The application of cyber-insurance in computer networks

Feng, Shaohan

2020

Feng, S. (2020). The application of cyber-insurance in computer networks. Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/143006>

<https://doi.org/10.32657/10356/143006>

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

Downloaded on 26 Apr 2023 18:01:53 SGT

The Application of Cyber-insurance in Computer Networks

Shaohan Feng

School of Computer Science and Engineering

A thesis submitted to the Nanyang Technological University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy

2020

Statement of Originality

I hereby certify that the work embodied in this thesis is the result of original research, is free of plagiarised materials, and has not been submitted for a higher degree to any other University or Institution.

23 December 2019

.....

Date

Shaohan Feng

.....

Shaohan Feng

Supervisor Declaration Statement

I have reviewed the content and presentation style of this thesis and declare it is free of plagiarism and of sufficient grammatical clarity to be examined. To the best of my knowledge, the research and writing are those of the candidate except as acknowledged in the Author Attribution Statement. I confirm that the investigations were conducted in accord with the ethics policies and integrity standards of Nanyang Technological University and that the research data are presented honestly and without prejudice.

7 January 2020

.....

Date

.....

Prof. Dusit Niyato

Authorship Attribution Statement

This thesis contains materials from 2 papers published in the following peer-reviewed journals and 3 papers accepted at conferences in which I am listed as an author.

Chapter 3 is published as [S. Feng, Z. Xiong, D. Niyato and P. Wang, “Dynamic Resource Management to Defend Against Advanced Persistent Threats in Fog Computing: A Game Theoretic Approach”, in IEEE Transactions on Cloud Computing, 2019. DOI: 10.1109/TCC.2019.2896632.](#) Part of the work in Chapter 3 is published as [S. Feng, Z. Xiong, D. Niyato, P. Wang, and A. Leshem, “Evolving Risk Management Against Advanced Persistent Threats in Fog Computing,” in 2018 IEEE 7th International Conference on Cloud Networking \(CloudNet\) \(pp. 1-6\).](#)

The contributions of the co-authors are as follows:

- Prof. Dusit Niyato suggested the research direction and edited the manuscript.
- Prof. Ping Wang assisted in designing the system model.
- I wrote the draft and performed all the results. The manuscript was revised together with Dr. Zehui Xiong.

Chapter 4 is published as [S. Feng, W. Wang, Z. Xiong, D. Niyato, P. Wang and S. S. Wang, “On Cyber Risk Management of Blockchain Networks: A Game Theoretic Approach”, in IEEE Transactions on Services Computing, 2018. DOI: 10.1109/TSC.2018.2876846.](#) Part of the work in Chapter 4 is published as [S. Feng, Z. Xiong, D. Niyato, P. Wang, S. S. Wang, and Y. Zhang, “Cyber Risk Management with Risk Aware Cyber-Insurance in Blockchain Networks,” in 2018 IEEE Global Communications Conference \(GLOBECOM\) \(pp. 1-7\).](#)

The contributions of the co-authors are as follows:

- Prof. Dusit Niyato provided the initial project direction and edited the manuscript.
- I prepared the manuscript. The manuscript was revised by Dr. Zehui Xiong and Prof. Ping Wang.
- I co-designed the system model with Dr. Wenbo Wang and performed all the mathematical and numerical studies.
- Prof. Shaun Shuxun Wang assisted in the theoretical model for the risk-adjusted insurance.

Chapter 5 is published as [S. Feng, Z. Xiong, D. Niyato, P. Wang, S. S. Wang, and X. S. Shen, “Joint Pricing and Security Investment in Cloud Security Service Market with User Interdependency,” IEEE Transactions on Services Computing \(2020\).](#)

DOI: [10.1109/TSC.2020.2996382](https://doi.org/10.1109/TSC.2020.2996382). Part of the work in Chapter 5 is published as **S. Feng**, Z. Xiong, D. Niyato, P. Wang, and S. S. Wang, “Joint pricing and security investment for cloud-insurance: A security interdependency perspective,” in 2018 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6).

The contributions of the co-authors are as follows:

- Prof. Dusit Niyato provided the initial research direction.
- I designed the system model with the help of Prof. Shaun Shuxun Wang and performed all the mathematical and numerical studies.
- Prof. Shaun Shuxun Wang assisted in the theoretical model for the assessment of system vulnerability.
- I wrote the manuscript. The manuscript was revised by Dr. Zehui Xiong, Prof. Ping Wang, and Prof. Xuemin Sherman Shen.

23 December 2019

.....

Date

Shaohan Feng

.....

Shaohan Feng

Acknowledgements

First, I wish to express my greatest gratitude to my advisor Prof. Dusit Niyato for the great support, guidance, and unwavering encouragement of my Ph.D. study. He shares his immense knowledge and experience as well as cutting-edge research directions and rigorous working style with me, which inspires me to keep learning and being creative throughout my Ph.D. study for now and will benefit the rest of my life in the future.

Second, I would like to thank my co-advisor Prof. Ping Wang for her insightful suggestions and discussions about the research. These suggestions do motivate me to reexamine my research from various perspectives and give me a lot of inspirations, which help me a lot in completing my Ph.D. research study.

In addition to my advisors, I am also very grateful to Prof. Dong In Kim from Sungkyunkwan University, Korea, Prof. Shaun Shuxun Wang from Nanyang Business School, Singapore, and Dr. Wenbo Wang from Nanyang Technological University, Singapore, for their scientific advices, knowledge, and many insightful discussions as well as suggestions.

Last but not the least, I would like to give my greatest gratitude to my parents and friends for their spiritual support throughout writing this thesis and my life in general.

Shaohan Feng
3 December 2019

Abstract

Due to the increasing complexity in the network attacks, perfectly securing the computer networks by relying solely on the security techniques might no longer be a sufficient and suitable solution. In this thesis, we adopt the cyber-insurance, i.e., an alternative means of cyber risk management, to manage the cyber risks due to the cyber attacks in computer networks. By enabling the transfer of the cyber risks from the computer networks to a third party, i.e., cyber insurer, cyber-insurance has been recognized as a promising and efficient approach to manage the cyber risks. Specifically, our three major research issues focus on three application scenarios of the cyber-insurance in computer networks, which are summarized as follows.

For the first research issue, considering the highly virtualized environment of the fog computing, which may lead to vulnerability to the cyber attacks, we adopt the cyber-insurance to transfer cyber risks from the fog computing platform to a third party, i.e., an insurer, so as to defend against the advanced persistent threat attacks. In particular, the system model under consideration consists of three main entities, i.e., the fog computing provider working as the service provider to secure its provisioned fog computing service by jointly allocating its defense computing resources and purchasing the cyber-insurance, the attacker optimizing its attack computing resources allocation to increase the probability of successful attack, and the cyber-insurer. We model the interaction among these three entities as a dynamic Stackelberg game. In the lower level of the game, we formulate an evolutionary subgame to analyze the provider's defense and cyber-insurance subscription strategies as well as the attacker's attack strategy. In the upper level of the game, the cyber-insurer optimizes its premium pricing strategy by taking into account the evolutionary equilibrium of the lower-level evolutionary subgame. We analytically prove that the evolutionary equilibrium is unique and stable, and study the Stackelberg equilibrium based on the optimal control theory. Moreover, we provide a series of insightful analytical and numerical results on the equilibrium of the dynamic Stackelberg game.

For the second research issue, as the open-access blockchains based on the proof-of-work consensus protocols are vulnerable to cyber-attacks, we adopt the cyber-insurance as an economic tool for neutralizing the cyber risks. Specifically, we consider a blockchain service market, which is composed of the infrastructure provider, the blockchain provider, the cyber-insurer, and the users. The blockchain provider purchases from the infrastructure provider, e.g., a cloud, the computing resources to maintain the blockchain consensus, and then offers the blockchain services to the users. The blockchain provider strategizes its investment in the infrastructure and the service price charging to the users in order to improve the security of the blockchain and thus optimize its profit. Meanwhile, the blockchain provider also purchases a cyber-insurance from the cyber-insurer to protect itself from the potential damage due to the attacks. In return, the cyber-insurer adjusts the insurance premium according to the perceived risk level of the blockchain service. Based on the assumption of rationality for the market entities, we model the interaction among the blockchain provider, the users, and the cyber-insurer as a two-level Stackelberg game. Namely, the blockchain provider and the cyber-insurer lead to set their pricing/investment strategies, and then the users follow to determine their demand of the blockchain service. Specifically, we consider the scenario of double-spending attacks and provide a series of analytical results about the Stackelberg equilibrium in the market game.

For the third research issue, we study a cloud security service market, which is composed of cloud users and cloud security service vendors (CSSVs). The CSSVs work as the insurers for selling the cloud security plan, which is consisted of cloud security service and cloud-insurance. The users in the cloud platform can purchase the cloud security plan from the CSSVs to secure their cloud service. If the cloud service is attacked and loss happens, the users will receive the claim from the CSSVs. To lower the successful attack probability, the CSSV has an incentive to invest in improving its cloud security service. Specifically, we model and study the cloud security service market in the framework of a two-stage Stackelberg game. On the upper stage, the CSSVs lead to decide on their own strategies, i.e., the price of the cloud security plan and the security investment to improve their offered cloud security service. On the lower stage, the users follow to decide on the purchase of the cloud security plan according to the prices of the cloud security plan and the perceived cyber breach probability of the cloud security service. We analytically

verify that the Stackelberg equilibrium exists and is unique. Extensive simulations have been conducted to evaluate the performance of the Stackelberg game.

In summary, this thesis investigates and demonstrates a few application scenarios of cyber-insurance in computer networks. Due to the inevitability of cyber attacks, defending against cyber attacks through economic means, i.e., cyber-insurance, introduces a novel approach of cyber risk management for the computer networks. Compared with the conventional defense mechanisms, i.e., security techniques, in the computer networks, the cyber-insurance enables the security to be provided as a service such that the computer networks can be secured from the economic perspective as well. In the application scenarios, game theoretical approaches have been adopted to obtain the optimal policies in computer networks, the optimality of which has been demonstrated by comparing with the policies obtained by the baselines.

Contents

Acknowledgements	ix
Abstract	xi
List of Figures	xix
List of Tables	xxi
Symbols and Acronyms	xxiii
1 Introduction	1
1.1 Background of Research and Motivation	1
1.1.1 Cyber Attacks in Computer Networks	1
1.1.2 Motivations	2
1.2 Research Focus	3
1.2.1 Fog Computing Platform - A Study on Dynamic Resource Allocation and Cyber-insurance Purchase for Risk Management	4
1.2.2 Securing Blockchain Networks via Computing Resource Investment and Cyber-insurance	7
1.2.3 Joint Pricing and Security Investment in Cloud Security Service Market	10
1.2.4 Connections among Research Issues	11
1.3 Major Contributions	13
1.4 Organization of the Thesis	15
2 Literature Review	17
2.1 Risk Management in Defending Against Advanced Persistent Threats in Fog Computing	17
2.1.1 Security issues in the Networks	17
2.1.2 Game Theoretical Approaches in the Networks	18
2.1.3 An Economic Security Tool	19
2.2 Defending Against Double-spending Attacks in Blockchain Networks by Resource Management and Cyber-insurance	21
2.2.1 Permissionless Blockchain Networks	21

2.2.2	Security Issues in the Permissionless Blockchain Networks	22
2.2.3	Cyber-insurance Approaches	22
2.2.4	Risk-adjusted Premium	23
2.3	Joint Cyber-insurance and Security Investment Approach in Safe-guarding Cloud Platform	24
2.3.1	Security Issues in Cloud Platform	24
2.3.2	Vulnerability Assessment	24
2.4	Game Theoretic Approaches for Computer Networks	25
2.4.1	Dynamic Game Approaches	26
2.4.2	Stackelberg Game Approaches	26
2.5	Cyber-insurance Products	27
2.6	Summary	28
3	Dynamic Resource Management to Defend Against Advanced Persistent Threats in Fog Computing: A Game Theoretic Approach	31
3.1	System Model	31
3.2	A Dynamic Stackelberg Game Formulation	35
3.2.1	Formulation of the Lower-Level Evolutionary Subgame	37
3.2.2	Formulation of the Stackelberg Differential Game	39
3.3	Equilibrium Analysis	40
3.3.1	Equilibrium Analysis for the Lower-Level Evolutionary Subgame	40
3.3.2	Solution to Optimal Control Problem	43
3.4	Performance Evaluation	45
3.4.1	Numerical Results	45
3.4.1.1	The stability of evolutionary equilibrium	45
3.4.1.2	Demonstration of the unique solvability of the lower-level evolutionary subgame	46
3.4.1.3	Evolution process of the dynamic strategies	47
3.4.1.4	The impact of the number of total CPUs owned by the APT attacker	49
3.4.1.5	Comparison between static and dynamic games	50
3.4.1.6	Multiple fog nodes	51
3.5	Summary	52
4	On Cyber Risk Management of Blockchain Networks: A Game Theoretic Approach	53
4.1	System Description and Game Formulation	53
4.1.1	Preliminaries	54
4.1.1.1	Successful Attack Probability	54
4.1.1.2	Premium Determination	55
4.1.2	System Model	57
4.1.2.1	The User's Utility	57

4.1.2.2	Profits of the Blockchain Provider and the Cyber-insurer	58
4.1.3	Stackelberg Game Formulation	59
4.2	Game Equilibrium Analysis	61
4.2.1	Equilibrium Analysis for User-Level Noncooperative Subgame	61
4.2.2	Equilibrium Analysis for Leader-Level Noncooperative Subgame	66
4.2.3	Equilibrium Searching for Leader-Level Noncooperative Subgame	67
4.3	Performance Evaluation	68
4.3.1	Numerical Results	69
4.3.1.1	Demonstration of best response and NE	69
4.3.1.2	The impact of the number of users	71
4.3.1.3	The impact of social externality	72
4.3.1.4	The impact of attacker's computing resource	74
4.4	Summary	75
5	Joint Pricing and Security Investment in Cloud Security Service Market	77
5.1	System Description	77
5.1.1	Preliminaries	78
5.1.2	System Model	80
5.1.3	Stackelberg Game Formulation	83
5.2	Stackelberg Equilibrium Analysis	84
5.2.1	Equilibrium Analysis for the User-level Game	86
5.2.2	Equilibrium Analysis for the CSSV-level Game	88
5.3	Performance Evaluation	89
5.3.1	Parameters Setting	89
5.3.2	Numerical Results	90
5.4	Summary	96
6	Conclusion and Future Work	99
6.1	Conclusion	99
6.2	Future Work	100
6.2.1	Future Work on the APT Attack of the Fog Computing	100
6.2.2	Future Work on the Fog Computing	101
6.2.3	Future Work on the Double-spending Attack of the Blockchain Networks	101
A	Proofs for Chapter 3	103
A.1	Proof of Proposition 3.3.1	103
A.2	Proof of Theorem 3.3.2	107
B	Proofs for Chapter 4	111

B.1 Proof of Theorem 4.2.3	111
B.2 Proof of Theorem 4.2.4	114
C Proofs for Chapter 5	119
C.1 Proof of Theorem 5.2.4	119
C.2 Proof of Theorem 5.2.5	120
List of Author's Awards, Patents, and Publications	125
Bibliography	129

List of Figures

1.1	Operation of the cyber-insurance	4
1.2	System model for the fog computing platform.	5
1.3	An overview of the blockchain service market.	8
1.4	System model for the cloud security service market.	12
1.5	An overview of the connections among the research issues.	13
3.1	An illustration of internal benefit.	34
3.2	The dynamic strategies of the fog computing provider and cyber-insurer.	36
3.3	The direction field of the replicator dynamics	46
3.4	The defense CPU ratio and attack CPU ratio of each fog node with different premium of fog node 1 showing the uniqueness of the evolutionary equilibrium	47
3.5	Evolutionary Equilibrium	47
3.6	Payoffs and learning rate	48
3.7	Evolutionary equilibrium of fog node 1 with different values of M^A	49
3.8	Cumulative payoffs of the APT attacker and fog computing provider as well as cumulative profit of the cyber-insurer under dynamic and static Stackelberg games	50
3.9	Evolutionary equilibrium with multiple fog nodes	51
4.1	An illustration of Assumption 1.	63
4.2	Best response	70
4.3	Nash equilibrium	71
4.4	The results with increasing number of users.	72
4.5	The results with increasing social externality.	73
4.6	The result with increasing attacker's computing resource: (a) profit of the blockchain provider, i.e., (4.8), (b) profit of the cyber insurer, i.e., (4.9), (c) average price of the blockchain service, i.e., decision variable $\mathbf{p}$ in (4.8), (d) total demand of the users, i.e., (4.17), (e) the investment of the blockchain provider, i.e., decision variable $\bar{h}$ in (4.8), and (f) the premium coefficient, i.e., decision variable γ in (4.9).	74

5.1	(a) The relationship between the cyber breach probability $v(z)$ and the investment z and (b) the relationship between the security level $q = 1 - v(z)$ and the investment z	79
5.2	Best response of the CSSV-A under (a) strong and (b) weak interdependency as well as that of the CSSV-B under (c) strong and (d) weak interdependency.	90
5.3	NE for (a) price and (b) security level.	91
5.4	(a) Total users' utilities, (b) profit, (c) price and (d) security level with increasing users and different levels of interdependency.	92
5.5	(a) Total users' utilities, (b) profit, (c) price and (d) security level with increasing probability of being breached $v(1)$	93
5.6	(a) Total utilities, (b) profit, (c) price, and (d) security level with varying interdependency.	93
5.7	(a) Total users' utilities, (b) profit, (c) price and (d) security level under competition and cooperation.	94
5.8	(a) Total users' utilities, (b) & (c) profit for the CSSVs A & B, (d) & (e) price for the CSSVs A & B, and (f) & (g) security level for the CSSVs A & B with increasing number of the users and increasing numbers of threats.	96

List of Tables

2.1	Cyber breach probability	25
2.2	Cyber-insurance products	27
3.1	Notations for the Fog Computing Platform	32
5.1	Notations	81

Symbols and Acronyms

Symbols

Chapter 3: Dynamic Resource Management to Defend Against Advanced Persistent Threats in Fog Computing: A Game Theoretic Approach

i, j	Fog nodes i, j .
$\mathcal{N}, N$	The set of fog nodes in the fog computing platform and its cardinality, respectively.
M^A, M^P	The numbers of all the CPUs owned by the APT attacker and fog computing provider, respectively.
u_i	The fraction of total available CPUs that the fog computing provider employs to defend fog node i . It is also called “defense CPU ratio of fog node i ”.
v_i	The fraction of total available CPUs that the APT attacker employs to attack fog node i . It is also called “attack CPU ratio of fog node i ”.
x_i, p_i	The cyber-insurance subscription ratio and premium of cyber-insurance for fog node i , respectively.
σ	The basic security effort of the fog computing provider on the fog computing platform.
λ_i	The amount of asset, e.g., size and value of private information, stored in fog node $i \in \mathcal{N}$.
U^P_i, U^A_i	The expected payoffs of the fog computing provider and the APT attacker on fog node i , respectively.

Chapter 4: On Cyber Risk Management of Blockchain

Networks: A Game Theoretic Approach

$\mathcal{N}$	The set of active users.
T	Time period.
H	The total computing resource of the blockchain network measured by the hash rate.
T_0	The average time for a new block to be mined in the blockchain network.
h	The investment in computing resources by the blockchain provider.
a	The investment in computing resources by the attackers.
$\bar{h} = \frac{h}{a+h}$	The investment ratio of the blockchain provider.
$\bar{a} = \frac{a}{a+h}$	The investment ratio of the attackers.
$I_w(u, v)$	The regularized incomplete Beta function.
$\Gamma(\cdot)$	The gamma function.
N_T	The number of transactions in a block.
r	The block mining reward for each block.
q	The total compensation rate for each block.
θ_i	Intrinsic value for user i , i.e., the probability for user i to buy the blockchain service.
p_i	The price of the service for user i .
g_{ij}	The level of the social externality (influence) that user j has on user i .
α	A constant controlling the level of social externality for the entire network.
u_i	The utility of user i .
Π_P	The payoff functions of the blockchain provider.
Π_I	The cyber-insurer's payoff function.
γ	The cyber-insurer's decision variable, i.e., the premium coefficient which decides on the insurance policy.
x_i	The service demand of user i .

Chapter 5: Joint Pricing and Security Investment In Cloud Platform

i, j	Users i, j .
--------	----------------

A, B	Cloud security service vendors (CSSVs).
$\mathcal{N}$	A set of users.
$x_i, 1 - x_i$	Demand from user i to the CSSV-A and CSSV-B, respectively.
$\mathbf{x}_{-i}$	Demands to the CSSV-A without user i .
$\mathbf{G}, g_{ij}$	Security interdependency matrix and its elements, respectively.
a_i, b_i	Parameters of concave utility functions.
d^A, d^B	Coefficient of congestion of the CSSV-A and CSSV-B, respectively.
p_i^A, p_i^B	Prices of the cloud security plan for user i from the CSSV-A and CSSV-B, respectively.
q^A, q^B	Security levels of the cloud security service from the CSSV-A and CSSV-B, respectively.
z^A, z^B	Investments of the CSSV-A and CSSV-B, respectively.
$v(\cdot)$	Probability of being breached for the cloud service.
α	$\alpha > 0$ is the parameter for the family of security breach probability functions.

Acronyms

Chapter 3: Dynamic Resource Management to Defend Against Advanced Persistent Threats in Fog Computing: A Game Theoretic Approach

APT	Advanced Persistent Threats
SECaaS	Security-as-a-Service
DoS	Denial-of-Service
ODEs	Ordinary Differential Equations

Chapter 4: On Cyber Risk Management of Blockchain Networks: A Game Theoretic Approach

P2P	Peer-to-Peer
PoW	Proof-of-work
PHEV	Plug-in Hybrid Electric Vehicle
PH	Proportional Hazard
NE	Nash Equilibrium

Chapter 5: Joint Pricing and Security Investment In

Cloud Platform

BBR Beazley Breach Response

NE Nash Equilibrium

CSSV Cloud Security Service Vendor

Chapter 1

Introduction

In this chapter, we first present an overview of the cyber attacks in the computer networks. Then, we give a brief discussion on the research motivation. Moreover, the introductions to our research focuses are discussed, which are followed by the research contributions.

1.1 Background of Research and Motivation

1.1.1 Cyber Attacks in Computer Networks

A computer network is a network constituted of connected computing devices, which enables the resources sharing among the computing devices through the wired and wireless media, e.g., fiber-optic cables and Wi-Fi. The computer networks can support enormous applications and services such as communication using email, video, and instant messaging, devices sharing (e.g., printers, scanners, and photocopiers), and access to the online files and systems as well as many others. However, as everything of value operating online, the cyber attacks in the computer networks are inevitable. The damage caused by these cyber attacks to the world are surging and countless. For example, in October 2013, Adobe announced that its infrastructure has been massively hacked, which resulted in the leakage of personal information (including logins, passwords, names, credit cards, and expiration dates) of 2.9 million accounts [1]. Even worse, in 2014, Yahoo! announced that it

had suffered a cyber attack, which affected the privacy (including the names, dates of birth, telephone numbers, and passwords) of 500 million user accounts [1].

1.1.2 Motivations

In order to reduce the damage caused by these cyber threats, the concept of cyber risk management has been recently proposed. The cyber risk management is a process of identifying, analysing, evaluating, and addressing the organisation's cyber risks. The management process includes the following steps: 1) identification of the risks that may compromise the organization's cyber security; 2) assessment of the severity of each identified risk with respect to the probability that it may happen and the corresponding damage; 3) evaluation of each analysed risk with respect to whether it fits within the organization's risk appetite or not; 4) response to each risk. The risks will be monitored on a long-run manner such that the response can be adjusted accordingly to make sure that the risks are still acceptable.

The responses to the risks can be classified into four categories, i.e., treatment (security control implementation to modify the risk's impact), toleration (risk retention), termination (ending the risk-related activities), and transfer (sharing the risk with a third party through outsourcing or taking out insurance).

Intuitively, among these aforementioned responses to the cyber risks, treatment is the most common and conventional. In order to respond to the cyber risks by using treatment, world-wide researchers has proposed and designed extensive security techniques. And, most of them have already been applied to safeguard the cyber space. For example, a system, named Panorama, was proposed in [2] to detect and analyze the malware by capturing the fundamental features of the malware, e.g., malicious information access and processing behaviors, which remarkably differentiates the malware from the benign applications/software. A defense mechanism has been proposed in [3] for addressing the insider attack problem.

Nevertheless, essentially stopping the cyber threats from happening is still impossible. As estimated in [1], the cyber crime damages is going to surge and reach \$5 trillion by 2020. In the case that the traditional cyber defense strategies, such as firewalls, antivirus software, and password protection, are ineffective and insufficient, we resort to an alternative response to reduce the damage caused by the

cyber threats to the computer network, which is risk transfer. In the response of risk transfer, the risks to the computer networks will be shared and reduced by transferring to a third-party, which can be realized in two ways, i.e., outsourcing and taking out insurance. For example, to transfer the cyber risks by outsourcing, a business company can outsource its database, computing, and data storage by purchasing these services from a cloud provider. As such, the risks related to these services, like system failure and data leakage, will be transferred to the cloud provider along with the service payment. In the other way, the organization can also transfer the cyber risks by taking out insurance, and the insurance product for transferring the cyber risk is widely named as cyber-insurance. As shown in Fig. 1.1, similar to the traditional insurance, a customer of a cyber-insurance product, e.g., a computer network operator/provider, is insured once it settles the contract with the cyber insurer by paying a premium. Being insured, the losses of the customer incurred by the cyber attacks will be fully/partly covered by the cyber insurer's claim. As a result, the customer can transfer its cyber risks to an insurer and reduce the damage caused by the cyber risks to it.

In this thesis, we mainly focus on the second way of the response of risk transfer, i.e., taking out insurance. Cyber-insurance is an insurance product that protect the network users from the Internet-based risks related to the information technologies and activities, e.g., cyber attacks, by providing the coverage on the losses and the reliabilities resulted from the network breaches. To date, there are already a number of cyber-insurance products available in the market [4], which can be categorized into specific groups based on the types of their targeted system, e.g., clouds, fogs, Internet service providers, and dedicated cyber-physical/industrial systems. In this thesis, we introduce a novel approach of cyber risk management to the computer network operators and users against the cyber attacks through jointly utilizing two aforementioned responses, i.e., risk transfer (taking out insurance) and treatment (network defense resource allocation).

1.2 Research Focus

Regarding to the aforementioned research background and motivation, three main research issues are presented in the following.

FIGURE 1.1: Operation of the cyber-insurance

1.2.1 Fog Computing Platform - A Study on Dynamic Resource Allocation and Cyber-insurance Purchase for Risk Management

Fog computing essentially extends cloud computing services to an edge of a network by using the decentralized computing infrastructure. As such, the cloud service gets closer to the position where the data is created and acted upon, resulting in improved performance and reduced cost. Due to the decentralized computing infrastructure, fog computing has been applied in extensive domains, e.g., smart home, smart grid, and health data management [5]. However, as everything else of value operating online, cyber attacks in fog computing are inevitable. As one of the most popular cyber attacks, Advanced Persistent Threats (APT) [6] are created and launched by advanced and well-resourced attackers through applying multiple sophisticated methods to continuously and stealthily steal data from the targeted networking system. The attacks have caused serious privacy leakage and millions of dollars' loss [7]. For example, in mid August 2014, healthcare provider community revealed that its computer system fell victim to an APT attack, and the sensitive information of 4.5 million of its patients might be compromised [8]. Even worse, the APT attack creates a growing and emerging risk to organizations'

FIGURE 1.2: System model for the fog computing platform.

reputation which results in a considerable economic/financial loss. For example, in 2013, retailer Target fell victim to the APT attack which stole large number of customers' credit card information [9]. According to business magazine Forbes, Target's sales declined by almost 50% during the final quarter of that year, and around 5% and 10% of its customers indicated that they would never shop there again [10].

In this research issue, we consider a fog computing platform under the cyber risk of the APT attack as shown in Fig. 1.2. The fog computing platform is composed of a group of fog nodes which perform different types of networking functions, e.g., storage and caching. There are mainly three entities involved in the platform, namely, the fog computing provider, the APT attacker, and the cyber-insurer. The APT attacker launches the APT attack to the fog computing platform and then steals information continuously and stealthily through malwares, e.g., Stuxnet [11]. Meanwhile, the fog computing provider can apply countermeasure to protect the platform from the APT attack. Specifically, the APT attacker installs the malware in the memory of each fog node rather than a file to evade the attack detection [12]. To defend against the APT attack, the fog computing provider scans the platform, i.e., each fog node, to extract the changed features of the operating systems, e.g., memory usage [13]. These changed features are analyzed by using a trained machine-learning-based classification model, which is maintained by the fog computing provider, for APT attack detection [14]. Without comparatively

sufficient computing resources, e.g., enough number of CPUs, to support fast processing speed, neither the installation of the malware in the memory to evade the attack detection nor the platform scanning and the changed features extraction to detect the APT attack will succeed [15]. Therefore, the APT attacker and fog computing provider have to optimize the allocation of their attack and defense computing resources. However, due to the imperfectness of the security techniques and an incentive to cover the economic/financial loss incurred by the APT attacks, the fog computing provider will consider to purchase the cyber-insurance. The cyber-insurance enables the security to be provided as a service by the cyber-insurer which adopts a premium (service fee) pricing strategy according to its perceived risk level of the fog computing platform.

To model and analyze the time-varying interaction of the fog computing platform, we propose a hierarchical dynamic Stackelberg game framework. The framework consists of the following components:

- In the lower level, the fog computing provider's defense and cyber-insurance subscription strategies as well as the APT attacker's attack strategy are formulated as an evolutionary subgame. We model the learning and adaptation of these strategies by using replicator dynamics. The evolutionary equilibrium is the solution of this subgame.
- In the upper level, the cyber-insurer optimizes its premium for payoff maximization based on the feedback, i.e., strategies, of the lower-level evolutionary subgame. We formulate a dynamic Stackelberg game based on optimal control theory to enable the dynamic optimization of the strategies.

The major benefit of the proposed dynamic game model is that the evolutionary game is able to capture the bounded rationality of the APT attacker and fog computing provider. The bounded rationality exists in the real network environment, e.g., due to lack of complete information to make a rational decision. In this regard, the APT attacker and fog computing provider tend to evolve their strategies rather than to make exact decisions. This phenomenon cannot be well analyzed using static games. Another important advantage of the proposed dynamic game is at the capability to achieve optimal or best response strategies and cumulative payoffs of the players in a long-term basis, i.e., over a certain time horizon. The proposed game clearly outperforms standard static games under this metric.

1.2.2 Securing Blockchain Networks via Computing Resource Investment and Cyber-insurance

In the past few years, blockchain technologies have attracted tremendous attention from both industry and academia for distributively providing the irreversible, tamper-evident database of tokenized asset transactions [16]. Moreover, with the smart contracts [17] enabled on top of the decentralized consensus [16], blockchains are envisaged to be the “game changer” in various areas ranging from Peer-to-Peer (P2P) resource allocation/trading, e.g., distributed cloud storage [18], to financial services, e.g., digital identity management [19] and online markets for crowdsourcing services [20]. Although with the advantages such as open access, disintermediation, and pure self-organization, open-access/permissionless blockchains rely on the condition of honest majority to guarantee the data integrity and service security, especially when the Nakamoto consensus protocol based on proof-of-work (PoW) is adopted [16]. Since permissionless blockchain networks admit no identity control, they can be vulnerable to a series of insider attacks by malicious consensus nodes [21]. Among different types of attacks, double spending [22] is the most fundamental one and can be executed through various attacks such as goldfinger attacks, netsplit attacks and brute-force attacks [21]. In brief, a double-spending attacker attempts to simultaneously spend the same set of blockchain tokens in two different transactions. This can be performed by first persuading part of the network and the transaction receiver to confirm one transaction, and then persuading the majority of the network to override that transaction with a conflicting transaction spending the same set of tokens. In other words, double-spending attacks are executed through intentional blockchain forking. Due to the factors such as randomness in solving the PoW puzzles [16] and information propagation delay, the malicious nodes, i.e., attackers, only need to hold a certain level of PoW computing power to succeed with a high probability in the double-spending attacks. Note here that although the double-spending attack is initially devised for Bitcoin, the attack is also applicable to other blockchain-based resource trading services and systems, for example, energy trading [23], plug-in hybrid electric vehicle (PHEV) charging credit management [24], wireless spectrum trading [25], bandwidth exchange in community networks [26] and cache storage trading [27].

In this research issue, we introduce a novel approach of jointly providing the risk management and security enhancement to the blockchain users and providers

FIGURE 1.3: An overview of the blockchain service market.

against attacks through the means of the cyber-insurance. As in other insurable cyber-systems, the market design of cyber-insurance for blockchain networks also has to address a few important issues. Firstly, from the cyber-insurer's perspective, the scope and policy of the cyber-insurance have to be clearly defined in regard to what kind of attacks to be covered and how to quantify the risk, the possible damage and thus the insurance premium. Secondly, alongside the reactive risk transfer with the cyber-insurance, rational blockchain providers also have to consider the proactive strategy in security improvement and thus balance the investment in the infrastructure and in the cyber-insurance.

To answer these questions, we consider a PoW-based blockchain service market under the threat of double-spending attacks (see Fig. 1.3). The market is composed of three entities, namely, the users, the blockchain provider, and the cyber-insurer. The users subscribe to a service, e.g., P2P energy trading for smart grids, which is implemented on top of the blockchain provided by the blockchain provider. We consider that the blockchain provider is composed of a group of individual honest machines which are responsible for maintaining the data consensus in the framework of PoW-based permissionless blockchains. The blockchain provider purchases

the computing resource from cloud-based infrastructure providers¹ or deploys more computing power internally for maintaining the network consensus. Meanwhile, in order to lower the cost on infrastructure, third-party devices are encouraged to join the decentralized consensus process by dedicating their individual computing resources into the network. Working as a single blockchain provider, the group of consensus machines make profit by charging the users with the transaction processing fees and block mining fees [16]. To neutralize the economic/financial loss incurred by double-spending attacks, the blockchain provider purchases the insurance from the cyber-insurer, which adopts an adjustable premium pricing strategy according to its perceived risk level of the blockchain.

We propose a two-stage Stackelberg game model to analyze the dynamics of the considered market. On the upper stage of the game, the blockchain provider and the cyber-insurer lead to adopt their best-response strategies for profit maximization. On the lower stage, the users adjust their service demands according to the cost and the security level of the blockchain. The proposed market framework introduces a novel incentive-compatible business ecosystem, where the blockchain service users benefit from enjoying more resilient services, and both the blockchain provider and the cyber-insurer are able to gain more profits. In fact, the potential of cyber-insurance for blockchain, Bitcoin specifically, has been perceived in the market. For example, Petra Insurance Brokers (www.insurewithpetra.com) introduces the concept of insurance for Bitcoin transactions. Likewise, BitCoin Financial Group unveils “BitSecure”, which is a Bitcoin theft insurance policy (www.bitcoinfinancialgroup.com). This product covers both external hacking and employee theft. Moreover, more insurance products are emerging in which a few of them focus on general blockchain services. Therefore, our proposed concept and framework of cyber-insurance for blockchain services has a clear and direct practical implication. Moreover, from the perspective of market design, the blockchain services are typically highly customized for a certain environment and application. Thus, we consider the mutual trading between single insurer and single provider. The model of a many-to-many market for multiple insurers and providers is likely to be intractable and needs further development, and hence it is beyond the scope of this paper. Finally, the model developed in this paper can be readily extended to blockchains with the emerging consensus protocols based on the generalized proof

¹For example, Amazon AWS provides the blockchain infrastructures through its partner ecosystem [28].

of concepts [16], where investment in other resources, e.g., stakes, is needed to prevent attacks.

1.2.3 Joint Pricing and Security Investment in Cloud Security Service Market

Since the cloud services offer many benefits, e.g., improving efficiency and resource utilization, it has gained widespread use such as sensory data processing in vehicular networks [29] and storage services for overcoming the storage constraints of the mobile devices. However, like everything else of value operating online, cyber attacks in cloud services, e.g., unauthorized access and availability risks, are inevitable [30]. To address such security problems, many cloud security service vendors (CSSVs), e.g., IBM security [31] and Oracle [32], are providing security service to secure cloud for the users. Nevertheless, even though the cyber space in cloud is much more robust than before due to the significant progress on cyber security techniques, e.g., cryptographic methods [33], completely securing the cyber space still remains as an open research field [34, 35]. Even worse, cyber attacks on organizations across all sectors remain rampant. The financial losses due to the cyber risks were estimated by McAfee to be between USD 300 billion and USD 1 trillion in 2014 [36]. There were 873 recorded breaches in the US with over 29 million records exposed for November 2016, indicated by the Identity Theft Resource Center's 2016 data breach category summary [37].

In this regard, an economic tool, i.e., cyber-insurance, has been introduced to enable effective cyber risk management [38–40]. Cloud-insurance, which is one of the cyber-insurance products, is a risk management technique via transferring the cyber risks faced by users to an insurance company with a fee in return, i.e., premium [41]. Similar to the conventional insurance products, cloud-insurance can align the economic incentives of different parties. For example, the CSSVs can be regarded as cloud-insurers selling cloud security plan products consisted of cloud security service and cloud-insurance. This setting is well adopted in the literature such as in [38]. In this way, the CSSVs can improve their profits by appropriately pricing cloud security plan and investing in improving their cloud security services. For the cloud users, they can buy the cloud security plan and use the cloud security service to secure their cloud service. Along with the cloud

security service contained in the cloud security plan, the cloud-insurance can help the user to transfer their cyber risks to a third-party company, i.e., CSSV. For the security service consumption, the users are interdependent [38, 42], which will affect the decision-making of the CSSV and further the corresponding profit.

In this research issue, we model and study the cloud security service market. As shown in Fig. 1.4, the CSSVs compete for selling substitutable security services, e.g., intrusion detection and virus scanning, to the users. The users who have the incentive to buy the security service are usually businesses due to their strict requirement of high-level service security. These security services protect the users' access to the cloud platform. For example, Oracle and IBM security offer substitutable cloud security services, e.g., Oracle CASB Cloud Service [32] and IBM Trusteer [31], to protect the cloud access. Similar to travel insurance in airline industry, the CSSVs can offer cloud-insurance to these security services and guarantee that the user will receive a financial compensation, i.e., claim, once a cyber attack, e.g., data loss, happens. The offer of cloud-insurance can ensure the competitiveness of the CSSVs in the cloud security service market and improves the users' confidence of using the cloud security service even when the attacks happen. Moreover, motivated by the desire to lower the probability of paying the claim, the CSSV has an incentive to invest in improving its own security service in order to reduce the cyber breach probability. As a representative example, IBM security can invest in IBM Trusteer to fight an identity fraud attack with a solution infused with layers of cognitive fraud detection and analytics. Otherwise, IBM security has a high probability of paying claim to the users. As such, if the users are attacked upon their access to the cloud platform, the users are less affected which helps the CSSV pay less claim accordingly. The cloud security service together with the cloud-insurance is named as "cloud security plan".

