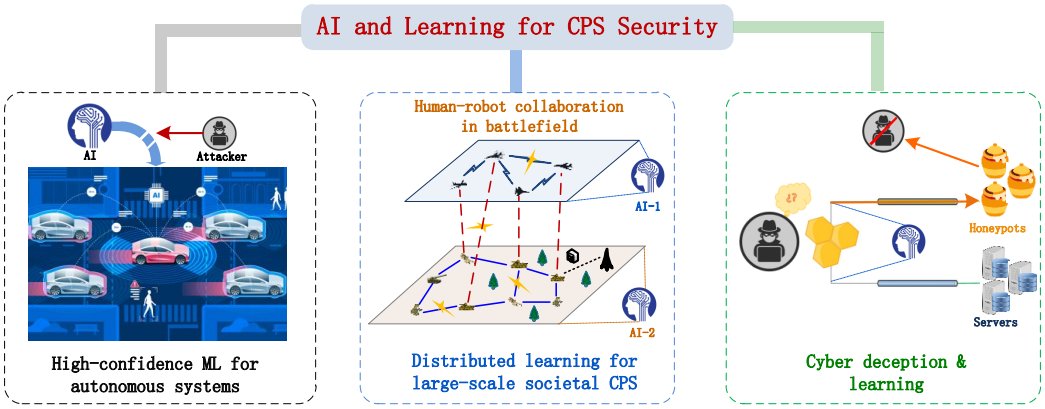


Figure 9.2: Future research directions on AI and learning for high-confidence CPS.

9.2.1 High-Confidence Real-Time Machine Learning for Autonomous Systems

Reinforcement learning (RL) has been shown powerful in many decision making problems with partial or unknown information, ranging from computer games to control of engineering systems. RL algorithms have also been applied to CPS which enables real-time data-driven control, improving the CPS resilience to failures. However, the integration of RL mechanisms with CPS creates new security concerns. For example, the adversary can obscure and manipulate the data (possibly collected by sensors) that are required during determining online decisions, which poses a substantial threat to CPS especially in the mission-critical applications such as autonomous driving and Internet of battlefield things. Therefore, RL algorithms should be reliable and secure enough to guarantee a satisfactory performance when applied to CPS in the adversarial environment. The goal is to lay a theoretical and computational-efficient foundation to assure that RL algorithms can be deployed in the autonomous systems with high confidence. This endeavor starts with under-

standing adversarial behaviors in RL synthesis with dynamic CPS and establishing frameworks to quantify the impacts of attacks to RL algorithms, which are essential to the development of countermeasures against strategic and stealthy attacks. It is possible to implement the developed provably-secure RL algorithms on mobile autonomous cars, which have a substantial market ($556.67 billion by 2026), to test practical cyberattacks, e.g., delayed signal and falsified data during feedback on-line decision making.

9.2.2 Distributed Learning for Large-Scale Human-in-the-Loop CPS

Classical ML algorithms are generally designed to optimize a single performance criterion based on expected utility theory. However, this framework cannot be directly applied to the modern CPS that often cooperate and interact closely with humans. One major reason is that, different from cyber and physical components, human's valuations on gains and losses are different due to emotional and cognitive biases; i.e., human's preferences are inconsistent with expected utilities. To capture the hybrid and heterogeneous features of modern CPS, we need to develop human-centered ML algorithms applicable to societal CPS, where humans could interact with the CPS directly. Besides the human factor consideration, another challenge to deal with is the efficiency of learning algorithms applied to the control of large-scale CPS due to the curse of dimensionality. Thus, the development of distributed and scalable federated learning algorithms for dynamic operations of large-scale CPS becomes critical. One possible idea is to first divide the CPS network into subnetworks based on the online data using statistical inference and learning methods. This partitioning is possible as large-scale CPS exhibit many redundancies

in their dynamics. Then, the control policy can be learned independently for each subnetwork, and composed to achieve the global optimal objective. The broader application of this research lies in the multi-agent human-robot interaction, such as a group of aerial robots collaborating with another group of soldiers to accomplish missions in the battlefield.

