Attack-Aware Cyber Insurance of Interdependent Computer Networks

Rui Zhang Quanyan Zhu *

May 22, 2017

Abstract

Cyber insurance is a valuable approach to mitigate further the cyber risk and its loss in addition to the deployment of technological cyber defense solutions such as intrusion detection systems and firewalls. An effective cyber insurance policy can reduce the number of successful cyber attacks by incentivizing the adoption of preventative measures and the implementation of best practices of the users. To study cyber insurance in a holistic manner, we first establish a bi-level game-theoretic model that nests a zero-sum game in a moral-hazard type of principal-agent game to capture complex interactions between a user, an attacker, and the insurer. The game framework provides an integrative view of the cyber insurance and enables a systematic design of incentive compatible and attack-aware insurance policy. The framework is further extended to study a network of users and their risk interdependencies. We completely characterize the equilibrium solutions of the bi-level game. Our analytical results provide a fundamental limit on insurability, predict the Peltzman effect, and reveal the principles of zero operating profit and the linear insurance policy of the insurer. We provide analytical results and numerical experiments to corroborate the analytical results and demonstrate the network effects as a result of the strategic interactions among three types of players.

Keywords: Cyber Insurance, Network Security, Moral Hazard, Information Asymmetry, Network Effects, Security Games, Mechanism Design.

*The authors are with the Department of Electrical and Computer Engineering, New York University, USA. E-mail:{rz885,qz494}@nyu.edu

1 Introduction

Network security becomes more challenging than ever as today's computer networks become increasingly complex. The deployment of defense mechanisms such as firewalls [1], intrusion detection systems [2], and moving target defenses [3] can effectively reduce the success rate of cyber attacks but cannot guarantee perfect network security as attacks are becoming more stealthy and sophisticated [4]. Network users can still be hacked, resulting in severe data breaches, disruption of services and financial losses. Cyber insurance provides users a valuable additional layer of protection to mitigate potential vulnerabilities to unknown threats, hacking, and human errors. An incentive compatible cyber insurance policy could help reduce the number of successful cyber attacks by incentivizing the adoption of preventative measures in return for more coverage and the implementation of best practices by basing premiums on an insured level of self-protection [5, 6].

Different from the traditional insurance paradigm, cyber insurance has two unique features. Firstly, the cyber insurance policy should be designed to mitigate risks that are not created by natural failures but by intelligent attackers who deliberately inflict damages on the network. The behaviors of the attackers play an equally important role in the design of insurance policy as the user behaviors do. An effective scheme of cyber insurance should take into account the adversary model as well as the user behaviors. Secondly, cyber risks can propagate over a network. The insecurity of one user can directly affect the security of users with whom he is connected (see Fig. 1). The global network failures could be caused and exacerbated because of the lack of protection of one single user. Hence, the cyber insurance needs to understand the interlinkages and the interdependencies among users and the insurance policy should be used not only to mitigate individual risks but also the systemic cyber risks over the network.

To address these two features of the cyber insurance, we first establish a bi-level game-theoretic model to capture the complex interactions among different types of players. Three parties coexist in the framework, including users, attackers, and insurers. Each one of them has distinct objectives. The users aim to reduce its cyber risk by deploying cyber defense

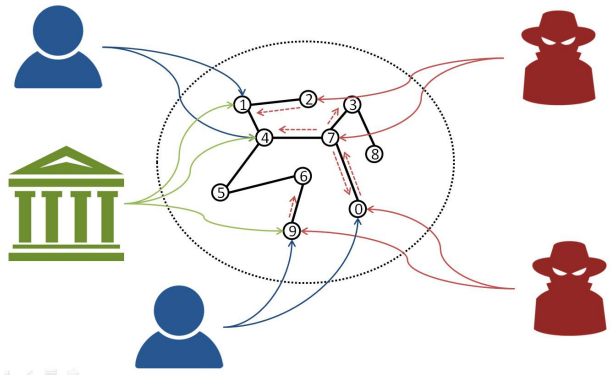


Figure 1: Cyber insurance over a network. Nodes and links of the network are represented by black circles and solid black lines. Three parties co-exist in this network. The blue icons represent users who employ the service of the network while the red icons represent attackers who launch cyber attacks with malicious ambitions. The users aim to mitigate the cyber-security loss in the network using local cyber defense strategies as well as the cyber insurance provided by the insurer, represented by the green icon. The networked environment increases the risks of the users as cyber attacks can spread to neighboring nodes, which is indicated by red dotted lines. As a result, the user at node 1 and 4 faces cyber risks even though the nodes are not directly compromised by the attacker.

mechanisms, such as intrusion detection/prevention systems [2, 7], honeypots [8], and route mutations [9], and at the same time adopting cyber insurance as an additional layer of protection to mitigate its loss, including data breaches and network damage. Attackers are adversaries who aim to inflict damages on the nodes by strategically choosing efficient attack strategies. An insurer is a person or company that underwrites an insurance risk by designing an incentive compatible cyber-insurance policy that includes a premium and the level of coverage.