1.2.4 Connections among Research Issues

In this thesis, we aim to use the cyber-insurance, i.e., an novel economic tool, to manage the cyber risks and alleviate the damage of the cyber attacks for the computer networks. Although the system models in the aforementioned three research issues differ with each other due to the unique features and properties of the specifical backgrounds, the motivations that utilizing the cyber-insurance to

FIGURE 1.4: System model for the cloud security service market.

defend against the cyber attacks are similar, which result in some certain similarities in the cyber risk estimation and further the premium pricing model for the cyber-insurance. In this case, the connection among the aforementioned three research issues exhibits in terms of the cyber-insurance, which has been presented in Fig. 1.5. For the first research issue, i.e., Chapter 3, the premium pricing model of the cyber-insurance is based on the probability of successful attack, which is estimated by comparing the defense/attack computing resources of the defender and the attacker in the fractional form. For the second research issue, i.e., Chapter 4, by taking into account the computing resources of the defender and the total computing resource of the network, the probability of successful attack is estimated by using a regularized incomplete Beta function, i.e., (4.2), which together with the concept of risk-adjusted premium (see [43]) constitute the premium pricing model for the cyber-insurance. For the third research issue, i.e., Chapter 5, a assessment approach of the system vulnerability was adopted to evaluate the breach probability of the cloud security service. Then, the breach probability was used to price the cloud security plan, which includes the cloud-insurance and the cloud security service.

FIGURE 1.5: An overview of the connections among the research issues.

1.3 Major Contributions

Our main contributions can be stated as follows:

- *Chapter 3:*
 - We model the interactions among the fog computing provider, APT attacker, and cyber-insurer of the fog computing platform as a dynamic Stackelberg game framework based on optimal control theory and evolutionary game theory. Unlike traditional static game models in the existing literature, we propose a new framework to consider the dynamic (i.e., time-dependent) behaviors of the fog computing provider, APT attacker, and cyber-insurer.
 - We show that the replicator dynamics of the lower-level evolutionary subgame for the fog computing provider's defense strategy and cyber-insurance subscription strategy as well as the APT attacker's attack strategy globally converge to the evolutionary equilibrium. We both analytically and numerically demonstrate the stability and uniqueness

of the evolutionary equilibrium. The Stackelberg equilibrium is investigated by capitalizing on the optimal control theory.

- We show the advantages of dynamic strategies over static strategies in terms of higher payoff for the fog computing provider and higher profit for the cyber-insurer while less payoff for the APT attacker. We also investigate the scalability of our proposed dynamic Stackelberg game model by showing that it is tractable under reasonably large number of fog nodes.
- *Chapter 4:*
 - We formulate the mechanisms of blockchain service pricing, blockchain infrastructure investment and cyber-insurance premium adjustment as a joint market equilibrium problem. We model the interactions among the three parties in the market as a two-level Stackelberg game. We provide and prove a few important theoretical discoveries regarding the properties of the equilibrium in the market game.
 - We incorporate the social externality [44, 45] among blockchain users in our end-user utility model. Also, by modeling the impact of computing power on the blockchain security, we consider the blockchain provider’s strategy to incorporate both dimensions of infrastructure investment and insurance spendings. Furthermore, by adopting the concept of “risk-adjusted premium”, we mathematically capture the impact of attack probability on premium pricing from the cyber-insurer’s perspective.
 - We conduct extensive evaluation to assess the performance of the three parties with their equilibrium strategies at different levels of the attacker-controlled computing power.
- *Chapter 5:*
 - We investigate a joint pricing and security investment problem in the cloud security service market. Therein, we have proposed a two-stage game to model and study the interaction between the CSSVs and the users and the interplay among the users as well as the competition between the CSSVs.

- We incorporate the security interdependency among the users, which is captured by an interdependency matrix. As such, the enhancement in the security level due to the interdependency among the users can be accordingly studied.
- Moreover, in the proposed model, we incorporate the relationship between the cyber breach probability and the CSSVs' security investments, where the effort that the CSSVs make to improve their offered cloud security service is modeled.
- Furthermore, we evaluate our proposed model by conducting extensive simulation. The equilibrium strategies are obtained at different levels of security interdependency.

1.4 Organization of the Thesis

The rest of this thesis is organized as follows:

- *Chapter 2*: We review the related works. Therein, for the first research issue focused on the fog computing, the works related to the network security, game theoretic approach, and cyber-insurance are presented. For the second research issue on the blockchain networks, the works related to the permissionless blockchain, cyber-insurance, and risk-adjusted premium are reviewed.
- *Chapter 3*: We model and study the fog computing platform with the threats of APT attack in the framework of two-level Stackelberg differential game. In particular, the dynamic strategies of the fog computing provider and the APT attacker is modeled in the framework of an evolutionary game in the lower level. Then, we model the premium pricing problem of the cyber-insurer as a dynamic game in the upper level by taking into account the lower-level evolutionary game for the fog computing provider and the APT attacker.
- *Chapter 4*: The problem of defending against the double-spending attacks in the permissionless blockchain is modeled as a two-level Stackelberg game. In the lower level of the Stackelberg game, the users determine the service demand. In the upper level, the blockchain provider jointly strategizes its

investment in the infrastructure and the service fee, and the insurer decides on its insurance premium by determining the risk-averse coefficient.

- *Chapter 5:* We study a problem of defending against the cyber attacks in the cloud platform by formulating a two-stage Stackelberg game. The users has been modeled as the followers and they interact with each other on the lower stage. The CSSVs are the leaders on the upper stage, and their interaction, i.e., competition, has been modeled as a noncooperative game.
- *Chapter 6:* We conclude the thesis, summarize the main research contributions for each research issue, and outline the possible research directions for the future work of each research issue.

Chapter 2

Literature Review

In this chapter, part of the existing works related to our major research issues are reviewed. Therein, specific discussion on the background such as the cyber-insurance, the permissionless blockchain networks, and the risk-adjusted premium are presented. Also, the theoretical tools adopted in our major research issues including the dynamic game and the Stackelberg game are introduced. Moreover, the applications of the adopted theoretical tools in the computer networks are presented.

2.1 Risk Management in Defending Against Advanced Persistent Threats in Fog Computing

2.1.1 Security issues in the Networks

Nowadays, due to the fact that security tops the list of requirements in the networks, a number of works are proposed by researchers to investigate how to efficiently improve the security level of the networks. A secure caching scheme was proposed in [46] for the edge nodes to meet the stringent requirements on the privacy of the mobile social networks. Therein, encryption method was designed to prevent the sensitive data leakage, and the encrypted data was replicated and stored over multiple servers to prevent the loss. The authors in [47] proposed a joint optimization of traffic scheduling and power allocation problem to minimize

the total power consumption while meeting both the mobile users' traffic demand and secrecy requirement. The specific application scenario focused on the dual connectivity, where the mobile user is simultaneously served by the licensed channel of a macro base station and the unlicensed channel of a small-cell access point. In [48], a privacy-friendly and efficient data aggregation scheme was proposed to protect the users' privacy from the security threats caused by the bidirectional communications. Compared with the existing schemes, the proposed scheme performed to be better in terms of privacy protection and computational efficiency. A similar security issue in the contents exchanging among the mobile users has been investigated in [49] based on a joint match-coalition game. Specifically, a coalition game was formulated to study the coalition processes of the base stations, and a matching game was employed to model the selecting processes between the coalitions of the base stations and the communities of the mobile social users. Two low-cost secure-architecture-based techniques were proposed in [50] to decrease the probability of successful attack and further enhanced the security level with respect to the attacks of the sensor-node fabrication. Specifically, a root of trust, which was embedded in the hardware, was used by the new architecture to protect the long-term keys, which disabled the adversary from fabricating new nodes through a captured node. The authors in [51] considered an even more challenging attack scenario in cognitive radio networks, where multiple attackers cooperatively maximize their aggregating spectrum utilization. To prevent such attacks, two attack prevention mechanisms, i.e., direct and indirect punishments, were proposed, which have been demonstrated to be effective in preventing the attackers.

2.1.2 Game Theoretical Approaches in the Networks

As a set of efficient tools for performance assessment and network design, game theoretic approaches have been widely applied to model and analyze the performance of various networks. For example, a Stackelberg game framework was adopted in [52] to study the economics of the femtocell service provision. The numerical results have revealed some insights. Only the femtocell service will be provisioned by the cellular operator when the the spatial coverage of the femtocell service is the same as the macrocell service. The behaviors of the entities (including the network manager and the users) in the crowdsourced network have been studied in [53], and their interaction has been modeled as a two-level Stackelberg game. Also, game

theoretic approaches were introduced to model and study security against cyber attacks, e.g., the APT attacks. For instance, the authors in [54] introduced a two-player game defined as FLIPIT to model the stealthy and continuous attacks of the APT. Unlike the most existing games, FLIPIT provides a simple and effective framework that an attacker and a defender compete for a shared resource and can move at any given time, which enables to study the interaction between the attackers and defenders in a more practical scenarios. Moreover, the FLIPIT model has been extended to a three-player game model in [55], where the selfish insider can sell system information of the defender to the APT attacker for a profit. In such a challenging scenario, each move of the defender will incur a fixed cost. In contrast, by utilizing the insider's information, the cost of the attacker incurred by its movement will be reduced. Additionally, the authors in [56] adopted FLIPIT to derive the optimal strategies of the defender by considering a special application scenario that only part of the foothold of the APT attacker in the system can be eliminated. The optimal scheduling for the deployment of the defense activities, e.g., passwords reset and systems reinstallation, was studied for mitigating the information leakage.

2.1.3 An Economic Security Tool

Recently, a novel economic security tool, i.e., cyber-insurance, has attracted great attention due to its capability of enabling effective cyber risk management for the insured customers. For example, a joint pricing and security investment problem in a cloud-insurance market was studied in [57], where the cloud security service vendors jointly strategize its service price and security investment. The cyber-insurance not only provides loss coverage, i.e., the losses and liabilities from network/information security breaches, but also offers other additional services, e.g., the repairment of the company's and individual's reputation [58]. CyberEdge, which is a cyber-insurance product provided by AIG, provides the coverage on data reliability and defence costs, which introduces massive benefits to the insured such as data crisis response and data administrative investigation. However, compared with classical insurance products, cyber-insurance has introduced a number of unique issues. For example, it is difficult to predict the frequency of breaches [59], especially in the case of the APT attacks, one characteristic of which is stealthy. Moreover, due to the high complexity of the techniques, accurately detecting the attacks

through a mere few malicious behaviours of the attackers may not be a feasible solution. Furthermore, the vulnerability of the cyber system is extremely hard to be assessed due to the system-dependent architecture and features. All of the aforementioned issues result in the difficulty of estimating the risk transferred to the cyber-insurer [4], which further introduces challenges into the risk management policy making. Moreover, compared with the insurance in other fields, it is even more challenging to determine when and where an attack has actually taken place, since many are lengthy and leave liability unclear [60]. In this case, we follow the approaches adopted in the literature of [15, 61], where the probability of risk is associated with the cyber security effort and the attack effort. As such, the risk level of the system can be estimated, and the cyber insurance policy can be accordingly studied.

In recent years, there have been some works that adopt the cyber-insurance as an economic tool to manage the risk incurred by the attacks in the networks. In [62], a joint Security-as-a-Service (SECaaS) allocation and cyber-insurance management problem was proposed. The SECaaS is deployed to protect Internet-connected applications and their data against threats such as malware, man-in-the-middle, and denial-of-service (DoS) attacks. Due to the impossibility to ensure mitigation of all possible threats, the authors incorporated the cyber-insurance as an economic tool for neutralizing these threats. Additionally, the authors in [63] investigated the epidemic risks such as virus and worm attacks in heterogeneous networks. Therein, cyber-insurance was adopted as a supplement of security measures to manage the epidemic risks. The effectiveness of cyber-insurance in managing the epidemic risks was validated by showing that cyber-insurance significantly improves the utilities of the nodes in heterogeneous networks. In [64], considering the fact that no security system can completely guard the cloud computing system, cyber-insurance has been introduced to transfer the cyber risks from the customers to a third-party insurer. Therein, by taking into account the uncertainty in the cloud, a stochastic optimization model was proposed to study the cost-efficient policy for the provision of security and insurance.

2.2 Defending Against Double-spending Attacks in Blockchain Networks by Resource Management and Cyber-insurance

2.2.1 Permissionless Blockchain Networks

The permissionless blockchain network was originally conceptualized in the famous grassroot cryptocurrency project “Bitcoin” as a decentralized database for tamper-proof recording and trusted timestamping for the transactional data between P2P users. Permissionless blockchains have been widely recognized for the superb consensus scalability, the tamper-evidence data organization and the capability of supporting the distributed, general-purpose virtual machines [16, 65]. For this reason, in recent years there has seen a plethora of emerging application based on blockchains such as Internet finance and property digitization [66], self-organization for Internet of Things [67] and other nonfinancial applications, e.g., notary documents and anti-counterfeit solutions [68]. For example, to answer the question that how the information related to the cyber security can be shared in an anonymous way, e.g., prevent the organization’s competitors from achieving a comparative advantage on the competition, blockchain-enabled information-sharing framework has been proposed in Chapter 7 of [69]. Therein, a one-way attack in the proposed framework has been investigated. Specifically, consider two groups, i.e., groups 1 and 2, group 2 can launch one-way attack to group 1 by dedicating part of its group members to participate in group 1 while not participating into the legitimate block formation of group 1. This will hinder the blockchain-building process for group 1. The major difference between the double-spending attack under our consideration and the one-way attack is that the malicious nodes in double-spending attack aim at controlling the majority of the mining power while the malicious members in the one-way attack try to hinder the blockchain-building process by hiding their ability/information to the legitimate block formation.

2.2.2 Security Issues in the Permissionless Blockchain Networks

Permissionless blockchain networks creatively solve the problems of replicated consensus in open-access networks by introducing the financial incentive and cryptical zero-knowledge proof into the consensus process [16]. More specifically, any node in the blockchain network is allowed to issue digitally signed transactions to other nodes by “broadcasting” the transactions in a gossip manner over the P2P links between the nodes. The consensus nodes pack up an arbitrary subset of unapproved transactions into a cryptographically protected data structure, i.e., the “block”, and rival with each other in a block publishing race (also known as block mining) to acquire the block mining reward [70]. Following the Nakamoto protocol for blockchain state maintenance [16], the consensus nodes only accept the longest chain among all the locally observable candidates of the blockchain state as their canonical view of the blockchain. To determine the winner of a block mining race, the consensus nodes have to perform an exhaustive search for the solutions of the crypto-puzzles built upon their proposed blocks. In other words, the nodes that acquire more computing power will have higher probability of winning the race and hence the more power of controlling the blockchain state [16]. Therefore, the honest consensus nodes have to secure a sufficiently large amount of computing power to guarantee the well-being of the blockchain services, e.g., data integrity [70]. Grabbing more computing power, on the other hand, is also from which the malicious nodes start to breach the blockchain networks.

2.2.3 Cyber-insurance Approaches

Cyber-insurance, in the meanwhile, has been recognized as an innovative tool to manage the cyber risks and alleviate the damage of cyber-attacks for the insured customers [57]. Cyber-insurance provides the coverage on the losses and liabilities from the network/information security breaches. This greatly incentivizes the security investments by cyber-physical systems. However, compared with classical insurance, cyber-insurance introduces a number of unique issues. For example, due to the interdependence of security systems or lack of statistical data, it is difficult to assess the systems’ vulnerability and hence hard to estimate the risk transferred to the cyber-insurer [71]. For the transaction-oriented cyber services

built upon permissionless blockchains, the designer of cyber-insurance also faces the similar issues. Nevertheless, recent studies on the mechanisms of double-spending attacks [72–74] have shed light upon the possible approaches in analytically assessing the risks of this fundamental threat on the blockchain systems. For example, in [72], the authors proposed a new protocol which requires the consensus nodes, i.e., block miners, to confirm transactions only if the inputs of the transactions have not been spent, hence preventing users from double-spending their funds. Based on the characteristics of intentional forking in double-spending attacks, the authors in [73, 74] introduced the methods to estimate the probability of successful double-spending attacks by analyzing the investments in computing resource of both the blockchain maintainers and attackers. With these studies, it is now possible to estimate the probability of successful double spending and evaluate the potential risks transferred to the cyber-insurers.

2.2.4 Risk-adjusted Premium

Furthermore, under the condition that the probability distribution of risk can be estimated, the authors in [75] proposed a risk-adjusted premium for pricing risks based on the Proportional Hazard (PH) transform, namely, a power transform in the decumulative distribution function of the risks. Since the PH transform satisfies the elementary principles of assigning premiums, i.e., scale-invariance and translation-invariance, it has been adopted in a number of works concerning the premium determination. In addition, a class of premium functions which are comonotonicity additive and stochastic dominance preservative were studied in [43]. Therein, the premium determination method based on the PH transform was generalized with an axiomatic approach, and the principles such as the absolute deviation principle [76] were thoroughly studied and compared. In addition to the PH transform, a new transform was proposed in [77], which used the features of the standard normal cumulative distribution. Compared with the PH transform, this new transform can be applied simultaneously to the assets and liabilities and, moreover, has demonstrated its effectiveness in terms of its lognormal property and the recovery of the Black-Scholes formula. In [78], different determination principles of the risk-adjusted premium have been compared in the reinsurance market. The results has shown that all the transforms except the PH transform behave to be similar to the expected value principle. Moreover, the results have

illustrated the major difference between the PH transform and the expected value principle. The numerical calculation method for different risk-adjusted premium principles has been illustrated in [79], where the excess of loss reinsurance with paid reinstatements was the real-world application scenario. Therein, the evaluated risk-adjusted premium principles includes the PH transform, the logarithmic transform, the exponential transform, the quadratic transform, and the dual-power transform.

2.3 Joint Cyber-insurance and Security Investment Approach in Safeguarding Cloud Platform

2.3.1 Security Issues in Cloud Platform

As cloud computing has gained extensive popularity recently, it is undoubtedly becoming the target of cyber attacks. In this case, there are some works investigating the security issues in the cloud platform. In [80], the authors proposed a new secure provenance scheme to tackle the public concerns on the confidentiality and privacy issues in cloud computing. Based on the bilinear pairing techniques, the proposed scheme is able to record the ownership and process history of the data objects such that the sensitive documents are secure in the cloud. A client-based approach was adopted in [81] to reduce the cyber risks in the cloud such as data leakage and privacy. Specifically, a privacy manager was introduced to coordinate with the cloud service provider to protect the privacy of the users' data. To mitigate the new cyber risks faced by the administrators and users of a cloud's image repository, e.g., the retriever's risks and publisher's risks, an image management system was proposed in [82].

2.3.2 Vulnerability Assessment

An economic model that studies the optimal investment in information security was derived in [83]. The model is applicable to investigate the investment related

TABLE 2.1: Cyber breach probability

Cyber breach probability function	Functional form	Multiple areas of vulnerability	Multiple data assets
Exponential Power	$v(1)^{z^\alpha}$		✓
Proportional Hazard	$1 - [1 - v(1)]^{z^{-\alpha}}$	✓	✓
Wang Transform	$\Phi[\Phi^{-1}(v(1)) - \alpha \ln(z)]$		

tradeoff among the various information security goals such as confidentiality, authenticity, and information integrity. With limited resources, the economic model can provide a framework for deciding on the allocation of scarce information security resource. The author in [84] presented mathematical models for tractably analyzing the cyber breach probability of an information and communications technology (ICT) system, where the vulnerability of an ICT system is quantified as a function of the cyber security spending. Specifically, let $v(z)$ denote the cyber breach probability of an ICT system corresponding to the cyber security spending z , three classes of cyber breach probability function have been introduced in [84] as presented in Table 2.1. Therein, $v(1) > 0$ is the efficiency of the cyber security spending, i.e., the cyber breach probability corresponding to the cyber security spending of 1 unit, $\alpha > 0$ quantifies the effect of the historical information of the ICT system on its cyber breach probability, and Φ is the cumulative distribution of the standard Gaussian distribution. The author has mathematically demonstrated the feasibility of adopting Proportional Hazard class to study the ICT system with multiple areas of vulnerability and multiple data assets as well as that of adopting exponential power class to study the ICT system with multiple data assets.

2.4 Game Theoretic Approaches for Computer Networks

Game theory has been recognized as an efficient tool for modeling and studying the interactions among the decision-making entities in the computer networks. In a game, each entity decides on its strategy for optimizing (including minimizing and maximizing) its objective (such as losses and payoff, respectively). In the computer networks, the entities could be infrastructure providers, service providers, and users competing for maximizing their utilities/payoffs. There are numerous types of

games such as differential games and mean field games. In this thesis, we mainly focus on the dynamic game, i.e., the theoretical approach for the first research issue in Chapter 3, and the Stackelberg game, i.e., the theoretical approach for the second research issue in Chapter 4 and the third research issue in Chapter 5.

2.4.1 Dynamic Game Approaches

Dynamic game approaches have been widely adopted to model and study the long-run interaction among the entities in the computer networks. For instance, the authors in [85] adopted a dynamic game model to study the interaction between the botnet distributed denial-of-service (DDoS) attacker and defender, where the players (including the attacker and defender) repeat the competition with incomplete information. The numerical results has demonstrated the benefits of the adoption of the dynamic game model in terms of the lower false alarm rate for the defender and the improved exposure rate for the attacker. To model the long-run interaction between the intrusion attacker and the defender in the ad-hoc networks, a multi-stage non-cooperative dynamic game has been formulated in [86]. By providing the mathematical framework for the intrusion detection, the strategies of both the malicious nodes and the target nodes can be accordingly studied. Based on the Markov game theory, a novel risk assessment model was proposed in [87]. Therein, the spreading process of potential threats in the network information system was described by using the Markov chain, and extensive simulation experiments were conducted to validate the effectiveness of the proposed approach in the risk assessment.

2.4.2 Stackelberg Game Approaches

The Stackelberg game is a strategic game, where the leader player moves first and the follower players move sequentially. Numerous existing works have deployed the Stackelberg game framework to model and study the resource management and performance optimization in the computer networks. A graph-based security game was formulated in [88] for detecting the potential threats in large computer networks, where the different importances of the numerous computers and the heterogeneous capabilities among the various resources have been taken into account.

TABLE 2.2: Cyber-insurance products

Company	AIG [91]	Chubb [92]	Beazley [93]
Product	CyberEdge	Enterprise Risk Management (ERM)	Beazley Breach Response (BBR)
Business interruption	✓	✓	✓
Reputation Safeguard		✓	✓
Data loss and restoration	✓	✓	✓
Incident response	✓	✓	✓
eCrime coverage	✓	✓	✓

Therein, a novel polynomial time algorithm named Grande has been proposed to find the solution for the game with the guarantee on the bounded error and scalability. In [89], a Stackelberg game based cloud scheduling model was defined. The tradeoff between the task completion time and the energy efficiency has been achieved, and the network performance of which has been demonstrated to outperform the energy-aware baseline. Considering a two-tier network constituted of a macrocell and multiple distributed femtocells, the Stackelberg game framework is adopted to model the interference pricing problem of the macrocell [90]. Specifically, both the macrocell and the femtocells aim to maximize their utilities under the constraint on the interference at the macrocell. Two real-world application scenarios for the femtocells have been studied, including the rural area and the urban areas. In the numerical results, the effectiveness of the proposed model has been validated in the spectrum-sharing femtocell networks.

2.5 Cyber-insurance Products

To date, there have been a few cyber-insurance products available in the market. For example, CyberEdge from AIG not only provides the loss coverage approaches but also helps the insured organization develop effective cyber risk management programs [94]. Therein, the cyber risk management programs include internet facing system examination and cyber security maturity assessment. A cyber-insurance product named “Cyber Enterprise Risk Management (ERM) Insurance” is provided by Chubb [95]. The ERM insurance mainly focuses on covering the business losses

due to the cyber failures or attacks. Both losses coverage and reputation safeguard service are included in Beazley Breach Response (BBR) service [96]. These cyber-insurance products provide different services according to the requirements of the customers they are targeting at. For example, the cyber-insurance products provided by Chubb and Beazley include the reputation safeguard service, which is not included in the policy of the cyber-insurance product provided by AIG. The reason is that the cyber-insurance products provided by Chubb and Beazley target at the business-related customers.

2.6 Summary

In summary, to the best of our knowledge, the aforementioned works in the literature do not consider the following aspects:

- Regarding the works related to the APT attacks and the cyber-insurance, it still remains an open research question that how to employ the cyber-insurance to alleviate the damage of the APT attacks on the fog computing. Moreover, regarding the existing works on the dynamic game frameworks, how to model and study the long-run competition between the APT attacker and the fog computing provider also remain as an open question. The aforementioned questions are our major focuses of the first research issue in Chapter 3. By adopting the cyber-insurance to efficiently manage the cyber risks in the fog computing, i.e., transferring the cyber risks of the APT attacks to the cyber-insurer, the robustness of the services provisioned by the fog computing can be promised. Based on the evolutionary game theory, the long-run competition between the APT attacker and the fog computing provider has been modeled as a dynamic game.
- Regarding the works related to the permissionless blockchain networks, the cyber-insurance, and the risk-adjusted premium, employing the cyber-insurance for alleviating the damage of double-spending attack for the blockchain providers still remains an open research field. The aforementioned works inspire a vision of quantifying the risk of double-spending attacks based on the computing resources owned by the blockchain maintainers and attackers. Then, the corresponding insurance premium can be determined under the framework based

on the PH transform. By transferring the risks caused by double spending to the cyber-insurers, the cyber-physical services residing on the blockchains can be much more robust. This is the major focus of the second research issue in Chapter 4.

- Regarding the works related to the security issues in the cloud platform, the cyber-insurance, and the vulnerability assessment of an information and communication system, it still remains an open research field that safeguarding the cloud service customers through a joint cyber-insurance and security investment approach. Specifically, we study a cloud security service market in Chapter 5, where the users can buy the cloud security plan, which is constituted of cloud security service and cloud-insurance, from the CSSVs to protect them from suffering the cyber attacks. If the attacks happen, the users can receive the claim from the CSSVs. The CSSVs will invest in improving their offered cloud security service in order to decrease the probability of paying claim.

The aforementioned aspects will be investigated in the research issues of this thesis.

Chapter 3

Dynamic Resource Management to Defend Against Advanced Persistent Threats in Fog Computing: A Game Theoretic Approach

In this chapter, we adopt the cyber-insurance and resource management to defend against the APT attacks in the fog computing platform¹.

3.1 System Model

In this section, we present the attack and defense strategies in the fog computing platform as well as the pricing problem of the cyber-insurance. Both the APT attacker and fog computing provider optimize their attack and defense strategies, respectively, by optimally allocating their attack and defense computing resources.

¹The work in this chapter has been published as S. Feng, Z. Xiong, D. Niyato and P. Wang, “Dynamic Resource Management to Defend Against Advanced Persistent Threats in Fog Computing: A Game Theoretic Approach”, in IEEE Transactions on Cloud Computing, 2019. DOI: 10.1109/TCC.2019.2896632. Part of the work in this chapter has been published as S. Feng, Z. Xiong, D. Niyato, P. Wang, and A. Leshem, “Evolving Risk Management Against Advanced Persistent Threats in Fog Computing,” in 2018 IEEE 7th International Conference on Cloud Networking (CloudNet) (pp. 1-6).

TABLE 3.1: Notations for the Fog Computing Platform

Symbol	Description
i, j	Fog nodes i, j
$\mathcal{N}, N$	The set of fog nodes in the fog computing platform and its cardinality
M^A, M^P	The numbers of all the CPUs owned by the APT attacker and fog computing provider, respectively
u_i	The fraction of total available CPUs that the fog computing provider employs to defend fog node i . It is also called “defense CPU ratio of fog node i ”.
v_i	The fraction of total available CPUs that the APT attacker employs to attack fog node i . It is also called “attack CPU ratio of fog node i ”.
x_i, p_i	The cyber-insurance subscription ratio and premium of cyber-insurance for fog node i , respectively
σ	The basic security effort of the fog computing provider on the fog computing platform
λ_i	The amount of asset, e.g., size and value of private information, stored in fog node $i \in \mathcal{N}$
U^P_i, U^A_i	The expected payoffs of the fog computing provider and the APT attacker on fog node i , respectively

Similar to [15], we assume that the APT attacker and fog computing provider need to employ CPUs from other servers to attack and defend the fog nodes, respectively. Moreover, the fog computing provider decides on how much to subscribe for cyber-insurance for each fog node. Accordingly, the cyber-insurer determines the price of the cyber-insurance, i.e., premium, for each fog node. Here, we consider one cyber-insurer in the model. As explained in Section II, the cyber risk is typically system-dependent. Moreover, it is necessary to embrace the dependency of the cyber-risk in designing the cyber-insurance [97]. Therefore, the cyber-insurance is also system-dependent. That is, a cyber-insurance must be developed and offered specifically for a certain system which is the fog computing platform in our work.²

As shown in Fig. 1.2, there exists a set of fog nodes in the fog computing platform, denoted by $\mathcal{N}$. The numbers of all the CPUs owned by the APT attacker and fog computing provider are denoted by M^A and M^P , respectively. To attack fog node $i \in \mathcal{N}$, the APT attacker decides on the number of CPUs employed to attack this node, i.e., $v_i M^A$, where v_i is the fraction of total available CPUs that the APT

²Our game model can be extended for multiple cyber-insurers. However, the corresponding game formulation will be completely different from that of the current model presented in this chapter, and hence it deserves a separate study in the future work.

attacker employs to attack fog node i . It is also called “attack CPU ratio of fog node i ”³. The fog computing provider decides on the number of CPUs employed to defend fog node i , i.e., $u_i M^P$, where u_i is the fraction of total available CPUs that the fog computing provider employs for the defense. It is also called “defense CPU ratio of fog node i ”. According to [98, 99], the probability of successful APT attack and the probability of successful defense are⁴

$$\frac{v_i M^A}{u_i M^P + v_i M^A + \sigma} \quad \text{and} \quad \frac{u_i M^P + \sigma}{u_i M^P + v_i M^A + \sigma}, \quad (3.1)$$

respectively, where σ is the basic security level of fog nodes [100]. The basic security level of fog nodes comes from elemental security measures, e.g., firewall, installed in each fog node. The amount of asset, i.e., size and value of private information, targeted by the APT attacker in each fog node $i \in \mathcal{N}$ is denoted by λ_i . Based on the probability of successful APT attack in (3.1), the expected payoffs excluding the costs of the APT attacker and the fog computing provider on fog node i resulted from the attack and defense strategies are therefore

$$\lambda_i \frac{v_i M^A}{u_i M^P + v_i M^A + \sigma} \quad \text{and} \quad \lambda_i \frac{u_i M^P + \sigma}{u_i M^P + v_i M^A + \sigma}, \quad (3.2)$$

respectively. To attack as well as to protect the fog node i , there exist costs for both of them, which are proportional to the number of CPUs employed from other servers and working time, e.g., energy consumption in $J/(CPU \cdot Sec)$, to attack and defend fog node i , i.e., $a_i v_i M^A$ and $d_i u_i M^P$, respectively. a_i is the APT attacker’s attack cost of employing one CPU to attack fog node i , and d_i is the fog computing provider’s defense cost of employing one CPU to defend fog node i . Therefore, with the expected payoff excluding cost of the APT attacker shown in (3.2), its expected payoff is as follows

$$U_i^A(u_i, v_i) = \lambda_i \frac{v_i M^A}{u_i M^P + v_i M^A + \sigma} - a_i v_i M^P, \quad \sum_{i \in \mathcal{N}} v_i = 1. \quad (3.3)$$

To rationally manage the cyber risk, the fog computing provider subscribes to

³The CPUs, i.e., computing resource, are employed in the form of computing power and hence can be optimized as continuous variables.

⁴The more sophisticated and complicated scenario, e.g., incomplete information and stochastic differential game, can be considered in the future work.

FIGURE 3.1: An illustration of internal benefit.

one cyber-insurance offered by a cyber-insurer⁵. The cyber-insurer determines the premium of fog node i , i.e., p_i . Accordingly, the fog computing provider decides on the cyber-insurance subscription ratio for each fog node, i.e., x_i [101]. Therefore, the fog computing provider needs to pay the expected premium of $p_i x_i$ for fog node i . In return, for fog node i , the fog computing provider receives the claim of $\lambda_i x_i$ paid by the cyber-insurer once the APT attack happens and also will gain the internal benefits of $\frac{2}{\gamma} (1 - e^{-\frac{\gamma}{2} \lambda_i x_i})$ from subscribing to the cyber-insurance [102, 103]. Here, we use the exponential utility function, i.e., $\frac{2}{\gamma} (1 - e^{-\frac{\gamma}{2} \lambda_i x_i})$ which is an increasing concave function of $\lambda_i x_i$, to capture the decreasing marginal returns. Specifically, the exponential utility function measures the risk-averse level of the fog computing provider, where the risk-averse level of the fog computing provider increases as the value of γ becomes larger as shown in Fig. 3.1. Note that the internal benefits come from two facts: 1) the fog computing provider transfers the status of the payoff of $\lambda_i x_i$ from unsafe to safe by subscribing to the cyber-insurance [103], and 2) the cyber-insurer not only provides the loss coverage to the fog computing provider but also attaches some other additional services to the subscribed cyber-insurance. For example, the cyber-insurance provided by AIG not only covers the data security liability, but also includes the repairment of the

⁵The scenario that the fog computing provider subscribes to multiple cyber-insurances can be easily achieved by adjusting the constraint, i.e., $\sum_{i \in \mathcal{N}} x_i = 1$, as shown below (3.4) to $\sum_{i \in \mathcal{N}} x_i = 2, 3, \dots$

company's and individual's reputation as an additional service attached to the cyber-insurance [58].

As a result, based on the expected payoff excluding cost of the fog computing provider as shown in (3.2), its expected payoff on fog node i is expressed as follows:

$$U_i^P(u_i, v_i, x_i, p_i) = \lambda_i \frac{u_i M^P + \sigma}{u_i M^P + v_i M^A + \sigma} - d_i u_i M^P - p_i x_i + \frac{2}{\gamma} \left(1 - e^{-\frac{\gamma}{2} \lambda_i x_i}\right) + \lambda_i x_i \frac{v_i M^A}{u_i M^P + v_i M^A + \sigma}, \quad (3.4)$$

where $\sum_{i \in \mathcal{N}} u_i = 1$ and $\sum_{i \in \mathcal{N}} x_i = 1$.

By pricing the cyber-insurance, the cyber-insurer receives the expected revenue $p_i x_i$ on fog node i from the fog computing provider. On the contrary, the cyber-insurer needs to pay the expected claim, i.e., $\lambda_i x_i$, once the APT attack happens. From (3.1), recall that the probability of successful APT attack is denoted by $\frac{v_i M^A}{u_i M^P + v_i M^A + \sigma}$. Let

$$\begin{aligned} \mathbf{u} &= [u_1, \dots, u_N]^\top \in \mathcal{D}_{\mathbf{u}} = \times_{i \in \mathcal{N}} \mathcal{D}_{u_i}, \quad \mathbf{v} = [v_1, \dots, v_N]^\top \in \mathcal{D}_{\mathbf{v}} = \times_{i \in \mathcal{N}} \mathcal{D}_{v_i}, \\ \mathbf{x} &= [x_1, \dots, x_N]^\top \in \mathcal{D}_{\mathbf{x}} = \times_{i \in \mathcal{N}} \mathcal{D}_{x_i}, \quad \mathbf{p} = [p_1, \dots, p_N]^\top \in \mathcal{D}_{\mathbf{p}} = \times_{i \in \mathcal{N}} \mathcal{D}_{p_i}, \end{aligned} \quad (3.5)$$

where $\times$ is the Cartesian product, then the overall expected profit function of the cyber-insurer is

$$\Pi_I(\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{p}) = \sum_{i \in \mathcal{N}} \left(p_i x_i - \lambda_i x_i \frac{v_i M^A}{u_i M^P + v_i M^A + \sigma} \right), \quad (3.6)$$

where N is the cardinality of set $\mathcal{N}$, $\mathcal{D}_{u_i} = [0, 1]$, $\mathcal{D}_{v_i} = [0, 1]$, $\mathcal{D}_{x_i} = [0, 1]$, and $\mathcal{D}_{p_i} = [0, p^u]$, $\forall i \in \mathcal{N}$ are the domains of definition of u_i , v_i , x_i , and p_i , $\forall i \in \mathcal{N}$, respectively.

3.2 A Dymanic Stackelberg Game Formulation

In this section, we study the long-run interactions among the fog computing provider, APT attacker, and cyber-insurer by formulating a dynamic Stackelberg game.

FIGURE 3.2: The dynamic strategies of the fog computing provider and cyber-insurer.

Specifically, in the lower-level of the dynamic Stackelberg game, the long-run interaction between the fog computing provider and APT attacker is formulated as an evolutionary game based on the replicator dynamics. For the cyber-insurer, it prices the cyber-insurance over a continuous time space in the upper-level, i.e., the fog computing provider is required to pay the current premium [104]. Figure 3.2 shows how the pricing of the cyber-insurance affects the revenue of the cyber-insurer in discrete time slots, where the revenue is the income that a cyber-insurer has from its pricing of cyber-insurance, i.e., premium, excluding its cost, i.e., claim. The cyber-insurance subscription ratio of fog node i is a function of time, i.e., $x_i(t)$, while the fog computing provider currently pays the premium $p_i(t)$ for fog node i at time t . Therefore, the accrued premium income rate on fog node i at time t is $p_i(t) x_i(t)$ and the change in the revenue of cyber-insurer between time t and time $t + \Delta t$ due to the accrued premium income rate of fog node i is denoted by the term $\int_t^{t+\Delta t} p_i(t) x_i(t) dt$ [104–106]. This means that the fog computing provider needs to pay the premium of $\int_t^{t+\Delta t} p_i(t) x_i(t) dt$ for fog node i at time t for the insured period of Δt . Note here that the value of the insured period, i.e., Δt , can be varied.

3.2.1 Formulation of the Lower-Level Evolutionary Subgame

The evolutionary game in the lower-level under our consideration is composed of two entities with three strategies, i.e., the cyber-insurance subscription strategy and defense strategy of the fog computing provider as well as the attack strategy of the APT attacker. The reason that both the fog computing provider and APT attacker are in the lower-level is due to the fact that they simultaneously make decisions based on the same set of information. This is different from the cyber-insurer that usually chooses its strategy before the fog computing provider does as the cyber-insurer is the seller in the cyber-insurance market. Hence, we consider the cyber-insurer to be the leader and the problem of which is studied in the upper-level.