9.2.3 Cyber Deception for Proactive CPS Security

Deception has played a crucial role in the history of military combat and Sun Tzu has said: *all warfare is based on deception*. The philosophy still holds in the modern days. There is a growing amount of interest from security and defense sectors national-wide on the investigation and design of deceptive mechanisms in safeguarding the cyberspace. To this end, the first challenge is to scientifically model the attacker's behavior and quantify the corresponding impacts to the system. The other one is that the designed defensive mechanism should be robust under incomplete information and adaptive to the evolution of attacks. By leveraging game theory and AI, it is possible to develop a systematic framework to understand deceptions and counterdeceptions, and design new data-driven autonomous mechanisms to mitigate cyber risks using strategic learning algorithms. This research direction is a new avenue toward building high-confidence CPS with built-in proactive security.

Bibliography

[1] Upguard. https://www.upguard.com/. Accessed: 2020-01-25.

[2] D. M. Akos. Who's afraid of the spoofer? gps/gnss spoofing detection via automatic gain control (agc). *Navigation*, 59(4):281–290, 2012.

[3] D. L. Alderson, G. G. Brown, W. M. Carlyle, and R. K. Wood. Solving defender-attacker-defender models for infrastructure defense. In *Operations Research, Computing and Homeland Defense, INFORMS*, 2011.

[4] T. Alpcan and T. Başar. *Network security: A decision and game-theoretic approach*. Cambridge University Press, 2010.

[5] E. Altman, A. Singhal, C. Touati, and J. Li. Resilience of routing in parallel link networks. In *International Conference on Decision and Game Theory for Security*, pages 3–17. Springer, 2016.

[6] H. Attouch, J. Bolte, P. Redont, and A. Soubeyran. Proximal alternating minimization and projection methods for nonconvex problems: An approach based on the kurdyka-lojasiewicz inequality. *Mathematics of Operations Research*, 35(2):438–457, 2010.

[7] R. J. Aumann, M. Maschler, and R. E. Stearns. *Repeated games with incomplete information*. MIT press, 1995.

[8] T. Başar. An equilibrium theory for multiperson decision making with multiple probabilistic models. *IEEE Transactions on Automatic Control*, 30(2):118–132, 1985.

[9] T. Başar and G. J. Olsder. *Dynamic Noncooperative Game Theory*. Classics in Applied Mathematics, SIAM, Philadelphia, 2nd edition, 1999.

[10] V. Bala and S. Goyal. A noncooperative model of network formation. *Econometrica*, 68(5):1181–1229, 2000.

[11] A. Baldwin, I. Gheyas, C. Ioannidis, D. Pym, and J. Williams. Contagion in cyber security attacks. *Journal of the Operational Research Society*, 68(7):780–791, 2017.

[12] R. Bansal and T. Başar. Stochastic teams with nonclassical information revisited: When is an affine law optimal? *IEEE Transactions on Automatic Control*, 32(6):554–559, 1987.

[13] R. G. Baraniuk. Compressive sensing. *IEEE signal processing magazine*, 24(4), 2007.

[14] T. Başar. Affine incentive schemes for stochastic systems with dynamic information. *SIAM Journal on Control and Optimization*, 22(2):199–210, 1984.

[15] T. Başar. Stochastic incentive problems with partial dynamic information

and multiple levels of hierarchy. *European Journal of Political Economy*, 5(2-3):203–217, 1989.

[16] T. Başar. Stochastic differential games and intricacy of information structures. In *Dynamic Games in Economics*, pages 23–49. Springer, Berlin, Heidelberg, 2014.

[17] T. Başar and R. Bansal. Optimum design of measurement channels and control policies for linear-quadratic stochastic systems. *European Journal of Operational Research*, 73(2):226–236, 1994.

[18] T. Basar and G. J. Olsder. *Dynamic noncooperative game theory*, volume 23. SIAM, 1999.

[19] H. H. Bauschke and P. L. Combettes. *Convex analysis and monotone operator theory in Hilbert spaces*. Springer, 2011.

[20] A. Beck and M. Teboulle. Fast gradient-based algorithms for constrained total variation image denoising and deblurring problems. *IEEE Transactions on Image Processing*, 18(11):2419–2434, 2009.

[21] D. P. Bertsekas. *Dynamic programming and optimal control*, volume 1. Athena Scientific Belmont, MA, 1995.

[22] B. Bollobás. *Modern graph theory*, volume 184. Springer, 2013.

[23] J. Bolte, S. Sabach, and M. Teboulle. Proximal alternating linearized minimization for nonconvex and nonsmooth problems. *Mathematical Programming*, 146(1-2):459–494, 2014.