To capture individual objectives and their interdependencies in an integrative framework, we build on the recent game-of-games concept [10] in which one game is nested in another game to provide an enriched game-theoretic model to capture complex interactions. In our framework, a zero-sum game is used to capture the conflicting goals between an attacker and a defender where the defender aims to protect the system for the worst-case attack. In addition, a moral-hazard type of principal-agent game with incomplete information is used to model the interactions between the insurer and the user. The user has a complete information

about his action while the insurer cannot directly observe it but indirectly measures the loss as a consequence of the user's security strategy. The zero-sum game is nested in the incomplete information game to constitute a bi-level problem which provides a holistic model for designing attack-aware insurance policy by taking into account the cyber attack models and the rational behaviors of the users.

We further extend the one-user game framework to a network of N nodes to investigate the impact of the network parameters on the cyber risks of the entire network for the case when the network is controlled by one administrator and the case when the network is fully distributed. The game-of-games concept can be used to capture the complex interactions where the outcome of a bi-level game at one node will influence the outcome of another game at the neighboring node. We show that the interactions between users and attackers at each node constitute zero-sum games, whose outcomes are influenced by the actions of other players' at other nodes with network effects. The insurers' insurance policies at each node are coupled due to the network coupling between users.

The major contributions of the paper can be summarized as follows:

- We propose a bi-level game-theoretic framework that incorporates a zero-sum security game nested with a moral-hazard type of principal-agent model. The network equilibrium concepts developed in this work provides methods to assess interdependent cyber risks and design effective attack-aware insurance policy.

- We study four distinct scenarios including single node case, centralized and decentralized network cases. For each scenario, we show that the optimal insurance mechanism design problems are linear programs, and their solutions are completely characterized and compared.

- We show the zero-operating profit principle of the insurer under the optimal insurance policy. The insurer's profit is determined by the premium subscription fee, which is found to be a linear function of the coverage level.

- The equilibrium of the bi-level game predicts the Peltzman effect [11] in which the user and attacker have no incentives to take actions when they are fully insured.

- We use analytical results and numerical experiments to show that the network coupling among users requires users to spend more efforts of protection at the equilibrium, and as network size increases, we see that the saddle-point equilibrium solutions of the user and the attacker exhibit less network effects.

In the previous discussion, we have assumed that the user's risk is static and does not change with time. However, both the user and the attacker can change their actions at some point, and the cyber system can also be different due to damage, failure, or upgrade. Thus, the risks of the user will vary with time, and the user will encounter dynamic losses. To capture the shifts of the user's risks in a time-varying world, we further extend our static models into dynamic settings. Stochastic differential equations and the Markov decision processes are used to model the dynamic environment and the user's behaviors. We further present two numerical examples and show the Peltzman effect where the user tends to act riskily when he is protected by the insurance.

1.1 Related Works

The challenges of cyber security are not only technical issues but also economic and policy issues [6]. Recently, the use of cyber insurance to enhance the level of security in cyber-physical systems has been studied [12, 13]. While these works deal with externality effects of cyber security in networks, few of them take into account in the model the cyber attack from a malicious adversary to distinguish from classical insurance models. In [14], the authors have considered direct and indirect losses, respectively due to cyber attacks and indirect infections from other nodes in the network. However, the cyber attacks are taken as random inputs rather than a strategic adversary. The moral hazard model in economics literature [15, 16] deal with hidden actions from an agent, and aims to address the question: How does a

principal design the agent's wage contract to maximize his effort? This framework is related to insurance markets and has been used to model cyber insurance [17] as a solution for mitigating losses from cyber attacks. In addition, in [18], the authors have studied a security investment problem in a network with externality effect. Each node determines his security investment level and competes with a strategic attacker. Their model does not focus on the insurance policies and hidden-action framework. In this work, we enrich the moral-hazard type of economic frameworks by incorporating attack models, and provide a holistic viewpoint towards cyber insurance and a systematic approach to design insurance policies. The network effect on security decision process has been studied in [19]. The authors have considered a variation of the linear influence networks model in which each node represents a network company and directed links model the positive or negative influence between neighbor nodes.