With the expected payoff of the fog computing provider on fog node i defined in (3.4), the average expected payoff of the fog computing provider on the fog computing platform from the defense is expressed by

$$\bar{U}_D^P(\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{p}) = \sum_{i \in \mathcal{N}} u_i U_i^P(u_i, v_i, x_i, p_i). \quad (3.7)$$

Likewise, the average expected payoff of the fog computing provider from the cyber-insurance subscription strategy is

$$\bar{U}_I^P(\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{p}) = \sum_{i \in \mathcal{N}} x_i U_i^P(u_i, v_i, x_i, p_i). \quad (3.8)$$

The average expected payoffs, i.e., (3.7) and (3.8), are derived from (3.4) above. Similarly, derived from (3.3), the average expected payoff of the APT attacker on the fog computing platform is given as

$$\bar{U}^A(\mathbf{u}, \mathbf{v}) = \sum_{i \in \mathcal{N}} v_i U_i^A(u_i, v_i). \quad (3.9)$$

For the convenience of equilibrium analysis to be presented in Section 3.3, we define

$$\begin{aligned}
f_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)) &= u_i(t) \left[U_i^P(u_i(t), v_i(t), x_i(t), p_i(t)) \right. \\
&\quad \left. - \bar{U}_D^P(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)) \right], \\
g_i(\mathbf{u}(t), \mathbf{v}(t)) &= v_i(t) \left[U_i^A(u_i(t), v_i(t)) - \bar{U}^A(\mathbf{u}(t), \mathbf{v}(t)) \right], \\
h_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)) &= x_i(t) \left[U_i^P(u_1(t), v_i(t), x_i(t), p_i(t)) \right. \\
&\quad \left. - \bar{U}_I^P(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)) \right],
\end{aligned} \tag{3.10}$$

$\forall i \in \mathcal{N}$, and, in a vector form, we have

$$\begin{aligned}
\mathbf{f}(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)) &= [f_1(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)), \dots, f_N(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t))]^\top, \\
\mathbf{g}(\mathbf{u}(t), \mathbf{v}(t)) &= [g_1(\mathbf{u}(t), \mathbf{v}(t)), \dots, g_N(\mathbf{u}(t), \mathbf{v}(t))]^\top, \\
\mathbf{h}(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)) &= [h_1(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)), \dots, h_N(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t))]^\top.
\end{aligned} \tag{3.11}$$

Basically, $f_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t))$ quantifies the difference between the current payoff of the fog computing provider on fog node i and its average current payoff on the fog computing platform magnified by the ratio of $u_i(t)$. This function indicates how fast the defense strategy of the fog computing provider on fog node i should change, i.e., $\nabla_t u_i(t)$ in (3.12), and evolves its defense strategy which is an important factor in replicator dynamics. The explanations of $g_i(\mathbf{u}(t), \mathbf{v}(t))$ and $h_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t))$ can be derived in a similar way.

According to the pairwise proportional imitation protocol [107] and conditioned on the cyber-insurer's premium strategy, i.e., $\mathbf{p}(t) \in \mathcal{D}_\mathbf{p}$, the lower-level evolutionary subgame is as follows:

$$\nabla_t \begin{pmatrix} \mathbf{u}(t) \\ \mathbf{v}(t) \\ \mathbf{x}(t) \end{pmatrix} = \begin{pmatrix} \mathbf{f}(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)) \\ \mathbf{g}(\mathbf{u}(t), \mathbf{v}(t)) \\ \mathbf{h}(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)) \end{pmatrix}, \tag{3.12}$$

with the initial strategies $\left[(\mathbf{u}(0))^\top, (\mathbf{v}(0))^\top, (\mathbf{x}(0))^\top \right]^\top = \left[(\mathbf{u}^0)^\top, (\mathbf{v}^0)^\top, (\mathbf{x}^0)^\top \right]^\top$, and $\mathcal{D}_\mathbf{u}$, $\mathcal{D}_\mathbf{v}$, $\mathcal{D}_\mathbf{x}$, and $\mathcal{D}_\mathbf{p}$ have been transferred into Banach spaces with a norm,

such as $\forall \mathbf{p} \in \mathcal{D}_{\mathbf{p}}, \|\mathbf{p}\| = \left(\int_{\mathcal{T}} |\mathbf{p}(t)|^q dt \right)^{\frac{1}{q}}, q \in (1, +\infty)$, which is a system of Ordinary Differential Equations (ODEs). Therein, ∇_t is the differential operator, i.e., $\frac{d}{dt}$, with respect to t , and the usage of the differential operator is defined similarly in the rest of this chapter. The replicator dynamics of the lower-level evolutionary subgame defined in (3.12) is to model dynamic decisions making of the players. In particular, the player measures its current payoff with the average payoff and switches its strategy if its current payoff is lower than the average payoff. Note that in practical systems, the average payoff can be calculated by observing the past outcome of the game or through an intermediary [108].

3.2.2 Formulation of the Stackelberg Differential Game

Based on (3.6), the instantaneous expected profit of the cyber-insurer is as follows

$$\begin{aligned} & \Pi_I(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)) \\ &= \sum_{i \in \mathcal{N}} \left[p_i(t) x_i(t) - \lambda_i x_i(t) \frac{v_i(t) M^A}{u_i(t) M^P + v_i(t) M^A + \sigma} \right], \end{aligned} \quad (3.13)$$

and the corresponding cumulative expected profit of the cyber-insurer within the time horizon of $\mathcal{T} = [0, T]$ is given by

$$\begin{aligned} & \int_{\mathcal{T}} \Pi_I(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)) dt \\ &= \int_{\mathcal{T}} \sum_{i \in \mathcal{N}} \left[p_i(t) x_i(t) - \lambda_i x_i(t) \frac{v_i(t) M^A}{u_i(t) M^P + v_i(t) M^A + \sigma} \right] dt. \end{aligned} \quad (3.14)$$

Then, the Stackelberg differential game for the cyber-insurer is

$$\begin{aligned} & \max_{\mathbf{p} \in \mathcal{D}_{\mathbf{p}}} \int_{\mathcal{T}} \Pi_I(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)) dt \\ \text{s.t. } & \nabla_t \begin{pmatrix} \mathbf{u}(t) \\ \mathbf{v}(t) \\ \mathbf{x}(t) \end{pmatrix} = \begin{pmatrix} \mathbf{f}(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)) \\ \mathbf{g}(\mathbf{u}(t), \mathbf{v}(t)) \\ \mathbf{h}(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)) \end{pmatrix} \\ & \left[(\mathbf{u}(0))^{\top}, (\mathbf{v}(0))^{\top}, (\mathbf{x}(0))^{\top} \right]^{\top} = \left[(\mathbf{u}^0)^{\top}, (\mathbf{v}^0)^{\top}, (\mathbf{x}^0)^{\top} \right]^{\top}, \end{aligned} \quad (3.15)$$

where the lower-level evolutionary subgame formulated in (3.12) has been taken into account and (3.15) is an optimal control problem. Note that the optimal control problem defined in (3.15) maximizes the cumulative expected profit for the cyber-insurer under the constraint of the strategy evolution processes of the APT attacker and fog computing provider. Since our dynamic Stackelberg game is a standard optimal control problem, the solution of which can be found by using the standard algorithm in [109].

3.3 Equilibrium Analysis

In this section, we present the equilibrium analysis for the lower-level evolutionary subgame and the Stackelberg game. Due to the time-varying property of the Stackelberg game, we first prove that the solution of the lower-level evolutionary subgame is unique based on the Cauchy-Lipschitz theorem, i.e., Lemma 3.3.1, in Theorem 3.3.2. Moreover, Theorem 3.3.2 adopts the result from Proposition 3.3.1. Then, based on the Lyapunov's second method for stability presented in Lemma 3.3.3, we study the stability of the solution to the lower-level evolutionary subgame in Theorem 3.3.4. In Theorem 3.3.6, we prove that the objective of the formulated optimal control problem, i.e., the objective of the Stackelberg game defined in (3.15), approaches its supremum in a bounded set and admits a solution by using the result of Lemma 3.3.5.

3.3.1 Equilibrium Analysis for the Lower-Lever Evolutionary Subgame

First, based on Lemma 3.3.1, we study the solution of the lower-level evolutionary subgame defined in (3.12) with respect to its uniqueness.

Lemma 3.3.1. Cauchy-Lipschitz theorem [110]: Consider a system of ODEs

$$\nabla_t \mathbf{y}(t) = \mathbf{F}(\mathbf{y}(t), t), \forall t \in \mathcal{T}, \mathbf{y}(0) = \mathbf{y}^0, \quad (3.16)$$

where $\mathbf{y}(t) \in \mathcal{D} \subseteq \mathbb{R}^n$ denotes the system state vector, $\mathcal{D}$ is the domain of definition of $\mathbf{y}(t)$ containing the origin point, and $\mathbf{F} : \mathcal{D} \times \mathcal{T} \mapsto \mathbb{R}^n$ is continuous on $\mathcal{D} \times \mathcal{T}$.

$$\begin{aligned}
& \left| \frac{df_i(\mathbf{u}_{-j}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p})}{dz} \right|_{z=u_j(t)}, \quad \left| \frac{df_i(\mathbf{u}(t), \mathbf{v}_{-j}(t), \mathbf{x}(t), \mathbf{p})}{dz} \right|_{z=v_j(t)}, \\
& \left| \frac{df_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}_{-j}(t), \mathbf{p})}{dz} \right|_{z=x_j(t)}, \quad \left| \frac{dg_i(\mathbf{u}_{-j}(t), \mathbf{v}(t))}{dz} \right|_{z=u_j(t)}, \\
& \left| \frac{dh_i(\mathbf{u}_{-j}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p})}{dz} \right|_{z=u_j(t)}, \quad \left| \frac{dh_i(\mathbf{u}(t), \mathbf{v}_{-j}(t), \mathbf{x}(t), \mathbf{p})}{dz} \right|_{z=v_j(t)}, \\
& \left| \frac{dh_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}_{-j}(t), \mathbf{p})}{dz} \right|_{z=x_j(t)}, \quad \left| \frac{dg_i(\mathbf{u}(t), \mathbf{v}_{-j}(t))}{dz} \right|_{z=v_j(t)},
\end{aligned} \tag{3.18}$$

If there exists a constant $M \in \mathbb{R}$ such that

$$\begin{aligned}
|\mathbf{F}(\mathbf{y}_1(t), t) - \mathbf{F}(\mathbf{y}_2(t), t)| &\leq M |\mathbf{y}_1(t) - \mathbf{y}_2(t)|, \\
\forall [\mathbf{y}_1(t), t], [\mathbf{y}_2(t), t] &\in \mathcal{D} \times \mathcal{T},
\end{aligned} \tag{3.17}$$

then $\mathbf{F} : \mathcal{D} \times \mathcal{T} \mapsto \mathbb{R}^n$ satisfies the Lipschitz condition, and for any $\mathbf{y}^0 \in \mathbb{R}^n$, the system of ODEs defined in (3.16) is uniquely solvable.

To prove that the lower-level evolutionary subgame defined in (3.12) satisfies the Lipschitz condition, i.e., Lemma 3.3.1, we need to first present Proposition 3.3.1 that defines the upper bounds for the absolute value of the derivatives of replicator dynamics.

Proposition 3.3.1. Let $\mathbf{u}_{-j}(t) = [u_1(t), \dots, u_{j-1}(t), z, u_{j+1}(t), \dots, u_N(t)]^\top$, $\mathbf{v}_{-j}(t) = [v_1(t), \dots, v_{j-1}(t), z, v_{j+1}(t), \dots, v_N(t)]^\top$, $\mathbf{x}_{-j}(t) = [x_1(t), \dots, x_{j-1}(t), z, x_{j+1}(t), \dots, x_N(t)]^\top$, for any given $\mathbf{p} = \mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}$, there exist the upper bounds of (3.18), $\forall [\mathbf{u}(t)^\top, \mathbf{v}(t)^\top, \mathbf{x}(t)^\top]^\top \in \mathcal{D}_{\mathbf{u}} \times \mathcal{D}_{\mathbf{v}} \times \mathcal{D}_{\mathbf{x}}$, $\forall i, j \in \mathcal{N}$, denoted by M^{dfdu}_{ij} , M^{dfdv}_{ij} , M^{dfdx}_{ij} , M^{dgdu}_{ij} , M^{dhdu}_{ij} , M^{dhdv}_{ij} , and M^{dhdx}_{ij} , M^{dgdv}_{ij} , respectively, where all of the upper bounds are positive finite real numbers.

Proof. Please refer to Appendix A.1. □

With Proposition 3.3.1, we can prove that the replicator dynamics satisfy the Lipschitz condition, i.e., Lemma 3.3.1, and then the solution to the lower-level evolutionary subgame, i.e., (3.12), is unique as presented in Theorem 3.3.2.

Theorem 3.3.2. For any given $\mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}$, the solution of the lower-level evolutionary subgame (3.12) is unique.

Proof. Please refer to Appendix A.2. $\square$

Then, based on Lemma 3.3.3, we justify the stability of the unique evolutionary equilibrium to the lower-level evolutionary subgame defined in (3.12) as presented in Theorem 3.3.4.

Lemma 3.3.3. Lyapunov's second method for stability [111]: With the system of ODEs (3.16), if there is a function $V(\mathbf{y}(t)) : \mathbb{R}^n \mapsto \mathbb{R}$ satisfying the following conditions

- $V(\mathbf{y}(t)) = 0$, if $\mathbf{y}(t) = \mathbf{0}$,
- $V(\mathbf{y}(t)) > 0$, if $\mathbf{y}(t) \neq \mathbf{0}$,
- $\nabla_t V(\mathbf{y}(t)) = \frac{d}{d\mathbf{y}(t)} V(\mathbf{y}(t)) \times \frac{d}{dt} \mathbf{y}(t) = (\nabla_{\mathbf{y}} V)^\top \times \mathbf{F}(\mathbf{y}(t), t) \leq 0$, for all $\mathbf{y}(t) \neq \mathbf{0}$,

the stability of the solution to (3.16) can be promised.

Theorem 3.3.4. Conditioned on $\mathbf{p}$, i.e., $\mathbf{p} = \mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}$, the evolutionary equilibrium of the lower-level evolutionary subgame defined in (3.12) is stable.

Proof. According to the Lyapunov's second method for stability, i.e., Lemma 3.3.3, the Lyapunov function can be given as follows:

$$V(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)) = \left\{ \sum_{i \in \mathcal{N}} [u_i(t) + v_i(t) + x_i(t)] \right\}^2, \quad (3.19)$$

where $V(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)) : \mathcal{D}_{\mathbf{u}} \times \mathcal{D}_{\mathbf{v}} \times \mathcal{D}_{\mathbf{x}} \mapsto \mathbb{R}$ satisfies

$$V(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)) \begin{cases} = 0, & \text{if } \mathbf{u}(t) = \mathbf{v}(t) = \mathbf{x}(t) = \mathbf{0} \in \mathcal{D}_{\mathbf{u}} \cap \mathcal{D}_{\mathbf{v}} \cap \mathcal{D}_{\mathbf{x}}, \\ > 0, & \text{otherwise.} \end{cases} \quad (3.20)$$

Conditioned on $\mathbf{p} \in \mathcal{D}_p$, the first derivative of $V(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t))$ with respect to t , i.e., $\nabla_t V(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t))$ in (3.21) is smaller than or equal to 0. Hence, based on Lemma 3.3.3, the evolutionary equilibrium of the lower-level evolutionary subgame, i.e., (3.12) is stable. This completes the proof. $\square$

$$\begin{aligned}
\nabla_t V(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)) &= \frac{d \left\{ \sum_{i \in \mathcal{N}} [u_i(t) + v_i(t) + x_i(t)] \right\}^2}{dt} \\
&= 2 \left\{ \sum_{i \in \mathcal{N}} [u_i(t) + v_i(t) + x_i(t)] \right\} \left\{ \sum_{i \in \mathcal{N}} [\nabla_t u_i(t) + \nabla_t v_i(t) + \nabla_t x_i(t)] \right\} \\
&= 2 \left\{ \sum_{i \in \mathcal{N}} [u_i(t) + v_i(t) + x_i(t)] \right\} \\
&\quad \times \left\{ \sum_{i \in \mathcal{N}} [f_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}) + g_i(\mathbf{u}(t), \mathbf{v}(t)) + h_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p})] \right\} \\
&\stackrel{(3.10)}{=} 2 \left\{ \sum_{i \in \mathcal{N}} [u_i(t) + v_i(t) + x_i(t)] \right\} \\
&\quad \times \left\{ \left[\sum_{i \in \mathcal{N}} u_i(t) U_i^P(u_i(t), v_i(t), x_i(t), p_i) - \bar{U}_D^P(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}) \right] \right. \\
&\quad \left. + \left[\sum_{i \in \mathcal{N}} v_i(t) U_i^A(u_i(t), v_i(t)) - \bar{U}^A(\mathbf{u}(t), \mathbf{v}(t)) \right] \right. \\
&\quad \left. \times + \left[\sum_{i \in \mathcal{N}} x_i(t) U_i^P(u_1(t), v_i(t), x_i(t), p_i) - \bar{U}_I^P(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}) \right] \right\} \leq 0.
\end{aligned} \tag{3.21}$$

3.3.2 Solution to Optimal Control Problem

According to Theorem 3.3.2, the lower-level evolutionary subgame defined in (3.12) is uniquely solvable with any given $\mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}$. That is, there exists an injective solution operator, which is denoted by $\Gamma : \mathcal{D}_{\mathbf{p}} \mapsto \mathcal{D}_{\mathbf{u}} \times \mathcal{D}_{\mathbf{v}} \times \mathcal{D}_{\mathbf{x}}$, such that $\left[(\mathbf{u}(t))^\top, (\mathbf{v}(t))^\top, (\mathbf{x}(t))^\top \right]^\top - \Gamma(\mathbf{p}(t), \mathbf{u}^0, \mathbf{v}^0, \mathbf{x}^0) = \mathbf{0}, \forall t \in \mathcal{T}$. This yields the equivalent problem of the optimal control problem defined in (3.15) as follows:

$$\begin{aligned}
&\max_{\mathbf{p} \in \mathcal{D}_{\mathbf{p}}} \int_{\mathcal{T}} \Pi_I(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t)) dt \\
&\text{s.t.} \quad \left[(\mathbf{u}(t))^\top, (\mathbf{v}(t))^\top, (\mathbf{x}(t))^\top \right]^\top \\
&\quad - \Gamma(\mathbf{p}(t), \mathbf{u}^0, \mathbf{v}^0, \mathbf{x}^0) = \mathbf{0}, \forall t \in \mathcal{T}.
\end{aligned} \tag{3.22}$$

We substitute the equality constraint in (3.22) into the objective function of (3.22)

and accordingly have the following more simplified equivalent problem of the optimal control problem defined in (3.15), i.e.,

$$\max_{\mathbf{p} \in \mathcal{D}_{\mathbf{p}}} \Psi(\mathbf{p}) := \max_{\mathbf{p} \in \mathcal{D}_{\mathbf{p}}} \int_{\mathcal{T}} \Pi_I(\Gamma(\mathbf{p}(t), \mathbf{u}^0, \mathbf{v}^0, \mathbf{x}^0), \mathbf{p}(t)) dt. \quad (3.23)$$

Lemma 3.3.5. Let $\mathcal{D}_{\mathbf{p}}^{\text{ad}} \subseteq \mathcal{D}_{\mathbf{p}}$ such that $\Psi(\mathbf{p}) : \mathcal{D}_{\mathbf{p}}^{\text{ad}} \mapsto \mathbb{R}$ is bounded, and let $\Upsilon := \sup \{\Psi(\mathbf{p}) \mid \mathbf{p} \in \mathcal{D}_{\mathbf{p}}\}$, if there exists a bounded set $\mathcal{D}_{\mathbf{p}}^{\text{bs}} \subseteq \mathcal{D}_{\mathbf{p}}$ and $\epsilon \in \mathbb{R}^+$ such that

$$\mathbf{p} \in \mathcal{D}_{\mathbf{p}}^{\text{ad}} \setminus \mathcal{D}_{\mathbf{p}}^{\text{bs}} \Rightarrow \Psi(\mathbf{p}) \leq \Upsilon - \epsilon, \quad (3.24)$$

then $\Psi(\mathbf{p})$ approaches its supremum in a bounded set.

Proof. As $\mathcal{D}_{\mathbf{p}}^{\text{bs}}$ is bounded, there is $\delta \in \mathbb{R}^+$ such that $\mathcal{D}_{\mathbf{p}}^{\text{bs}} \subseteq \mathcal{B}_{\delta}(\mathbf{0})$, where $\mathcal{B}_{\delta}(\mathbf{0})$ is a ball centered at original $\mathbf{0} \in \mathbb{R}^N$ with δ as its radius. Since $\epsilon \in \mathbb{R}^+$ defined in Lemma 3.3.5, there exists a sequence $\{\mathbf{p}_n\}_{n \in \mathbb{N}}$ in $\mathcal{D}_{\mathbf{p}}^{\text{ad}}$ such that $\lim_{n \rightarrow \infty} \Psi(\mathbf{p}_n) = \Upsilon$. Then, (3.24) implies that there is $n_0 \in \mathbb{N}$ such that $\mathbf{p}_n$ for each $n > n_0$, i.e., $\mathbf{p}_n \in \mathcal{D}_{\mathbf{p}}^{\text{ad}} \setminus (\mathcal{D}_{\mathbf{p}}^{\text{ad}} \setminus \mathcal{D}_{\mathbf{p}}^{\text{bs}}) = \mathcal{D}_{\mathbf{p}}^{\text{ad}} \cap \mathcal{D}_{\mathbf{p}}^{\text{bs}}$, showing that $\Psi(\mathbf{p}_n)$ approaches its supremum in a bounded set, i.e., $\mathcal{D}_{\mathbf{p}}^{\text{ad}}$. $\square$

Theorem 3.3.6. If $\mathcal{D}_{\mathbf{p}}^{\text{ad}} \subseteq \mathcal{D}_{\mathbf{p}}$ is nonempty, closed, and convex set, and $\Psi(\mathbf{p})$ approaches its supremum and is weakly sequentially semicontinuous, then the equivalent problem in (3.23) of the optimal control problem defined in (3.15) has a solution $\bar{\mathbf{p}} \in \mathcal{D}_{\mathbf{p}}^{\text{ad}}$, which means that the optimal control problem in (3.15) has a solution.

Proof. As proven in Lemma 3.3.5, there exists a sequence $\{\mathbf{p}_n\}_{n \in \mathbb{N}}$ in $\mathcal{D}_{\mathbf{p}}^{\text{ad}}$ such that $\lim_{n \rightarrow \infty} \Psi(\mathbf{p}_n) = \Upsilon$. Moreover, we can choose a bounded maximizing subsequence $\{\mathbf{p}_{n_k}\}_{k \in \mathbb{N}}$ from $\{\mathbf{p}_n\}_{n \in \mathbb{N}}$ such that $\{\mathbf{p}_{n_k}\}_{k \in \mathbb{N}}$ remains in a ball $\mathcal{B}_{\delta}(\mathbf{0})$ with a fixed δ .

Since $\mathcal{D}_{\mathbf{p}}$ is a Banach space with the norm defined as $\|\mathbf{p}\| = \left(\int_{\mathcal{T}} |\mathbf{p}(t)|^q dt \right)^{\frac{1}{q}}$, $q \in (1, +\infty)$, $\mathcal{D}_{\mathbf{p}}$ is a reflexive Banach space. As a closed, nonempty, bounded, and convex set of a reflexive Banach space, $\mathcal{D}_{\mathbf{p}}^{\text{ad}} \cap \overline{\mathcal{B}_{\delta}(\mathbf{0})}$ is weakly sequentially compact based on Theorem 6.10 in [112], where $\overline{\mathcal{B}_{\delta}(\mathbf{0})}$ is the closure of $\mathcal{B}_{\delta}(\mathbf{0})$. Thus, $\{\mathbf{p}_{n_k}\}_{k \in \mathbb{N}}$ has a subsequence $\{\mathbf{p}_{n_{k_l}}\}_{l \in \mathbb{N}}$ that weakly converges to $\bar{\mathbf{p}} \in \mathcal{D}_{\mathbf{p}}^{\text{ad}} \cap \overline{\mathcal{B}_{\delta}(\mathbf{0})}$.

Finally, since $\Psi(\mathbf{p})$ is weakly sequentially semicontinuous, we can have

$$\Upsilon = \lim_{l \rightarrow \infty} \Psi(\mathbf{p}_{n_{k_l}}) = \lim_{l \rightarrow \infty} \sup_k \Psi(\mathbf{p}_{n_{k_l}}) \leq \Psi(\bar{\mathbf{p}}), \quad (3.25)$$

which can be compared with the fact that $\Upsilon \geq \Psi(\bar{\mathbf{p}})$ to yield $\Upsilon = \Psi(\bar{\mathbf{p}})$, showing that $\bar{\mathbf{p}}$ is a solution to the equivalent problem in (3.23) of the optimal control problem defined in (3.15). Therefore, the optimal control problem defined in (3.15) has a solution, and the proof is completed. $\square$

3.4 Performance Evaluation

In this section, we evaluate the performance of the dynamic Stackelberg game. We consider a fog computing platform containing 3 fog nodes, i.e., $N = 3$, over the time horizon of $\mathcal{T} = [0, 100]$. The amounts of assets in, i.e., the size and value of data stored in, fog nodes 1, 2, and 3 are 1.2 (λ_1), 1.3 (λ_2), and 1.4 (λ_3), respectively. The initial strategies of the fog computing provider's defense as well as the cyber-insurance subscription, and the APT attacker's attack are $\mathbf{u}^0 = [0.35, 0.25, 0.4]$, $\mathbf{x}^0 = [0.35, 0.25, 0.4]$, and $\mathbf{v}^0 = [0.4, 0.4, 0.2]$, respectively. The numbers of total CPUs owned by the fog computing provider and the APT attacker are 50 (M^P) and 40 (M^A), respectively. The cost of employing one CPU for the APT attacker and fog computing provider to attack and defend the fog nodes are $\mathbf{a} = [0.03, 0.04, 0.04]$ and $\mathbf{d} = [0.03, 0.04, 0.04]$, respectively. The basic security effort of the fog computing provider on the fog computing platform is $\sigma = 4$. Moreover, the coefficient $\gamma > 0$ measuring the absolute risk-sensitivity is set to be 15, i.e., $\gamma = 15$. The upper bound of the premium of the cyber-insurer is $p^u = 2$.

3.4.1 Numerical Results

3.4.1.1 The stability of evolutionary equilibrium

To verify the stability of the evolutionary equilibrium, we study the direction field of the fog computing provider's defense and cyber-insurance subscription strategies as well as the APT attacker's attack strategy on fog nodes 1 and 2 are taken as

FIGURE 3.3: The direction field of the replicator dynamics

examples. The direction fields between u_1 and u_2 , v_1 and v_2 , x_1 and x_2 as well as u_1 and v_1 are shown in Figs. 3.3(a), (b), (c), and (d), respectively. In Fig. 3.3, we can observe that by following the blue arrows, the unstable strategy will reach and stabilize at the evolutionary equilibrium, which is pointed at by the black arrow with the text of “Evolutionary equilibrium”. This is consistent with Theorem 3.3.4 that the evolutionary equilibrium is stable.

3.4.1.2 Demonstration of the unique solvability of the lower-level evolutionary subgame

To verify the unique solvability of the lower-level evolutionary subgame, we adjust the premium of a selected fog node, which is the strategy determined by the cyber-insurer. Without loss of generality, we investigate the impact of the premium of fog

FIGURE 3.4: The defense CPU ratio and attack CPU ratio of each fog node with different premium of fog node 1 showing the uniqueness of the evolutionary equilibrium

FIGURE 3.5: Evolutionary Equilibrium

node 1 on the defense CPU ratio and attack CPU ratio of each fog node. As shown in Fig. 3.4, we can observe that both the defense CPU ratio and attack CPU ratio of each fog node change as the premium charged to fog node 1 increases from 0.5 to 1.5. The reason is that the evolutionary equilibrium of the lower-level evolutionary subgame is unique corresponding to different premiums charged to the fog nodes, which is consistent with Theorem 3.3.2. Note that the strategies shown in Fig. 3.4 are the stable ones, i.e., for $t = 80$.

3.4.1.3 Evolution process of the dynamic strategies

Next, we study the evolution process of the lower-level evolutionary subgame with the strategies at time $t = 0$ of $\mathbf{u}^0 = [0.35, 0.25, 0.4]$, $\mathbf{v}^0 = [0.4, 0.4, 0.2]$, and $\mathbf{x}^0 = [0.35, 0.25, 0.4]$, which is under the control of the cyber-insurer's premium strategies. The strategy adaptation of the fog computing provider and the APT

FIGURE 3.6: Payoffs and learning rate

attacker indicates the dynamic interaction among the entities in the lower-level evolutionary subgame. As shown in Figs. 3.5(b) and (c), the strategies of the fog computing provider and the APT attacker converge to the equilibrium state at which none of the entities has a willingness to adjust their strategies unilaterally. Although the defense cost of fog node 1, i.e., $d_1 = 0.03$, is the lowest among these three fog nodes, the fog computing provider's defense CPU ratio of fog node 1, i.e., u_1 , decreases from the large initial value to the smallest value at the equilibrium state. The reason is that the fog computing provider prefers the fog node with higher asset while the asset of fog node 1, i.e., $\lambda_1 = 1.2$, is the lowest among these three fog nodes. In contrast, due to the smallest initial defense effort of fog node 2, i.e., the smallest initial defense CPU ratio u_2 , in Fig. 3.5(b) and the higher amount of asset of fog node 2 than that of fog node 1, i.e., $\lambda_2 = 1.3 > \lambda_1 = 1.2$, the fog computing provider loses its payoff and cannot optimally protect the fog computing platform. In this case, the defense CPU ratio of fog node 2 increases from the initial value to the evolutionary equilibrium, i.e., the defense CPU ratio of fog node 2 is larger than that of fog node 1. Accordingly, as a rational entity, the APT attacker decreases the attack CPU ratio of fog node 2 and increases the attack CPU ratio of fog node 1 as shown in Fig. 3.5(c). This results in the largest probability of successful APT attack of fog node 1, and hence the premium of fog node 1 is the highest among these three fog nodes at the evolutionary equilibrium. Note here that even though the difference among the numerical results, e.g., Fig. 3.5(a), are small, they are worth studying from the cumulative perspective.

The adaption of the strategies of the fog computing provider and the APT attacker

FIGURE 3.7: Evolutionary equilibrium of fog node 1 with different values of M^A

can also be observed from Fig. 3.6. Specifically, from Fig. 3.6(a), we observe that the payoffs of both the fog computing provider and the APT attacker fluctuate at first due to their unstable strategies and converge to the stable payoff at the evolutionary equilibrium. Furthermore, Fig. 3.6(b) shows the frequency of the adaptation of the strategies, where the learning rate represents the convergence speed of the replicator dynamics, i.e., $\sum_{i \in \mathcal{N}} [|f_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t))| + |g_i(\mathbf{u}(t), \mathbf{v}(t))| + |h_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}(t))|]$ in (3.10). We observe that the convergence speed keeps increasing with the increasing learning rate. When all the strategies are involved in the adaption, the convergence speed is the fastest, i.e., for $t = 0$. Note that the value of the fastest learning rate depends on the gap between the initial strategies and stable strategies.

3.4.1.4 The impact of the number of total CPUs owned by the APT attacker

Figure 3.7 shows the impact of the number of total CPUs owned by the APT attacker on the fog computing platform with the strategies on fog node 1 as an example. In Fig. 3.7, with the fixed number of total CPUs owned by the fog computing provider, the more CPUs owned by the APT attacker, the faster convergence speed of the strategies on fog node 1 to the evolutionary equilibrium. Moreover, since the gap between the numbers of CPUs owned by the fog computing provider and the APT attacker becomes smaller, i.e., the gap between M^P and M^A , the APT attacker becomes more powerful, and the level of the risk faced by the fog computing provider becomes higher, especially on fog node 1 from which the attack cost is the lowest. Then, the fog computing provider tends to defend the fog node 1, which results in the increase of the defense CPU ratio on fog node 1 with the increasing number of total CPUs owned by the APT attacker. This leads

FIGURE 3.8: Cumulative payoffs of the APT attacker and fog computing provider as well as cumulative profit of the cyber-insurer under dynamic and static Stackelberg games

to the decrease of the probability of successful APT attack, and consequently the premium of fog node 1 decreases as the number of total CPUs owned by the APT attacker increases.

3.4.1.5 Comparison between static and dynamic games

We also compare the differences between dynamic and static Stackelberg games with respect to the cumulative payoffs of the APT attacker and fog computing provider as well as cumulative profit of the cyber-insurer. As shown in Fig. 3.8, we observe that the dynamic Stackelberg game yields higher cumulative payoff for the fog computing provider and cumulative profit for the cyber-insurer while less cumulative payoff for the APT attacker. The reason is that the maximization of the payoffs and profit in dynamic Stackelberg game considers both the transient period, i.e., the period before reaching the equilibrium, and the equilibrium state, i.e., after reaching the equilibrium, of the lower-level evolutionary subgame. However, the static Stackelberg game only considers the equilibrium of the lower-level subgame. Therefore, the dynamic Stackelberg game has advantages over static Stackelberg game in terms of defending against the APT attacks.

FIGURE 3.9: Evolutionary equilibrium with multiple fog nodes

3.4.1.6 Multiple fog nodes

To demonstrate the scalability, we increase the number of fog nodes in the fog computing platform, i.e., $N \geq 3$. We consider three cases, i.e., 3, 6, and 9 fog nodes in the fog computing platform. In each case, the fog nodes can be grouped into three sets. For example, in the case with 6 fog nodes, each set has two fog nodes with the same parameters, i.e., asset, defense cost, and attack cost. As shown in Fig. 3.9(b), we observe that the dynamic strategies on fog nodes with the same parameters converge to the same evolutionary equilibrium from different initial strategies. Moreover, from Fig. 3.9(b), the stable strategies on fog nodes 5 and 6 are the highest among all the fog nodes. This indicates that the fog computing provider prefers to defend the fog node with the largest asset. Additionally, a similar preference of the fog computing provider can be found in Figs. 3.9(b) and (c). This results in the lowest premium of fog nodes 5 and 6, as shown in Fig. 3.9(e). Note here that we increase the number of CPUs for both APT attacker and fog computing provider and σ by twofold in the case of 6 nodes and threefold in the case of 9 nodes.

3.5 Summary

We have studied the attack and defense strategy in the fog computing platform as well as the pricing problem of the cyber-insurance by using the hierarchical dynamic game framework. Specifically, we have modeled the interaction among the fog computing provider, the APT attacker, and cyber-insurer as a two-stage dynamic Stackelberg game. On the lower stage, the dynamics of the fog computing provider's defense strategy as well as the cyber-insurance subscription strategy, and the APT attacker's attack strategy are captured are formulated as an evolutionary subgame based on the replicator dynamics. On the upper stage, the premium pricing problem of the cyber-insurance has been formulated as an optimal control problem. Conditioned on the premium pricing strategy of the cyber-insurer, we have verified the stability and uniqueness of the evolutionary equilibrium theoretically. Moreover, we have numerically demonstrated the stability and uniqueness of the evolutionary equilibrium. In addition, we have demonstrated the scalability of our proposed hierarchical dynamic game framework. The numerical results show that the proposed dynamic game model outperforms the static game model with respect to the player's cumulative payoff/profit. For the future work, we will further explore the role of reinsurance on the fog computing platform.

Chapter 4

On Cyber Risk Management of Blockchain Networks: A Game Theoretic Approach

In this chapter, a joint security enhance approach constituted of infrastructure investment and cyber-insurance has been introduced to defend against the double-spending attacks in the blockchain networks¹.

4.1 System Description and Game Formulation

In this section, we first introduce the model of successful attack probability for double spending and the concept of risk-adjusted premium. After formulating the utilities of the blockchain provider, the users, and the cyber-insurer, we investigate the problem of users' service demand, service pricing and infrastructure, i.e., computing power, investment by the blockchain provider and premium pricing by the cyber-insurer jointly as a hierarchical market game.

¹The work in this chapter has been published as S. Feng, W. Wang, Z. Xiong, D. Niyato, P. Wang and S. S. Wang, "On Cyber Risk Management of Blockchain Networks: A Game Theoretic Approach", in IEEE Transactions on Services Computing, 2018. DOI: 10.1109/TSC.2018.2876846. Part of the work in this chapter has been published as S. Feng, Z. Xiong, D. Niyato, P. Wang, S. S. Wang, and Y. Zhang, "Cyber Risk Management with Risk Aware Cyber-Insurance in Blockchain Networks," in 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-7).

The cyber-insurance for blockchain-based service under our consideration works as follows. The blockchain provider firsts pay the premium determined by the cyber-insurer. If the double-spending attack happens, which is detected by the provider or users, the provider files the claims to the cyber-insurer. The cyber-insurer verifies the claim and makes the payment to the provider to compensate for the damage of the double spending. The methods to detect and verify the double spending attack are available and can be adopted, e.g., by deploying an observer as in [113], and hence they are not the focus of this chapter.

4.1.1 Preliminaries

4.1.1.1 Successful Attack Probability

We consider that the honest consensus nodes work jointly as a single blockchain provider and are responsible for maintaining a permissionless, PoW-based blockchain for service provision. Extending the analysis in [73] and [74], we assume that during a time period of T , the total computing resource of the blockchain network measured by the hash rate is fixed as H . Following the Nakamoto consensus protocol, every consensus node runs an independent Poisson process for puzzle-solving. The average time for a new block to be mined in the blockchain network is T_0 [16]. Then, in the time period of T , the expected number of blocks being successfully mined in the network is $\frac{T}{T_0}$. Let h denote the investment in computing resources by the blockchain provider, i.e., the honest nodes, and a denote the investment in computing resources by the attackers. Then, if the computing efficiencies for hash queries are roughly the same, the blockchain provider and the attackers divide the total computing resource H as $\bar{h}H$ and $\bar{a}H$, respectively, where $\bar{h} = \frac{h}{a+h}$ and $\bar{a} = \frac{a}{a+h}$ are the investment ratios. According to the probabilistic model for winning the PoW-based puzzle solving race [73], the number of blocks that are mined by the blockchain provider and waiting for confirmation during T is $\frac{T}{T_0} \frac{\bar{h}H}{H} = \frac{T}{T_0} \bar{h}$. On the other hand, instead of following the Poisson distribution based model, the number of blocks successfully mined by attackers during T can be accurately modeled as a negative binomial variable [73]. Therefore, with the investment ratio $\bar{h}$, the probability for attackers to succeed in double spending during T can be expressed as

follows (see Theorem 1 in [74]):

$$P(\bar{h}) = I_{4(1-\bar{h})\bar{h}}\left(\frac{T}{T_0}\bar{h}, \frac{1}{2}\right), \bar{h} \geq \frac{1}{2}, \quad (4.1)$$

where $I_w(u, v)$ is the regularized incomplete Beta function:

$$I_w(u, v) = \frac{\Gamma(u+v)}{\Gamma(u)\Gamma(v)} \int_0^w t^{u-1}(1-t)^{v-1} dt \quad (4.2)$$

with $\Gamma(\cdot)$ being the gamma function. The model of exponential decay in (4.1) is discovered in [114] and proved in [74].