[24] P. Bolton and M. Dewatripont. *Contract theory*. MIT press, 2005.

[25] C. Bravard, L. Charroin, and C. Touati. Optimal design and defense of networks under link attacks. *Journal of Mathematical Economics*, 68:62–79, 2017.

[26] R. Brewer. Advanced persistent threats: minimising the damage. *Network Security*, 2014(4):5–9, 2014.

[27] G. Brown, M. Carlyle, J. Salmerón, and K. Wood. Defending critical infrastructure. *Interfaces*, 36(6):530–544, 2006.

[28] E. J. Candes and T. Tao. Near-optimal signal recovery from random projections: Universal encoding strategies? *IEEE transactions on information theory*, 52(12):5406–5425, 2006.

[29] D. H. Cansever and T. Başar. On stochastic incentive control problems with partial dynamic information. *Systems & Control Letters*, 6(1):69–75, 1985.

[30] P. Cardaliaguet. Differential games with asymmetric information. *SIAM journal on Control and Optimization*, 46(3):816–838, 2007.

[31] P. Cardaliaguet and C. Rainer. On a continuous-time game with incomplete information. *Mathematics of Operations Research*, 34(4):769–794, 2009.

[32] R. Carmona, J.-P. Fouque, and L.-H. Sun. Mean field games and systemic risk. *Communications in Mathematical Sciences*, 13(4):911–933, 2015.

[33] C. D. Charalambous. The role of information state and adjoint in relating nonlinear output feedback risk-sensitive control and dynamic games. *IEEE Transactions on Automatic Control*, 42(8):1163–1170, 1997.

[34] J. Chen, C. Touati, and Q. Zhu. A dynamic game analysis and design of infrastructure network protection and recovery. *ACM SIGMETRICS Performance Evaluation Review*, 45(2):125–128, 2017.

[35] J. Chen, C. Touati, and Q. Zhu. Heterogeneous multi-layer adversarial network design for the iot-enabled infrastructures. In *IEEE Global Communications Conference*, pages 1–6. IEEE, 2017.

[36] 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*, 15:462 – 474, 2020.

[37] J. Chen, C. Touati, and Q. Zhu. Optimal secure two-layer IoT network design. *IEEE Transactions on Control of Network Systems*, 7(1):398–409, 2020.

[38] J. Chen and Q. Zhu. Optimal contract design under asymmetric information for cloud-enabled Internet of controlled things. In *International Conference on Decision and Game Theory for Security*, pages 329–348. Springer, 2016.

[39] J. Chen and Q. Zhu. Resilient and decentralized control of multi-level cooperative mobile networks to maintain connectivity under adversarial environment. In *IEEE Conference on Decision and Control (CDC)*, pages 5183–5188. IEEE, 2016.

[40] J. Chen and Q. Zhu. A game-theoretic framework for resilient and distributed generation control of renewable energies in microgrids. *IEEE Transactions on Smart Grid*, 8(1):285–295, 2017.

[41] J. Chen and Q. Zhu. Security as a service for cloud-enabled internet of controlled things under advanced persistent threats: A contract design approach.

IEEE Transactions on Information Forensics and Security, 12(11):2736–2750, 2017.

[42] J. Chen and Q. Zhu. A stackelberg game approach for two-level distributed energy management in smart grids. *IEEE Transactions on Smart Grid*, 2017.

[43] J. Chen and Q. Zhu. A linear quadratic differential game approach to dynamic contract design for systemic cyber risk management under asymmetric information. In *56th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 575–582, 2018.

[44] J. Chen and Q. Zhu. Control of multi-layer mobile autonomous systems in adversarial environments: A games-in-games approach. *IEEE Transactions on Control of Network Systems*, 2019.

[45] J. Chen and Q. Zhu. Interdependent strategic security risk management with bounded rationality in the internet of things. *IEEE Transactions on Information Forensics and Security*, 14(11):2958–2971, Nov 2019.

[46] J. Chen and Q. Zhu. *A Game-and Decision-Theoretic Approach to Resilient Interdependent Network Analysis and Design*. Springer, 2020.

[47] J. Chen, Q. Zhu, and T. Başar. Dynamic contract design for systemic cyber risk management of interdependent enterprise networks. *arXiv preprint arXiv:1908.04431*, 2019.