1.2 Organization of the Paper

The paper is organized as follows. In section 2, we describe the bi-level game-theoretic framework of cyber insurance for computer networks. We introduce four distinct cases of the cyber insurance model. In Section 3, we analyze the case when the network only has one node. Section 4 and Section 5 present the case of networks with N nodes. In addition, Section 4 deals with multiple users and attackers, with multiple distributed insurers and a single centralized insurer over networks. Section 5 deals with a single user, a single attacker and a single insurer over a network. Section 6 presents numerical experiments to corroborate the results. The paper is concluded in Section 8.

2 Overview of the Cyber-Insurance Framework

This section presents an overview of the bi-level game-theoretic framework of cyber insurance for computer networks to describe the complex interactions among three parties of players: $Users$, $Attackers$ and $Insurers$.

Users are the nodes of a computer network that face cyber threats from an attacker, making users vulnerable to data breaches, task failures, and severe financial losses.

Attackers are the adversaries who launch cyber-attacks to acquire private data from users or cause disruptions of the network services.

Insurers are persons or companies that underwrite insurance risks by providing users incentive compatible cyber-insurance policies that include premiums and levels of coverage. The premium is a subscription fee that is paid by the users to participate in the insurance program while the coverage level is the proportion of loss that will be compensated by the insurer as a consequence of successful cyber attacks.

2.1 *Users*, *Attackers* and *Insurers*: Objectives and Actions

The objective of the users is to find an efficient way to mitigate the loss due to the cyber attacks. To this end, there are two main approaches. One is to deploy local protections, such as firewalls and intrusion detection systems (IDSs) [2, 20], frequent change of passwords, timely software patching and proactive moving target defenses [3]. These defense mechanisms can reduce the success rate of the attacks, but cannot guarantee perfect network security for users. There are still chances for the users to be hacked by the attackers. The other approach is to adopt cyber-insurance. The users pay a premium fee so that the loss due to cyber attacks can be compensated by the insurer. This mechanism provides an additional layer of mitigation to reduce the loss further that the technical solutions of the first approach cannot prevent. To capture the two options in our framework, we allow users to decide their protection levels as well as their rational choice of participation in the insurance program as illustrated in Fig. 2.

The objective of the attackers is to inflict as much damage to the users as possible by launching various cyber-attacks, such as node capture attacks [21] and denial of services (DoS) attacks [22]. Note that the damage is often positively correlated with the loss of the user. For example, the denial of service attack on networks will disrupt the normal operation

of the infrastructures (e.g. blackout, airline breakdown). The security of the disruption will cause financial losses of the infrastructure users. Moreover, the goal of the attacker may not just stop at compromising the system but aim at higher objectives. For example, in advanced persistent threats [23], the attacker has to compromise multiple resources to attain its goal. In the case that the attacker successfully obtains the banking information or privacy information of the user is to steal money or ransom. The final objective of attacking the system is for profit. As a result, the objective of the attackers is taken to maximize the losses of the users by deciding the attack levels.

The insurers have two objectives. One is to make a profit from providing the insurance, and the other one is to reduce the average losses of the users, which is also directly related to the cost of the insurer. An insurer's problem is to determine the subscription fee and the coverage levels of the insurance. Note that the average losses depend on both the users' local protection levels and the attackers' attack levels. Moreover, the rational users will only enroll in the insurance when the average reduction in the loss is higher than or equal to the premium he paid to the insurer. As a result, the insurer's problem can be seen as finding an optimally acceptable insurance policy that makes profits while reducing the users' average losses.

2.2 *Users*, *Attackers* and *Insurers*: Information

In this subsection, we further identify the information of the *users*, *attackers* and *insurers*.

The user is assumed to have complete information about the attacker and the insurer. The complete information assumption of the user on the attacker captures the fact that the user aims to find a robust defense strategy against potential attackers. Since the insurer announces the insurance policy to the user so that the user can decide whether to accept it or not, the user has complete information of the insurer's policy.