We consider that the blockchain provider receives payments from the users in the form of transaction fees in a confirmed block. Under double-spending attacks, the blockchain provider has to compensate the loss of the users with a fixed rate for each transaction in the block that is finally overridden. Assume that the number of transactions included in each block is the same, and hence the transaction fee and compensation rate are fixed for each transaction. Let N_T denote the number of transactions in a block, r denote the block mining reward for each block and q denote the total compensation rate for each block. Then, with the investment ratio $\bar{h}$, the blockchain provider's potential loss is $\frac{T}{T_0}\bar{h}N_Tq$ under the double-spending attack, and the probability of successful attack is:

$$P(\bar{h}) = \begin{cases} I_{4(1-\bar{h})\bar{h}}\left(\frac{T}{T_0}\bar{h}, \frac{1}{2}\right), & \bar{h} \geq \frac{1}{2}, \\ 1, & \bar{h} < \frac{1}{2}. \end{cases} \quad (4.3)$$

Here, we only focus on the case where the investment ratio of the blockchain provider is no less than $1/2$. The reason is that when $\bar{h} < 1/2$, the probability of successful double spending is always equal to 1 as shown in (4.3), which is trivial and thus not our focus.

4.1.1.2 Premium Determination

The cyber-insurer offers a cyber-insurance service to the blockchain provider and covers its total loss when the attack happens. In other words, after the blockchain

provider buys the cyber-insurance, the risk of double-spending attack will be transferred to the cyber-insurer. By adopting the concept of risk-adjusted premium in [43], the cyber-insurer dynamically determines the price, i.e., premium, of its cyber-insurance product according to the insurance risk distribution. According to our previous discussion, the cyber-insurer has an insurance risk, i.e., paying the claim of $\frac{T}{T_0}\bar{h}N_Tq$ with the probability of $P(\bar{h})$ given by (4.3). Then, the expected loss for the cyber-insurer can be formulated as follows:

$$\begin{aligned}
E_{loss} &= \int_{1/2}^1 \frac{T}{T_0} \bar{h} N_T q P(\bar{h}) d\bar{h} = \frac{T}{T_0} N_T q \int_{1/2}^1 \bar{h} P(\bar{h}) d\bar{h} \\
&= \frac{T}{T_0} N_T q \left[\bar{h} F(\bar{h}) \Big|_{\bar{h}=1/2}^{\bar{h}=1} - \int_{1/2}^1 F(\bar{h}) d\bar{h} \right] \\
&\leq \frac{T}{T_0} N_T q \left[\frac{3}{4} - \int_{1/2}^1 F(\bar{h}) d\bar{h} \right] \\
&= \frac{T}{T_0} N_T q \left[\int_{1/2}^1 \frac{3}{2} d\bar{h} - \int_{1/2}^1 F(\bar{h}) d\bar{h} \right] \\
&= \frac{T}{T_0} N_T q \int_{1/2}^1 \frac{3}{2} - F(\bar{h}) d\bar{h} \\
&= \frac{T}{T_0} N_T q \int_{1/2}^1 \left[1 - \int_{1/2}^{\bar{h}} P(\theta) d\theta \right] d\bar{h},
\end{aligned} \tag{4.4}$$

where $F(\bar{h})$ is the cumulative distribution function for $P(\bar{h})$ ². Based on the formulated distribution of the insurance risk and the concept of risk-adjusted premium, the cyber-insurer can determine the premium as follows:

$$\Lambda(\gamma) = \frac{T}{T_0} N_T q \int_{1/2}^1 \omega \left(1 - \int_{1/2}^{\bar{h}} P(\theta) d\theta, \gamma \right) d\bar{h}, \tag{4.5}$$

where $\omega(x, \gamma)$ is an increasing concave function of x and belongs to the families of elementary transforms given in Section 5 of [43]. Without loss of generality, we adopt the PH transform in our study, i.e., $\omega(x, \gamma) = x^{\frac{1}{\gamma}}$, $\gamma \geq 1$ in Subsection 5.1 of [43]. Then, the corresponding premium can be expressed as follows:

$$\Lambda(\gamma) = \frac{T}{T_0} N_T q \int_{1/2}^1 \left[1 - \int_{1/2}^{\bar{h}} P(\theta) d\theta \right]^{1/\gamma} d\bar{h}, \tag{4.6}$$

²Note here that we assume that the cyber-insurer is considering the worst case.

where γ is the premium coefficient which decides on the insurance policy. Namely, the cyber-insurer adjusts the premium by controlling γ according to the insurance risk. It is worth noting that the term $\left[1 - \int_{1/2}^{\bar{h}} P(\theta) d\theta\right]$ in (4.6) is smaller than 1. Therefore, the larger γ is, the higher the premium $\Lambda(\gamma)$ will be.

4.1.2 System Model

4.1.2.1 The User's Utility

We suppose that each user in the blockchain service market has a service demand, which is determined by an intrinsic value θ_i from the uniform distribution F_U over the interval $[0, 1]$. Here, θ_i can be interpreted as the probability for user i to buy the blockchain service. We further assume that the intrinsic values of the users are independently distributed. The users also experience social externalities in which the decision of one user can influence the decisions of the other users. Let $\Pr[j \text{ buys the service}]$ denote the probability that user j subscribes to the service, then, the utility of user i can be expressed as follows [115]:

$$u_i = \bar{h} + \theta_i - p_i + \alpha \sum_{j \in \mathcal{N}} g_{ij} \Pr[j \text{ buys the service}]. \quad (4.7)$$

In (4.7), the first term, i.e., $\bar{h}$, is the investment ratio of the blockchain provider. $\bar{h}$ represents the positive effect owing to the effort of the blockchain provider in preventing the security breach due to double-spending attacks. According to (4.1), the larger $\bar{h}$ is, the lower the successful probability of double-spending attacks is, and consequently the less the users will be affected. The third term, i.e., p_i , is the price of the service for user i ³. The fourth term of (4.7), i.e., $\alpha \sum_{j \in \mathcal{N}} g_{ij} \Pr[j \text{ buys the service}]$, represents the positive social externality among the users. g_{ij} is the element of the externality matrix $\mathbf{G}$ [44], [45] and represents the level of the social externality (influence) that the decision of user j has on that of user i . We assume that $g_{ij} \neq 0, \forall i \neq j$ and $g_{ii} = 0, \forall i \in \mathcal{N}$ ⁴. Finally, α is a constant controlling the level of social externality for the entire network.

³Note here that the uniform pricing in which all users are charged with the same price is a special case of the discriminative pricing adopted in this chapter.

⁴Note here that our model can also be used to analyze the scenario that the users may act independently. For example, if $g_{ij} = g_{ji} = 0$, user j has zero level of the social externality (influence) on user i and vice versa. Hence, users i and j act independently.

4.1.2.2 Profits of the Blockchain Provider and the Cyber-insurer

The goals of the blockchain provider and the cyber-insurer are to maximize their individual profits. Based on our previous discussion, the payoff functions of the blockchain provider can be expressed as follows:

$$\Pi_p(\bar{h}, \mathbf{p}) = \sum_{i \in \mathcal{N}} p_i x_i - \frac{a\bar{h}}{1-\bar{h}} + \bar{h} \frac{T}{T_0} N_T r - \underbrace{\frac{T}{T_0} N_T q \int_{1/2}^1 \left[1 - \int_{1/2}^t P(\theta) d\theta \right]^{1/\gamma} dt}_{\text{premium}}, \quad (4.8)$$

where the first term $\sum_{i \in \mathcal{N}} p_i x_i$ is the revenue obtained from the users' payment for the blockchain service and x_i is the probability that user i buys the service defined in (4.13). The second term, i.e., $h = \frac{a\bar{h}}{1-\bar{h}}$, is the blockchain provider's investment in the infrastructure, and we have $h = \frac{a\bar{h}}{1-\bar{h}} \Leftrightarrow \bar{h} = \frac{h}{a+h}$. The third term, i.e., $\bar{h} \frac{T}{T_0} N_T r$, is the block mining reward received by the blockchain provider for maintaining the service. The last term, i.e., $\frac{T}{T_0} N_T q \int_{1/2}^1 \left[1 - \int_{1/2}^t P(\theta) d\theta \right]^{1/\gamma} dt$, is the premium paid by the blockchain provider to the cyber-insurer, and q is the compensation price for one transaction.

On the other hand, the premium paid by the blockchain provider is the revenue of the cyber-insurer. Due to the uncertainty of double-spending attacks, we adopt the expected claim as the cyber-insurer's cost. Then, the cyber-insurer's payoff function can be expressed as:

$$\Pi_I(\gamma) = \underbrace{\frac{T}{T_0} N_T q \int_{1/2}^1 \left[1 - \int_{1/2}^t P(\theta) d\theta \right]^{1/\gamma} dt}_{\text{premium}} - P(\bar{h}) \bar{h} \frac{T}{T_0} N_T q - \sigma(\bar{h}, \gamma), \quad (4.9)$$

where the first term is the premium paid by the blockchain provider. The second term, i.e., $P(\bar{h}) \bar{h} \frac{T}{T_0} N_T q$, is obtained as the product of the successful attack probability and the total claim paid to the blockchain provider for covering its loss. Finally, since the premium increases as the cyber-insurer's decision variable γ increases, a rational cyber-insurer will keep γ as high as possible to maximum its revenue. However, when the blockchain provider increases its investment ratio, the successful attack probability will decrease. As a result, the blockchain provider will have less incentive to pay an extremely high premium. Therefore, we introduce the last term in (4.9) to model the possibly negative impact on the expected payoff of the cyber-insurer as both the values of $\bar{h}$ and γ increase, which is similar

to the concept of the punishment on insurer adopted in [116]. Here, we define $\sigma(\bar{h}, \gamma) = \sigma_1(\bar{h}) \sigma_2(\gamma)$, where $\sigma_1(\bar{h})$ is an increasing convex function of $\bar{h}$ with the following properties:

$$\sigma_1(\bar{h}) \begin{cases} > 0, & \bar{h} > \frac{1}{2}, \\ = 0, & \bar{h} = \frac{1}{2}, \\ < 0, & \bar{h} < \frac{1}{2}. \end{cases} \quad (4.10)$$

The conditions in (4.10) indicates that with $\bar{h} > \frac{1}{2}$, the blockchain provider's effort in investing the computing resource effectively reduces the successful attack probability. Consequently, the probability of the cyber-insurer paying the claim to the blockchain provider is also reduced. Then, keeping the highest premium has a negative effect on the cyber-insurer's payoff, e.g., by hurting its reputation or curbing the incentive for the blockchain provider to buy the insurance. Under the other two conditions in (4.10), the lack of enough investment in infrastructure of the blockchain provider will induce higher probability of being successfully attacked, hence leading to a positive effect on the cyber-insurer's payoff due to the higher demand of financial protection. Additionally, $\sigma_2(\gamma)$ is an increasing convex function of γ and $\sigma_2(\gamma)|_{\gamma=1} = 0$. As such, when $\gamma = 1$, the expected loss in (4.4) is equal to the premium in (4.6), and there is no negative effect on the cyber-insurer's reputation. For tractable analysis, we adopt the following model:

$$\sigma(\bar{h}, \gamma) = \underbrace{\sigma_1(\bar{h})}_{\left(\bar{h} - \frac{1}{2}\right)^3} \underbrace{\sigma_2(\gamma)}_{(\gamma - 1)\gamma^\beta}, \quad \beta > 1. \quad (4.11)$$

It is worth noting that the cyber-insurer's payoff function in (4.9) may also adopt other models for $\sigma(\bar{h}, \gamma)$. The selected model in (4.11) has no effect on our subsequent analysis.

4.1.3 Stackelberg Game Formulation

Considering the payoff functions of the market entities given in (4.7)-(4.9), it is natural to model the interactions in the blockchain service market as a two-stage game. In the first upper stage, the blockchain provider determines the price of the blockchain service, namely, the levels of acceptable transaction fees for each

user p_i , and its ratio of investment in computing resources $\bar{h}$. Meanwhile, the cyber-insurer decides on the premium coefficient γ by considering the insurance risk transferred from the blockchain provider. In the second lower stage, each user determines whether it will buy the blockchain service or not based on the prices and the investment ratio set by the blockchain provider. Accordingly, the interactions among the blockchain provider, the cyber-insurer, and the users are formulated as a two-stage Stackelberg game with two leaders and multiple followers. Specifically, the mutual interaction between the blockchain provider and cyber-insurer forms a noncooperative two-player leader-level subgame for achieving the equilibrium of the service price, the investment ratio, and the cyber-insurance policy. Then, the interaction among a number of users forms the follower-level noncooperative subgame for determining the service demand from the blockchain provider⁵. The Stackelberg game can be formally defined as follows.

- *User-level noncooperative subgame:* Given the fixed investment ratio $\bar{h}$ as well as the price vectors $\mathbf{p} = [p_1, p_2, \dots, p_{|\mathcal{N}|}]^\top$, we can have the user-level noncooperative subgame defined by a four-tuple $\mathcal{G}_u = \{\mathcal{N}, \mathbf{x}, \mathcal{X}, \mathbf{u}\}$ as follows:
 - $\mathcal{N}$ denotes the set of users;
 - $\mathcal{X} = \left\{ [x_1, x_2, \dots, x_{|\mathcal{N}|}]^\top \mid x_i \in [0, 1], i \in \mathcal{N} \right\} \subset \mathbb{R}^{|\mathcal{N}|}$ denotes the domain of definition of $\mathbf{x}$;
 - $\mathbf{x} = [x_1, x_2, \dots, x_{|\mathcal{N}|}]^\top$ is the vector of the service demands of users and $\mathbf{x} \in \mathcal{X}$;
 - $\mathbf{u} = [u_1, u_2, \dots, u_{|\mathcal{N}|}]^\top$, where u_i given in (4.7) is the utility of user i corresponding to the strategy of $\mathbf{x}$, $\forall i \in \mathcal{N}$.
- *Leader-level noncooperative subgame:* Assume that the users' demand $\mathbf{x}$ has been found to be a parametric equilibrium as a function, i.e., mapping, of the leaders' strategies. Then, the blockchain provider and the cyber-insurer form a noncooperative game as a five-tuple $\mathcal{G}_L = \left\{ [\mathbf{p}^\top, \bar{h}]^\top, \mathcal{D}_P, \gamma, \mathcal{D}_I, \Pi \right\}$, where

⁵The reason that the users are in the same level, i.e., lower-level, is that they have the same set of information and make decisions simultaneously. This is different from the blockchain provider that usually invests in the infrastructure and buys the cyber-insurance first to improve the security level of its blockchain-based service and then provides the service to the users. The cyber-insurer sells the cyber-insurance to the blockchain provider and forms a noncooperative relationship with the blockchain provider. As such, the cyber-insurer and blockchain provider make their decisions simultaneously and hence before the users. As a result, the blockchain provider and cyber-insurer are considered to be the leaders and their problems are defined in the upper-level.

- $[\mathbf{p}^\top, \bar{h}]^\top = [p_1, p_2, \dots, p_{|\mathcal{N}|}, \bar{h}]^\top$ is the strategy vector of the service prices and the investment ratio set by the blockchain provider with $p_i > 0, \forall i \in \mathcal{N}$ and $\bar{h} \in [\frac{1}{2}, 1)$;
- $\mathcal{D}_P = \left\{ [\mathbf{p}^\top, \bar{h}]^\top \mid p^u \geq p_i > 0, \forall i \in \mathcal{N}, \bar{h} \in [\frac{1}{2}, 1) \right\}$ denotes the domain of the prices and investment ratio of the blockchain provider, where p^u is the upper bound of the price p_i imposed by the government or market regulators;
- γ is the cyber-insurer's premium coefficient for premium determination;
- $\mathcal{D}_I = \{\gamma \mid \gamma^u \geq \gamma > 1\}$ defines the domain of γ , where γ^u is the upper bound of γ imposed by the government or regulators;
- $\Pi = [\Pi_P, \Pi_I]^\top$ is the profit vector for the blockchain provider and the cyber-insurer.

4.2 Game Equilibrium Analysis

Based on the formulation of the Stackelberg game in Section 4.1.3, we are ready to analyze the market equilibrium using backward induction. We first obtain the Nash Equilibrium (NE) of the user-level noncooperative subgame $\mathcal{G}_u$ by characterizing a system of interdependent demands. We provide the sufficient conditions for the existence and uniqueness of the NE in the user-level noncooperative subgame $\mathcal{G}_u$ by solving the bounded linear complementarity problem of the subgame [115]. Then, we substitute the parametric NE of $\mathcal{G}_u$ into the leader-level noncooperative subgame $\mathcal{G}_L$. Under a reasonable assumption, we show that the Jacobian matrix constructed from the payoff functions of each player in the leader-level noncooperative subgame is negative definite. Hence, we prove that the Stackelberg Equilibrium (SE) of the market game exists and is unique.

4.2.1 Equilibrium Analysis for User-Level Noncooperative Subgame

Intuitively, user i only buys the service when it has a positive payoff, namely $u_i > 0$. This indicates that there exists a threshold $\tilde{\theta}_i$ for the intrinsic value θ_i in (4.7), such

that user i will buy the service only when $\theta_i > \tilde{\theta}_i$. $\tilde{\theta}_i$ can be obtained by setting $u_i = 0$:

$$\begin{aligned}
0 &= \bar{h} + \tilde{\theta}_i - p_i + \alpha \sum_{j \in \mathcal{N}} g_{ij} \Pr[j \text{ buys the service}] \\
&= \bar{h} + \tilde{\theta}_i - p_i + \alpha \sum_{j \in \mathcal{N}} g_{ij} \Pr[\theta_j > \tilde{\theta}_j] \\
&= \bar{h} + \tilde{\theta}_i - p_i + \alpha \sum_{j \in \mathcal{N}} g_{ij} [1 - F_U(\tilde{\theta}_j)] \\
&\Leftrightarrow \tilde{\theta}_i = p_i - \bar{h} - \alpha \sum_{j \in \mathcal{N}} g_{ij} [1 - F_U(\tilde{\theta}_j)],
\end{aligned} \tag{4.12}$$

where $1 - F_U(\tilde{\theta}_j)$ denotes the probability that user j draws a valuation above the threshold $\tilde{\theta}_j$. For ease of exposition, let $x_i = 1 - F_U(\tilde{\theta}_i)$ denote the probability that user i buys the service, and x_i can be further expressed as follows:

$$\begin{aligned}
x_i &= 1 - F_U(\tilde{\theta}_i) = 1 - F_U\left(p_i - \bar{h} - \alpha \sum_{j \in \mathcal{N}} g_{ij} [1 - F_U(\tilde{\theta}_j)]\right) \\
&= 1 - p_i + \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{ij} x_j.
\end{aligned} \tag{4.13}$$

From (4.13), we can characterize a system of the users' interdependent demands as follows:

$$x_i = \begin{cases} 0, & \text{if } 1 - p_i + \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{ij} x_j < 0, \\ 1, & \text{if } 1 - p_i + \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{ij} x_j > 1, \\ 1 - p_i + \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{ij} x_j, & \text{otherwise.} \end{cases} \tag{4.14}$$

After subtracting each condition in (4.14) by the value of its corresponding x_i , we convert (4.14) into the following form:

$$x_i = \begin{cases} 0, & \text{if } 1 - p_i + \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{ij} x_j - x_i < 0 - \underbrace{x_i}_{=0} = 0, \\ 1, & \text{if } 1 - p_i + \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{ij} x_j - x_i > 1 - \underbrace{x_i}_{=1} = 0, \\ 1 - p_i + \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{ij} x_j, & \text{if } 1 - p_i + \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{ij} x_j - x_i = 0. \end{cases} \tag{4.15}$$

FIGURE 4.1: An illustration of Assumption 1.

Furthermore, (4.15) can be rewritten into the following matrix form:

$$x_i = \begin{cases} 0, & \text{if } \{(1 + \bar{h}) \mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha \mathbf{G}) \mathbf{x}\}_i < 0, \\ 1, & \text{if } \{(1 + \bar{h}) \mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha \mathbf{G}) \mathbf{x}\}_i > 0, \\ \{(1 + \bar{h}) \mathbf{1} - \mathbf{p} + \alpha \mathbf{G} \mathbf{x}\}_i, & \text{if } \{(1 + \bar{h}) \mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha \mathbf{G}) \mathbf{x}\}_i = 0, \end{cases} \quad (4.16)$$

where $\mathbf{I}$ is the identity matrix, $\mathbf{1} = [1, 1, \dots, 1]^\top \in \mathbb{R}^{|\mathcal{N}| \times 1}$ and $\{\cdot\}_i$ represents the i -th entry of a vector. With (4.16), we are ready to investigate the properties of the NE in the user-level noncooperative subgame.

Assumption 1. $\alpha \rho(\mathbf{G}) < 1$, where $\rho(\cdot)$ is the spectral norm of a matrix.

The physical meaning of Assumption 1 is illustrated in Fig. 4.1, where the black area is the feasible area of $\alpha \rho(\mathbf{G})$. If $\alpha \rho(\mathbf{G})$ exceeds the feasible area, the social externality will be too strong such that every user will buy the service, which is impossible in reality.

Theorem 4.2.1. The user-level noncooperative subgame $\mathcal{G}_u$ admits a unique NE under Assumption 1.

Proof. (4.16) is defined as a bounded linear complementarity problem in [115]. It is a linear instance of the general mixed complementarity problems discussed in [117]. As discussed in [117], the linear instance of a complementarity problem admits a unique solution, i.e., the NE, to the user-level noncooperative subgame $\mathcal{G}_u$, if $(\mathbf{I} - \alpha \mathbf{G})$ is a P-matrix⁶.

⁶A matrix A is a P-matrix if all its principal minors are positive.

Since $\alpha\rho(\mathbf{G}) < 1$ under Assumption 1, all the eigenvalues of the matrix $\alpha\mathbf{G}$ belong to $(0, 1)$ and hence all the eigenvalues of the matrix $(\mathbf{I} - \alpha\mathbf{G})$ belong to $(0, 1)$. Therefore, $(\mathbf{I} - \alpha\mathbf{G})$ is a non-singular M-matrix⁷.

Based on Theorem 6.2.3 in [118] that “any non-singular M-matrix is a P-matrix”, $(\mathbf{I} - \alpha\mathbf{G})$ is a P-matrix and then there exists a unique NE in the user-level noncooperative subgame $\mathcal{G}_u$. Thereby, the proof is completed. $\square$

According to the system of interdependent demands (4.16), the set of users $\mathcal{N}$ can be partitioned into three subsets, i.e., $\mathcal{S}_0$, $\mathcal{S}_1$, and $\mathcal{S}$ as follows:

- $\mathcal{S}_0 = \{i \mid \{(1 + \bar{h})\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\mathbf{x}\}_i < 0, \forall i \in \mathcal{N}\}$ includes the users which will not buy the blockchain service,
- $\mathcal{S}_1 = \{i \mid \{(1 + \bar{h})\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\mathbf{x}\}_i > 0, \forall i \in \mathcal{N}\}$ includes the users which surely will buy the blockchain service,
- $\mathcal{S} = \mathcal{N} \setminus (\mathcal{S}_0 \cup \mathcal{S}_1) = \{i \mid \{(1 + \bar{h})\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\mathbf{x}\}_i = 0, \forall i \in \mathcal{N}\}$ includes the users which buy the blockchain service with a probability over $[0, 1]$.

Then, we obtain the following theorem:

Theorem 4.2.2. The users in the user-level noncooperative subgame $\mathcal{G}_u$ only belong to $\mathcal{S}$, i.e., $\mathcal{S} = \mathcal{N}$, $\mathcal{S}_0 = \emptyset$, and $\mathcal{S}_1 = \emptyset$. Given the service price vector $\mathbf{p}$, the optimal solution to the system of interdependent demands (4.16) is

$$\mathbf{x}^* = (\mathbf{I} - \alpha\mathbf{G})^{-1} [(1 + \bar{h})\mathbf{1} - \mathbf{p}]. \quad (4.17)$$

Proof. We denote the optimal price by $\mathbf{p}^*$ and the optimal demand by $\mathbf{x}^*$. Then, we show that $\mathcal{S}_0 = \emptyset$ and $\mathcal{S}_1 = \emptyset$.

- $\mathcal{S}_0 = \emptyset$: We first assume that $\mathcal{S}_0 \neq \emptyset$. This means that $\exists i \in \mathcal{N}$, such that $x_i^* = 0$ and $\{(1 + \bar{h})\mathbf{1} - \mathbf{p}^* - (\mathbf{I} - \alpha\mathbf{G})\mathbf{x}^*\}_i < 0$. Moreover, as $\{(1 + \bar{h})\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\mathbf{x}\}_i = 1 + \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{ij}x_j - x_i - p_i$ is continuous on p_i and $1 + \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{ij}x_j^* > 0$, there exists a p_i' where $p_i' < p_i^*$ such

⁷A matrix A is a non-singular M-matrix if $A = I - B$ for a positive matrix B with largest eigenvalue $\rho(B) < 1$.

that $1 + \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{ij} x_j^* - p_i' > 0$ and correspondingly $x_i' > 0$. This indicates that when the service price charged to user i decreases from p_i^* to p_i' , user i has an incentive to increase its demand from $x_i^* = 0$ to $x_i' > 0$. Consequently, the revenue of the blockchain provider will increase since $p_i^* x_i^* = 0$ while $p_i' x_i' > 0$. Therefore, x_i^* and p_i^* cannot be the optimal demand and price for user i , respectively. Hence, $i \notin \mathcal{S}_0, \forall i \in \mathcal{N}$ and $\mathcal{S}_0 = \emptyset$.

- $\mathcal{S}_1 = \emptyset$: Similarly, we assume that $\mathcal{S}_1 \neq \emptyset$. This means that $\exists l \in \mathcal{N}, x_l^* = 1$ and $\{(1 + \bar{h}) \mathbf{1} - \mathbf{p}^* - (\mathbf{I} - \alpha \mathbf{G}) \mathbf{x}^*\}_l > 0$. As $\{(1 + \bar{h}) \mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha \mathbf{G}) \mathbf{x}\}_l = 1 + \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{lj} x_j - x_l - p_l$ is continuous on p_l , there exists an ϵ where $\epsilon > 0$ such that $1 + \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{lj} x_j^* - (p_l^* + \epsilon) > 0$ and $x_l^* = 1$. Let $\epsilon = \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{lj} x_j^* - p_l^*$, we have $1 + \bar{h} + \alpha \sum_{j \in \mathcal{N}} g_{lj} x_j^* - (p_l^* + \epsilon) = 0$, and here $x_l^* = 1 - (p_l^* + \epsilon) + \bar{h} + \sum_{j \in \mathcal{N}} g_{lj} x_j^* = 1$. This means that even if the service price of user l increases from p_l^* to $(p_l^* + \epsilon)$, the demand of user l is still equal to 1 while the profit of the blockchain provider has been increased from $p_l^* x_l^* = p_l^*$ to $(p_l^* + \epsilon) x_l^* = p_l^* + \epsilon$. Moreover, since

$$\begin{aligned} & \{(1 + \bar{h}) \mathbf{1} - \mathbf{p}^* - (\mathbf{I} - \alpha \mathbf{G}) \mathbf{x}^*\}_l - \epsilon \\ &= 1 + \bar{h} - (p_l^* + \epsilon) - \underbrace{x_l^*}_1 + \alpha \sum_{j \in \mathcal{N}} g_{lj} x_j^* = 0, \end{aligned} \quad (4.18)$$

user l belongs to $\mathcal{S}$ instead of $\mathcal{S}_1$. Therefore, p_l^* and x_l^* are not the optimal price and demand for user l , respectively. Hence, $l \notin \mathcal{S}_1, \forall l \in \mathcal{N}$ and $\mathcal{S}_1 = \emptyset$.

To conclude, given any price vector $\mathbf{p}$ of the blockchain service, the condition

$$\{(1 + \bar{h}) \mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha \mathbf{G}) \mathbf{x}^*\}_i = 0 \quad (4.19)$$

will be satisfied for all user $i \in \mathcal{N}$. Therefore,

$$(1 + \bar{h}) \mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha \mathbf{G}) \mathbf{x}^* = \mathbf{0}, \quad (4.20)$$

$$(\mathbf{I} - \alpha \mathbf{G}) \mathbf{x}^* = (1 + \bar{h}) \mathbf{1} - \mathbf{p}. \quad (4.21)$$

Since we have already shown that the matrix $(\mathbf{I} - \alpha \mathbf{G})$ is a non-singular matrix in Theorem 4.2.1, the inverse of $(\mathbf{I} - \alpha \mathbf{G})$ exists. Multiply both sides of (4.21) by $(\mathbf{I} - \alpha \mathbf{G})^{-1}$, then, the optimal solution to the system of interdependent demands,

or equivalently, the NE to $\mathcal{G}_u$, is

$$\mathbf{x}^* = (\mathbf{I} - \alpha \mathbf{G})^{-1} [(1 + \bar{h}) \mathbf{1} - \mathbf{p}]. \quad (4.22)$$

The proof is completed. $\square$

4.2.2 Equilibrium Analysis for Leader-Level Noncooperative Subgame

After deriving the equilibrium demand of the users, we investigate the leader-level noncooperative subgame $\mathcal{G}_L$ for the blockchain provider and the cyber-insurer. At the NE, no player can increase its profit by choosing a different strategy provided that the other player's strategy is unchanged [119]. In what follows, we first prove that an NE exists in the leader-level noncooperative subgame $\mathcal{G}_L$. Then, we prove that this NE is unique.

Substituting the optimal demand of the users derived in (4.22) into the profit function of the blockchain provider, we can rewrite (4.8) into a matrix form as follows:

$$\begin{aligned} \Pi_p(\bar{h}, \mathbf{p}) = & \mathbf{p}^\top (\mathbf{I} - \alpha \mathbf{G})^{-1} [(1 + \bar{h}) \mathbf{1} - \mathbf{p}] - \frac{a\bar{h}}{1 - \bar{h}} + \bar{h} \frac{T}{T_0} N_{Tr} \\ & - \frac{T}{T_0} N_{Tq} \int_{1/2}^1 \left[1 - \int_{1/2}^t P(\theta) d\theta \right]^{1/\gamma} dt. \end{aligned} \quad (4.23)$$

The first-order partial derivative of the profit of blockchain provider as well as that of the cyber-insurer are shown in (4.24), and the second-order partial derivatives of the blockchain provider and cyber-insurer are shown in (4.25). Then, we can obtain the following theorem regarding the NE of the leader-level noncooperative subgame.

Theorem 4.2.3. The NE in the leader-level noncooperative subgame $\mathcal{G}_L$ exists if and only if $a > \frac{1}{8} \mathbf{1}^\top (\mathbf{I} - \alpha \mathbf{G})^{-1} \mathbf{1}$. Then, the Stackbelberg equilibrium of the market game exists.

Proof. Please refer to Appendix B.1. $\square$

$$\left\{ \begin{array}{l} \frac{\partial \Pi_P}{\partial \bar{h}} = \mathbf{p}^\top (\mathbf{I} - \alpha \mathbf{G})^{-1} \mathbf{1} - \frac{a}{(1 - \bar{h})^2} + \frac{1}{\gamma} \frac{T}{T_0} N_T r, \\ \frac{\partial \Pi_P}{\partial \mathbf{p}} = (\mathbf{I} - \alpha \mathbf{G})^{-1} [(1 + \bar{h}) \mathbf{1} - \mathbf{p}], \\ \frac{\partial \Pi_I}{\partial \gamma} = -\frac{1}{\gamma^2} \frac{T}{T_0} N_T q \int_{1/2}^1 \left[1 - \int_{1/2}^t P(\theta) d\theta \right]^{1/\gamma} \ln \left[1 - \int_{1/2}^t P(\theta) d\theta \right] dt \\ \quad - \left(\bar{h} - \frac{1}{2} \right)^3 [(\beta + 1) \gamma^\beta - \beta \gamma^{\beta-1}], \end{array} \right. \quad (4.24)$$

$$\left\{ \begin{array}{l} \frac{\partial^2 \Pi_P}{\partial \mathbf{p}^2} = -(\mathbf{I} - \alpha \mathbf{G})^{-1}, \quad \frac{\partial^2 \Pi_P}{\partial \mathbf{p} \partial \bar{h}} = (\mathbf{I} - \alpha \mathbf{G})^{-1} \mathbf{1}, \\ \frac{\partial^2 \Pi_P}{\partial \mathbf{p} \partial \gamma} = \left(\frac{\partial^2 \Pi_I}{\partial \gamma \partial \mathbf{p}} \right)^\top = \mathbf{0}, \quad \frac{\partial^2 \Pi_P}{\partial \bar{h} \partial \mathbf{p}} = \mathbf{1}^\top (\mathbf{I} - \alpha \mathbf{G})^{-1}, \\ \frac{\partial^2 \Pi_P}{\partial \bar{h}^2} = -\frac{2a}{(1 - \bar{h})^3}, \quad \frac{\partial^2 \Pi_P}{\partial \bar{h} \partial \gamma} = 0, \\ \frac{\partial^2 \Pi_I}{\partial \gamma \partial \bar{h}} = -3 \left(\bar{h} - \frac{1}{2} \right)^2 [(\beta + 1) \gamma^\beta - \beta \gamma^{\beta-1}], \\ \frac{\partial^2 \Pi_I}{\partial \gamma^2} = \frac{2}{\gamma^3} \frac{T}{T_0} N_T q \int_{1/2}^1 \left[1 - \int_{1/2}^t P(\theta) d\theta \right]^{1/\gamma} \ln \left[1 - \int_{1/2}^t P(\theta) d\theta \right] dt \\ \quad + \frac{1}{\gamma^4} \frac{T}{T_0} N_T q \int_{1/2}^1 \left[1 - \int_{1/2}^t P(\theta) d\theta \right]^{1/\gamma} \ln^2 \left[1 - \int_{1/2}^t P(\theta) d\theta \right] dt \\ \quad - \left(\bar{h} - \frac{1}{2} \right)^3 [\beta (\beta + 1) \gamma^{\beta-1} - \beta (\beta - 1) \gamma^{\beta-2}]. \end{array} \right. \quad (4.25)$$

Next, we show the uniqueness of the NE in the leader-level noncooperative subgame in Theorem 4.2.4, and hence the Stackbelberg equilibrium is unique.

Theorem 4.2.4. The NE in $\mathcal{G}_L$ is unique if and only if $a > \frac{9(\beta+1)^2(\gamma^u)^{\beta+1}}{128\beta}$ and hence the Stackbelberg equilibrium is unique.

Proof. Please refer to Appendix B.2. □

4.2.3 Equilibrium Searching for Leader-Level Noncooperative Subgame

Since in our previous discussion we have provided the closed-form NE to the user-level noncooperative subgame $\mathcal{G}_u$ in (4.22), we only have to focus on the derivation

Algorithm 1: Iterative best-response for searching leader noncooperative subgame NE

Require: Select any feasible initial strategies as $\mathbf{s}_I(0) = \gamma(0)$,

$\mathbf{s}_P(0) = [\mathbf{p}(0), \bar{h}(0)]^\top$ and set $t = 0$.

1: **while** $\mathbf{p}(0), \bar{h}(0), \gamma(0)$ do not satisfy the termination condition **do**

2: **for all** $k = \{P, I\}$ **do**

3: Set the adversary joint strategies as

$$\mathbf{s}_k(t+1) = \arg \max_{\mathbf{s}_k} \Pi_k(\mathbf{s}_k, \mathbf{s}_{-k}(t)) \text{ s.t. } \mathbf{s}_k \in \mathcal{D}_k, \quad (4.26)$$

where $\mathbf{s}_{-k}$ represents the adversary's strategy.

4: **end for**

5: Set $t \leftarrow t + 1$.

6: **end while**

of the NE in the leader-level noncooperative subgame $\mathcal{G}_L$. Given (4.22), the search for the SE is reduced to the search of the NE of a two-player noncooperative game. By Theorem 4.2.3, we know that $\mathcal{G}_L$ is a concave game with the convex and compact strategy space (see also the proof to Theorem 4.2.3). By Theorem 4.2.4, we know that $\mathcal{G}_L$ admits a unique NE when the condition given therein is satisfied. This suggests the use of the iterative best response to solve for the NE in $\mathcal{G}_L$. The iterative best-response algorithm is described in Algorithm 1, and its convergence property is guaranteed by Theorem 4.2.5.

Theorem 4.2.5. If the condition in Theorem 4.2.4 is satisfied, Algorithm 1 converges to the unique SE from anywhere of the strategy domains of the blockchain provider and cyber-insurer.

Proof. With the concavity of the payoff functions Π_P and Π_I proved in Theorem 4.2.3 and the negative definite Jacobian matrix $\mathbf{J}$ proved in Theorem 4.2.4, Theorem 4.2.5 immediately follows Theorem 10 in [120]. $\square$

4.3 Performance Evaluation

In this section, we present the numerical results to study the equilibrium strategies of the market entities on each stage. The number of the users in the blockchain service market is $|\mathcal{N}|$. The off-diagonal elements of social externality matrix $\mathbf{G}$, i.e., g_{ij} , $\forall i \neq j$, is generated following the uniform distribution over the interval of

$[0, 10]$. The domain of definition for α is set as $[5 \times 10^{-4}, 8 \times 10^{-4}]$ according to the parameter setting in [115]. Without loss of generality, we consider the social externality under three levels, i.e., weak ($\alpha = 6.5 \times 10^{-4}$), medium ($\alpha = 7 \times 10^{-4}$), and strong ($\alpha = 7.5 \times 10^{-4}$). The other default coefficients are given as follows: $\beta = 10$, $p^u = 1$, $\gamma^u = 2$, $T = 100$, $T_0 = 10$, $N_T = 100$, $r = 10$, $q = 10$ and $a = 100$. Note that the price that we present in the figures of simulation results is the mean value of the discriminatory prices. The triple integral in the premium-related term in the profit functions of the blockchain provider and the cyber-insurer, i.e., (4.8) and (4.9), is calculated using the method of rectangular integral with 100 as the number of intervals. Note that our proposed concept of cyber-insurer and blockchain service is the first in the literature. There is no similar work with which we can compare on a reasonably fair basis. For example, the authors in [61] formulated a bilevel game to investigate the interactions among the attackers, users, and cyber-insurer in computer networks. However, since we incorporate the specific and unique feature of the blockchain technology, i.e., successful attack probability in (4.1), reasonable comparison is therefore not applicable.