[48] I.-K. Cho and D. M. Kreps. Signaling games and stable equilibria. *The Quarterly Journal of Economics*, 102(2):179–221, 1987.

[49] A. Clark, Q. Zhu, R. Poovendran, and T. Başar. Deceptive routing in relay networks. In *International Conference on Decision and Game Theory for Security*, pages 171–185. Springer, 2012.

[50] J. Dattorro. *Convex optimization & Euclidean distance geometry*. Meboo Publishing, 2008.

[51] T. Denning, A. Borning, B. Friedman, B. T. Gill, T. Kohno, and W. H. Maisel. Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 917–926. ACM, 2010.

[52] J. Duan, D. Gao, D. Yang, C. H. Foh, and H.-H. Chen. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for iot applications. *IEEE Internet of Things Journal*, 1(1):58–69, 2014.

[53] A. Ellis. Foundations for optimal inattention. *Journal of Economic Theory*, 173:56–94, 2018.

[54] M. Fahrioglu and F. L. Alvarado. Designing incentive compatible contracts for effective demand management. *IEEE Transactions on power Systems*, 15(4):1255–1260, 2000.

[55] Y.-P. Fang, N. Pedroni, and E. Zio. Resilience-based component importance measures for critical infrastructure network systems. *IEEE Transactions on Reliability*, 65(2):502–512, 2016.

[56] H. Fawzi, P. Tabuada, and S. Diggavi. Secure estimation and control for

cyber-physical systems under adversarial attacks. *IEEE Transactions on Automatic Control*, 59(6):1454–1467, 2014.

[57] M. Fiedler. Algebraic connectivity of graphs. *Czechoslovak Mathematical Journal*, 23(2):298–305, 1973.

[58] A. Fielder, S. König, E. Panaousis, S. Schauer, and S. Rass. Risk assessment uncertainties in cybersecurity investments. *Games*, 9(2):34, 2018.

[59] J.-P. Fouque and T. Ichiba. Stability in a model of interbank lending. *SIAM Journal on Financial Mathematics*, 4(1):784–803, 2013.

[60] P. Frankel, G. Garrigos, and J. Peypouquet. Splitting methods with variable metric for Kurdyka–łojasiewicz functions and general convergence rates. *Journal of Optimization Theory and Applications*, 165(3):874–900, 2015.

[61] D. Fudenberg and J. Tirole. *Game Theory*. MIT press, 1991.

[62] X. Gabaix. A sparsity-based model of bounded rationality. *The Quarterly Journal of Economics*, 129(4):1661–1710, 2014.

[63] B. Ganter and R. Wille. *Formal concept analysis: mathematical foundations*. Springer Science & Business Media, 2012.

[64] J. Garnier, G. Papanicolaou, and T.-W. Yang. Diversification in financial networks may increase systemic risk. *Handbook on Systemic Risk*, page 432, 2013.

[65] I. Giannoccaro and P. Pontrandolfo. Supply chain coordination by revenue sharing contracts. *International journal of production economics*, 89(2):131–139, 2004.

[66] G. Gigerenzer and R. Selten. *Bounded rationality: The adaptive toolbox*. MIT press, 2002.

[67] I. L. Glicksberg. A further generalization of the kakutani fixed point theorem, with application to nash equilibrium points. *Proceedings of the American Mathematical Society*, 3(1):170–174, 1952.

[68] C. Godsil and G. F. Royle. *Algebraic graph theory*, volume 207. Springer, 2013.

[69] S. Goyal and A. Vigier. Attack, defence, and contagion in networks. *The Review of Economic Studies*, 81(4):1518–1542, 2014.

[70] A. Greenberg, J. Hamilton, D. A. Maltz, and P. Patel. The cost of a cloud: research problems in data center networks. *ACM SIGCOMM computer communication review*, 39(1):68–73, 2008.

[71] A. Gupta, C. Langbort, and T. Başar. Dynamic games with asymmetric information and resource constrained players with applications to security of cyberphysical systems. *IEEE Transactions on Control of Network Systems*, 4(1):71–81, 2016.

[72] A. Gupta, A. Nayyar, C. Langbort, and T. Başar. Common information based Markov perfect equilibria for linear–Gaussian games with asymmetric information. *SIAM Journal on Control and Optimization*, 52(5):3228–3260, 2014.