The attacker is assumed to have complete information about the user and the insurer. This assumption is used to capture two important facts, one is due to Kerckhoffs's principle [24]

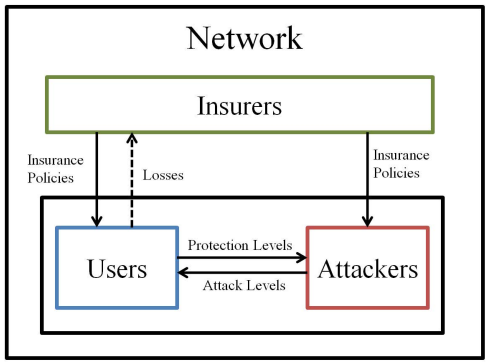


Figure 2: Bi-level game over networks: In a networked environment, the users and the attackers constitute zero-sum games at each node, the outcome of which are used by the insurers to design insurance policies. The interactions between the insurers and the users can be viewed as leader-follower type of games. Note that users and attackers have full information about the network, the other players in this network, and also the insurers' policies while the insurers have no information on the users' or attackers' actions but they know the losses of the users. This type of incomplete information game is a typical moral hazard problem.

which postulates that "the enemy knows the system"; the second fact is due to the increasingly advanced persistent threats (APTs) that enable attacks to behave stealthily and acquire knowledge about the system [23]. The complete information of the attacker enables us to anticipate the interactions of the user and the insurer under the worst-case attack scenarios.

The insurer is assumed to have incomplete information about the user and the insurer. The insurer cannot directly observe the defense actions and attack actions of the users and the attackers, respectively. However, the insurer can measure the loss of the user as he will provide coverage to mitigate that. Moreover, we assume that the insurer also knows the costs of conducting certain levels of local protections and attacks, which can be interpreted as the market prices for providing security services. For example, the costs of using firewalls and hiring hackers can be found in the market.

2.3 Bi-Level Game Framework

The objectives, actions and information of users, attackers, and insurers are all intertwined. We use a bi-level game to capture the complex interactions among the three parties, which is

illustrated in Fig. 2. The conflicting objectives of a user and an attacker can be captured by a local game at each node in which the user determines a defense strategy while the adversary chooses an attack strategy. The outcome of the local interactions at each node determines its cyber risk. The cyber insurance is then used as an additional method to further reduce the loss due to the cyber risk. Hence as illustrated in Fig. 2, the insurers are the leaders or principals in the framework who design insurance policies for the users while the users can be viewed as followers or agents who determine their defense strategies under a given insurance policy.

One main feature of the cyber-insurance is the information asymmetry between the insurers and the users. The insurer cannot directly observe the defense actions of the users but can be informed of the average losses of the users and the costs of conducting certain levels of local protections and attacks. Hence, this fact leads to a moral-hazard principal-agent model between an insurer and a user [25]. By further taking into account the attack behaviors, we can see that it is natural to establish a bi-level framework. The bottom level consists of multiple local games between a user and an attacker while the top level consists of the principal-agent games between a user and an insurer. Since both the user and the attacker have complete information, the conflicting objectives of them can be captured as a zero-sum game, where the assessed risks represent the worst-case scenario which will allow users to make attack-aware insurance decisions.

The users are connected in a network. The cyber risks of the users over the network are interdependent. From a game-theoretic perspective, the bi-level game with N users, N attacks and N insurers over a network can be viewed as a game of games in which N one-user, one-attacker and one-insurer games interact with each other, making the outcome of one game dependent on the others. This unique structure of games over networks is illustrated in Fig. 3. In this work, we will investigate several structures of network games under different contexts described below:

- **Case 1: 1 Node-1 User-1 Attacker-1 Insurer**: We consider a network with one

node. There co-exist 1 user, 1 attacker and 1 insurer interacting with each other at this node. This case excludes network effects.

- **Case 2(a):** N **Nodes-**N **Users-**N **Attackers-**N **Insurers**: We consider a network with N nodes. We assume that each node has one user, one attacker and one insurer. This case extends Case 1 to a fully distributed network game problem in which the game of one node interacts with a game of another node.

- **Case 2(b):** N **Nodes-**N **Users-**N **Attackers-1 Insurer.** This case differs from the preceding case in that there exists only 1 insurer in this network. The insurer's policy is designed by viewing the network as a whole system.