4.3.1 Numerical Results

4.3.1.1 Demonstration of best response and NE

Figure 4.2 demonstrates the NE obtained from iterative best responses with the given simulation parameters. In Fig. 4.2(a), the profit of the cyber-insurer changes with the different premium charged to the blockchain provider. According to our previous discussion, the profit of the cyber-insurer is controlled by the value of γ . For a given weak level of the social externality, e.g., $\alpha = 6.5 \times 10^{-4}$, there is a corresponding strategy where the cyber-insurer's profit is maximized. The strategy is marked by the arrowhead of "Best response" and constitutes the NE strategy of the cyber-insurer under the given social externality setting. We observe from Fig. 4.2(a) that as a function of the premium coefficient γ , the profit is unimodal, and thus the optimal solution can be obtained analytically. Similarly, there exists the optimal point in each of Figs. 4.2(b), (c), and (d) for the blockchain provider. The optimal points are marked by the arrowhead of "Best response" and constitute the NE strategy of the blockchain provider under different levels of social

FIGURE 4.2: Best response

externality. Note that all the results shown in the figures are obtained given that the users play the NE in the user-level game.

Figure 4.3 illustrates the equilibrium strategies for the investment of the blockchain provider and the premium coefficient γ for the cyber-insurer under different levels of social externality. The NE is the point at which the best responses for the blockchain provider and cyber-insurer intersect. Again, this is given that the users play the NE in the user-level game. Under different levels of social externality, different NE are observed. As the level of social externality grows higher, i.e., a decision of one user has stronger effect to the decisions of other users, the other users are more likely to buy the same service if one user buys the service. As expected, when the level of social externality grows higher, the users are more likely to also buy the service, the blockchain provider has more money and more incentives to invest in the infrastructure and accordingly the premium coefficient

FIGURE 4.3: Nash equilibrium

γ decreases (see Fig. 4.3). The reason for this result is explained in the subsequent discussions.

4.3.1.2 The impact of the number of users

We first evaluate the impacts by the number of users on the payoff of the market entities in Fig. 4.4, where the number of users increases from 50 to 120. Then, we evaluate the performance under three levels of social externality, e.g., 6.5×10^{-4} , 7×10^{-4} , and 7.5×10^{-4} which represent weak, medium, and strong levels of social externality, respectively. As expected, the profit of the blockchain provider increases significantly when the social externality becomes stronger. As the number of users increases, the profit of the blockchain provider also increases under the given social externality settings. Moreover, the increase of the profit of the blockchain provider becomes larger when the social externality is stronger. Intuitively, the reason is that the social externality stimulates the demand of each user. In return, the blockchain provider can raise the price of service accordingly and hence improves its profit. Meanwhile, as the social externality becomes stronger, the blockchain provider also achieves greater profit. This indicates that the attack

FIGURE 4.4: The results with increasing number of users.

may incur more loss to the blockchain provider. Therefore, the blockchain provider has a higher incentive to invest in the infrastructure to prevent double-spending attack. This explains the result that the investment by the blockchain provider increases at a higher rate with $\alpha = 7.5 \times 10^{-4}$ than with $\alpha = 6.5 \times 10^{-4}$. As a result, the stronger social externality reduces the successful attack probability at a higher rate. Correspondingly, as shown in Fig. 4.4(f), the premium coefficient γ decreases at a higher rate with the stronger social externality. This result indicates that the premium also decreases at a higher rate with stronger social externality. Thus, the cyber-insurer's profit decreases at a higher rate when the social externality becomes stronger as shown in Fig. 4.4(b).

4.3.1.3 The impact of social externality

Figure 4.5 illustrates the impact of social externality on the payoffs of the three market entities with 100 users. As expected, the users' total service demand increases as the social externality becomes stronger (see Fig. 4.5(d)). From Figs. 4.5(a)

FIGURE 4.5: The results with increasing social externality.

and (b), we observe that the profit of the blockchain provider increases while the profit of the cyber-insurer decreases. The reason is that the users with stronger social externality are more sensitive to the risk level of the blockchain service, which strongly depends on the investment ratio of the blockchain provider. Therefore, the blockchain provider will raise its investment as the social externality increases, which decreases the probability of successful double-spending attacks. Accordingly, the cyber-insurer reduces its premium as shown in Fig. 4.5(f), and this will lead to the decrease of the cyber-insurer's profit. Moreover, since the investment by the blockchain provider increases, the security level of the blockchain service is improved, and thus the service demand of users increases. This situation results in the increase of the blockchain provider's profit.

Additionally, recall that the investment ratio of the blockchain provider depends on not only the investment from the blockchain provider, but also the computing resource owned by the attackers. For this reason, in our performance evaluation, we also vary the attacker's investment in computing resource by considering three cases with $a = 50$, $a = 100$ and $a = 150$, respectively. From Fig. 4.5(f), we observe that the decreasing rate of the curves becomes higher as the attacker's investment increases, which means that decreasing rate of the premium becomes higher as the attacker's investment increases. The reason is that the increasing rate of the investment by the blockchain provider becomes faster as the attacker's investment

FIGURE 4.6: The result with increasing attacker's computing resource: (a) profit of the blockchain provider, i.e., (4.8), (b) profit of the cyber insurer, i.e., (4.9), (c) average price of the blockchain service, i.e., decision variable $\mathbf{p}$ in (4.8), (d) total demand of the users, i.e., (4.17), (e) the investment of the blockchain provider, i.e., decision variable $\bar{h}$ in (4.8), and (f) the premium coefficient, i.e., decision variable γ in (4.9).

increases, and this also results in a higher decreasing rate of the successful attack probability. Consequently, the decreasing rate of the probability of paying claim is the highest with $a = 150$ which is the largest attacker's investment.

4.3.1.4 The impact of attacker's computing resource

Finally, we evaluate in Fig. 4.6 the impact of the attackers' computing resource on the performance of the users, the blockchain provider and the cyber-insurer. We consider three different situations with different sizes of a block, i.e., the number of transactions included in that block, with $N_T = 100$, $N_T = 200$ and $N_T = 300$. We observe from Figs. 4.6(a) and (b) that as the attacker's computing resource increases, the profit of the blockchain provider decreases and the profit of the cyber-insurer remains unchanged. The reason is that the blockchain provider needs to increase its infrastructure investment when the attacker's computing resource increases (see Fig. 4.6(e)). Otherwise, the successful attack probability will significantly increase, and it results in the increase in the cost of the blockchain provider. With an increasing computing resource controlled by the attackers, the investment

ratio of the blockchain provider cannot remain as high as before. This result is illustrated in Fig. 4.6(e) with $\frac{h^*}{a+h^*}|_{a=50} \approx \frac{18}{19} > \frac{h^*}{a+h^*}|_{a=100} \approx \frac{12}{13}$ when $N_T = 300$. Therefore, as the attackers' computing resource increases, the successful attack probability and consequently the probability of the cyber-insurer paying the claim increases accordingly. Then, as shown in Fig. 4.6(f), the cyber-insurer increases the premium to keep its profit unchanged. Ultimately, the cost of the blockchain provider also increases. Moreover, as the attackers' computing resource increases, even when the blockchain provider reduces the price of its service to attract more users, the total demand from the users still decreases (see Figs. 4.6(c) and (d)). Consequently, this reduces the revenue and profit of the blockchain provider.

Furthermore, we show that the impact of the attackers' computing resource on the other parties in the market is subject to the number of transactions in one block N_T . With the fixed transaction fee and compensation rate, the more transactions in a single block is, the more reward that the blockchain provider obtains from mining a block. Moreover, since the compensation price of one block increases as the number of transactions in one block increases, the more compensation it will pay to the users once the attacks happen. Then, the blockchain provider has more incentive to invest in the computing resource. This is consistent with Fig. 4.6(e), where the increasing rate of the investment by the blockchain provider is higher with $N_T = 300$ than that with $N_T = 100$. On the other hand, as the attacker's computing resource increases, the increasing rate of the successful attack probability is lower with $N_T = 300$ than that with $N_T = 100$. Consequently, the increasing rate of the premium is lower with $N_T = 300$ than that with $N_T = 100$ (see Fig. 4.6(f)). Moreover, as N_T increases, the increasing rate of the successful attack probability will decrease, and the users' demand will be less affected. This is consistent with Figs. 4.6(c) and (d), where the decreasing rates of both the total user demand and the service price shrink as N_T increases.

4.4 Summary

In this chapter, we have proposed a risk management framework of the blockchain service market by introducing the cyber-insurance as a mean for protecting financially the blockchain provider from double-spending attacks. We have modeled the interaction among the blockchain provider, the cyber-insurer and the users

in the market as a two-stage Stackelberg game. For the blockchain provider, we have considered the problem of balancing between the proactive protection strategy, i.e., investing in computing power, and the reactive protection strategy, i.e., purchasing the cyber-insurance. For the users, we have considered the impact of both the social externality and the service security on the users' valuation of the blockchain service. In particular, for the cyber-insurer, we have incorporated the risk-adjusted pricing mechanism for premium adaptation. We have studied the equilibrium strategies of the three parties in the market using backward induction. We have analytically examined the conditions for the Stackelberg game to exist and to be unique. Furthermore, we have conducted extensive simulations to evaluate the performance of the market entities at the equilibrium. The numerical results reveals some interesting results. For example, the profit of the cyber insurer remains unchanged when the attacker is becoming powerful. For the future work, we will investigate the long-run competition between the blockchain provider and cyber-insurer.

Chapter 5

Joint Pricing and Security Investment in Cloud Security Service Market

In this chapter, a joint cyber-insurance and security investment has been proposed to eliminate the cyber risks faced by the users in the cloud platform¹.

5.1 System Description

We investigate the joint pricing and security investment problem in the competitive cloud security service market as shown in Fig. 1.4. In the market under our consideration, there are CSSVs competing to sell their substitutable cloud security plans. The plan is composed of cloud security service and cloud-insurance. The cloud security service is used to protect the basic cloud service enjoyed by users, and the cloud-insurance provides the users with the claim payment if the cloud security service cannot prevent an attack from happening. The CSSVs are able to set prices and invest to improve their offered cloud security service. The users

¹The work in this chapter has been published as S. Feng, Z. Xiong, D. Niyato, P. Wang, S. S. Wang, and X. S. Shen, “Joint Pricing and Security Investment in Cloud Security Service Market with User Interdependency,” *IEEE Transactions on Services Computing* (2020). DOI: 10.1109/TSC.2020.2996382. Part of the work in this chapter has been published as S. Feng, Z. Xiong, D. Niyato, P. Wang, and S. S. Wang, “Joint pricing and security investment for cloud-insurance: A security interdependency perspective,” in 2018 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6).

make their decisions to purchase a cloud security plan by considering the prices, the perceived cyber breach probability of the offered security service as well as the interaction with other users.

5.1.1 Preliminaries

Motivated by [84], we quantify the effectiveness of information security spending in addressing the vulnerability of an organization's information and communication system with a family of security breach probability functions. In particular, let $v(z)$ denote the cyber breach probability of the cloud security service when the corresponding investment is z . Accordingly, $q = 1 - v(z)$ is the probability of that the cloud security service is not breached corresponding to the security investment of z , which is named as "security level". [84] introduced a family of security breach probability functions, i.e., $v(\cdot)$, with tractably mathematical expression including

- The Exponential Power Class of cyber breach probability function, i.e.,

$$v_{\text{EP}}(z) = v(1)^{z^\alpha}; \quad (5.1)$$

- The Proportional Hazard Class of cyber breach probability function, i.e.,

$$v_{\text{PH}}(z) = 1 - [1 - v(1)]^{z^{-\alpha}}; \quad (5.2)$$

- The Wang Transform Class of cyber breach probability function, i.e.,

$$v_{\text{WT}}(z) = \Phi[\Phi^{-1}(v(1)) - \alpha \ln(z)]; \quad (5.3)$$

where Φ is the cumulative distribution function for the standard normal distribution, $v(1)$ is the cyber breach probability when investment is 1, i.e., $z = 1$, and $\alpha > 0$. Therein, α quantifies the effect of the historical information of the cloud security service on the security level, and $v(1)$ captures the effect of the efficiency of the investment on the improvement of the cyber breach probability. For example, if the security solution is highly effective and well developed as shown in the historical data, the value of α should be large while that of $v(1)$ should be small. Note that although the cyber breach probability depends on many factors such as type of

FIGURE 5.1: (a) The relationship between the cyber breach probability $v(z)$ and the investment z and (b) the relationship between the security level $q = 1 - v(z)$ and the investment z .

attack, the number of attackers, the techniques used in the attack and prevention, for tractability reason, we consider only these two parameters, i.e., α and $v(1)$. The more sophisticated function with more degrees of freedom will be considered in the future work. Note also that the above family of security breach probability functions is applicable to the analytical results presented in Section 5.2.2 due to their monotonic decreasing and convex properties.

To illustrate the quantitative effect of the investment on the improvement of the cyber breach probability and hence interpret the physical meaning of (5.1), (5.2), and (5.3), Fig. 5.1 plots the cyber breach probability and the security level against the investment for $v(1) = 0.5$ and $\alpha = 0.5$. As shown in Fig. 5.1(a), all the curves are monotonic decreasing and convex. This means that the cyber breach probability decreases as the investment increases, which results in higher security level and hence more reliable cloud security service. Moreover, the decreasing rate of the cyber breach probability becomes smaller when it is close to its minimum value, i.e., 0. This implies the fact that achieving a perfect cloud security solution is impossible. We observe that there are some differences among these three curves with respect to the convexity. These differences on convexity can be used to investigate the differences among the specific techniques adopted in the cloud security services provided by the CSSVs. For example, IBM Trusteer uses its patented analytics and machine learning for real-time risk level evaluation [121] while Oracle uses

LORIC's machine learning [32]. Consider the investment to be on computation resource for training machine learning algorithms. The more investment allows CSSV to adopt more sophisticated models, e.g., more number of hidden nodes in deep learning, which leads to higher security level, e.g., higher accuracy of intrusion detection. Many studies such as [122] experimented and showed such relationship which is consistent with our proposed functions. It is worth noting that the model parameters $v(1)$ and α can be estimated and set according to the real experimental results, e.g., from [122].

Additionally, due to the bijection in the family of security breach probability functions, i.e., (5.1), (5.2), and (5.3), shown in Fig. 5.1, the investment can be defined as a function of the cyber breach probability and further the security level as follows:

$$v(z) = 1 - q \Leftrightarrow z(q) = v^{-1}(1 - q). \quad (5.4)$$

Accordingly, the investment determination problem of the CSSVs is transformed into a security level determination problem of the CSSVs.

5.1.2 System Model

For ease of presentation, we study a cloud security service market, where two CSSVs, i.e., CSSV-A and CSSV-B, are competing to sell their cloud security plans to users as shown in Fig. 1.4. The set of the users is denoted by $\mathcal{N}$. Each user $i \in \mathcal{N}$ will buy one cloud security plan. Let $x_i \in [0, 1]$ denote user i 's demand of the cloud security plan to CSSV-A. Correspondingly, user i 's demand of cloud security plan to the CSSV-B is $1 - x_i$. The strategies of the user i are therefore x_i and $1 - x_i$. Note that the demand fraction x_i can indicate the probability that user i buys from the CSSV-A. Note also that we consider a unit demand that the user "will definitely purchase" the cloud security plan. Hence, the scenario that the user decides not to buy is not under our consideration.

The security levels of cloud security service provided by the CSSV-A and CSSV-B are denoted by q^A and q^B , respectively. The security levels have an impact on the users' purchasing demand. For example, the better security level can attract more demand. Furthermore, the security levels q^A and q^B depend on the investments by the CSSVs, which are denoted by z^A and z^B , respectively.

TABLE 5.1: Notations

Symbol	Description
i, j	Users i, j .
A, B	Cloud security service vendors (CSSVs).
$\mathcal{N}$	A set of users.
$x_i, 1 - x_i$	Demands from user i to the CSSV-A and CSSV-B, respectively.
$\mathbf{x}_{-i}$	Demands to the CSSV-A without user i .
$\mathbf{G}, g_{ij}$	Security interdependency matrix and its elements, respectively.
a_i, b_i	Parameters of concave utility functions [123].
d^A, d^B	Coefficient of congestion of the CSSV-A and CSSV-B, respectively.
p_i^A, p_i^B	Prices of the cloud security plan for user i from the CSSV-A and CSSV-B, respectively.
q^A, q^B	Security levels of the cloud security service from the CSSV-A and CSSV-B, respectively.
z^A, z^B	Investments of the CSSV-A and CSSV-B, respectively.
$v(\cdot)$	Probability of being breached for the cloud service.
α	$\alpha > 0$ is the parameter for the family of security breach probability functions.

The marginal cost for each the CSSV is decomposed into two parts, i.e., the investment for improving the security level of the cloud security service and the claim paid to the users if the cloud security service cannot prevent the attack from happening. Note that the investments are part of the CSSVs' running costs while they are independent of the users' demands. However, the costs incurred by the claims paid to the users are dependent on the users' demand. In this case, the marginal cost of providing cloud security plan by the CSSV-A is decomposed into two part as follows [84]:

$$z^A(q^A) \text{ and } (1 - q^A) n\lambda, \quad (5.5)$$

where n and λ represent the number of threats and the monetary value of the insured asset, respectively. Here, the terms $z^A(q^A)$ and $(1 - q^A) n\lambda$ account for the costs incurred by the investment and the claim paid to the users if the cloud security service provided by the CSSV-A cannot prevent the attack from happening, respectively. The cost for providing service is fixed and hence is not accounted. The marginal cost for the CSSV-B can be decomposed and expressed similarly, i.e., $z^B(q^B)$ and $(1 - q^B) n\lambda$.

We denote the strategies of the users on the CSSV-A by $\mathbf{x} \triangleq [x_1, \dots, x_{|\mathcal{N}|}]^\top$, where x_i for all $i \in \mathcal{N}$ is the demand of user i . Moreover, we define $\mathbf{x}_{-i} \triangleq$

$[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{|\mathcal{N}|}]^\top$. Then, by applying the strategy of x_i , user i can achieve the utility of [42]:

$$\begin{aligned} u_i(x_i, \mathbf{x}_{-i}, p_i^A, p_i^B, q^A, q^B) = & q^A a_i x_i - b_i x_i^2 + q^B a_i (1 - x_i) - b_i (1 - x_i)^2 \\ & + \sum_{j \in \mathcal{N}} g_{ij} x_i x_j + \sum_{j \in \mathcal{N}} g_{ij} (1 - x_i) (1 - x_j) - p_i^A x_i \\ & - p_i^B (1 - x_i) - \frac{d^A}{2} \left(\sum_{j \in \mathcal{N}} x_j \right)^2 - \frac{d^B}{2} \left(\sum_{j \in \mathcal{N}} (1 - x_j) \right)^2. \end{aligned} \quad (5.6)$$

In (5.6), we use the linear-quadratic functional from, i.e., $a_i x_i - b_i x_i^2$ and $a_i (1 - x_i) - b_i (1 - x_i)^2$, to capture the marginal decreasing gains of the user's utility. The reason is that the quadratic property not only allows for a tractable analysis and a good second order approximation of concave payoffs but also hints at the essence of the risk-averse users. Specifically, the coefficient $a_i \geq 0$ is the maximum intrinsic demand rate capturing a linear own-effort effect from the investment on the cloud security plan and hence is strongly dependent on the security level of products. The coefficient $b_i \geq 0$ is the intrinsic demand elasticity factor reflecting the convex cost in own-effort [44]. Moreover, if user i is highly risk-averse, the value of a_i should be large while that of b_i should be small. Regarding the terms $\sum_{j \in \mathcal{N}} g_{ij} x_i x_j$ and $\sum_{j \in \mathcal{N}} g_{ij} (1 - x_i) (1 - x_j)$, they measure the security interdependency among the users. Here, $g_{ij} \geq 0, \forall i, j \in \mathcal{N}$, i.e., the element of the interdependency matrix $\mathbf{G}$ on i -th row and j -th column, quantifies the security interdependency (influence) on user i from user j . The element of $\mathbf{G}$ on i -th row and i -th column, i.e., $g_{ii}, \forall i \in \mathcal{N}$, is assumed to be 0. The security interdependency among users comes from the users' security spending on the cloud security plan. Like the network externality in cloud services market [124], the users can exchange information on other channels, e.g., social networks, of what they buy for the security service plan and construct the interdependency with each other. To purchase x_i unit of cloud security plan from the CSSV-A, user i needs to pay $p_i^A x_i$ to the CSSV-A. Similarly, $p_i^B (1 - x_i)$ is the payment that the CSSV-B receives from user i . The terms $\frac{d^A}{2} \left(\sum_{j \in \mathcal{N}} x_j \right)^2$ and $\frac{d^B}{2} \left(\sum_{j \in \mathcal{N}} (1 - x_j) \right)^2$ describe the congestion of the cloud security service [125]. Again, we take Oracle CASB Cloud Service [32] as a representative example. Since Oracle CASB Cloud Service dynamically evaluate the user's risks in real-time due to LORIC's machine learning capabilities, the service delay appears when there exists

a large number of users. In this case, a quadratic function form, i.e., $\frac{d^A}{2} \left(\sum_{j \in \mathcal{N}} x_j \right)^2$ and $\frac{d^B}{2} \left(\sum_{j \in \mathcal{N}} (1 - x_j) \right)^2$, is adopted to capture that each user's utility will decrease dramatically as the number of the users that select the same plan increases.

The CSSV-A and CSSV-B aim at maximizing their own profits. The profits of the CSSV-A and CSSV-B are

$$\Pi^A = \sum_{i \in N} [p_i^A - (1 - q^A) n\lambda] x_i - z^A(q^A) \quad (5.7)$$

and

$$\Pi^B = \sum_{i \in N} [p_i^B - (1 - q^B) n\lambda] (1 - x_i) - z^B(q^B), \quad (5.8)$$

respectively. Note that the investments, $z^A(q^A)$ and $z^B(q^B)$, are used to improve the security level of cloud security service. Again, the investments are part of the CSSVs' operating costs while they are independent of the users' demands. However, the costs $(1 - q^A) n\lambda$ and $(1 - q^B) n\lambda$ are due to the claims paid to the users and hence are dependent on the users' demand. Therefore, recall from (5.5), the cost of each CSSV is divided into two parts based on the fact whether they are dependent on the users' demand or not, e.g., $z^A(q^A)$ and $(1 - q^A) n\lambda$ for the CSSV-A. By pricing the cloud security plan, the CSSV-A receives the revenue of $p_i^A x_i$ from user i while needs to pay the claim of $(1 - q^A) n\lambda x_i$ to user i when the cloud security service of the CSSV-A is breached. Therefore, the profit excluding the cost incurred by the security investment of CSSV-A is $\sum_{i \in N} [p_i^A - (1 - q^A) n\lambda] x_i$. After including the cost incurred by the investment, the total profit of CSSV-A is shown in (5.7). The total profit of CSSV-B as shown in (5.8) can be derived similarly.

5.1.3 Stackelberg Game Formulation

The CSSVs are the sellers making offers of their services to the market, and the users are the customers. The sellers typically make their decisions before the buyers. Based on the utility and profit functions given in (5.6), (5.7), and (5.8), it is intuitive to model the cloud security market as a two-stage Stackelberg game. Also, this Stackelberg setting is commonly adopted in a similar market situation [42].

Specifically, we consider the users to be the followers and they decide on the demand of the cloud security plan based on the price and the security levels. The interaction among the users is studied by formulating a noncooperative follower subgame. We model the interplay, i.e., competition, between the CSSV-A and CSSV-B as a noncooperative leader subgame on the upper stage. The CSSVs lead to make decision on their strategies, i.e., the prices of cloud security plans for every user and their investments for improving the security level of the cloud security service. The two-stage Stackelberg game is defined as follows:

- Given the strategies of the CSSVs, the noncooperative follower subgame for the users can be defined as a user-level noncooperative game $\mathcal{G}_u = \{\mathcal{N}, \mathbf{x}, \mathcal{X}, \mathbf{u}\}$. Therein, $\mathcal{N}$ denote the set of the users, and $\mathbf{x} = [x_1, \dots, x_{|\mathcal{N}|}]^\top$ is the demands of all the user i to the CSSV-A. $\mathcal{X} \subset \mathbb{R}^{|\mathcal{N}|}$ denotes the domain of definition for $\mathbf{x}$. $\mathbf{u} = [u_1, \dots, u_{|\mathcal{N}|}]^\top$ is the utility vector of the users defined in (5.6);
- Given the strategies of the users, i.e., $\mathbf{x}$, the noncooperative leader subgame for the CSSV-A and CSSV-B can be defined as a CSSV-level noncooperative game $\mathcal{G}_C = \left\{ \left[\mathbf{p}^A, q^A \right]^\top, \mathcal{D}^A, \left[\mathbf{p}^B, q^B \right]^\top, \mathcal{D}^B, \mathbf{\Pi} \right\}$. Here, $\left[\mathbf{p}^A, q^A \right]^\top = \left[p_1^A, \dots, p_{|\mathcal{N}|}^A, q^A \right]^\top$ is the vector of the prices and security level for the CSSV-A, and $\mathcal{D}^A = \left\{ \left[\mathbf{p}^A, q^A \right]^\top \mid p_i^A \in [0, p^u], \forall i \in \mathcal{N}, q^A \in [0, 1] \right\}$ is the domain of definition for the prices and security level of the CSSV-A. $\left[\mathbf{p}^B, q^B \right]^\top$ and $\mathcal{D}^B$ are defined in a similar way. $\mathbf{\Pi} = [\Pi^A, \Pi^B]^\top$ is the profit vector for the CSSVs.

In the next section, we analyze the equilibrium of the above game.

5.2 Stackelberg Equilibrium Analysis

Following the backward induction, we first obtain the Nash Equilibrium (NE) of the user-level game $\mathcal{G}_u$ by using the first order optimality condition. The concavity of the utility functions indicates the existence of the NE in the user-level game $\mathcal{G}_u$. This NE is proven to be unique by showing that the Jacobian matrix of the utility

$$\begin{aligned}
\frac{\partial u_i}{\partial x_i} &= q^A a_i - 2b_i x_i - q^B a_i + 2b_i (1 - x_i) + \sum_{j \in N} g_{ij} x_j + g_{ii} x_i - \sum_{j \in N} g_{ij} (1 - x_j) \\
&\quad - g_{ii} (1 - x_i) - d^A \sum_j x_j + d^B \sum_j (1 - x_j) - p_i^A + p_i^B \\
&= (q^A - q^B) a_i - 4b_i x_i + 2b_i + 2 \sum_{j \in N} g_{ij} x_j - \sum_{j \in N} g_{ij} - (d^A + d^B) \sum_j x_j \\
&\quad + |\mathcal{N}| d^B - p_i^A + p_i^B, \quad \forall i \in \mathcal{N}
\end{aligned} \tag{5.9}$$

$$\begin{aligned}
\frac{\partial \mathbf{u}}{\partial \mathbf{x}} &= (q^A - q^B) \mathbf{a} - 2\mathbf{B}\mathbf{x} + \mathbf{B}\mathbf{1} + 2\mathbf{G}\mathbf{x} - \mathbf{G}\mathbf{1} \\
&\quad - (d^A + d^B) \mathbf{I}\mathbf{x} + |\mathcal{N}| d^B \mathbf{1} - \mathbf{p}^A + \mathbf{p}^B.
\end{aligned} \tag{5.10}$$

$$\begin{aligned}
&(q^A - q^B) \mathbf{a} - 2\mathbf{B}\mathbf{x}^* + \mathbf{B}\mathbf{1} + 2\mathbf{G}\mathbf{x}^* - \mathbf{G}\mathbf{1} \\
&\quad - (d^A + d^B) \mathbf{I}\mathbf{x}^* + |\mathcal{N}| d^B \mathbf{1} - \mathbf{p}^A + \mathbf{p}^B = \mathbf{0} \\
&\Leftrightarrow (q^A - q^B) \mathbf{a} + (\mathbf{B} - \mathbf{G}) \mathbf{1} + |\mathcal{N}| d^B \mathbf{1} - \mathbf{p}^A + \mathbf{p}^B \\
&\quad = [2\mathbf{B} - 2\mathbf{G} + (d^A + d^B) \mathbf{I}] \mathbf{x}^*
\end{aligned} \tag{5.11}$$

$$\begin{aligned}
\mathbf{x}^* &= [2\mathbf{B} - 2\mathbf{G} + (d^A + d^B) \mathbf{I}]^{-1} \\
&\quad \times [(q^A - q^B) \mathbf{a} + (\mathbf{B} - \mathbf{G}) \mathbf{1} + |\mathcal{N}| d^B \mathbf{1} - \mathbf{p}^A + \mathbf{p}^B]
\end{aligned} \tag{5.12}$$

$$\begin{aligned}
&\{[2\mathbf{B} - 2\mathbf{G} + (d^A + d^B) \mathbf{I}]\}_{ii} = 4b_i + (d^A + d^B) \\
&> \sum_{j \neq i} [2g_{ij} - (d^A + d^B)] = \sum_{j \neq i} |2g_{ij} - (d^A + d^B)| \\
&= \sum_{j \neq i} \left| \{[2\mathbf{B} - 2\mathbf{G} + (d^A + d^B) \mathbf{I}]\}_{ij} \right|
\end{aligned} \tag{5.13}$$

functions of the user-level game $\mathcal{G}_u$ satisfies the dominance solvability condition². Then, we substitute the NE of the user-level game $\mathcal{G}_u$ into the CSSV-level game $\mathcal{G}_C$ and prove that the Jacobian matrix of the profit functions of the CSSV-level game $\mathcal{G}_C$ is negative definite. This demonstrates the existence and uniqueness of the NE to the CSSV-level game $\mathcal{G}_C$. The Stackelberg equilibrium therefore exists and is unique.

²The dominance solvability condition for a concave game is $-\frac{\partial^2 u_i}{\partial x_i^2} \geq \sum_j \left| \frac{\partial^2 u_i}{\partial x_i \partial x_j} \right|$, where u_i and x_i are the utility function and strategy for user i , respectively.

5.2.1 Equilibrium Analysis for the User-level Game

To obtain the optimal solution for the user-level game $\mathcal{G}_u$, we take the partial derivative of (5.6) with respect to x_i , which has been shown in (5.9).

Let $\mathbf{a} = [a_1, a_2, \dots, a_{|\mathcal{N}|}]^\top$, $\mathbf{p}^A = [p_1^A, p_2^A, \dots, p_{|\mathcal{N}|}^A]^\top$, $\mathbf{p}^B = [p_1^B, p_2^B, \dots, p_{|\mathcal{N}|}^B]^\top$, $\mathbf{1} = \text{ones}(|\mathcal{N}|, 1)$, $\mathbf{B} = \text{diag}([2b_1, 2b_2, \dots, 2b_{|\mathcal{N}|}])$, and $\mathbf{I} = \text{ones}(|\mathcal{N}|, |\mathcal{N}|)$, $\frac{\partial u_i}{\partial x_i}$, $\forall i \in \mathcal{N}$ can be rewritten in a matrix form, i.e., (5.10).

Let $\frac{\partial u_i}{\partial x_i} = 0$, $\forall i \in \mathcal{N}$, we have $\mathbf{x}^*$, i.e., the best responses of the users, as shown in (5.11).

Lemma 5.2.1. The matrix $[2\mathbf{B} - 2\mathbf{G} + (d^A + d^B)\mathbf{I}]$ is invertible and positive definite if $\frac{\sum_{j \neq i} [2g_{ij} - (d^A + d^B)]}{4b_i + (d^A + d^B)} < 1$, $\forall i \in \mathcal{N}$.

Proof. We have $\frac{2g_{ij} - (d^A + d^B)}{4b_i + (d^A + d^B)} \geq 0$, $(d^A + d^B) > 0$, and $b_i > 0$. Moreover, we also have $2g_{ij} - (d^A + d^B) \geq 0$ and $4b_i + (d^A + d^B) > \sum_{j \neq i} [2g_{ij} - (d^A + d^B)] = \sum_{j \neq i} |2g_{ij} - (d^A + d^B)|$. Therefore, the inequality (5.13) is certainly satisfied, where $\{\cdot\}_{ij}$ denotes the ij -th element of a matrix. This implies the strictly diagonal dominance of the matrix $[2\mathbf{B} - 2\mathbf{G} + (d^A + d^B)\mathbf{I}]$. Moreover, according to Gershgorin circle theorem [126], every eigenvalue λ of the matrix $[2\mathbf{B} - 2\mathbf{G} + (d^A + d^B)\mathbf{I}]$ satisfies

$$\begin{aligned} & \left| \{ [2\mathbf{B} - 2\mathbf{G} + (d^A + d^B)\mathbf{I}] \}_{ii} - \lambda \right| \\ & \leq \sum_{j \neq i} \left| \{ [2\mathbf{B} - 2\mathbf{G} + (d^A + d^B)\mathbf{I}] \}_{ij} \right|. \end{aligned} \quad (5.14)$$

Due to the strictly diagonal dominance of $[2\mathbf{B} - 2\mathbf{G} + (d^A + d^B)\mathbf{I}]$ and, moreover, $\{ [2\mathbf{B} - 2\mathbf{G} + (d^A + d^B)\mathbf{I}] \}_{ii} = 4b_i + (d^A + d^B)$ is larger than 0, we can conclude that λ is positive. Consequently, $[2\mathbf{B} - 2\mathbf{G} + (d^A + d^B)\mathbf{I}]$ is positive definite due to the fact that all its eigenvalues are larger than 0. In addition, $[2\mathbf{B} - 2\mathbf{G} + (d^A + d^B)\mathbf{I}]$ is invertible because of its positive definiteness. $\square$

Since $[2\mathbf{B} - 2\mathbf{G} + (d^A + d^B)\mathbf{I}]$ is invertible as proven in Lemma 5.2.1, we can left multiply both the sides of (5.11) by its inverse matrix and obtain the optimal solution to $\mathcal{G}_u$ as shown in (5.12). Moreover, we can have

$$\mathbf{x}^* = \mathbf{K} [(\mathbf{q}^A - \mathbf{q}^B)\mathbf{a} + (\mathbf{B} - \mathbf{G})\mathbf{1} + |\mathcal{N}|d^B\mathbf{1} - \mathbf{p}^A + \mathbf{p}^B], \quad (5.19)$$

$$\begin{aligned}
 & [\nabla_{i,j} u_i(\mathbf{x})]_{\forall i,j \in \mathcal{N}} + [\nabla_{i,j} u_i(\mathbf{x})]_{\forall i,j \in \mathcal{N}}^\top = \begin{bmatrix} \nabla_{1,1} u_1(\mathbf{x}) & \nabla_{1,2} u_1(\mathbf{x}) & \cdots & \nabla_{1,|\mathcal{N}|} u_1(\mathbf{x}) \\ \nabla_{2,1} u_2(\mathbf{x}) & \nabla_{2,2} u_2(\mathbf{x}) & \cdots & \nabla_{2,|\mathcal{N}|} u_2(\mathbf{x}) \\ \vdots & \vdots & \ddots & \vdots \\ \nabla_{|\mathcal{N}|,1} u_{|\mathcal{N}|}(\mathbf{x}) & \nabla_{|\mathcal{N}|,2} u_{|\mathcal{N}|}(\mathbf{x}) & \cdots & \nabla_{|\mathcal{N}|,|\mathcal{N}|} u_{|\mathcal{N}|}(\mathbf{x}) \end{bmatrix} \\
 & + \begin{bmatrix} \nabla_{1,1} u_1(\mathbf{x}) & \nabla_{1,2} u_1(\mathbf{x}) & \cdots & \nabla_{1,|\mathcal{N}|} u_1(\mathbf{x}) \\ \nabla_{2,1} u_2(\mathbf{x}) & \nabla_{2,2} u_2(\mathbf{x}) & \cdots & \nabla_{2,|\mathcal{N}|} u_2(\mathbf{x}) \\ \vdots & \vdots & \ddots & \vdots \\ \nabla_{|\mathcal{N}|,1} u_{|\mathcal{N}|}(\mathbf{x}) & \nabla_{|\mathcal{N}|,2} u_{|\mathcal{N}|}(\mathbf{x}) & \cdots & \nabla_{|\mathcal{N}|,|\mathcal{N}|} u_{|\mathcal{N}|}(\mathbf{x}) \end{bmatrix}^\top \quad (5.15)
 \end{aligned}$$

$$= 2 \begin{bmatrix} -4b_1 - (d^A + d^B) & 2g_{12} - (d^A + d^B) & \cdots & 2g_{1|\mathcal{N}|} - (d^A + d^B) \\ 2g_{21} - (d^A + d^B) & -4b_2 - (d^A + d^B) & \cdots & 2g_{2|\mathcal{N}|} - (d^A + d^B) \\ \vdots & \vdots & \ddots & \vdots \\ 2g_{|\mathcal{N}|1} - (d^A + d^B) & 2g_{|\mathcal{N}|2} - (d^A + d^B) & \cdots & -4b_{|\mathcal{N}|} - (d^A + d^B) \end{bmatrix} \quad (5.16)$$

$$= -2 [2\mathbf{B} - 2\mathbf{G} + (d^A + d^B) \mathbf{I}]$$

$$\begin{aligned}
 \Pi^A &= \sum_{i \in \mathcal{N}} (p_i^A - (1 - q^A) n\lambda) x_i - z^A(q^A) = [\mathbf{p}^A - (1 - q^A) n\lambda \mathbf{1}]^\top \mathbf{x} - z^A(q^A) \\
 &= [\mathbf{p}^A - (1 - q^A) n\lambda \mathbf{1}]^\top \mathbf{K} [(q^A - q^B) \mathbf{a} + (\mathbf{B} - \mathbf{G}) \mathbf{1} + |\mathcal{N}| d^B \mathbf{1} - \mathbf{p}^A + \mathbf{p}^B] - z^A(q^A) \quad (5.17)
 \end{aligned}$$

$$\begin{aligned}
 \Pi^B &= \sum_{i \in \mathcal{N}} (p_i^B - (1 - q^B) n\lambda) (1 - x_i) - z^B(q^B) = [\mathbf{p}^B - (1 - q^B) n\lambda \mathbf{1}]^\top (\mathbf{1} - \mathbf{x}) - z^B(q^B) \\
 &= [\mathbf{p}^B - (1 - q^B) n\lambda \mathbf{1}]^\top \{ \mathbf{1} - \mathbf{K} [(q^A - q^B) \mathbf{a} + (\mathbf{B} - \mathbf{G}) \mathbf{1} + |\mathcal{N}| d^B \mathbf{1} - \mathbf{p}^A + \mathbf{p}^B] \} - z^B(q^B) \quad (5.18)
 \end{aligned}$$

where $\mathbf{K} = [2\mathbf{B} - 2\mathbf{G} + (d^A + d^B) \mathbf{I}]^{-1}$ is positive definite thanks to the positive definiteness of its inverse matrix as proven in Lemma 5.2.1.

Proposition 5.2.1. If the game $\mathcal{G}_u$ can satisfy: 1) $\mathcal{X} \subset \mathbb{R}^{|\mathcal{N}|}$ is nonempty, convex, and compact; 2) $\mathbf{u}$ is continuous with respect to $\mathbf{x}$, and u_i is concave with respect to x_i , there exists one NE (Theorem 1.1 in [127]).

Theorem 5.2.2. There exists NE in the user-level noncooperative game $\mathcal{G}_u = \{\mathcal{N}, \mathbf{x}, \mathcal{X}, \mathbf{u}\}$.