[73] M. Hamdi and H. Abie. Game-based adaptive security in the internet of things for ehealth. In *IEEE International Conference on Communications*, pages 920–925, 2014.

[74] Y. Han, T. Alpcan, J. Chan, C. Leckie, and B. I. Rubinstein. A game theoretical approach to defend against co-resident attacks in cloud computing: Preventing co-residence using semi-supervised learning. *IEEE Transactions on Information Forensics and Security*, 11(3):556–570, 2016.

[75] E. A. Hansen, D. S. Bernstein, and S. Zilberstein. Dynamic programming for partially observable stochastic games. In *AAAI*, volume 4, pages 709–715, 2004.

[76] F. Harary. The maximum connectivity of a graph. *Proceedings of the National Academy of Sciences*, 48(7):1142–1146, 1962.

[77] R. Harper. *Inside the smart home*. Springer, 2006.

[78] D. Helbing. Globally networked risks and how to respond. *Nature*, 497(7447):51–59, 2013.

[79] R. A. Horn and C. R. Johnson. *Matrix analysis*. Cambridge university press, 2012.

[80] M. A. Hsieh, A. Cowley, V. Kumar, and C. J. Taylor. Maintaining network connectivity and performance in robot teams. *Journal of Field Robotics*, 25(1-2):111–131, 2008.

[81] P. Hu, H. Li, H. Fu, D. Cansever, and P. Mohapatra. Dynamic defense strategy against advanced persistent threat with insiders. In *IEEE Conference on Computer Communications*, pages 747–755, 2015.

[82] L. Huang, J. Chen, and Q. Zhu. A factored mdp approach to optimal mechanism design for resilient large-scale interdependent critical infrastructures.

In *Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, pages 1–6. IEEE, 2017.

[83] L. Huang, J. Chen, and Q. Zhu. A large-scale markov game approach to dynamic protection of interdependent infrastructure networks. In *International Conference on Decision and Game Theory for Security*, pages 357–376. Springer, 2017.

[84] Y. Huang, V. Kavitha, and Q. Zhu. Continuous-time markov decision processes with controlled observations. In *Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 32–39, 2019.

[85] O. C. Imer, S. Yüksel, and T. Başar. Optimal control of LTI systems over unreliable communication links. *Automatica*, 42(9):1429–1439, 2006.

[86] M. R. James and J. Baras. Partially observed differential games, infinite-dimensional Hamilton–Jacobi–Isaacs equations, and nonlinear H_∞ control. *SIAM Journal on Control and Optimization*, 34(4):1342–1364, 1996.

[87] M. R. James, J. S. Baras, and R. J. Elliott. Risk-sensitive control and dynamic games for partially observed discrete-time nonlinear systems. *IEEE Transactions on Automatic Control*, 39(4):780–792, 1994.

[88] I. Karatzas and S. Shreve. *Brownian Motion and Stochastic Calculus*. Springer, 2012.

[89] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys. Unmanned aircraft capture and control via gps spoofing. *Journal of Field Robotics*, 31(4):617–636, 2014.

[90] M. M. Khalili, P. Naghizadeh, and M. Liu. Designing cyber insurance policies: The role of pre-screening and security interdependence. *IEEE Transactions on Information Forensics and Security*, 13(9):2226–2239, 2018.

[91] M. Khouzani and S. Sarkar. Maximum damage battery depletion attack in mobile sensor networks. *IEEE Transactions on Automatic Control*, 56(10):2358–2368, 2011.

[92] Y. Kim and M. Mesbahi. On maximizing the second smallest eigenvalue of a state-dependent graph laplacian. *IEEE Transactions on Automatic Control*, 51(1):116–120, 2006.

[93] D. E. Kirk. *Optimal control theory: an introduction*. Courier Corporation, 2004.

[94] H. Kunreuther and G. Heal. Interdependent security. *Journal of risk and uncertainty*, 26(2):231–249, 2003.

[95] H. J. Kushner. Numerical methods for stochastic control problems in continuous time. *SIAM Journal on Control and Optimization*, 28(5):999–1048, 1990.

[96] J.-J. Laffont and D. Martimort. *The theory of incentives: the principal-agent model*. Princeton university press, 2009.

[97] R. Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3):49–51, 2011.

[98] T. G. Lewis. *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons, 2014.