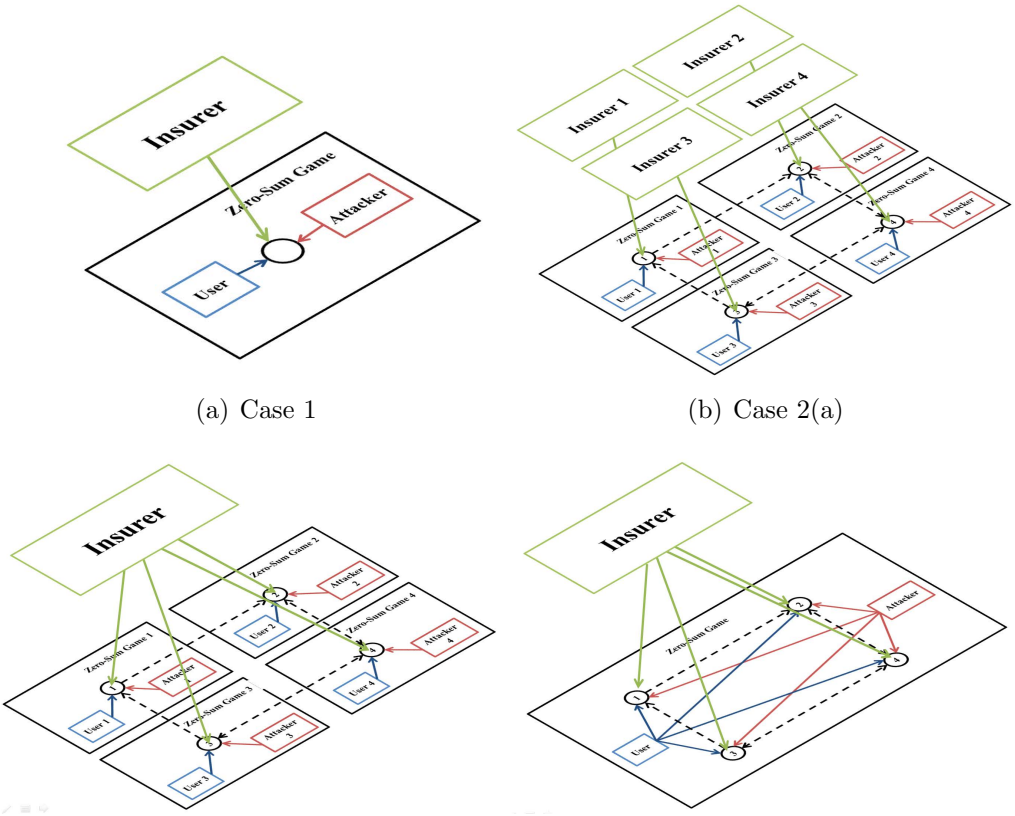
- **Case 3:** N **Nodes-1 User-1 Attacker-1 Insurer.** This case corresponds to a centralized insurer who designs the entire network insurance policy while one network administrator coordinates the defense strategies of all nodes against one attacker.

3 Case 1: 1 Node-1 User-1 Attacker-1 Insurer

In this section, we consider Case 1 with 1 node, 1 user, 1 attacker, and 1 insurer. We first formulate the game between the user and the attacker, then we describe the insurer's problem under the equilibrium of the user and the attacker's game. An illustration of the cyber-insurance model of Case 1 is shown in Fig. 4. This case lays the basic cyber-insurance framework for understanding multi-player scenarios in Section 4 and 5.

3.1 Zero-Sum Game between User And Attacker

Let $p_u \in [0, 1]$ and $p_a \in [0, 1]$ denote the local protection level of the user and the attack level of the attacker. On one hand, a large p_u indicates a cautious user while a small p_u indicates that the user is reckless. A reckless user may click on suspicious links of received spam emails, fail to patch the computer system frequently, and leave cyber footprints for an



(a) Case 1

(b) Case 2(a)

(c) Case 2(b)

(d) Case 3

Figure 3: Different cases of the bi-level game between users, attackers and insurers. Black circles indicate the nodes of the network. Black dotted lines represent the network connections between neighboring nodes. In Case 1, the network has 1 node, and there exist 1 user, 1 attacker, and 1 insurer. In Case 2(a) and 2(b), the network has 4 nodes. Each node has 1 user and 1 attacker. Case 2(a) has 4 insurers corresponding to each node while Case 2(b) has only 1 insurer that announces insurance policies to each node. In Case 3, the network has 4 nodes, but there exist only 1 user, 1 attacker and 1 insurer in this network. Each player makes a decision at a node.

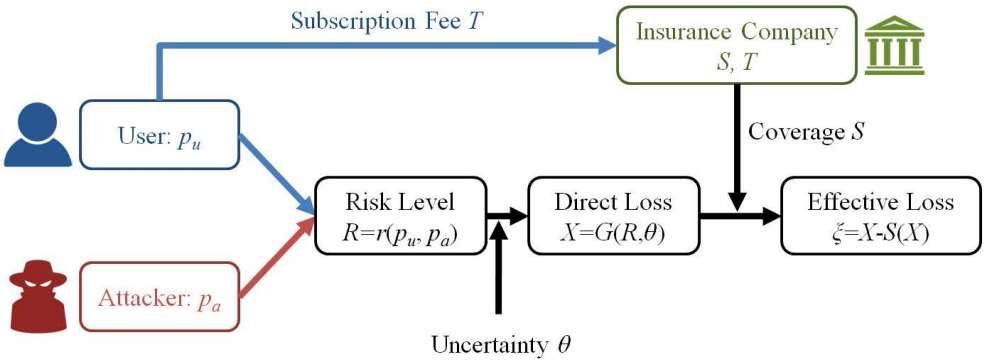


Figure 4: Illustration of the interactions between three players: The action pair (p_u, p_a) chosen by the user and the attacker results in a risk level not directly observable by the insurer. The insurer designs an insurance policy that includes a premium subscription fee and the coverage level to cover part of the loss due to the cyber attack.