Proof. Based on (5.6), we can have

$$\frac{\partial^2 u_i}{\partial x_i^2} = -4b_i + 2g_{ii} - (d^A + d^B) = -4b_i - (d^A + d^B) \leq 0, \quad (5.20)$$

which implies that $u_i(x_i, \mathbf{x}_{-i}, \mathbf{p}^A, \mathbf{p}^B, q^A, q^B)$ is concave with respect to x_i , $\forall i \in \mathcal{N}$. Moreover, as $\mathcal{X} = \{[x_1, \dots, x_{|\mathcal{N}|}] | x_i \in [0, 1], \forall i \in \mathcal{N}\}$ satisfies the first condition of Proposition 5.2.1, there exists one NE in the user-level noncooperative game $\mathcal{G}_u = \{\mathcal{N}, \mathbf{x}, \mathcal{X}, \mathbf{u}\}$. $\square$

Theorem 5.2.3. According to Lemma 5.2.1, if the Jacobian matrix of $\mathbf{u}(\mathbf{x}) = [u_1(\mathbf{x}), \dots, u_{|\mathcal{N}|}(\mathbf{x})]^\top$ can satisfy the dominance solvability condition, there exists one unique NE for the user-level noncooperative game $\mathcal{G}_u = \{\mathcal{N}, \mathbf{x}, \mathcal{X}, \mathbf{u}\}$.

Proof. According to Theorem 4.1 (Moulin) in [127], we will prove that the Jacobian matrix of the utility functions of $\mathcal{G}_u$ satisfies the dominance solvability condition in the following. The Jacobian matrix of $\mathbf{u}(\mathbf{x}) = [u_1(\mathbf{x}), \dots, u_{|\mathcal{N}|}(\mathbf{x})]^\top$ is shown in (5.15), where $\nabla_{i,j}u_i(\mathbf{x})$ is the second partial derivative of $u_i(\mathbf{x})$ with respect to x_i firstly and x_j secondly, i.e., $\frac{\partial^2 u_i}{\partial x_i \partial x_j}$, $\forall i, j \in \mathcal{N}$. Then, based on (5.15), we can obtain (5.16).

Based on Lemma 5.2.1 and the strictly diagonally dominance of $-\left[\nabla_{i,j}u_i(\mathbf{x})\right]_{\forall i,j \in \mathcal{N}} - \left[\nabla_{i,j}u_i(\mathbf{x})\right]_{\forall i,j \in \mathcal{N}}^\top$, the specifical Jacobian matrix (5.16) satisfies the dominance solvability condition. Therefore, $\left[\nabla_{i,j}u_i(\mathbf{x})\right]_{\forall i,j \in \mathcal{N}} + \left[\nabla_{i,j}u_i(\mathbf{x})\right]_{\forall i,j \in \mathcal{N}}^\top$, i.e., the Jacobian matrix, satisfies the dominance solvability condition [128]. This implies that the user-level noncooperative game $\mathcal{G}_u = \{\mathcal{N}, \mathbf{X}, \mathcal{X}, \mathbf{u}\}$ admits an unique NE to Theorems 3.1 (Rosen) and 4.1 (Moulin) in [127]. The proof is completed. $\square$

5.2.2 Equilibrium Analysis for the CSSV-level Game

Given the users' strategies, for the CSSV-A and CSSV-B in the competitive market, the profit of each CSSV is affected not only by its own price and security level, but also by the price and security level offered by the other CSSV. Therefore, the price and security level determination between the CSSVs is a noncooperative game $\mathcal{G}_C$. The NE of the CSSV-level game is a strategy that no CSSV can increase its profit by choosing a different strategy with the other players' strategies unchanged [119]. In this case, we firstly prove that the CSSV-level noncooperative game $\mathcal{G}_C$ admits one NE, and the uniqueness of which will be proven later.

Given the users' strategies in (5.12), we can rewrite the profit functions for the CSSVs in a matrix form as shown in (5.17) and (5.18). In (5.17) and (5.18), the investments z^A and z^B are in the functional form as shown in (5.4), in which security levels q^A and q^B are their independent variables, respectively. Then, we calculate the second partial derivatives of (5.17) with respect to $\mathbf{p}^A$ and q^A as well as that of (5.18) with respect to $\mathbf{p}^B$ and q^B as shown in (C.3), where $z^{A''} = \frac{\partial^2 z^A}{\partial q^{A^2}}$ and $z^{B''} = \frac{\partial^2 z^B}{\partial q^{B^2}}$.

Theorem 5.2.4. The CSSV-level noncooperative game $\mathcal{G}_C$ admits one NE if $z^{A''} = \frac{\partial^2 z^A}{\partial q^{A^2}} > (\mathbf{a} + n\lambda\mathbf{1})^\top \mathbf{K}(\mathbf{a} + n\lambda\mathbf{1})$ and $z^{B''} = \frac{\partial^2 z^B}{\partial q^{B^2}} > (\mathbf{a} + n\lambda\mathbf{1})^\top \mathbf{K}(\mathbf{a} + n\lambda\mathbf{1})$. Then, the Stackbelberg equilibrium of the market game exists.

Proof. Please refer to Appendix C.1. □

Theorem 5.2.5. The CSSV-level noncooperative game $\mathcal{G}_C$ admits one unique NE if $z^{A''} = \frac{\partial^2 z^A}{\partial q^{A^2}} > (\mathbf{a} + n\lambda\mathbf{1})^\top \mathbf{K}(\mathbf{a} + n\lambda\mathbf{1})$ and $z^{B''} = \frac{\partial^2 z^B}{\partial q^{B^2}} > (\mathbf{a} + n\lambda\mathbf{1})^\top \mathbf{K}(\mathbf{a} + n\lambda\mathbf{1})$. Then, the Stackbelberg equilibrium of the market game is unique.

Proof. Please refer to Appendix C.2. □

5.3 Performance Evaluation

5.3.1 Parameters Setting

In this section, we present the numerical results to study the behaviours of the players in the cloud security service market. The number of the users in the cloud security service market is $|\mathcal{N}|$. The parameter setting for the users are $a_i \sim N(\mu_a, \sigma)$ and $b_i \sim N(\mu_b, \sigma)$ with $\mu_a = 10$, $\mu_b = 2.5$, and $\sigma = 1/3$. Due to the diversity of the CSSVs, we set the intrinsic parameters for the congestion of the CSSVs as $d^A \sim N(\mu_d, \sigma)$ and $d^B = d^A + d$, where $\mu_d = 0.1$ and $d \sim N(\sigma, \sigma/3)$. The off-diagonal elements of interdependency matrix $\mathbf{G}$, i.e., g_{ij} , $\forall i \neq j$, is generated following $N(\mu_g, \sigma)$, where $\mu_g = 0.13$ for strong interdependency and 0.12 for weak interdependency. The diagonal elements of interdependency matrix $\mathbf{G}$, i.e., g_{ii} , $\forall i \in \mathcal{N}$, equal 0. The other default coefficients are set as follows: $v(1) = 0.5$, $n = 1$, $\lambda = 1$, $p^u = 10$, and $\alpha = 2$. Without loss of generality, we choose the functional form for the Proportional Hazard Class of security breach probability as expressed in (5.2), as the specific formulation for $v(z)$. However, similar results are expected for the other classes of security breach probability. Note that the price shown in the following figures is the mean of the discriminative prices.

FIGURE 5.2: Best response of the CSSV-A under (a) strong and (b) weak interdependency as well as that of the CSSV-B under (c) strong and (d) weak interdependency.

5.3.2 Numerical Results

Figures 5.2 and 5.3 show the best response and NE, respectively. We first evaluate the profit of the CSSV. In Fig. 5.2, the CSSVs serve 80 users. The profit of the CSSV-A changes due to the different prices charging the users and different investments to improve the security level of cloud security service. From Fig. 5.2(a), there is a point where the profit of the CSSV-A is maximized, which is pointed by the arrowhead of “Best response”. This point constitutes the Stackelberg equilibrium for the CSSV-A. As is evident from Fig. 5.2(a), this profit, which is a function of price and security level, is unimodal, and the optimal solution can be obtained analytically.

FIGURE 5.3: NE for (a) price and (b) security level.

Figure 5.3 illustrates the NEs of the price and security level for the CSSV-A and CSSV-B under different levels of interdependency. The NE is the point at which the best responses for the CSSV-A and CSSV-B intersect. Under different levels of interdependency among the users, different NEs are observed. As expected, when the level of interdependency is strong, the prices of cloud security plans provided by the CSSV-A and CSSV-B decrease, which can be observed in Fig. 5.3(a). Furthermore, when the level of interdependency is strong, the security level of the cloud security service for the CSSV-A increases slightly while that for the CSSV-B decreases slightly, as shown in Fig. 5.3(b). The reason for this phenomenon is explained in the subsequent discussions.

We evaluate the impact of number of users in Fig. 5.4. From Fig. 5.4(a), the total utilities in the cloud security service market under strong interdependency are always higher than those under weak interdependency. The reason is that the users will become safer if many of other user also buy the same cloud security plan. In other words, the security level of user j is enhanced if its associated neighbor user i also buys the same cloud security plan. Clearly, this enhancement in the users' security level under strong interdependency is larger than that under weak interdependency. This is also consistent with the results that the increasing rate of the users' total utilities under strong interdependency is faster than that under weak interdependency. As shown in Fig. 5.4(b), the profits of both the CSSV-A and CSSV-B decrease as the interdependency becomes stronger. The main reason is that when the users are strongly interdependent, the CSSVs need to remain

FIGURE 5.4: (a) Total users' utilities, (b) profit, (c) price and (d) security level with increasing users and different levels of interdependency.

competitive by improving the security level of the cloud security service. However, this requires much more investment as the increasing rate of the security level becomes smaller when it is close to the maximum level as shown in Fig. 5.1. Thus, the CSSVs may not want to invest too much in improving the near perfect security level. From Fig. 5.4(d), the security level is therefore not affected much by the changes in the level of interdependency. As a result, the CSSVs have to adjust their prices appropriately, which can be observed from the numerical results in Fig. 5.4(c).

We evaluate the impact of the parameter $v(1)$ (i.e., the probability of being breached when investment is 1). We set the number of users to be 80 and $v(1)$ is varied from 0.1 to 0.9. As shown in Fig. 5.5(d), the security level of cloud security service decreases as $v(1)$ increases, which leads to the increase of the probability of being breached. Correspondingly, this further leads to the decrease in the users' total utilities as shown in Fig. 5.5(a). The reason is that the users may become unsafer as the probability of being breached increases, even when they are covered by the cloud-insurance. Additionally, the decrease in the security level of cloud security service has an impact on the profits of the CSSVs. The decrease in the security level of cloud security service leads to the increase of the probability of paying claims. In this case, even when the prices of the cloud security plan do not change simultaneously, the profits of both the CSSVs decrease as $v(1)$ increases.

FIGURE 5.5: (a) Total users' utilities, (b) profit, (c) price and (d) security level with increasing probability of being breached $v(1)$.

FIGURE 5.6: (a) Total utilities, (b) profit, (c) price, and (d) security level with varying interdependency.

Figure 5.6 shows the impact of user's interdependency. The number of users is 80 in the market, and μ_g is increased. As expected, the users' total utilities increase as the level of interdependency becomes stronger while both the profits and prices of the CSSVs decrease, as shown in Figs. 5.6(a), (b) and (c). From Fig. 5.6(d), the

FIGURE 5.7: (a) Total users' utilities, (b) profit, (c) price and (d) security level under competition and cooperation.

security level for the CSSV-A increases slightly as the level of interdependency becomes stronger for the purpose of remaining competitive. In contrast, the security level of cloud security service for the CSSV-B decreases. This is due to the fact that the CSSV-B may not be capable of maintaining such a high security level for the cloud security service when both its price of cloud security plan and profit are much lower than that of the CSSV-A. Furthermore, as aforementioned, the investment becomes larger since the increasing rate of the security level becomes smaller, when the security level is close to the maximum level. This means even a slight decrease in the security level will reduce substantial amount of investment. Therefore, the security level of cloud security service for the CSSV-B decreases slightly as the level of interdependency becomes stronger, which reduces much investment while maintaining a similar security level.

We compare the performance of the proposed competitive market with that of the cooperative market in Fig. 5.7. In the cooperative market, the CSSV-A and CSSV-B jointly optimize their total profit, i.e., sum of individual profits. From Fig. 5.7(c), in the cooperative market, the price of cloud security plan is always at the maximum level, i.e., p^u . Thus, the total profit in the cooperative market under strong interdependency is exactly the same as that under weak interdependency,

as shown in Fig. 5.7(b). Furthermore, we observe that the total profit in the cooperative market is always higher than that in the competitive market. This result is not only from the changes in the price but also from the changes in the security level of the cloud security service. First, the prices of cloud security plan in the cooperative market is higher than those in the competitive market, which leads to the increase in the CSSVs' revenue from the users. Second, as shown in Fig. 5.7(d), the security levels of cloud security service in the cooperative market is lower than that in the competitive market. As a result, the CSSVs can reduce their investment. However, in Fig. 5.7(a), compared with the competitive market, the higher price of cloud security plan and lower security level of cloud security service in the cooperative market result in a negative value for the users' total utilities. The reason is that the cooperative market enables the existing CSSVs to collude and extensively exploit the users. However, in the real market, the CSSVs are generally selfish, and the cooperative market scenario rarely happens. The future work on the collusive cloud security service market can be studied.

Figure 5.8 shows the impact of n , i.e., the number of threats, on the users' total utilities, the CSSVs' profits, the prices of cloud security plan, and the security level of cloud security service. The security level of cloud security service is improved by the CSSVs through raising the investment when the number of threats increases from 5 to 15, as shown in Figs. 5.8(f) and (g). In this case, we observe that the users' total utilities do not change much accordingly. Furthermore, we observe that the CSSVs' profits are not affected by the increase in the number of threats, even when the investment is increased due to the improvement in the security level of the cloud security service. This due to the fact that the improvement in the security level of cloud security service not only results in the decrease in the probability of paying the claims to the users, but also makes the cloud security plan more attractive to the users. Accordingly, the price of cloud security plan increases as the number of threats increases as shown in Figs. 5.8(d) and (e). This increase in the price of cloud security plan can help to compensate for the cost incurred by the more investment for improving the security level. Additionally, the different levels of interdependency still have an impact on these metrics. However, as observed in Figs. 5.8(f) and (g), the impact of interdependency on the security level of cloud security service is smaller than that of the number of threats. For example, in Fig. 5.8(f), the improvement in the security level between the curves of "Weak Interdependency with 15 threats" and "Weak Interdependency with 10 threats" is

FIGURE 5.8: (a) Total users' utilities, (b) & (c) profit for the CSSVs A & B, (d) & (e) price for the CSSVs A & B, and (f) & (g) security level for the CSSVs A & B with increasing number of the users and increasing numbers of threats.

larger than that between the curves of “Strong Interdependency with 10 threats” and “Weak Interdependency with 10 threats” for the CSSV-A. The reason is that the number of threats has stronger impact than the interdependency on the users.

5.4 Summary

In this chapter, we have studied the cloud security service market, where a joint pricing and security investment problem has been investigated. In particular, this problem has been investigated in the framework of a two-stage Stackelberg game. The CSSVs offer the cloud security plan, which is constituted of cloud-insurance and cloud security service, to the users and act as the leaders on the upper stage.

The CSSVs lead to decide on their strategies, i.e., the price and the security investment, and the competition between which has been model as a CSSV-level noncooperative subgame on the upper stage. The interaction among the users has been modeled as a user-level noncooperative subgame on the lower stage. Therein, the security interdependency among the users has been incorporated. The equilibrium of the proposed Stackelberg game has been proven to be existence and unique. We have presented extensive numerical results of the proposed game. The performance evaluation shows some insightful results. For example, when the user have strong interdependency, the profits of the CSSVs become lower. We will incorporate the reinsurance in the cloud security service market as the future work.

Chapter 6

Conclusion and Future Work

In this chapter, we conclude this thesis and discuss the potential research directions for the future work.

6.1 Conclusion

In this thesis, we have adopted the cyber-insurance, i.e., an alternative means of cyber risk management, to neutralize the cyber risks incurred by the cyber attacks for the computer networks. The main research contributions of the research issues presented in this thesis are summarized as follows:

- *Chapter 3*: A two-level Stackelberg differential game based on the evolutionary game theory and the optimal control theory is adopted to investigate the dynamic behaviors of the fog computing provider and the APT attacker as well as that of the cyber insurer. Specifically, the interaction between the fog computing provider and the APT attacker has been formulated as an evolutionary game based on the replicator dynamics in the lower level, where the bounded rationality of the entities has been captured. By taking into account the dynamic strategies of the entities in the lower level, the cyber insurer prices its cyber-insurance in the upper level, and the premium pricing problem of which has been modeled as an optimal control problem.
- *Chapter 4*: A novel security approach of jointly providing the risk management and security enhancement to the users and the service providers in the

blockchain service market has been proposed. The blockchain service market under our consideration has been formulated as a two-stage Stackelberg game. On the lower stage, the users determine their service demands according to the perceived risk level of the blockchain service and the service fee as well as the social externality. On the upper stage, the blockchain provider and the cyber insurer lead to adjust their best-response strategies in order to maximize their individual profits.

- *Chapter 5:* To secure the users in the cloud platform, a joint cloud-insurance and security investment approach has been proposed. Specifically, the cloud security service market has been modeled as a two-stage Stackelberg game. On the lower stage, the users act as the followers and decide on the purchase of the cloud security plan. Therein, the security interdependency among the users has been taken into account. On the upper stage, the cloud insurers decide on the price of the cloud security plan and the investment in improving the security level of the cloud security service, and the competition between which has been modeled as a noncooperative game.

6.2 Future Work

6.2.1 Future Work on the APT Attack of the Fog Computing

In the current fog computing platform, the cyber insurer will suffer the cyber risks transferred from the fog computing provider. In this case, we consider to include the concept of “reinsurance” in the future work such that the cyber insurer can manage the cyber risks transferred from the fog computing provider. This due to the fact that by enabling to transfer portions of the insurer’s suffering cyber risks to other parties, reinsurance is an effective way to spread the risks for the insurer. Consequently, along with the cyber-insurance and by incorporating the concept of “reinsurance” in the current fog computing platform, both the fog computing provider and the cyber insurer can effectively and efficiently manage and neutralize the cyber risks incurred by the cyber attacks.

6.2.2 Future Work on the Fog Computing

In the current fog computing platform under our consideration, we did not take into account the fog computing users. However, the user plays an important role in the fog computing platform. The reason for that can be explained as follows: 1) facing the heterogeneous capacities of the various fog computing nodes, the user needs to decide on the subscription to the appropriate fog computing node in order to perform its task; 2) due to the fact that the past service experience may seriously affect the user's current preferences for each fog computing node, this will consequently affect the value of the asset of each fog computing node. In this case, it is difficult to determine the importance of each fog computing node for the fog computing provider. For future work, we will include the users as players and incorporate the concept of "power-law memory", which is described by using the fractional calculus, in the future work. As such, the memory-affecting behaviors of the users' fog computing node subscription can be evaluated and studied accordingly.

6.2.3 Future Work on the Double-spending Attack of the Blockchain Networks

The two-level Stackelberg game in the current system model is based on the assumption that the total computing resources of the network is fixed over a certain time period. However, in order to lower the infrastructure cost, third-party devices are encouraged to join the decentralized consensus process by dedicating their individual computing resources into the network, which may result in uncertainty of the total computing resources of the network. In this case, two major issues arise. First, under the uncertain amount of the total computing resources of the network, it is difficult to assess the system's vulnerability and hence hard to estimate the risk level, which will further affect the decision making of the blockchain provider. Second, over a certain time period, the blockchain provider and the attacker should adjust their strategies dynamically rather than following the static best-response strategies so as to maximize their own cumulative profit/payoff. Therefore, to study the considered blockchain service market in a long-run manner and take into account the computing resources dedicated by the third-party devices, we will resort to the Hierarchical differential game, which is a typical tool for studying the

long-run interaction among different entities, and include the third-party devices as players in the market.

Appendix A

Proofs for Chapter 3

A.1 Proof of Proposition 3.3.1

Proof. Due to the space limit, we prove the existences of M^{dfdu}_{ij} , $M^{\text{dfd}\mathbf{v}}_{ij}$, and M^{dfdx}_{ij} , $\forall i, j \in \mathcal{N}$ as examples. The existences of $M^{\text{dgd}\mathbf{u}}_{ij}$, $M^{\text{dgd}\mathbf{v}}_{ij}$, M^{dhdu}_{ij} , M^{dhdv}_{ij} , and M^{dhdx}_{ij} , $\forall i, j \in \mathcal{N}$ can be proven in a similar way.

Since $U^{\text{P}}_i(u_i(t), v_i(t), x_i(t), p_i)$ is continuous with respect to $[u_i(t), v_i(t), x_i(t)]^\top$ over the closed set $\mathcal{D}_{u_i} \times \mathcal{D}_{v_i} \times \mathcal{D}_{x_i}$, it has a upper bound denoted by $b^{U^{\text{P}}\mathbf{u}_i}$, i.e.,

$$b^{U^{\text{P}}\mathbf{u}_i} \geq \max_{u_i(t), v_i(t), x_i(t)} |U^{\text{P}}_i(u_i(t), v_i(t), x_i(t), p_i)|. \quad (\text{A.1})$$

Accordingly, from the following inequality equation

$$\begin{aligned}
& \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \left| \overline{U}_D^P(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}) \right| \\
&= \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \left| \sum_{i \in \mathcal{N}} [u_i(t) U_i^P(u_i(t), v_i(t), x_i(t), p_i)] \right| \\
&\leq \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \sum_{i \in \mathcal{N}} |u_i(t) U_i^P(u_i(t), v_i(t), x_i(t), p_i)| \\
&= \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \sum_{i \in \mathcal{N}} [|u_i(t)| |U_i^P(u_i(t), v_i(t), x_i(t), p_i)|] \tag{A.2} \\
&\leq \sum_{i \in \mathcal{N}} \left\{ \left[\max_{u_i(t)} |u_i(t)| \right] \right. \\
&\quad \times \left. \left[\max_{u_i(t), v_i(t), x_i(t)} |U_i^P(u_i(t), v_i(t), x_i(t), p_i)| \right] \right\} \\
&\leq \sum_{i \in \mathcal{N}} \left\{ 1 \times b^{U^P \mathbf{u}_i} \right\} = \sum_{i \in \mathcal{N}} b^{U^P \mathbf{u}_i},
\end{aligned}$$

we find the upper bound of $\left| \overline{U}_D^P(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}) \right|$ over $\mathcal{D}_{\mathbf{u}} \times \mathcal{D}_{\mathbf{v}} \times \mathcal{D}_{\mathbf{x}}$, $\forall \mathbf{p} = \mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}$ to be $\sum_{i \in \mathcal{N}} b^{U^P \mathbf{u}_i}$.

Additionally, with respect to $[u_i(t), v_i(t), x_i(t)]^\top$ over the closed set $\mathcal{D}_{u_i} \times \mathcal{D}_{v_i} \times \mathcal{D}_{x_i}$, $\left[\frac{dU_i^P(z, v_i(t), x_i(t), p_i)}{dz} \right]_{z=u_i(t)} = \frac{v_i(t) M^A M^P}{(u_i(t) M^P + v_i(t) M^A + \sigma)^2} \lambda_i - d_i M^P - \lambda_i x_i(t) \frac{v_i(t) M^A M^P}{(u_i(t) M^P + v_i(t) M^A + \sigma)^2}$ is continuous, $\forall i \in \mathcal{N}$. Accordingly, $\forall i \in \mathcal{N}$, $\forall \mathbf{p} = \mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}$, there exists an upper bound of $\left| \frac{dU_i^P(z, v_i(t), x_i(t), p_i)}{dz} \right|_{z=u_i(t)}$ over the set $\mathcal{D}_{u_i} \times \mathcal{D}_{v_i} \times \mathcal{D}_{x_i}$ denoted by $b^{dU^P \mathbf{u}_i}$, i.e., $\forall i \in \mathcal{N}$, $\forall \mathbf{p} = \mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}$,

$$b^{dU^P \mathbf{u}_i} \geq \max_{u_i(t), v_i(t), x_i(t)} \left| \frac{dU_i^P(z, v_i(t), x_i(t), p_i)}{dz} \right|_{z=u_i(t)}. \tag{A.3}$$

Similarly, there exist $b^{dU^P \mathbf{dv}_i}$ and $b^{dU^P \mathbf{dx}_i}$ such that $\forall i \in \mathcal{N}$, $\forall \mathbf{p} = \mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}$,

$$\begin{aligned}
b^{dU^P \mathbf{dv}_i} &\geq \max_{u_i(t), v_i(t), x_i(t)} \left| \frac{dU_i^P(u_i(t), z, x_i(t), p_i)}{dz} \right|_{z=v_i(t)}, \\
b^{dU^P \mathbf{dx}_i} &\geq \max_{u_i(t), v_i(t), x_i(t)} \left| \frac{dU_i^P(u_i(t), v_i(t), z, p_i)}{dz} \right|_{z=x_i(t)},
\end{aligned} \tag{A.4}$$

Then, in order to prove the existences of M^{dfdu}_{ij} , M^{dfdv}_{ij} , and M^{dfdx}_{ij} , $\forall i, j \in \mathcal{N}$, $\forall \mathbf{p} = \mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}$, we need to take the first derivatives of $f_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p})$

with respect to $\left[(\mathbf{u}(t))^\top, (\mathbf{v}(t))^\top, (\mathbf{x}(t))^\top \right]^\top, \forall i \in \mathcal{N}$ as shown in (A.7).

Firstly, from the inequality equation, i.e., (A.8), then M^{dfdu}_{ij} exists and is a positive finite valued real number and can be defined as follows:

$$M^{\text{dfdu}}_{ij} = \begin{cases} b^{U^P \mathbf{u}}_i + \sum_{k \in \mathcal{N}} b^{U^P \mathbf{u}}_k + \frac{1}{4} b^{\text{d}U^P \text{du}}_i, & j = i \\ b^{\text{d}U^P \text{du}}_j, & j \neq i \end{cases} \quad (\text{A.5})$$

such that

$$M^{\text{dfdu}}_{ij} \geq \left| \frac{\text{d}f_i(\mathbf{u}_{-j}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p})}{\text{d}z} \right|_{z=\mathbf{u}_j(t)}, \quad (\text{A.6})$$

$$\forall \left[(\mathbf{u}(t))^\top, (\mathbf{v}(t))^\top, (\mathbf{x}(t))^\top \right]^\top \in \mathcal{D}_{\mathbf{u}} \times \mathcal{D}_{\mathbf{v}} \times \mathcal{D}_{\mathbf{x}}, \forall i, j \in \mathcal{N}, \forall \mathbf{p} = \mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}.$$

Then, from the inequality equation as shown in (A.9), then M^{dfdv}_{ij} exists and is a positive finite real number and can be defined as follows:

$$M^{\text{dfdv}}_{ij} = \begin{cases} \frac{1}{4} b^{\text{d}U^P \text{dv}}_i, & j = i \\ b^{\text{d}U^P \text{dv}}_j, & j \neq i \end{cases} \quad (\text{A.11})$$

such that

$$M^{\text{dfdv}}_{ij} \geq \left| \frac{\text{d}f_i(\mathbf{u}(t), \mathbf{v}_{-j}(t), \mathbf{x}(t), \mathbf{p})}{\text{d}z} \right|_{z=\mathbf{v}_j(t)}, \quad (\text{A.12})$$

$$\forall \left[(\mathbf{u}(t))^\top, (\mathbf{v}(t))^\top, (\mathbf{x}(t))^\top \right]^\top \in \mathcal{D}_{\mathbf{u}} \times \mathcal{D}_{\mathbf{v}} \times \mathcal{D}_{\mathbf{x}}, \forall i, j \in \mathcal{N}, \forall \mathbf{p} = \mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}.$$

At last, from the inequality equation as shown in (A.10), then M^{dfdxx}_{ij} exists to be a positive finite real number and can be defined as follows:

$$M^{\text{dfdxx}}_{ij} = \begin{cases} \frac{1}{4} b^{\text{d}U^P \text{dxx}}_i, & j = i \\ b^{\text{d}U^P \text{dxx}}_j, & j \neq i \end{cases} \quad (\text{A.13})$$

such that

$$M^{\text{dfdxx}}_{ij} \geq \left| \frac{\text{d}f_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}_{-j}(t), \mathbf{p})}{\text{d}z} \right|_{z=\mathbf{x}_j(t)}, \quad (\text{A.14})$$

$$\forall \left[(\mathbf{u}(t))^\top, (\mathbf{v}(t))^\top, (\mathbf{x}(t))^\top \right]^\top \in \mathcal{D}_{\mathbf{u}} \times \mathcal{D}_{\mathbf{v}} \times \mathcal{D}_{\mathbf{x}}, \forall i, j \in \mathcal{N}, \forall \mathbf{p} = \mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}.$$

Therefore, the existences of M^{dfdu}_{ij} , M^{dfdv}_{ij} , and M^{dfdxx}_{ij} , $\forall i, j \in \mathcal{N}$ have been proven. $\square$

$$\begin{aligned}
\nabla_{u_j(t)} f_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}) &= \\
\begin{cases} [1 - u_i(t)] U_i^P(u_i(t), v_i(t), x_i(t), p_i) \\ -\bar{U}_D^P(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}) \\ + u_i(t) [1 - u_i(t)] \frac{dU_i^P(u_i(t), v_i(t), x_i(t), p_i)}{du_i(t)}, & i = j \\ -u_i(t) u_j(t) \frac{dU_j^P(u_j(t), v_j(t), x_j(t), p_j)}{du_j(t)}, & i \neq j \end{cases} \\
\nabla_{v_j(t)} f_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}) &= \\
\begin{cases} u_i(t) [1 - u_i(t)] \frac{dU_i^P(u_i(t), v_i(t), x_i(t), p_i)}{dv_i(t)}, & i = j \\ -u_i(t) u_j(t) \frac{dU_j^P(u_j(t), v_j(t), x_j(t), p_j)}{dv_j(t)}, & i \neq j \end{cases} \quad (\text{A.7}) \\
\nabla_{x_j(t)} f_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}) &= \\
\begin{cases} u_i(t) [1 - u_i(t)] \frac{dU_i^P(u_i(t), v_i(t), x_i(t), p_i)}{dx_i(t)}, & i = j \\ -u_i(t) u_j(t) \frac{dU_j^P(u_j(t), v_j(t), x_j(t), p_j)}{dx_j(t)}, & i \neq j \end{cases}
\end{aligned}$$

$$\begin{aligned}
& \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \left| \frac{df_i(\mathbf{u}_j(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p})}{dz} \right|_{z=u_j(t)} \\
& \stackrel{(\text{A.7})}{=} \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \left\{ \begin{aligned} & \left| \underbrace{[1 - u_i(t)]}_{\leq 1} U_i^P(u_i(t), v_i(t), x_i(t), p_i) \right. \\ & \left. - \bar{U}_D^P(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}) + \underbrace{u_i(t) [1 - u_i(t)]}_{\leq \frac{1}{4}} \right|, \quad j = i \\ & \times \left| \left[\frac{dU_i^P(z, v_i(t), x_i(t), p_i)}{dz} \right]_{z=u_i(t)} \right| \\ & \left| - \underbrace{u_i(t) u_j(t)}_{\leq 1} \left[\frac{dU_j^P(z, v_j(t), x_j(t), p_j)}{dz} \right]_{z=u_j(t)} \right|, \quad j \neq i \end{aligned} \right. \quad (\text{A.8}) \\
& \leq \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \left\{ \begin{aligned} & \left| U_i^P(u_i(t), v_i(t), x_i(t), p_i) \right| \\ & + \left| \bar{U}_D^P(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}) \right| \\ & + \frac{1}{4} \left| \left[\frac{dU_i^P(z, v_i(t), x_i(t), p_i)}{dz} \right]_{z=u_i(t)} \right|, \quad j = i \\ & \left| \left[\frac{dU_j^P(z, v_j(t), x_j(t), p_j)}{dz} \right]_{z=u_j(t)} \right|, \quad j \neq i \end{aligned} \right. \\
& \leq \begin{cases} b^{U^P \mathbf{u}_i} + \sum_{k \in \mathcal{N}} b^{U^P \mathbf{u}_k} + \frac{1}{4} b^{dU^P \mathbf{u}_i}, & j = i, \\ b^{dU^P \mathbf{u}_j}, & j \neq i, \end{cases}
\end{aligned}$$

$$\begin{aligned}
& \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \left| \frac{df_i(\mathbf{u}(t), \mathbf{v}_{-j}(t), \mathbf{x}(t), \mathbf{p})}{dz} \right|_{z=v_j(t)} \\
& \stackrel{(A.7)}{=} \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \left\{ \left| \underbrace{u_i(t) [1 - u_i(t)]}_{\leq \frac{1}{4}} \left[\frac{dU_i^P(u_i(t), z, x_i(t), p_i)}{dz} \right]_{z=v_i(t)} \right|, j = i \right. \\
& \quad \left. \left| - \underbrace{u_i(t) u_j(t)}_{\leq 1} \left[\frac{dU_j^P(u_j(t), z, x_j(t), p_j)}{dz} \right]_{z=v_j(t)} \right|, j \neq i \right\} \\
& \leq \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \left\{ \begin{aligned} & \frac{1}{4} \left| \frac{dU_i^P(u_i(t), z, x_i(t), p_i)}{dz} \right|_{z=v_i(t)}, j = i \\ & \left| \frac{dU_j^P(u_j(t), z, x_j(t), p_j)}{dz} \right|_{z=v_j(t)}, j \neq i \end{aligned} \right\} \leq \begin{cases} \frac{1}{4} b^{dU^P d\mathbf{v}}_i, j = i, \\ b^{dU^P d\mathbf{v}}_j, j \neq i, \end{cases} \quad (A.9)
\end{aligned}$$

$$\begin{aligned}
& \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \left| \frac{df_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}_{-j}(t), \mathbf{p})}{dz} \right|_{z=x_j(t)} \\
& \stackrel{(A.7)}{=} \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \left\{ \left| \underbrace{u_i(t) [1 - u_i(t)]}_{\leq \frac{1}{4}} \left[\frac{dU_i^P(u_i(t), v_i(t), z, p_i)}{dz} \right]_{z=x_i(t)} \right|, j = i \right. \\
& \quad \left. \left| - \underbrace{u_i(t) u_j(t)}_{\leq 1} \left[\frac{dU_j^P(u_j(t), v_j(t), z, p_j)}{dz} \right]_{z=x_j(t)} \right|, j \neq i \right\} \\
& \leq \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \left\{ \begin{aligned} & \frac{1}{4} \left| \frac{dU_i^P(u_i(t), v_i(t), z, p_i)}{dz} \right|_{z=x_i(t)}, j = i \\ & \left| \frac{dU_j^P(u_j(t), v_j(t), z, p_j)}{dz} \right|_{z=x_j(t)}, j \neq i \end{aligned} \right\} \leq \begin{cases} \frac{1}{4} b^{dU^P d\mathbf{x}}_i, j = i, \\ b^{dU^P d\mathbf{x}}_j, j \neq i, \end{cases} \quad (A.10)
\end{aligned}$$

A.2 Proof of Theorem 3.3.2

Proof. According to Lemma 3.3.1, if we want to prove that the lower-level evolutionary subgame defined in (3.12) is uniquely solvable with any given $\mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}$, we need to ensure that

$$\begin{pmatrix} \mathbf{f}(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}) \\ \mathbf{g}(\mathbf{u}(t), \mathbf{v}(t)) \\ \mathbf{h}(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}) \end{pmatrix} \quad (A.15)$$

$$\begin{aligned}
& |\mathbf{f}(\tilde{\mathbf{u}}(t), \tilde{\mathbf{v}}(t), \tilde{\mathbf{x}}(t), \mathbf{p}) - \mathbf{f}(\hat{\mathbf{u}}(t), \hat{\mathbf{v}}(t), \hat{\mathbf{x}}(t), \mathbf{p})| \\
& \leq \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \sum_{i \in \mathcal{N}} \left| \left[\nabla_{[(\mathbf{u}(t))^\top, (\mathbf{v}(t))^\top, (\mathbf{x}(t))^\top]^\top} f_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p}) \right]^\top \right. \\
& \quad \times \left. \left([(\tilde{\mathbf{u}}(t))^\top, (\tilde{\mathbf{v}}(t))^\top, (\tilde{\mathbf{x}}(t))^\top]^\top - [(\hat{\mathbf{u}}(t))^\top, (\hat{\mathbf{v}}(t))^\top, (\hat{\mathbf{x}}(t))^\top]^\top \right) \right| \\
& = \max_{\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}(t)} \sum_{i \in \mathcal{N}} \left\{ \sum_{j \in \mathcal{N}} \left| \frac{df_i(\mathbf{u}_{-j}(t), \mathbf{v}(t), \mathbf{x}(t), \mathbf{p})}{dz} \right|_{z=u_j(t)} |\tilde{u}_j(t) - \hat{u}_j(t)| \right. \\
& \quad + \sum_{j \in \mathcal{N}} \left| \frac{df_i(\mathbf{u}(t), \mathbf{v}_{-j}(t), \mathbf{x}(t), \mathbf{p})}{dz} \right|_{z=v_j(t)} |\tilde{v}_j(t) - \hat{v}_j(t)| \\
& \quad \left. + \sum_{j \in \mathcal{N}} \left| \frac{df_i(\mathbf{u}(t), \mathbf{v}(t), \mathbf{x}_{-j}(t), \mathbf{p})}{dz} \right|_{z=x_j(t)} |\tilde{x}_j(t) - \hat{x}_j(t)| \right\} \\
& \stackrel{(A.6)(A.12)(A.14)}{\leq} \sum_{i \in \mathcal{N}} \left\{ \sum_{j \in \mathcal{N}} [M^{\text{dfdu}}_{ij} |\tilde{u}_j(t) - \hat{u}_j(t)| + M^{\text{dfdv}}_{ij} |\tilde{v}_j(t) - \hat{v}_j(t)| \right. \\
& \quad \left. + M^{\text{dfdxx}}_{ij} |\tilde{x}_j(t) - \hat{x}_j(t)| \right\} \tag{A.16} \\
& = \left| \begin{pmatrix} \mathbf{f}(\tilde{\mathbf{u}}(t), \tilde{\mathbf{v}}(t), \tilde{\mathbf{x}}(t), \mathbf{p}) \\ \mathbf{g}(\tilde{\mathbf{u}}(t), \tilde{\mathbf{v}}(t)) \\ \mathbf{h}(\tilde{\mathbf{u}}(t), \tilde{\mathbf{v}}(t), \tilde{\mathbf{x}}(t), \mathbf{p}) \end{pmatrix} - \begin{pmatrix} \mathbf{f}(\hat{\mathbf{u}}(t), \hat{\mathbf{v}}(t), \hat{\mathbf{x}}(t), \mathbf{p}) \\ \mathbf{g}(\hat{\mathbf{u}}(t), \hat{\mathbf{v}}(t)) \\ \mathbf{h}(\hat{\mathbf{u}}(t), \hat{\mathbf{v}}(t), \hat{\mathbf{x}}(t), \mathbf{p}) \end{pmatrix} \right| \\
& = |\mathbf{f}(\tilde{\mathbf{u}}(t), \tilde{\mathbf{v}}(t), \tilde{\mathbf{x}}(t), \mathbf{p}) - \mathbf{f}(\hat{\mathbf{u}}(t), \hat{\mathbf{v}}(t), \hat{\mathbf{x}}(t), \mathbf{p})| \\
& \quad + |\mathbf{g}(\tilde{\mathbf{u}}(t), \tilde{\mathbf{v}}(t)) - \mathbf{g}(\hat{\mathbf{u}}(t), \hat{\mathbf{v}}(t))| \\
& \quad + |\mathbf{h}(\tilde{\mathbf{u}}(t), \tilde{\mathbf{v}}(t), \tilde{\mathbf{x}}(t), \mathbf{p}) - \mathbf{h}(\hat{\mathbf{u}}(t), \hat{\mathbf{v}}(t), \hat{\mathbf{x}}(t), \mathbf{p})| \\
& \stackrel{(A.18)(A.19)(A.20)}{\leq} (M^{\mathbf{f}} + M^{\mathbf{g}} + M^{\mathbf{h}}) N \\
& \quad \times \left| [(\tilde{\mathbf{u}}(t))^\top, (\tilde{\mathbf{v}}(t))^\top, (\tilde{\mathbf{x}}(t))^\top]^\top - [(\hat{\mathbf{u}}(t))^\top, (\hat{\mathbf{v}}(t))^\top, (\hat{\mathbf{x}}(t))^\top]^\top \right|, \tag{A.17}
\end{aligned}$$

satisfies the Lipschitz condition with respect to $[(\mathbf{u}(t))^\top, (\mathbf{v}(t))^\top, (\mathbf{x}(t))^\top]^\top \in \mathcal{D}_{\mathbf{u}} \times \mathcal{D}_{\mathbf{v}} \times \mathcal{D}_{\mathbf{x}}, \forall \mathbf{p} = \mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}$.