[99] J. Li, X. Ou, and R. Rajagopalan. Uncertainty and risk management in cyber situational awareness. In *Cyber Situational Awareness*, pages 51–68. Springer, 2010.

[100] W. Liao, S. Salinas, M. Li, P. Li, and K. A. Loparo. Cascading failure attacks in the power system: a stochastic game perspective. *IEEE Internet of Things Journal*, 4(6):2247–2259, 2017.

[101] J. Lofberg. Yalmip: A toolbox for modeling and optimization in matlab. In *IEEE International Symposium on Computer Aided Control Systems Design*, pages 284–289. IEEE, 2004.

[102] M. Maasoumy Haghighi. Modeling and optimal control algorithm design for hvac systems in energy efficient buildings. Master's thesis, EECS Department, University of California, Berkeley, Feb 2011.

[103] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux. Game theory meets network security and privacy. *ACM Computing Surveys (CSUR)*, 45(3):25, 2013.

[104] L. Martirano. A smart lighting control to save energy. In *International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)*, volume 1, pages 132–138, 2011.

[105] N. Michael, M. M. Zavlanos, V. Kumar, and G. J. Pappas. Maintaining connectivity in mobile robot networks. In *Experimental Robotics*, pages 117–126. Springer, 2009.

[106] R. A. Miura-Ko, B. Yolken, N. Bambos, and J. Mitchell. Security investment

games of interdependent organizations. In *Annual Allerton Conference on Communication, Control, and Computing*, pages 252–260, 2008.

[107] D. Monderer and L. S. Shapley. Potential games. *Games and economic behavior*, 14(1):124–143, 1996.

[108] A. Mosenia and N. K. Jha. A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing*, 5(4):586–602, 2017.

[109] A. Mukherjee. Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints. *Proceedings of the IEEE*, 103(10):1747–1761, 2015.

[110] R. B. Myerson. Incentive compatibility and the bargaining problem. *Econometrica: journal of the Econometric Society*, pages 61–73, 1979.

[111] J. F. Nash et al. Equilibrium points in n-person games. *Proceedings of the national academy of sciences*, 36(1):48–49, 1950.

[112] K. C. Nguyen, T. Alpcan, and T. Başar. Stochastic games for security in networks with interdependent nodes. In *IEEE Conference on Game Theory for Networks*, pages 697–703, 2009.

[113] J. Nocedal and S. Wright. *Numerical optimization*. Springer, 2006.

[114] U. D. of Energy. *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, August 2013. https://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.

[115] G. Owen. *Game Theory*, volume 4th edition. Academic Press, 2013.

[116] N. Parikh, S. P. Boyd, et al. Proximal algorithms. *Foundations and Trends in optimization*, 1(3):127–239, 2014.

[117] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. In *IEEE Symposium on Security and Privacy*, pages 49–63, 2005.

[118] J. Pawlick, J. Chen, and Q. Zhu. iSTRICT: An interdependent strategic trust mechanism for the cloud-enabled internet of controlled things. *IEEE Transactions on Information Forensics and Security*, 14(6):1654–1669, 2019.

[119] J. Pawlick, S. Farhang, and Q. Zhu. Flip the cloud: Cyber-physical signaling games in the presence of advanced persistent threats. In *International Conference on Decision and Game Theory for Security*, pages 289–308. Springer, 2015.

[120] A. Refsdal, B. Solhaug, and K. Stølen. *Cyber-risk management*. Springer, 2015.

[121] R. T. Rockafellar and R. J.-B. Wets. *Variational analysis*, volume 317. Springer, 2009.

[122] Y. Saad. *Iterative methods for sparse linear systems*. SIAM, 2003.

[123] R. Salo, B. Pederson, A. Olive, W. Lincoln, and T. Wallner. Continuous ventricular volume assessment for diagnosis and pacemaker control. *Pacing and clinical electrophysiology: PACE*, 7(6 Pt 2):1267, 1984.

[124] Y. Sannikov. A continuous-time version of the principal-agent problem. *The Review of Economic Studies*, 75(3):957–984, 2008.

[125] S. Shen, H. Li, R. Han, A. V. Vasilakos, Y. Wang, and Q. Cao. Differential game-based strategies for preventing malware propagation in wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 9(11):1962–1973, 2014.