adversary to acquire system information. On the other hand, a large p_a indicates a powerful attacker, and a small p_a indicates a powerless attacker. The abstraction of using p_u and p_a captures the effectiveness of a wide range of heterogeneous defense and attack strategies without a fine-grained modeling of individual mechanisms. This will allow us to focus on the consequence of security issues and the choice of a mechanism that induces the result.

The action pair of the user and the attacker (p_u, p_a) determines the risk level of the user $R \in \mathbb{R}_{\geq 0}$. A smaller p_u and a larger p_a indicate a higher risk level of the user. We use the following risk function r to denote the connections between the user's and the attacker's actions and the risk level of the user.

Definition 1 *Risk Function* $r(p_u, p_a) : [0,1]^2 \to \mathbb{R}_{\geq 0}$ *gives the risk level* R *of the user with respect to the user's local protection level* p_u *and the attacker's attack level* p_a*. Moreover, it is assumed to be continuous on* $(0,1]^2$*, convex and monotonically decreasing on* $p_u \in [0,1]$*, and concave and monotonically increasing on* $p_a \in [0,1]$*.*

Note that the monotonicity in $p_u \in [0,1]$ indicates that a larger local protection level of the user leads to a smaller risk level while the monotonicity in $p_a \in [0,1]$ indicates that a larger attack level of the attacker leads to a larger risk level. Since r is convex on p_u, the risk decreases slower when the user adopts a larger local protection level. Since r is concave on

p_a, the risk increases slower when the attacker conducts a higher attack level. Without loss of generality, we use the following risk function,

$$r(p_u, p_a) = \ln(\frac{p_a}{p_u} + 1). \tag{1}$$

Similar types of functions have also been widely used in jamming attacks in wireless networks [26, 27] and rate control problems [7, 28]. Under the risk level of R, the economic loss of the user can be represented as a random variable X measured in dollars, which can be expressed as $X = G(R, \theta)$, where θ is a random variable with probability density function g that captures the uncertainties in the measurement or system parameters. For example, a data breach due to the compromise of a server can be a consequence of low security level at the user end. The magnitude of the loss depends on the content and the significance of the data, and the extent of the breach. The variations in these parameters are captured by the random variable θ. Since the risks of being attacked cannot be perfectly eliminated, the user can transfer the remaining risks to the third party, the insurer, by paying a premium or subscription fee T for a coverage of $S(X)$ when he faces a loss of X, where $S : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is the insurance coverage function that reduces the loss of the user if he is insured. Thus, the effective loss ξ to the user becomes $\xi = X - S(X)$.

Given the attacker's action p_a and the insurer's coverage function S, the user aims to minimize the average effective loss by finding the optimal local protection level p_u^*. Such objective can be captured by the following optimization problem

$$\min_{p_u \in [0,1]} \mathbb{E}[H(\xi)] = \mathbb{E}[H(X - S(X))], \tag{2}$$

where $H : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is the loss function of the user, which is increasing on ξ. Note that the expectation is taken with respect to the statistics of θ. The subscription fee T is not included in this optimization problem, as the fee is a constant decided by the insurer.

The loss function $H(\xi)$ indicates the user's risk propensity. A convex $H(\xi)$ indicates that

the user is risk-averse, i.e., the user cares more about the risk, while a concave $H(\xi)$ indicates that the user is risk-taking, i.e., he cares more about the cost, rather than the risk. A linear $H(\xi)$ indicates that the user is risk-neutral. In this paper, we consider a risk-averse user, and use a typical risk-averse loss function that $H(\xi) = e^{\gamma\xi}$ with $\gamma > 0$, where γ indicates how much the user cares about the loss.