Firstly, $\forall \mathbf{p} = \mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}, \forall \tilde{\mathbf{u}}(t), \hat{\mathbf{u}}(t) \in \mathcal{D}_{\mathbf{u}}, \forall \tilde{\mathbf{v}}(t), \hat{\mathbf{v}}(t) \in \mathcal{D}_{\mathbf{v}}, \forall \tilde{\mathbf{x}}(t), \hat{\mathbf{x}}(t) \in \mathcal{D}_{\mathbf{x}}$, we have (A.16) and define $M^{\mathbf{f}} = \max_{i,j \in \mathcal{N}} \{M^{\text{dfdu}}_{ij}, M^{\text{dfdv}}_{ij}, M^{\text{dfdxx}}_{ij}\}$ be a positive

finite real number, then we have the following inequality equation

$$\begin{aligned}
& |\mathbf{f}(\tilde{\mathbf{u}}(t), \tilde{\mathbf{v}}(t), \tilde{\mathbf{x}}(t), \mathbf{p}) - \mathbf{f}(\hat{\mathbf{u}}(t), \hat{\mathbf{v}}(t), \hat{\mathbf{x}}(t), \mathbf{p})| \\
& \leq M^{\mathbf{f}} \sum_{i \in \mathcal{N}} \left\{ \sum_{j \in \mathcal{N}} [|\tilde{u}_j(t) - \hat{u}_j(t)| + |\tilde{v}_j(t) - \hat{v}_j(t)| + |\tilde{x}_j(t) - \hat{x}_j(t)|] \right\} \\
& = NM^{\mathbf{f}} \left| \left[(\tilde{\mathbf{u}}(t))^{\top}, (\tilde{\mathbf{v}}(t))^{\top}, (\tilde{\mathbf{x}}(t))^{\top} \right]^{\top} - \left[(\hat{\mathbf{u}}(t))^{\top}, (\hat{\mathbf{v}}(t))^{\top}, (\hat{\mathbf{x}}(t))^{\top} \right]^{\top} \right|.
\end{aligned} \tag{A.18}$$

Next, similar to (A.16) and (A.18), with any given $\mathbf{p} = \mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}$, we have

$$\begin{aligned}
& |\mathbf{g}(\tilde{\mathbf{u}}(t), \tilde{\mathbf{v}}(t)) - \mathbf{g}(\hat{\mathbf{u}}(t), \hat{\mathbf{v}}(t))| \\
& \leq NM^{\mathbf{g}} \left| \left[(\tilde{\mathbf{u}}(t))^{\top}, (\tilde{\mathbf{v}}(t))^{\top} \right]^{\top} - \left[(\hat{\mathbf{u}}(t))^{\top}, (\hat{\mathbf{v}}(t))^{\top} \right]^{\top} \right|,
\end{aligned} \tag{A.19}$$

and

$$\begin{aligned}
& |\mathbf{h}(\tilde{\mathbf{u}}(t), \tilde{\mathbf{v}}(t), \tilde{\mathbf{x}}(t), \mathbf{p}) - \mathbf{h}(\hat{\mathbf{u}}(t), \hat{\mathbf{v}}(t), \hat{\mathbf{x}}(t), \mathbf{p})| \\
& \leq NM^{\mathbf{h}} \left| \left[(\tilde{\mathbf{u}}(t))^{\top}, (\tilde{\mathbf{v}}(t))^{\top}, (\tilde{\mathbf{x}}(t))^{\top} \right]^{\top} - \left[(\hat{\mathbf{u}}(t))^{\top}, (\hat{\mathbf{v}}(t))^{\top}, (\hat{\mathbf{x}}(t))^{\top} \right]^{\top} \right|,
\end{aligned} \tag{A.20}$$

for all $\left[(\tilde{\mathbf{u}}(t))^{\top}, (\tilde{\mathbf{v}}(t))^{\top}, (\tilde{\mathbf{x}}(t))^{\top} \right]^{\top}, \left[(\hat{\mathbf{u}}(t))^{\top}, (\hat{\mathbf{v}}(t))^{\top}, (\hat{\mathbf{x}}(t))^{\top} \right]^{\top} \in \mathcal{D}_{\mathbf{u}} \times \mathcal{D}_{\mathbf{v}} \times \mathcal{D}_{\mathbf{x}}$, where $M^{\mathbf{h}} = \max_{i,j \in \mathcal{N}} \{M^{\text{dfdu}}_{ij}, M^{\text{dfdv}}_{ij}, M^{\text{dfdx}}_{ij}\}$ and $M^{\mathbf{g}} = \max_{i,j \in \mathcal{N}} \{M^{\text{dgdu}}_{ij}, M^{\text{dgdv}}_{ij}\}$ are positive finite valued real numbers.

At last, we prove that the condition in (A.15) satisfies the Lipschitz condition. $\forall \left[(\tilde{\mathbf{u}}(t))^{\top}, (\tilde{\mathbf{v}}(t))^{\top}, (\tilde{\mathbf{x}}(t))^{\top} \right]^{\top}, \left[(\hat{\mathbf{u}}(t))^{\top}, (\hat{\mathbf{v}}(t))^{\top}, (\hat{\mathbf{x}}(t))^{\top} \right]^{\top} \in \mathcal{D}_{\mathbf{u}} \times \mathcal{D}_{\mathbf{v}} \times \mathcal{D}_{\mathbf{x}}, \mathbf{p} = \mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}$, we can derive (A.17) in which $(M^{\mathbf{f}} + M^{\mathbf{g}} + M^{\mathbf{h}})N$ is a positive finite real number. Therefore, the condition in (A.15) satisfies the Lipschitz condition with respect to $\left[(\mathbf{u}(t))^{\top}, (\mathbf{v}(t))^{\top}, (\mathbf{x}(t))^{\top} \right]^{\top} \in \mathcal{D}_{\mathbf{u}} \times \mathcal{D}_{\mathbf{v}} \times \mathcal{D}_{\mathbf{x}}$, and hence the lower-level evolutionary subgame defined in (3.12) is uniquely solvable and thus admits a unique evolutionary equilibrium. The proof is completed. $\square$

Appendix B

Proofs for Chapter 4

B.1 Proof of Theorem 4.2.3

Proof. Substituting the second partial derivatives of Π_P in (4.25), the Hessian matrix of the blockchain provider's payoff is

$$\mathbf{H}_P = \begin{bmatrix} \frac{\partial^2 \Pi_P}{\partial \mathbf{p}^2} & \frac{\partial^2 \Pi_P}{\partial \mathbf{p} \partial \bar{h}} \\ \frac{\partial^2 \Pi_P}{\partial \bar{h} \partial \mathbf{p}} & \frac{\partial^2 \Pi_P}{\partial \bar{h}^2} \end{bmatrix} = \begin{bmatrix} -(\mathbf{I} - \alpha \mathbf{G})^{-1} & (\mathbf{I} - \alpha \mathbf{G})^{-1} \mathbf{1} \\ \mathbf{1}^\top (\mathbf{I} - \alpha \mathbf{G})^{-1} & -\frac{2a}{(1 - \bar{h})^3} \end{bmatrix}. \quad (\text{B.1})$$

We can partition the Hessian matrix in (B.1) into two matrices as follows:

$$\begin{aligned} \mathbf{H}_P &= \underbrace{\begin{bmatrix} -(\mathbf{I} - \alpha \mathbf{G})^{-1} & (\mathbf{I} - \alpha \mathbf{G})^{-1} \mathbf{1} \\ \mathbf{1}^\top (\mathbf{I} - \alpha \mathbf{G})^{-1} & -\frac{a}{(1 - \bar{h})^3} \end{bmatrix}}_{\mathbf{H}_{P_1}} + \underbrace{\begin{bmatrix} \mathbf{O} & \mathbf{0} \\ \mathbf{0}^\top & -\frac{a}{(1 - \bar{h})^3} \end{bmatrix}}_{\mathbf{H}_{P_2}} \\ &= \mathbf{H}_{P_1} + \mathbf{H}_{P_2}, \end{aligned} \quad (\text{B.2})$$

where $\mathbf{H}_{P_2}$ is obviously a negative semidefinite matrix.

Let $\mathbf{Q}_P = \begin{bmatrix} \mathbf{I} & \mathbf{1} \\ \mathbf{0}^\top & 1 \end{bmatrix}$. The congruent matrix of $\mathbf{H}_{P_1}$ is:

$$\mathbf{Q}_P^\top \mathbf{H}_{P_1} \mathbf{Q}_P = \begin{bmatrix} -(\mathbf{I} - \alpha \mathbf{G})^{-1} & \mathbf{0} \\ \mathbf{0}^\top & -\frac{a}{(1 - \bar{h})^3} + \mathbf{1}^\top (\mathbf{I} - \alpha \mathbf{G})^{-1} \mathbf{1} \end{bmatrix}. \quad (\text{B.3})$$

Therefore, the negative definiteness of $\mathbf{H}_{P_1}$ depends on the negative definiteness of (B.3). According to the proof of Theorem 4.2.1, all the eigenvalues of $(\mathbf{I} - \alpha\mathbf{G})^{-1}$ belong to $(0, 1)$. This means that $-(\mathbf{I} - \alpha\mathbf{G})^{-1}$ in (B.3) is a negative definite matrix. We know that the domain of $\bar{h}$ is $[\frac{1}{2}, 1)$, and the inequality equation in (B.4) will be satisfied.

$$\begin{aligned} & -\frac{a}{(1-\bar{h})^3} + \mathbf{1}^\top (\mathbf{I} - \alpha\mathbf{G})^{-1} \mathbf{1} < -\frac{a}{(1-\frac{1}{2})^3} + \mathbf{1}^\top (\mathbf{I} - \alpha\mathbf{G})^{-1} \mathbf{1} \\ & = -8a + \mathbf{1}^\top (\mathbf{I} - \alpha\mathbf{G})^{-1} \mathbf{1}. \end{aligned} \tag{B.4}$$

$-8a + \mathbf{1}^\top (\mathbf{I} - \alpha\mathbf{G})^{-1} \mathbf{1} < 0$ is satisfied according to Theorem 4.2.3 and hence the second block in (B.3), i.e., $-\frac{a}{(1-\bar{h})^3} + \mathbf{1}^\top (\mathbf{I} - \alpha\mathbf{G})^{-1} \mathbf{1}$, is also negative. With the two negative definite blocks on the diagonal positions and zero blocks on the off-diagonal positions, the matrix in (B.3) is a negative definite matrix. Therefore, $\mathbf{H}_{P_1}$ is a negative definite matrix. Then, as the sum of one negative definite matrix and one negative semidefinite matrix, i.e., $\mathbf{H}_{P_1}$ and $\mathbf{H}_{P_2}$, respectively, the Hessian matrix $\mathbf{H}_P$ in (B.1) is a negative definite matrix. Therefore, Π_P is a strictly concave function of $[\mathbf{p}^\top, \bar{h}]^\top$.

In what follows, we prove that Π_I is also a concave function of its own decision variable γ . Recall the second partial derivative of Π_I on γ in (4.25) as follows:

$$\begin{aligned}
\frac{\partial^2 \Pi_I}{\partial \gamma^2} &= \frac{2}{\gamma^3} \frac{T}{T_0} N_T q \int_{1/2}^1 \left[1 - \int_{1/2}^t P(\theta) d\theta \right]^{1/\gamma} \ln \left[1 - \int_{1/2}^t P(\theta) d\theta \right] dt \\
&\quad + \frac{1}{\gamma^4} \frac{T}{T_0} N_T q \int_{1/2}^1 \left[1 - \int_{1/2}^t P(\theta) d\theta \right]^{1/\gamma} \ln^2 \left[1 - \int_{1/2}^t P(\theta) d\theta \right] dt \\
&\quad - \left(\bar{h} - \frac{1}{2} \right)^3 [\beta(\beta+1)\gamma^{\beta-1} - \beta(\beta-1)\gamma^{\beta-2}] \\
&= \frac{1}{\gamma^3} \frac{T}{T_0} N_T q \underbrace{\int_{1/2}^1 \left[1 - \int_{1/2}^t P(\theta) d\theta \right]^{1/\gamma}}_{>0} \underbrace{\ln \left[1 - \int_{1/2}^t P(\theta) d\theta \right]}_{<0} dt \\
&\quad + \frac{1}{\gamma^3} \frac{T}{T_0} N_T q \underbrace{\int_{1/2}^1 \left[1 - \int_{1/2}^t P(\theta) d\theta \right]^{1/\gamma}}_{>0} \underbrace{\ln \left[1 - \int_{1/2}^t P(\theta) d\theta \right]}_{<0} dt \\
&\quad \times \left\{ 1 + \frac{1}{\gamma} \ln \left[1 - \int_{1/2}^t P(\theta) d\theta \right] \right\} dt \\
&\quad - \underbrace{\left(\bar{h} - \frac{1}{2} \right)^3}_{>0} \underbrace{[(\beta+1)\gamma - (\beta-1)]}_{>0} \beta \gamma^{\beta-2}.
\end{aligned} \tag{B.5}$$

To ensure the concavity of Π_I with respect to γ , we need the following inequality to be satisfied:

$$\left\{ 1 + \frac{1}{\gamma} \ln \left[1 - \int_{1/2}^t P(\theta) d\theta \right] \right\} \geq 0. \tag{B.6}$$

From (B.6), we have

$$\begin{aligned}
&\left\{ 1 + \frac{1}{\gamma} \ln \left[1 - \int_{1/2}^t P(\theta) d\theta \right] \right\} \geq 0 \\
&\Leftrightarrow \frac{1}{\gamma} \ln \left[1 - \int_{1/2}^t P(\theta) d\theta \right] \geq -1 \\
&\Leftrightarrow \frac{1}{\gamma} \ln \left[1 - \int_{1/2}^t P(\theta) d\theta \right] \geq \frac{1}{\gamma} \ln \left[\int_0^1 P(\theta) d\theta - \int_{1/2}^1 P(\theta) d\theta \right] \geq -1 \\
&\Rightarrow \frac{1}{\gamma} \ln \left[\int_0^{1/2} P(\theta) d\theta \right] \geq -1 \Leftrightarrow \frac{1}{\gamma} \ln \frac{1}{2} \geq -1 \Leftrightarrow \gamma \geq \ln 2
\end{aligned} \tag{B.7}$$

From (B.7) we learn that the sufficient condition to ensure the inequality in (B.6) is $\gamma \geq \ln 2$. Such a condition holds on $(1, \gamma^u]$. Therefore, Π_I is a concave function on γ . Then, the profit functions of the blockchain provider and the cyber-insurer, i.e.,

$$\mathbf{J} = \begin{bmatrix} \frac{\partial^2 \Pi_p}{\partial \mathbf{p}^2} & \frac{\partial^2 \Pi_p}{\partial \mathbf{p} \partial \bar{h}} & \frac{\partial^2 \Pi_p}{\partial \mathbf{p} \partial \gamma} \\ \frac{\partial^2 \Pi_p}{\partial \bar{h} \partial \mathbf{p}} & \frac{\partial^2 \Pi_p}{\partial \bar{h}^2} & \frac{\partial^2 \Pi_p}{\partial \bar{h} \partial \gamma} \\ \frac{\partial^2 \Pi_I}{\partial \gamma \partial \mathbf{p}} & \frac{\partial^2 \Pi_I}{\partial \gamma \partial \bar{h}} & \frac{\partial^2 \Pi_I}{\partial \gamma^2} \end{bmatrix} + \begin{bmatrix} \frac{\partial^2 \Pi_p}{\partial \mathbf{p}^2} & \frac{\partial^2 \Pi_p}{\partial \mathbf{p} \partial \bar{h}} & \frac{\partial^2 \Pi_p}{\partial \mathbf{p} \partial \gamma} \\ \frac{\partial^2 \Pi_p}{\partial \bar{h} \partial \mathbf{p}} & \frac{\partial^2 \Pi_p}{\partial \bar{h}^2} & \frac{\partial^2 \Pi_p}{\partial \bar{h} \partial \gamma} \\ \frac{\partial^2 \Pi_I}{\partial \gamma \partial \mathbf{p}} & \frac{\partial^2 \Pi_I}{\partial \gamma \partial \bar{h}} & \frac{\partial^2 \Pi_I}{\partial \gamma^2} \end{bmatrix}^\top \quad (\text{B.8})$$

$$= \begin{bmatrix} 2 \frac{\partial^2 \Pi_p}{\partial \mathbf{p}^2} & \frac{\partial^2 \Pi_p}{\partial \mathbf{p} \partial \bar{h}} + \left(\frac{\partial^2 \Pi_p}{\partial \bar{h} \partial \mathbf{p}} \right)^\top & \frac{\partial^2 \Pi_p}{\partial \mathbf{p} \partial \gamma} + \left(\frac{\partial^2 \Pi_I}{\partial \gamma \partial \mathbf{p}} \right)^\top \\ \frac{\partial^2 \Pi_p}{\partial \bar{h} \partial \mathbf{p}} + \left(\frac{\partial^2 \Pi_p}{\partial \mathbf{p} \partial \bar{h}} \right)^\top & 2 \frac{\partial^2 \Pi_p}{\partial \bar{h}^2} & \frac{\partial^2 \Pi_p}{\partial \bar{h} \partial \gamma} + \frac{\partial^2 \Pi_I}{\partial \gamma \partial \bar{h}} \\ \frac{\partial^2 \Pi_I}{\partial \gamma \partial \mathbf{p}} + \left(\frac{\partial^2 \Pi_p}{\partial \mathbf{p} \partial \gamma} \right)^\top & \frac{\partial^2 \Pi_I}{\partial \gamma \partial \bar{h}} + \frac{\partial^2 \Pi_p}{\partial \bar{h} \partial \gamma} & 2 \frac{\partial^2 \Pi_I}{\partial \gamma^2} \end{bmatrix}$$

$$= \begin{bmatrix} -2(\mathbf{I} - \alpha \mathbf{G})^{-1} & 2(\mathbf{I} - \alpha \mathbf{G})^{-1} \mathbf{1} & -3 \left(\bar{h} - \frac{1}{2} \right)^2 \\ 2\mathbf{1}^\top (\mathbf{I} - \alpha \mathbf{G})^{-1} & -\frac{4a}{(1-\bar{h})^3} & \times \left[(\beta + 1) \gamma^\beta - \beta \gamma^{\beta-1} \right] \\ \mathbf{0}^\top & -3 \left(\bar{h} - \frac{1}{2} \right)^2 & \frac{4}{\gamma^3} \frac{T}{T_0} N_T q \int_{1/2}^1 \left[1 - \int_{1/2}^t P(\theta) d\theta \right]^{1/\gamma} \ln \left[1 - \int_{1/2}^t P(\theta) d\theta \right] dt \\ & \times \left[(\beta + 1) \gamma^\beta - \beta \gamma^{\beta-1} \right] & + \frac{2}{\gamma^4} \frac{T}{T_0} N_T q \int_{1/2}^1 \left[1 - \int_{1/2}^t P(\theta) d\theta \right]^{1/\gamma} \ln \left[1 - \int_{1/2}^t P(\theta) d\theta \right] dt \\ & -2 \left(\bar{h} - \frac{1}{2} \right)^3 \left[\beta (\beta + 1) \gamma^{\beta-1} - \beta (\beta - 1) \gamma^{\beta-2} \right] \end{bmatrix}. \quad (\text{B.9})$$

Π_p and Π_I , are concave with respect to their own decision variables, i.e., $[\mathbf{p}^\top, \bar{h}]^\top$ and γ , respectively. According to [129], the NE in the leader-level game $\mathcal{G}_L$ exists hence the Stackbelberg equilibrium exists. The proof is completed. $\square$

B.2 Proof of Theorem 4.2.4

Proof. According to Theorem 3.1 (Rosen's Theorem) in [127], the uniqueness of the NE in $\mathcal{G}_L$ holds if the Jacobian matrix constructed from the profit functions of the two players, i.e., $\mathbf{J}$ given in (B.8), is negative definite. After substituting the relevant second partial derivatives given in (4.25) into (B.8), we are able to rewrite (B.8) as in (B.9).

Then, we partition the Jacobian matrix (B.8) into two matrices as shown in (B.10).

In $\mathbf{J}_1$ given by (B.10), we have $\begin{bmatrix} -2(\mathbf{I} - \alpha \mathbf{G})^{-1} & 2(\mathbf{I} - \alpha \mathbf{G})^{-1} \mathbf{1} \\ 2\mathbf{1}^\top (\mathbf{I} - \alpha \mathbf{G})^{-1} & -\frac{2a}{(1-\bar{h})^3} \end{bmatrix} = 2\mathbf{H}_{P_1}$, where $\mathbf{H}_{P_1}$ is the matrix in (B.2). As shown in the proof to Theorem 4.2.3, $\mathbf{H}_{P_1}$ is a negative definite matrix, and thus the first block in the matrix $\mathbf{J}_1$ of (B.10), i.e.,

positions, $\mathbf{J}_1$ in (B.10) is a negative definite matrix.

After defining

$$\mathbf{R}_1 = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0}^\top & 1 & \times \left\{ -2 \left(\bar{h} - \frac{1}{2} \right)^3 \right\}^{-1} \\ \mathbf{0}^\top & 0 & 1 \end{bmatrix}, \quad (\text{B.13})$$

we can obtain the congruent matrix of $\mathbf{J}_2$ in (B.10) as shown in (B.11). In (B.11), we observe that $-2 \left(\bar{h} - \frac{1}{2} \right)^3 [(\beta + 1) \gamma - (\beta - 1)] \beta \gamma^{\beta-2} < 0$. Then, to ensure the negative semidefiniteness of $\mathbf{J}_2$, we need the following inequality to hold:

$$-\frac{2a}{(1 - \bar{h})^3} + \frac{9 \left(\bar{h} - \frac{1}{2} \right)^4 [(\beta + 1) \gamma^\beta - \beta \gamma^{\beta-1}]^2}{2 \left(\bar{h} - \frac{1}{2} \right)^3 [\beta (\beta + 1) \gamma^{\beta-1} - \beta (\beta - 1) \gamma^{\beta-2}]} \leq 0. \quad (\text{B.14})$$

Then, we can determine the upper bound for (B.14) as follows:

$$\begin{aligned} & -\frac{2a}{(1 - \bar{h})^3} + \frac{9 \left(\bar{h} - \frac{1}{2} \right)^4 [(\beta + 1) \gamma^\beta - \beta \gamma^{\beta-1}]^2}{2 \left(\bar{h} - \frac{1}{2} \right)^3 [\beta (\beta + 1) \gamma^{\beta-1} - \beta (\beta - 1) \gamma^{\beta-2}]} \\ &= -\frac{2a}{(1 - \bar{h})^3} + \frac{9 \left(\bar{h} - \frac{1}{2} \right) [(\beta + 1) \gamma - \beta]^2 \gamma^\beta}{2 [\beta (\beta + 1) \gamma - \beta (\beta - 1)]} \\ &< -\frac{2a}{(1 - \bar{h})^3} + \frac{9 \left(\bar{h} - \frac{1}{2} \right) (\beta + 1)^2 \gamma^{\beta+2}}{2 [\beta (\beta + 1) \gamma - \beta (\beta - 1)]} \\ &< -\frac{2a}{(1 - \bar{h})^3} + \frac{9 \left(\bar{h} - \frac{1}{2} \right) (\beta + 1)^2 \gamma^{\beta+2}}{2 [\beta (\beta + 1) \gamma - \beta (\beta - 1) \gamma]} \\ &= -\frac{2a}{(1 - \bar{h})^3} + \frac{9 \left(\bar{h} - \frac{1}{2} \right) (\beta + 1)^2 \gamma^{\beta+2}}{2 \beta \gamma (\beta + 1 - \beta + 1)} \\ &= -\frac{2a}{(1 - \bar{h})^3} + \frac{9 \left(\bar{h} - \frac{1}{2} \right) (\beta + 1)^2 \gamma^{\beta+1}}{4 \beta} \end{aligned} \quad (\text{B.15})$$

Since $\bar{h} \in [\frac{1}{2}, 1)$, the last equation in (B.15), i.e., $-\frac{2a}{(1 - \bar{h})^3} + \frac{9 \left(\bar{h} - \frac{1}{2} \right) (\beta + 1)^2 \gamma^{\beta+1}}{4 \beta}$, is

smaller than $-\frac{2a}{(1-\frac{1}{2})^3} + \frac{9(1-\frac{1}{2})(\beta+1)^2\gamma^{\beta+1}}{4\beta} = -16a + \frac{9(\beta+1)^2(\gamma^u)^{\beta+1}}{8\beta}$. $-16a + \frac{9(\beta+1)^2(\gamma^u)^{\beta+1}}{8\beta} < 0$ is satisfied according to Theorem 4.2.4 and hence the matrix in (B.11) has zero and negative definite blocks on its diagonal positions and zero blocks on the off-diagonal positions. This means that the matrix (B.11) is a negative semidefinite matrix. Since $\mathbf{J}_2$ is congruent with the matrix (B.11), $\mathbf{J}_2$ is also a negative semidefinite matrix.

To summarize, as the sum of a negative definite matrix $\mathbf{J}_1$ and a negative semidefinite matrix $\mathbf{J}_2$, the Jacobian matrix in (B.8), i.e., $\mathbf{J}$, is a negative definite matrix. Thus, the NE in the leader-level noncooperative subgame $\mathcal{G}_L$ is unique and the Stackbelberg equilibrium is unique. The proof is completed. $\square$

Appendix C

Proofs for Chapter 5

C.1 Proof of Theorem 5.2.4

Proof. Firstly, the decision vectors including prices and security levels, $\left[\mathbf{p}^A, q^A\right]^\top$ and $\left[\mathbf{p}^B, q^B\right]^\top$ belong to nonempty, convex, and compact sets, $\mathcal{D}^A \subset \mathbb{R}^{|\mathcal{N}|+1}$ and $\mathcal{D}^B \subset \mathbb{R}^{|\mathcal{N}|+1}$, respectively. The Hessian matrix of the profit function for the CSSV-A is

$$\begin{bmatrix} -2\mathbf{K} & \mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) \\ (\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K} & 2n\lambda\mathbf{1}^\top \mathbf{K} \mathbf{a} - z^{A''} \end{bmatrix}. \quad (\text{C.1})$$

To obtain the congruent matrix of (C.1), we respectively left and right multiply it by $\begin{bmatrix} \Phi & \mathbf{0} \\ \frac{1}{2}(\mathbf{a} + n\lambda\mathbf{1})^\top & 1 \end{bmatrix}$ and $\begin{bmatrix} \Phi & \frac{1}{2}(\mathbf{a} + n\lambda\mathbf{1}) \\ \mathbf{0}^\top & 1 \end{bmatrix}$. Correspondingly, the congruent matrix of (C.1) is

$$\begin{bmatrix} -2\mathbf{K} & \mathbf{0} \\ \mathbf{0} & \frac{1}{2} \left(-2z^{A''} + (\mathbf{a} + n\lambda\mathbf{1})^\top \mathbf{K} (\mathbf{a} + n\lambda\mathbf{1}) \right) \end{bmatrix}. \quad (\text{C.2})$$

The determinants for the first $|\mathcal{N}|$ leading principal minors of (C.2) are negative because of the positive definiteness of $\mathbf{K}$ as proven in Lemma 5.2.1. Regarding the last element in (C.2), as we have $\frac{1}{2} \left(-2z^{A''} + (\mathbf{a} + n\lambda\mathbf{1})^\top \mathbf{K} (\mathbf{a} + n\lambda\mathbf{1}) \right) < \frac{1}{2} \left(-z^{A''} + (\mathbf{a} + n\lambda\mathbf{1})^\top \mathbf{K} (\mathbf{a} + n\lambda\mathbf{1}) \right)$, it is definitely less than 0 according to Theorem 5.2.4. That means Π^A is a strictly concave function on $\left[\mathbf{p}^A, q^A\right]^\top$. The property that Π^B is a strictly concave function on $\left[\mathbf{p}^B, q^B\right]^\top$ can be proven in a

$$\begin{aligned}
\frac{\partial^2 \Pi^A}{\partial \mathbf{p}^{A^2}} &= \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^{B^2}} = -2\mathbf{K}, & \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial \mathbf{p}^B} &= \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^A \partial \mathbf{p}^B} = \mathbf{K}, \\
\frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial q^A} &= \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial q^B} = \mathbf{K}(\mathbf{a} - n\lambda \mathbf{1}), & \frac{\partial^2 \Pi^A}{\partial q^{A^2}} &= 2n\lambda \mathbf{1}^\top \mathbf{K} \mathbf{a} - z^{A''}, \\
\frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial q^B} &= \frac{\partial^2 \Pi^B}{\partial q^A \partial \mathbf{p}^B} = -\mathbf{K} \mathbf{a}, & \frac{\partial^2 \Pi^A}{\partial q^A \partial \mathbf{p}^B} &= \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^A \partial q^B} = n\lambda \mathbf{K} \mathbf{1}, \\
\frac{\partial^2 \Pi^A}{\partial q^A \partial q^B} &= \frac{\partial^2 \Pi^B}{\partial q^A \partial q^B} = -n\lambda \mathbf{1}^\top \mathbf{K} \mathbf{a}, & \frac{\partial^2 \Pi^B}{\partial q^{B^2}} &= 2n\lambda \mathbf{1}^\top \mathbf{K} \mathbf{a} - z^{B''},
\end{aligned} \tag{C.3}$$

$$\begin{aligned}
& \begin{bmatrix} \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^{A^2}} & \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial q^A} & \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial \mathbf{p}^B} & \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial q^B} \\ \left(\frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial q^A} \right)^\top & \frac{\partial^2 \Pi^A}{\partial q^{A^2}} & \left(\frac{\partial^2 \Pi^A}{\partial q^A \partial \mathbf{p}^B} \right)^\top & \frac{\partial^2 \Pi^A}{\partial q^A \partial q^B} \\ \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial \mathbf{p}^A} & \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial q^A} & \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^{B^2}} & \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial q^B} \\ \left(\frac{\partial^2 \Pi^B}{\partial \mathbf{p}^A \partial q^B} \right)^\top & \frac{\partial^2 \Pi^B}{\partial q^A \partial q^B} & \left(\frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial q^B} \right)^\top & \frac{\partial^2 \Pi^B}{\partial q^{B^2}} \end{bmatrix} \\
& + \begin{bmatrix} \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^{A^2}} & \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial q^A} & \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial \mathbf{p}^B} & \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial q^B} \\ \left(\frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial q^A} \right)^\top & \frac{\partial^2 \Pi^A}{\partial q^{A^2}} & \left(\frac{\partial^2 \Pi^A}{\partial q^A \partial \mathbf{p}^B} \right)^\top & \frac{\partial^2 \Pi^A}{\partial q^A \partial q^B} \\ \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial \mathbf{p}^A} & \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial q^A} & \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^{B^2}} & \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial q^B} \\ \left(\frac{\partial^2 \Pi^B}{\partial \mathbf{p}^A \partial q^B} \right)^\top & \frac{\partial^2 \Pi^B}{\partial q^A \partial q^B} & \left(\frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial q^B} \right)^\top & \frac{\partial^2 \Pi^B}{\partial q^{B^2}} \end{bmatrix}^\top \\
& = \begin{bmatrix} 2 \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^{A^2}} & 2 \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial q^A} & \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial \mathbf{p}^B} + \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial \mathbf{p}^A} & \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial q^B} + \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial q^A} \\ 2 \left(\frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial q^A} \right)^\top & 2 \frac{\partial^2 \Pi^A}{\partial q^{A^2}} & \left(\frac{\partial^2 \Pi^A}{\partial q^A \partial \mathbf{p}^B} + \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial q^A} \right)^\top & \frac{\partial^2 \Pi^A}{\partial q^A \partial q^B} + \frac{\partial^2 \Pi^B}{\partial q^A \partial q^B} \\ \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial \mathbf{p}^A} + \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial \mathbf{p}^B} & \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial q^A} + \frac{\partial^2 \Pi^A}{\partial q^A \partial \mathbf{p}^B} & 2 \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^{B^2}} & 2 \frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial q^B} \\ \left(\frac{\partial^2 \Pi^B}{\partial \mathbf{p}^A \partial q^B} + \frac{\partial^2 \Pi^A}{\partial \mathbf{p}^A \partial q^B} \right)^\top & \frac{\partial^2 \Pi^B}{\partial q^A \partial q^B} + \frac{\partial^2 \Pi^A}{\partial q^A \partial q^B} & 2 \left(\frac{\partial^2 \Pi^B}{\partial \mathbf{p}^B \partial q^B} \right)^\top & 2 \frac{\partial^2 \Pi^B}{\partial q^{B^2}} \end{bmatrix} \tag{C.4} \\
& \begin{bmatrix} -4\mathbf{K} & 2\mathbf{K}(\mathbf{a} - n\lambda \mathbf{1}) & 2\mathbf{K} & \mathbf{K}(n\lambda \mathbf{1} - \mathbf{a}) \\ 2(\mathbf{a} - n\lambda \mathbf{1})^\top \mathbf{K} & 4n\lambda \mathbf{1}^\top \mathbf{K} \mathbf{a} - 2z^{A''} & (n\lambda \mathbf{1} - \mathbf{a})^\top \mathbf{K} & -2n\lambda \mathbf{1}^\top \mathbf{K} \mathbf{a} \\ 2\mathbf{K} & \mathbf{K}(n\lambda \mathbf{1} - \mathbf{a}) & -4\mathbf{K} & 2\mathbf{K}(\mathbf{a} - n\lambda \mathbf{1}) \\ (n\lambda \mathbf{1} - \mathbf{a})^\top \mathbf{K} & -2n\lambda \mathbf{1}^\top \mathbf{K} \mathbf{a} & 2(\mathbf{a} - n\lambda \mathbf{1})^\top \mathbf{K} & 4n\lambda \mathbf{1}^\top \mathbf{K} \mathbf{a} - 2z^{B''} \end{bmatrix} \tag{C.5}
\end{aligned}$$

similar way. Hence, in the CSSV-level game $\mathcal{G}_C$, there is at least one NE based on [128], [129]. $\square$

C.2 Proof of Theorem 5.2.5

Proof. We recall the Jacobian matrix to prove the uniqueness of the NE of the CSSV-level game $\mathcal{G}_C$. The Jacobian matrix of the profit functions of $\mathcal{G}_C$ is shown in (C.4).

We substitute the specific formulation of these second partial derivatives into the Jacobian matrix in (C.4) and obtain the specific Jacobian matrix in (C.5).

There are two cases, i.e., $z^{A''} \geq z^{B''}$ and $z^{B''} > z^{A''}$, to prove that the Jacobian matrix of the profit functions of the CSSV-level game $\mathcal{G}_C$ in (C.5) is negative definite.

- $z^{B''} > z^{A''}$:

Let $\Phi_{|\mathcal{N}|+1} \in \mathbb{R}^{(|\mathcal{N}|+1) \times (|\mathcal{N}|+1)}$ be the identity matrix, we multiply the right and left sides of (C.5) by

$$\begin{bmatrix} \Phi_{|\mathcal{N}|+1} & \mathbf{0} \\ \frac{\Phi_{|\mathcal{N}|+1}}{2} & \Phi_{|\mathcal{N}|+1} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \Phi_{|\mathcal{N}|+1} & \mathbf{0} \\ \frac{\Phi_{|\mathcal{N}|+1}}{2} & \Phi_{|\mathcal{N}|+1} \end{bmatrix}^\top, \quad (\text{C.6})$$

respectively. The congruent matrix of (C.5) is shown in (C.9), which can be decomposed into three symmetric matrices as shown in (C.10).

For the first matrix of (C.10), the condition to hold its negative semi-definiteness is that the nonzero block, i.e., $\begin{bmatrix} -4\mathbf{K} & 2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) \\ 2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K} & (4n\lambda\mathbf{1}^\top \mathbf{K} \mathbf{a} - z^{A''}) - 3z^{B''} \end{bmatrix}$, is negative definite. Since $\mathbf{K}$ is a positive definite matrix as proven in Lemma 5.2.1, which means the determinants of the first $|\mathcal{N}|$ leading principal minors of this nonzero block are negative. We need to guarantee that the determinant of the $|\mathcal{N}| + 1$ -th leading principal minor of this nonzero block is negative, which has been shown in (C.11).

The first equality in (C.11) uses the fact that $z^{B''} > 0$, and we can definitely hold the second inequality in (C.11) based on Theorem 5.2.5.

As for the second matrix in (C.10), diagonally dominant is satisfied for the opposite matrix of it when $z^{B''} > z^{A''}$, and hence it is negative semi-definite.