[126] A. Simonetto, T. Keviczky, and R. Babuška. Constrained distributed algebraic connectivity maximization in robotic networks. *Automatica*, 49(5):1348–1357, 2013.

[127] P. Smith, D. Hutchison, J. P. Sterbenz, M. Schöller, A. Fessi, M. Karaliopoulos, C. Lac, and B. Plattner. Network resilience: a systematic approach. *IEEE Communications Magazine*, 49(7):88–97, 2011.

[128] R. Srikant and T. Başar. Asymptotic solutions to weakly coupled stochastic teams with nonclassical information. *IEEE Transactions on Automatic Control*, 37(2):163–173, 1992.

[129] C. Tankard. Advanced persistent threats and how to monitor and deter them. *Network security*, 2011(8):16–19, 2011.

[130] The Council of Economic Advisers. The cost of malicious cyber activity to the U.S. economy. 2018.

[131] D. Tse and P. Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[132] G. Tuna, B. Nefzi, and G. Conte. Unmanned aerial vehicle-aided communications system for disaster recovery. *Journal of Network and Computer Applications*, 41:27–36, 2014.

[133] M. Van Dijk, A. Juels, A. Oprea, and R. L. Rivest. FlipIt: The game of "stealthy takeover". *Journal of Cryptology*, 26(4):655–713, 2013.

[134] E. Y. Vasserman and N. Hopper. Vampire attacks: draining life from wireless ad hoc sensor networks. *IEEE transactions on mobile computing*, 12(2):318–332, 2013.

[135] R. H. Weber. Internet of things–new security and privacy challenges. *Computer law & security review*, 26(1):23–30, 2010.

[136] D. B. West. *Introduction to graph theory*, volume 2. Prentice hall Upper Saddle River, NJ, 1996.

[137] R. West. The psychology of security. *Communications of the ACM*, 51(4):34–40, 2008.

[138] Wikipedia. https://en.wikipedia.org/wiki/Red_October_(malware).

[139] Z. Xu and Q. Zhu. A cyber-physical game framework for secure and resilient multi-agent autonomous systems. In *IEEE Conference on Decision and Control (CDC)*, pages 5156–5161, 2015.

[140] J. Yong and X. Y. Zhou. *Stochastic controls: Hamiltonian systems and HJB equations*, volume 43. Springer, 1999.

[141] S. Yüksel and T. Başar. Stochastic networked control systems: Stabilization and optimization under information constraints. In *Systems & Control: Foundations and Applications Series*. Birkhäuser, Boston, MA, 2013.

[142] M. Zhang, Z. Zheng, and N. B. Shroff. A game theoretic model for defending

against stealthy attacks with limited resources. In *International Conference on Decision and Game Theory for Security*, pages 93–112. Springer, 2015.

[143] Y. Zhang, C. Jiang, L. Song, M. Pan, Z. Dawy, and Z. Han. Incentive mechanism for mobile crowdsourcing using an optimized tournament model. *IEEE Journal on Selected Areas in Communications*, 35(4):880–892, 2017.

[144] Y. Zhou, Y. Fang, and Y. Zhang. Securing wireless sensor networks: a survey. *IEEE Communications Surveys Tutorials*, 10(3):6–28, 2008.

[145] Q. Zhu and T. Başar. Robust and resilient control design for cyber-physical systems with an application to power systems. In *IEEE Conference on Decision and Control and European Control Conference*, pages 4066–4071. IEEE, 2011.

[146] Q. Zhu and T. Başar. A dynamic game-theoretic approach to resilient control system design for cascading failures. In *Proceedings of the 1st international conference on High Confidence Networked Systems*, pages 41–46. ACM, 2012.

[147] Q. Zhu and T. Başar. Game-theoretic approach to feedback-driven multi-stage moving target defense. In *International Conference on Decision and Game Theory for Security*, pages 246–263. Springer, 2013.

[148] 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 Systems*, 35(1):46–65, 2015.

[149] Q. Zhu, H. Tembine, and T. Başar. Heterogeneous learning in zero-sum

stochastic games with incomplete information. In *IEEE Conference on Decision and Control (CDC)*, pages 219–224, 2010.

[150] Q. Zhu, H. Tembine, and T. Başar. Hybrid learning in stochastic games and its application in network security. *Reinforcement Learning and Approximate Dynamic Programming for Feedback Control*, pages 303–329, 2012.