Note that the loss function in (2) can be expressed explicitly as a function of X. Thus, Problem (2) can be rewritten by taking expectations with respect to the sufficient statistics of X. Let f be the probability density function of X. Clearly, f is a transformation from the density function g (associated with the random variable θ) under the mapping G. In addition, f also depends on the action pair (p_u, p_a) through the risk variable R. Therefore, we can write $f(x|p_u, p_a)$ to capture the parameterization of the density function. Furthermore, we assume that X follows an exponential distribution, i.e., $X \sim \exp(\frac{1}{R})$, where $R := r(p_u, p_a)$ is the risk level of the user. The exponential distribution has been widely used in risk and reliability analysis [29–32]. Thus the density function can be written as,

$$f(x|p_u, p_a) = \frac{1}{R} e^{-\frac{1}{R}x} = \frac{1}{r(p_u, p_a)} e^{-\frac{1}{r(p_u, p_a)}x} = \frac{1}{\ln(\frac{p_a}{p_u} + 1)} e^{-\frac{1}{\ln(\frac{p_a}{p_u}+1)}x}, \forall x \in \mathbb{R}_{\geq 0}.$$

The average amount of loss given actions p_u and p_a is $\mathbb{E}(X) = R = r(p_u, p_a) = \ln(\frac{p_a}{p_u} + 1)$. For small p_u and large p_a, the risk level of the user R tends to be large, which leads to a large average loss of the user. We further assume that the insurance coverage $S(X)$ is linear in X, i.e., $S(X) = sX$, where $s \in [0, 1]$ indicates the coverage level of the insurance. Hence, the average effective loss given the insurance coverage level s and the action pair (p_u, p_a) is $\mathbb{E}(\xi) = \mathbb{E}(X - S(X)) = \mathbb{E}((1 - s)X) = (1 - s)\mathbb{E}(X) = (1 - s)\ln(\frac{p_a}{p_u} + 1)$. Furthermore, we

have:

$$\begin{aligned}\mathbb{E}[H(\xi)] &:= \int_{x\in\mathbb{R}_{\geq 0}} H(x-S(x))f(x|p_u,p_a)dx \\ &= \tfrac{1}{R}\int_0^{\infty} e^{[\gamma(1-s)-\frac{1}{R}]x}dx \\ &= \tfrac{1}{1-\gamma(1-s)R} \\ &= \tfrac{1}{1-\gamma(1-s)\ln(\frac{p_a}{p_u}+1)}.\end{aligned} \tag{3}$$

The third equality holds when

$$\gamma(1-s)-\frac{1}{R}<0, \text{ i.e., } 1-\gamma(1-s)\ln(\frac{p_a}{p_u}+1)>0. \tag{4}$$

Otherwise, the loss will be infinite, i.e., $\mathbb{E}[H(\xi)]\to\infty$. In this regime, no insurance scheme can be found to mitigate the loss. Condition (4) gives a feasible set of parameters under which cyber insurance is effective and provides a fundamental limit on the level of mitigation. Note that minimizing (3) is equivalent as minimizing $\gamma(1-s)\ln(\frac{p_a}{p_u}+1)$ under the feasible equality (4). The user's problem (2) can be rewritten as follows:

$$\begin{aligned}&\min_{p_u\in[0,1]} J_u(p_u,p_a,s) := \gamma(1-s)R = \gamma(1-s)\ln(\tfrac{p_a}{p_u}+1) \\ &\text{s.t.} \quad 1-\gamma(1-s)\ln(\tfrac{p_a}{p_u}+1)>0.\end{aligned} \tag{5}$$

Problem (5) captures the user's objective to minimize the average effective loss given the attack level p_a and the insurance coverage level s. On the other hand, the attacker aims to find the optimal attack level p_a^* that maximizes the average loss of the user given user's local protection level and insurer's coverage level s. Such conflicting interests of the user and the attacker constitutes a zero-sum game, which takes the following minimax or max-min form,

$$\begin{aligned}&\min_{p_u\in[0,1]}\max_{p_a\in[0,1]} K(p_u,p_a,s) \\ &\text{s.t.} \quad (p_u,p_a)\in\mathcal{S}_{u,a}(s).\end{aligned} \quad \text{or} \quad \begin{aligned}&\max_{p_a\in[0,1]}\min_{p_u\in[0,1]} K(p_u,p_a,s) \\ &\text{s.t.} \quad (p_u,p_a)\in\mathcal{S}_{u,a}(s).\end{aligned} \tag{6}$$

where

$$K(p_u, p_a, s) := \gamma(1-s)R + c_u p_u - c_a p_a = \gamma(1-s)\ln(\frac{p_a}{p_u}+1) + c_u p_u - c_a p_a, \tag{7}$$

$$\mathcal{S}_{u,a}(s) := \left\{ (p_u, p_a) \middle| 1 - \gamma(1-s)\ln(\frac{p_a}{p_u}+1) > 0 \right\}. \tag{8}$$