At last, the third matrix in (C.10) consists of two nonzero blocks on its diagonal positions, which are the matrices expressed as follows:

$$2 \begin{bmatrix} -4\mathbf{K} & 2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) \\ 2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K} & 4n\lambda\mathbf{1}^\top \mathbf{K} \mathbf{a} - z^{A''} \end{bmatrix} \quad (\text{C.7})$$

and

$$\begin{bmatrix} -4\mathbf{K} & 2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) \\ 2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K} & 4n\lambda\mathbf{1}^\top \mathbf{K} \mathbf{a} - z^{A''} \end{bmatrix}, \quad (\text{C.8})$$

$$\begin{bmatrix} -4\mathbf{K} & 2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) & \mathbf{0} & \mathbf{0} \\ 2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K} & 4n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - 2z^{A''} & \mathbf{0} & -z^{A''} \\ \mathbf{0} & \mathbf{0} & -3\mathbf{K} & \frac{3}{2}\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) \\ \mathbf{0} & -z^{A''} & \frac{3}{2}(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K} & 3n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - \frac{z^{A''}}{2} - 2z^{B''} \end{bmatrix} \quad (\text{C.9})$$

$$\begin{aligned} &= \frac{1}{4} \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & -4\mathbf{K} & 2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) \\ \mathbf{0} & \mathbf{0} & 2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K} & (4n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - z^{A''}) - 3z^{B''} \end{bmatrix} + \frac{1}{2} \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & -z^{A''} & \mathbf{0} & -z^{A''} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & -z^{A''} & \mathbf{0} & -z^{B''} \end{bmatrix} \\ &+ \frac{1}{2} \begin{bmatrix} -2 \times 4\mathbf{K} & 2[2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1})] & \mathbf{0} & \mathbf{0} \\ 2[2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K}] & 2(4n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - z^{A''}) & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & -4\mathbf{K} & 2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) \\ \mathbf{0} & \mathbf{0} & 2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K} & 4n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - z^{A''} \end{bmatrix} \quad (\text{C.10}) \end{aligned}$$

$$\begin{aligned} & \left(4n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - z^{A''} \right) - 3z^{B''} - 2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K}(-4\mathbf{K})^{-1}2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) \\ & < \left(4n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - z^{A''} \right) - 2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K}(-4\mathbf{K})^{-1}2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) \quad (\text{C.11}) \\ & = \left(4n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - z^{A''} \right) + (\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) \\ & = (\mathbf{a} + n\lambda\mathbf{1})^\top \mathbf{K}(\mathbf{a} + n\lambda\mathbf{1}) - z^{A''} < 0 \end{aligned}$$

where the negative definiteness of the matrix in (C.7) depends on the negative definiteness of the matrix (C.8). Since $\mathbf{K}$ is a positive definite matrix as proven in Lemma 5.2.1, this means that all the determinants of the first $|\mathcal{N}|$ leading principal minors of the matrix in (C.8) are negative. The determinant of the $|\mathcal{N}| + 1$ -th leading principal minor of the matrix (C.8) is $(\mathbf{a} + n\lambda\mathbf{1})^\top \mathbf{K}(\mathbf{a} + n\lambda\mathbf{1}) - z^{A''}$, which is definitely less than 0 according to Theorem 5.2.5. Therefore, we can conclude that the matrix in (C.9), i.e., the congruent matrix for the Jacobian matrix of the profit functions of the CSSV-level noncooperative game $\mathcal{G}_C$ given in (C.5), is negative definite in this case. Note that the matrix in (C.9) is the sum of the two negative semi-definite matrices and one negative definite matrix. Therefore, the Jacobian matrix of the profit functions of the CSSV-level game is negative definite in this case.

$$\begin{aligned}
& \begin{bmatrix} -3\mathbf{K} & \frac{3}{2}\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) & \mathbf{0} & \mathbf{0} \\ \frac{3}{2}(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K} & 3n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - \frac{z^{B''}}{2} - 2z^{A''} & \mathbf{0} & -z^{B''} \\ \mathbf{0} & \mathbf{0} & -4\mathbf{K} & 2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) \\ \mathbf{0} & -z^{B''} & 2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K} & 4n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - 2z^{B''} \end{bmatrix} \\
& \quad (C.13) \\
& = \frac{1}{4} \begin{bmatrix} -4\mathbf{K} & 2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) & \mathbf{0} & \mathbf{0} \\ 2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K} & (4n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - z^{B''}) - 3z^{A''} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix} + \frac{1}{2} \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & -z^{A''} & \mathbf{0} & -z^{B''} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & -z^{B''} & \mathbf{0} & -z^{B''} \end{bmatrix} \\
& + \frac{1}{2} \begin{bmatrix} -4\mathbf{K} & 2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) & \mathbf{0} & \mathbf{0} \\ 2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K} & 4n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - z^{B''} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & -2 \times 4\mathbf{K} & 2[2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1})] \\ \mathbf{0} & \mathbf{0} & 2[2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K}] & 2(4n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - z^{B''}) \end{bmatrix} \\
& \quad (C.14)
\end{aligned}$$

- $z^{A''} \geq z^{B''}$:

We multiply the right and left sides of (C.5) by

$$\begin{bmatrix} \Phi_{|\mathcal{N}|+1} & \frac{\Phi_{|\mathcal{N}|+1}}{2} \\ \mathbf{0} & \Phi_{|\mathcal{N}|+1} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \Phi_{|\mathcal{N}|+1} & \frac{\Phi_{|\mathcal{N}|+1}}{2} \\ \mathbf{0} & \Phi_{|\mathcal{N}|+1} \end{bmatrix}^\top, \quad (C.12)$$

respectively. The congruent matrix of (C.5) is shown in (C.13), which can be decomposed into three symmetric matrices as shown in (C.14).

For the first matrix of (C.14), the condition to hold its negative semi-definiteness is similar to that for the first matrix of (C.10), $(4n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - z^{B''}) - 3z^{A''} - 2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K}(-4\mathbf{K})^{-1} \times 2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) < (\mathbf{a} + n\lambda\mathbf{1})^\top \mathbf{K}(\mathbf{a} + n\lambda\mathbf{1}) - z^{B''} < 0$, which can be satisfied by Theorem 5.2.5.

The opposite matrix of the second matrix in (C.14) is diagonally dominant according to $z^{A''} \geq z^{B''}$, which means that the second matrix in (C.14) is negative semi-definite.

Note that the blocks

$$2 \begin{bmatrix} -4\mathbf{K} & 2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) \\ 2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K} & 4n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - z^{B''} \end{bmatrix} \quad (C.15)$$

and

$$\begin{bmatrix} -4\mathbf{K} & 2\mathbf{K}(\mathbf{a} - n\lambda\mathbf{1}) \\ 2(\mathbf{a} - n\lambda\mathbf{1})^\top \mathbf{K} & 4n\lambda\mathbf{1}^\top \mathbf{K}\mathbf{a} - z^{A''} \end{bmatrix} \quad (C.16)$$

on the diagonal positions of the last matrix in (C.14) are negative definite matrices based on Theorem 5.2.5, and the matrix with only two negative definite nonzero blocks on its diagonal positions is negative definite. Hence, the last matrix in (C.14) is negative definite. Therefore, the matrix in (C.13) is negative definite, which is the sum of two negative semi-definite matrices and one negative definite matrix. Hence, the Jacobian matrix of the profit functions of the CSSV-level game $\mathcal{G}_C$ in (C.5) is negative definite in this case, which is congruent with (C.13).

In conclusion, the negative definiteness of the Jacobian matrix in (C.5) is validated. This indicates that the CSSV-level noncooperative game $\mathcal{G}_C$ admits one unique NE according to Theorem 3.1 (Rosen) in [127], which further demonstrates the uniqueness of the Stackelberg equilibrium. This completes the proof. $\square$

List of Author's Awards, Patents, and Publications¹

Book Chapter

- **S. Feng**, “Application of Game theory in Internet of Things”, in Game Theory for Next Generation Wireless and Communication Networks: Modeling, Analysis, and Design, Cambridge University Press, 2019.

Journal Articles

Articles Related to Thesis

- **S. Feng**, Z. Xiong, D. Niyato, and P. Wang, “Dynamic Resource Management to Defend Against Advanced Persistent Threats in Fog Computing: A Game Theoretic Approach,” **Accepted by** IEEE Transactions on Cloud Computing, pp. 1–1, 2019.
- **S. Feng**, W. Wang, Z. Xiong, D. Niyato, P. Wang, and S. S. Wang, “On Cyber Risk Management of Blockchain Networks: A Game Theoretic Approach,” **Accepted by** IEEE Transactions on Services Computing, pp. 1–1, 2018.
- **S. Feng**, Z. Xiong, D. Niyato, P. Wang, S. S. Wang, and S. X. Shen, “Joint Pricing and Security Investment in Cloud Security Service Market with User Interdependency,” **Accepted by** IEEE Transactions on Services Computing, pp. 1–1, 2020.

¹The superscript * indicates joint first authors

Articles not Related to Thesis

- **S. Feng**, D. Niyato, X. Lu, P. Wang, and D. I. Kim, "Dynamic Model for Network Selection in Next Generation HetNets with Memory-affecting Rational Users," **Accepted by** IEEE Transactions on Mobile Computing, 2019.
- **S. Feng**, D. Niyato, X. Lu, P. Wang, and D. I. Kim, "Dynamic Game and Pricing for Data Sponsored 5G Systems with Memory Effect," **Accepted by** IEEE Journal on Selected Areas in Communications, 2020.
- **S. Feng**, Z. Xiong, D. Niyato, P. Wang, Z. Han, and D. I. Kim, "Joint Traffic Routing and Virtualized Security Function Activation in Wireless Multihop Networks," **Accepted by** IEEE Transactions on Vehicular Technology, pp. 1–1, 2019.
- X. Lu, E. Hossain, T. Shafique, **S. Feng**, H. Jiang, and D. Niyato, "Intelligent reflecting surface (IRS)-enabled covert communications in wireless networks," **Accepted by** IEEE Network Magazine, pp. 1–1, 2020.
- Z. Xiong, **S. Feng**, D. Niyato, P. Wang, A. Leshem, and Z. Han, "Joint Sponsored and Edge Caching Content Service Market: A Game-Theoretic Approach," **Published in** IEEE Transactions on Wireless Communications, vol. 18, no. 2, pp. 1166–1181, Feb. 2019.
- Z. Xiong, **S. Feng**, W. Wang, D. Niyato, P. Wang, and Z. Han, "Cloud/Fog Computing Resource Management and Pricing for Blockchain Networks," **Published in** IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4585–4600, Jun. 2018.
- X. Gao, **S. Feng**, D. Niyato, P. Wang, K. Yang, and Y.-C. Liang, "Dynamic Access Point and Service Selection in Backscatter-Assisted RF-Powered Cognitive Networks," **Accepted by** IEEE Internet of Things Journal, pp. 1–1, 2019.
- Y. Jiao, P. Wang, **S. Feng**, and D. Niyato, "Profit Maximization Mechanism and Data Management for Data Analytics Services," **Published in** IEEE Internet of Things Journal, vol. 5, no. 3, pp. 2001–2014, Jun. 2018.

Conference Proceedings

Articles Related to Thesis

- **S. Feng**, Z. Xiong, D. Niyato, P. Wang, S. S. Wang, and Y. Zhang, "Cyber Risk Management with Risk Aware Cyber-Insurance in Blockchain Networks," **Published in** 2018 IEEE Global Communications Conference (GLOBECOM), Dec. 2018.
- **S. Feng**, Z. Xiong, D. Niyato, P. Wang, and A. Leshem, "Evolving Risk Management Against Advanced Persistent Threats in Fog Computing," **Published in** 2018 IEEE 7th International Conference on Cloud Networking (CloudNet), Oct. 2018.
- **S. Feng**, Z. Xiong, D. Niyato, P. Wang, and S. S. Wang, "Joint pricing and security investment for cloud-insurance: A security interdependency perspective," **Published in** 2018 IEEE Wireless Communications and Networking Conference (WCNC), Apr. 2018.

Articles not Related to Thesis

- **S. Feng**, Z. Xiong, D. Niyato, and P. Wang, "Competitive Security Pricing in Cyber-Insurance Market: A Game-Theoretic Analysis," **Published in** 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Aug. 2018.
- Z. Xiong, **S. Feng**, D. Niyato, P. Wang, and Z. Han, "Optimal Pricing-Based Edge Computing Resource Management in Mobile Blockchain," **Published in** 2018 IEEE International Conference on Communications (ICC), May 2018.
- Z. Xiong, **S. Feng**, D. Niyato, P. Wang, and Y. Zhang, "Competition and cooperation analysis for data sponsored market: A network effects model," **Published in** 2018 IEEE Wireless Communications and Networking Conference (WCNC), Apr. 2018.
- Z. Xiong, **S. Feng**, D. Niyato, P. Wang, and Y. Zhang, "Economic Analysis of Network Effects on Sponsored Content: A Hierarchical Game Theoretic Approach," **Published in** 2017 IEEE Global Communications Conference (GLOBECOM), Dec. 2017.

- Z. Xiong, **S. Feng**, D. Niyato, P. Wang, and Z. Han, “Network Effect-Based Sequential Dynamic Pricing for Mobile Social Data Market,” **Published in** 2017 IEEE Global Communications Conference (GLOBECOM), Dec. 2017.
- Y. Jiao, P. Wang, D. Niyato, M. Abu Alsheikh, and **S. Feng**, “Profit Maximization Auction and Data Management in Big Data Markets,” **Published in** 2017 IEEE Wireless Communications and Networking Conference (WCNC), Mar. 2017.

Bibliography

- [1] Outpost24. Top 10 of the world’s largest cyberattacks. <https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks>, 2018. 1, 2
- [2] Heng Yin, Dawn Song, Manuel Egele, Christopher Kruegel, and Engin Kirda. Panorama: capturing system-wide information flow for malware detection and analysis. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 116–127. ACM, 2007. 2
- [3] Brian M Bowen, Shlomo HersHKop, Angelos D Keromytis, and Salvatore J Stolfo. Baiting inside attackers using decoy documents. In *International Conference on Security and Privacy in Communication Systems*, pages 51–70. Springer, 2009. 2
- [4] Angelica Marotta, Fabio Martinelli, Stefano Nanni, Albina Orlando, and Artsiom Yautsiukhin. Cyber-insurance survey. *Computer Science Review*, 24:35–61, 2017. 3, 20
- [5] Shanhe Yi, Zijiang Hao, Zhengrui Qin, and Qun Li. Fog computing: Platform and applications. In *Hot Topics in Web Systems and Technologies (HotWeb), 2015 Third IEEE Workshop on*, pages 73–78. IEEE, 2015. 4
- [6] Saad Khan, Simon Parkinson, and Yongrui Qin. Fog computing security: a review of current applications and security solutions. *Journal of Cloud Computing*, 6(1):19, 2017. 4
- [7] J Vukalović and D Delija. Advanced persistent threats-detection and defense. In *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on*, pages 1324–1330. IEEE, 2015. 4
- [8] Trend Micro. Healthcare provider hit by advanced persistent threat: Protecting client information. <https://blog.trendmicro.com/healthcare-provider-hit-advanced-persistent-threat-protecting-client-information/>, 2014. 4
- [9] David Higgins. The growing challenge of advanced persistent threats. <https://www.cso.com.au/article/603403/growing-challenge-advanced-persistent-threats/>, 2016. 5

- [10] Maggie McGrath. Target profit falls 46% on credit card breach and the hits could keep on coming. <https://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/#1d0dd38d7326>, 2014. 5
- [11] Josh Fruhlinger. What is stuxnet, who created it and how does it work? <https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html>, 2017. 5
- [12] Ming Zhang, Zizhan Zheng, and Ness 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. 5
- [13] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Başar, and Jean-Pierre Hubaux. Game theory meets network security and privacy. *ACM Computing Surveys (CSUR)*, 45(3):25, 2013. 5
- [14] Saranya Chandran, P Hrudya, and Prabakaran Poornachandran. An efficient classification model for detecting advanced persistent threat. In *Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on*, pages 2001–2009. IEEE, 2015. 5
- [15] Minghui Min, Liang Xiao, Caixia Xie, Mohammad Hajimirsadeghi, and Narayan B Mandayam. Defense against advanced persistent threats in dynamic cloud storage: A colonel blotto game approach. *arXiv preprint arXiv:1801.06270*, 2018. 6, 20, 32
- [16] D. T. T. Anh, M. Zhang, B. C. Ooi, and G. Chen. Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering*, PP(99):1–1, 2018. ISSN 1041-4347. doi: 10.1109/TKDE.2017.2781227. 7, 9, 10, 21, 22, 54
- [17] Massimo Bartoletti and Livio Pompianu. An empirical analysis of smart contracts: platforms, applications, and design patterns. *arXiv preprint arXiv:1703.06322*, 2017. 7
- [18] H. Kopp, D. Mödinger, F. Hauck, F. Kargl, and C. Bösch. Design of a privacy-preserving decentralized file storage with financial incentives. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, Paris, France, 2017. 7
- [19] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki. A novel blockchain-based product ownership management system (poms) for anti-counterfeits in the post supply chain. *IEEE Access*, 5:17465–17477, 2017. doi: 10.1109/ACCESS.2017.2720760. 7
- [20] J. Zou, b. ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li. A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services.

- IEEE Transactions on Services Computing*, pages 1–1, 2018. ISSN 1939-1374. doi: 10.1109/TSC.2018.2823705. 7
- [21] Mauro Conti, Chhagan Lal, Sushmita Ruj, et al. A survey on security and privacy issues of bitcoin. *arXiv preprint arXiv:1706.00916*, 2017. 7
- [22] Ghassan O. Karame, Elli Androulaki, and Srdjan Capkun. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security, CCS '12*, pages 906–917, Raleigh, NC, USA, October 2012. ACM. ISBN 978-1-4503-1651-4. doi: 10.1145/2382196.2382292. 7
- [23] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics*, PP(99):1–1, 2017. ISSN 1551-3203. doi: 10.1109/TII.2017.2786307. 7
- [24] X. Huang, C. Xu, P. Wang, and H. Liu. Lnscc: A security model for electric vehicle and charging pile management based on blockchain ecosystem. *IEEE Access*, PP(99):1–1, 2018. doi: 10.1109/ACCESS.2018.2812176. 7
- [25] K. Kotobi and S. G. Bilén. Blockchain-enabled spectrum access in cognitive radio networks. In *2017 Wireless Telecommunications Symposium (WTS)*, pages 1–6, April 2017. doi: 10.1109/WTS.2017.7943523. 7
- [26] L. Ghiro, L. Maccari, and R. L. Cigno. Proof of networking: Can blockchains boost the next generation of distributed networks? In *2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, pages 29–32, February 2018. doi: 10.23919/WONS.2018.8311658. 7
- [27] Wenbo Wang, Dusit Niyato, Ping Wang, and Amir Leshem. Decentralized caching for content delivery based on blockchain: A game theoretic perspective. In *IEEE ICC 2018 Next Generation Networking and Internet Symposium*, Kansas City, USA, May 2018. 7
- [28] AWS. Aws blockchain partners. <https://aws.amazon.com/cn/partners/blockchain/>. 9
- [29] Guowen Xu, Hongwei Li, Sen Liu, Mi Wen, and Rongxing Lu. Efficient and privacy-preserving truth discovery in mobile crowd sensing systems. *IEEE Transactions on Vehicular Technology*, 68(4):3854–3865, 2019. 10
- [30] CALYPTIX. Top 5 risks of cloud computing. <https://www.calyptix.com/research-2/top-5-risks-of-cloud-computing/>. 10
- [31] IBM security. Cloud security. <https://www.ibm.com/security/saas>. 10, 11
- [32] Oracle Cloud Security. Cloud security: A reason to move to cloud. <https://www.oracle.com/security/index.html>. 10, 11, 80, 82

- [33] Alessandro Piva, Franco Bartolini, and Mauro Barni. Ieee internet computing: Issue addendum - managing copyright: Watermark and cryptography algorithms. *IEEE Distributed Systems Online*, 3(5), 2002. 10
- [34] Ross Anderson and Tyler Moore. Information security economics—and beyond. In *Annual International Cryptology Conference*, pages 68–91. Springer, August 2007, USA. 10
- [35] Marc Lelarge and Jean Bolot. Economic incentives to increase security in the internet: The case for insurance. In *INFOCOM*, pages 1494–1502. IEEE, April 2009, Brazil. 10
- [36] McAfee. Net losses: Estimating the global cost of cybercrime. Technical report, Center for Strategic and International Studies, Economic Impact of Cybercrime II, Jun, 2014. 10
- [37] Identity Theft Resource Center and CyberScout. Identity theft resource center data breach reports. <http://www.idtheftcenter.org/2016databreaches.html>. 10
- [38] Ranjan Pal, Leana Golubchik, Konstantinos Psounis, and Pan Hui. On a way to improve cyber-insurer profits when a security vendor becomes the cyber-insurer. In *IFIP Networking Conference, 2013*, pages 1–9. IEEE, 2013. 10, 11
- [39] Parinaz Naghizadeh and Mingyan Liu. Opting out of incentive mechanisms: A study of security as a non-excludable public good. *IEEE Transactions on Information Forensics and Security*, 11(12):2790–2803, 2016.
- [40] Xiao Lu, Dusit Niyato, Hai Jiang, Ping Wang, and H Vincent Poor. Cyber insurance for heterogeneous wireless networks. *arXiv preprint arXiv:1709.07198*, 2017. 10
- [41] TechTarget. cloud insurance. <http://searchcloudstorage.techtarget.com/definition/cloud-insurance>. 10
- [42] Ranjan Pal, Leana Golubchik, Konstantinos Psounis, and Pan Hui. Security pricing as enabler of cyber-insurance a first look at differentiated pricing markets. *IEEE Transactions on Dependable and Secure Computing*, March 2017. 11, 82, 83
- [43] Shaun Wang. Premium calculation by transforming the layer premium density. *ASTIN Bulletin: The Journal of the IAA*, 26(1):71–92, 1996. 12, 23, 56
- [44] Xiaowen Gong, Lingjie Duan, Xu Chen, and Junshan Zhang. When social network effect meets congestion effect in wireless networks: Data usage equilibrium and optimal pricing. *IEEE Journal on Selected Areas in Communications*, 35(2):449–462, 2017. 14, 57, 82

- [45] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Y. Zhang. Economic analysis of network effects on sponsored content: A hierarchical game theoretic approach. In *2017 IEEE Global Communications Conference*, pages 1–6, Singapore, December 2017. doi: 10.1109/GLOCOM.2017.8254738. [14](#), [57](#)
- [46] Zhou Su, Qichao Xu, Jun Luo, Huayan Pu, Yan Peng, and Rongxing Lu. A secure content caching scheme for disaster backup in fog computing enabled mobile social networks. *IEEE Transactions on Industrial Informatics*, 14(10):4579–4589, 2018. [17](#)
- [47] Yuan Wu, Kuanyang Guo, Jianwei Huang, and Xuemin Sherman Shen. Secrecy-based energy-efficient data offloading via dual connectivity over unlicensed spectrums. *IEEE Journal on Selected Areas in Communications*, 34(12):3252–3270, 2016. [17](#)
- [48] Prosanta Gope and Biplab Sikdar. An efficient data aggregation scheme for privacy-friendly dynamic pricing-based billing and demand-response management in smart grids. *IEEE Internet of Things Journal*, 2018. [18](#)
- [49] Zhou Su and Qichao Xu. Security-aware resource allocation for mobile social big data: A matching-coalitional game solution. *IEEE Transactions on Big Data*, (1):1–1, 2017. [18](#)
- [50] Jeffrey Dwoskin, Dahai Xu, Jianwei Huang, Mung Chiang, and Ruby Lee. Secure key management architecture against sensor-node fabrication attacks. In *Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE*, pages 166–171. IEEE, 2007. [18](#)
- [51] Lingjie Duan, Alexander W Min, Jianwei Huang, and Kang G Shin. Attack prevention for collaborative spectrum sensing in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 30(9):1658–1665, 2012. [18](#)
- [52] Lingjie Duan, Jianwei Huang, and Biying Shou. Economics of femtocell service provision. *Journal of Economics*, 12(11):2261–2273, 2013. [18](#)
- [53] Qian Ma, Lin Gao, Ya-Feng Liu, and Jianwei Huang. Economic analysis of crowdsourced wireless community networks. *IEEE Transactions on Mobile Computing*, 16(7):1856–1869, 2017. [18](#)
- [54] Dijk Marten, Juels Ari, Oprea Alina, and L. Rivest Ronald. Flipit: The game of “stealthy takeover”. In *Journal of Cryptology*, pages 655–713. ACM, 2013. [19](#)
- [55] Xiaotao Feng, Zizhan Zheng, Pengfei Hu, Derya Cansever, and Prasant Mohapatra. Stealthy attacks meets insider threats: a three-player game model. In *Military Communications Conference, MILCOM 2015-2015 IEEE*, pages 25–30. IEEE, 2015. [19](#)

- [56] Sadegh Farhang and Jens Grossklags. Flipleakage: a game-theoretic approach to protect against stealthy attackers in the presence of information leakage. In *International Conference on Decision and Game Theory for Security*, pages 195–214. Springer, 2016. [19](#)
- [57] Shaohan Feng, Zehui Xiong, Dusit Niyato, Ping Wang, and Shaun Shuxun Wang. Joint pricing and security investment for cloud-insurance: A security interdependency perspective. In *Accepted by Wireless Communications and Networking Conference (WCNC)*. IEEE, 2018. [19](#), [22](#)
- [58] AIG. Cyber insurance. <https://www.aig.com.sg/business/business-products-and-services/financial-lines/cyber-insurance0>, 2018. [19](#), [35](#)
- [59] B Filkins. Quantifying risk: Closing the chasm between cybersecurity and cyber insurance. *SANS Institute InfoSec Reading Room, Tech. Rep., Mar*, 2016. [19](#)
- [60] Tridib Bandyopadhyay. Organizational adoption of cyber insurance instruments in it security risk management: a modeling approach. *Proceedings. Paper*, 5, 2012. [20](#)
- [61] Rui Zhang, Quanyan Zhu, and Yezekael Hayel. A bi-level game approach to attack-aware cyber insurance of computer networks. *IEEE Journal on Selected Areas in Communications*, 35(3):779–794, 2017. [20](#), [69](#)
- [62] Sivadon Chaisiri, Ryan KL Ko, and Dusit Niyato. A joint optimization approach to security-as-a-service allocation and cyber insurance management. In *Trustcom/BigDataSE/ISPA, 2015 IEEE*, volume 1, pages 426–433. IEEE, 2015. [20](#)
- [63] Zichao Yang and John CS Lui. Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation*, 74: 1–17, 2014. [20](#)
- [64] J. Chase, D. Niyato, P. Wang, S. Chaisiri, and R. K. L. Ko. A scalable approach to joint cyber insurance and security-as-a-service provisioning in cloud computing. *IEEE Transactions on Dependable and Secure Computing*, 16(4): 565–579, July 2019. ISSN 2160-9209. doi: 10.1109/TDSC.2017.2703626. [20](#)
- [65] F. Tschorsch and B. Scheuermann. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys Tutorials*, 18(3):2084–2123, third quarter 2016. ISSN 1553-877X. doi: 10.1109/COMST.2016.2535718. [21](#)
- [66] J Leon Zhao, Shaokun Fan, and Jiaqi Yan. Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*, 2(1):28, 2016. [21](#)

- [67] K. Christidis and M. Devetsikiotis. Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303, May 2016. ISSN 2169-3536. doi: 10.1109/ACCESS.2016.2566339. 21
- [68] Huaiqing Wang, Kun Chen, and Dongming Xu. A maturity model for blockchain adoption. *Financial Innovation*, 2(1):12, 2016. 21
- [69] Shetty Sachin, A. Kamhoua Charles, and L. Njilla Laurent. Blockchain for distributed systems security. <https://www.wiley.com/en-us/Blockchain+for+Distributed+Systems+Security-p-9781119519621>, 2019. 21
- [70] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In *Advances in Cryptology - EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Part II*, pages 281–310, Sofia, Bulgaria, April 2015. ISBN 978-3-662-46803-6. doi: 10.1007/978-3-662-46803-6_10. 22
- [71] Angelica Marotta, Fabio Martinelli, Stefano Nanni, Albina Orlando, and Artsiom Yautsiukhin. Cyber-insurance survey. *Computer Science Review*, 24:35 – 61, 2017. ISSN 1574-0137. doi: <https://doi.org/10.1016/j.cosrev.2017.01.001>. URL <http://www.sciencedirect.com/science/article/pii/S1574013716301137>. 22
- [72] Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse. Bitcoin-ng: A scalable blockchain protocol. In *NSDI*, pages 45–59, 2016. 23
- [73] Meni Rosenfeld. Analysis of hashrate-based double spending. *arXiv preprint arXiv:1402.2009*, 2014. 23, 54
- [74] Cyril Grunspan and Ricardo Pérez-Marco. Double spend races. *arXiv preprint arXiv:1702.02867*, 2017. 23, 54, 55
- [75] Shaun Wang. Insurance pricing and increased limits ratemaking by proportional hazards transforms. *Insurance: Mathematics and Economics*, 17(1): 43–54, 1995. 23
- [76] Dieter Denneberg. Premium calculation: Why standard deviation should be replaced by absolute deviation. *ASTIN Bulletin: The Journal of the IAA*, 20(2):181–190, 1990. 23
- [77] Shaun S Wang. A class of distortion operators for pricing financial and insurance risks. *Journal of risk and insurance*, pages 15–36, 2000. 23
- [78] João Manuel Andrade e Silva and Maria de Lourdes Centeno. Comparing risk adjusted premiums from the reinsurance point of view. *ASTIN Bulletin: The Journal of the IAA*, 28(2):221–239, 1998. 23
- [79] Antonella Campana. Risk adjusted premiums for excess of loss reinsurance with reinstatements. *Forthcoming on Mathematical Methods in Economics and Finance*, 2010. 24

- [80] Rongxing Lu, Xiaodong Lin, Xiaohui Liang, and Xuemin Shen. Secure provenance: the essential of bread and butter of data forensics in cloud computing. In *Proceedings of the 5th acm symposium on information, computer and communications security*, pages 282–292, 2010. [24](#)
- [81] Miranda Mowbray and Siani Pearson. A client-based privacy manager for cloud computing. In *Proceedings of the fourth international ICST conference on COMmunication system softWARE and middlewaRE*, pages 1–8, 2009. [24](#)
- [82] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, and Peng Ning. Managing security of virtual machine images in a cloud environment. In *Proceedings of the 2009 ACM workshop on Cloud computing security*, pages 91–96, 2009. [24](#)
- [83] Lawrence A Gordon and Martin P Loeb. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):438–457, 2002. [24](#)
- [84] Shaun Wang. Optimal level and allocation of cybersecurity spending: Model and formula. *Available at SSRN 3010029*, 2017. [25](#), [78](#), [81](#)
- [85] Yichuan Wang, Jianfeng Ma, Liumei Zhang, Wenjiang Ji, Di Lu, and Xinhong Hei. Dynamic game model of botnet ddos attack and defense. *Security and Communication Networks*, 9(16):3127–3140, 2016. [26](#)
- [86] Animesh Patcha and J-M Park. A game theoretic approach to modeling intrusion detection in mobile ad hoc networks. In *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004.*, pages 280–284. IEEE, 2004. [26](#)
- [87] Cui Xiaolin, Tan Xiaobin, Zhang Yong, and Xi Hongsheng. A markov game theory-based risk assessment model for network information system. In *2008 International Conference on Computer Science and Software Engineering*, volume 3, pages 1057–1061. IEEE, 2008. [26](#)
- [88] Ondřej Vaněk, Zhengyu Yin, Manish Jain, Branislav Bošanský, Milind Tambe, and Michal Pěchouček. Game-theoretic resource allocation for malicious packet detection in computer networks. In *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems-Volume 2*, pages 905–912. International Foundation for Autonomous Agents and Multiagent Systems, 2012. [26](#)
- [89] Damián Fernández-Cerero, Alejandro Fernández-Montes, Agnieszka Jakobik, and Joanna Kolodziej. Stackelberg game-based models in energy-aware cloud scheduling. In *ECMS*, pages 460–467, 2018. [27](#)
- [90] Xin Kang, Rui Zhang, and Mehul Motani. Price-based resource allocation for spectrum-sharing femtocell networks: A stackelberg game approach. *IEEE Journal on Selected areas in Communications*, 30(3):538–549, 2012. [27](#)

- [91] AIG. Cyberedge. <https://www.aig.com/business/insurance/cyber-insurance>. 27
- [92] CHUBB. Cyber enterprise risk management. <https://www2.chubb.com/uk-en/business/by-category-computer-risks-cyber-enterprise-risk-management.aspx>. 27
- [93] Beazley. Beazley breach response (bbr). https://www.beazley.com/usa/specialty_lines/professional_liability/technology_media_and_business_services/beazley_breach_response.html. 27
- [94] AIG. Cyberedge. <https://www.aig.com/content/dam/aig/america-canada/us/documents/microsites/appetite-guides/aig-cyberedge-appetite.pdf>, 2017. 27
- [95] CHUBB. Cyber insurance. <https://www.chubb.com/sg-en/business/cyber-insurance.aspx>, 2019. 27
- [96] Mike Donovan. Beautifully designed cyber insurance for a dangerous world. https://www.beazley.com/usa/cyber_and_executive_risk/cyber_and_tech/beazley_breach_response.html, 2019. 28
- [97] Mohammad Mahdi Khalili, Parinaz Naghizadeh, and Mingyan Liu. Embracing risk dependency in designing cyber-insurance contracts. In *Communication, Control, and Computing (Allerton), 2017 55th Annual Allerton Conference on*, pages 926–933. IEEE, 2017. 32
- [98] Skaperdas Stergios. Contest success functions. In *Economic Theory*, pages 283–290. Springer, 1996. 33
- [99] Andrey Garnaev, Melike Baykal-Gursoy, and H Vincent Poor. Security games with unknown adversarial strategies. *IEEE transactions on cybernetics*, 46(10):2291–2299, 2016. 33
- [100] Gordon Tullock. Efficient rent seeking. In *Efficient Rent-Seeking*, pages 3–16. Springer, 2001. 33
- [101] Joseph Alfred Kazenas. System and method for providing financial products for a deductible portion of an insurance policy, January 28 2014. US Patent 8,639,535. 34
- [102] Frederick van der Ploeg. Economic policy rules for risk-sensitive decision making. *IEEE Transactions on Mobile Computing*, 44:207–235, 1984. 34
- [103] Hans U Gerber and Gérard Pafum. Utility functions: from risk theory to finance. *North American Actuarial Journal*, 2(3):74–91, 1998. 34
- [104] Paul Emms and Steven Haberman. Pricing general insurance using optimal control theory. *ASTIN Bulletin: The Journal of the IAA*, 35(2):427–453, 2005. 36

- [105] Hailiang Yang and Lihong Zhang. Optimal investment for insurer with jump-diffusion risk process. *Insurance: Mathematics and Economics*, 37(3):615–634, 2005.
- [106] Kristen S Moore and Virginia R Young. Optimal insurance in a continuous-time model. *Insurance: Mathematics and Economics*, 39(1):47–68, 2006. [36](#)
- [107] William H Sandholm. Potential games with continuous player sets. *Journal of Economic theory*, 97(1):81–108, 2001. [38](#)
- [108] Acemoglu Daron and Ozdaglar Asu. Repeated games and cooperation. <https://economics.mit.edu/files/4754>, 2009. [39](#)
- [109] Dimitri P Bertsekas, Dimitri P Bertsekas, Dimitri P Bertsekas, and Dimitri P Bertsekas. *Dynamic programming and optimal control*, volume 1. Athena scientific Belmont, MA, 2005. [40](#)
- [110] Encyclopedia of Mathematics. Cauchy-lipschitz theorem. https://www.encyclopediaofmath.org/index.php/Cauchy-Lipschitz_theorem. [40](#)
- [111] Shankar Sastry. Lyapunov stability theory. In *Nonlinear Systems*, pages 182–234. Springer, 1999. [42](#)
- [112] Hans Wilhelm Alt. *Lineare Funktionalanalysis: Eine anwendungsorientierte Einführung*. Springer-Verlag, 2012. [44](#)
- [113] Ghassan O Karame, Elli Androulaki, and Srdjan Capkun. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 906–917. ACM, 2012. [54](#)
- [114] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. bitcoin, 2009. [55](#)
- [115] Francis Bloch and Nicolas Quérou. Pricing in social networks. *Games and economic behavior*, 80:243–261, 2013. [57](#), [61](#), [63](#), [69](#)
- [116] Francis Bloch, Garance Genicot, and Debraj Ray. Informal insurance in social networks. *Journal of Economic Theory*, 143(1):36–58, 2008. [59](#)
- [117] Alp Simsek, Asuman Ozdaglar, and Daron Acemoglu. On the uniqueness of solutions for nonlinear and mixed complementarity problems. Technical report, Massachusetts Institute of Technology, 2005. [63](#)
- [118] Abraham Berman and Robert J Plemmons. *Nonnegative matrices in the mathematical sciences*. SIAM, 1994. [64](#)
- [119] Martin J Osborne. *An introduction to game theory*, volume 3. Oxford university press New York, 2004. [66](#), [88](#)
- [120] Gesualdo Scutari, Francisco Facchinei, Jong-Shi Pang, and Daniel P Palomar. Real and complex monotone communication games. *IEEE Transactions on Information Theory*, 60(7):4197–4231, 2014. [68](#)

- [121] IBM Trusteer. Ibm trustee fraud protection suite. <https://www.ibm.com/sg-en/marketplace/trusteer-fraud-protection-suite/details#product-header-top>. 79
- [122] Chuanlong Yin, Yuefei Zhu, Jinlong Fei, and Xinzheng He. A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, 5:21954–21961, 2017. 80
- [123] Arastoo Fazeli and Ali Jadbabaie. Duopoly pricing game in networks with local coordination effects. In *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*, pages 2684–2689. IEEE, February 2012, USA. 81
- [124] Yang Zhang, Zehui Xiong, Dusit Niyato, Ping Wang, and Jiangming Jin. A game-theoretic analysis of complementarity, substitutability and externalities in cloud services. In *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pages 1–6. IEEE, 2017. 82
- [125] Xiaowen Gong, Lingjie Duan, and Xu Chen. When network effect meets congestion effect: Leveraging social services for wireless services. In *Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pages 147–156. ACM, June 2015, China. 82
- [126] Semyon Aronovich Gershgorin. Gershgorin circle theorem. https://en.wikipedia.org/wiki/Gershgorin_circle_theorem. 86
- [127] Peng Shi. Summary of what’s known about convergence in concave games. April 10, 2009. 87, 88, 114, 124
- [128] J Ben Rosen. Existence and uniqueness of equilibrium points for concave n-person games. *Econometrica: Journal of the Econometric Society*, pages 520–534, July 1965. 88, 120
- [129] Gerard Debreu. A social equilibrium existence theorem. *Proceedings of the National Academy of Sciences*, 38(10):886–893, 1952. 114, 120