The first term of the objective function K captures the average effective loss given an insurance coverage level s, the local protection level p_u and the attack level p_a. The second and third terms indicate the cost of the user and the attacker, respectively. $c_u \in \mathbb{R}_{>0}$ is the cost parameter of the user. A larger c_u indicates that local protection is costly. $c_a \in \mathbb{R}_{>0}$ denotes the cost parameter of the attacker to conduct an attack level of p_a. A larger c_a indicates that a cyber-attack is costly. Note that c_u and c_a can be interpreted as the market price of local protections and cyber-attacks, and they are known by the insurer. The constraint indicates the feasible set of the user. Note that if s, p_u, and p_a are not feasible, K is taken to be an infinite cost. Minimizing $K(p_u, p_a, s)$ captures the user's objective to minimize the average effective loss with the most cost-effective local protection level. Maximizing $K(p_u, p_a, s)$ captures the attacker's objective to maximize the average effective loss of the user with the lowest attack level. Note that the minimax form of (6) can also be interpreted as a worst-case solution for a user who uses the best security strategies by anticipating the worst-case attack scenarios.

Furthermore, Problem (6) yields a saddle-point equilibrium (SPE) to the insurance coverage level s which can be defined as follows:

Definition 2 *Let $\mathcal{S}_u(s)$, $\mathcal{S}_a(s)$ and $\mathcal{S}_{u,a}(s)$ be the action sets for the user and the attacker given an insurance coverage level s. Then, the strategy pair (p_u^*, p_a^*) is a saddle-point equilibrium (SPE) of the zero-sum game defined by the triple*

$$G_z := \langle \{User, Attacker\}, \{\mathcal{S}_u(s), \mathcal{S}_a(s), \mathcal{S}_{u,a}(s)\}, K \rangle,$$

if

$$K(p_u^*, p_a, s) \leq K(p_u^*, p_a^*, s) \leq K(p_u, p_a^*, s), \quad \forall p_u \in \mathcal{S}_u(s), p_a \in \mathcal{S}_a(s), (p_u, p_a) \in \mathcal{S}_{u,a}(s) \tag{9}$$

where K and $\mathcal{S}_{u,a}(s)$ is the objective function and feasible set defined in (7) and (8).

The definition indicates that if a pair (p_u^*, p_a^*) satisfies (9), then it is a SPE of the game between the user and the attacker to the insurer's insurance policy. Note that under a given insurance coverage level s, (p_u^*, p_a^*) must satisfy the feasible constraint (4). Thus, we aim to look for a constrained SPE of the zero-sum game with coupled constraints on the strategies of the players.

Proposition 1 *Given an insurance coverage level s that satisfies*

$$1 - \gamma(1-s)\ln(\frac{c_u}{c_a} + 1) > 0, \tag{10}$$

there exists a unique SPE of the zero-sum game defined in Definition 2, given by

$$p_u^* = \tfrac{\gamma(1-s)}{c_u + c_a}, \quad p_a^* = \tfrac{c_u \gamma(1-s)}{c_a(c_u + c_a)}. \tag{11}$$

Proof. See Appendix A. ■

Proposition 1 shows that the SPE of the zero-sum game between the user and the attacker is related to the insurer's policy s. Note that when s is large, both the p_u^* and p_a^* is small, indicating that both the user and the attacker will take weak actions. Moreover, we have the following observations regarding the SPE.

Remark 1 (Peltzman Effect) *When the insurer provides a higher coverage level s, the SPE of the user p_u^* tends to be smaller, i.e., the user takes a weaker local protection. Such risky behavior of the user in response to insurance is usually referred as Peltzman effect [11].*

Corollary 1 (Invariability of The SPE Ratio) *The SPE satisfies* $p_u^* c_u = p_a^* p_a$. *Specially, when* $p_u^*, p_a^* \neq 0$, $\frac{p_a^*}{p_u^*} = \frac{c_u}{c_a}$, *i.e., the ratio of the actions of the user and the attacker is only related to* c_u *and* c_a, *and it is independent of the insurer's policy* s. *Note that when* $c_u = c_a$, $\frac{p_a^*}{p_u^*} = 1$, *i.e., the SPE becomes symmetric, as* $p_u^* = p_a^* = \frac{\gamma(1-s)}{c_u + c_a} = \frac{\gamma(1-s)}{2c_u} = \frac{\gamma(1-s)}{2c_a}$.

Remark 2 (Constant Cost Determined SPE Risk) *The user has a constant SPE risk level* $R^* = r(p_u^*, p_a^*) = \ln(\frac{p_a^*}{p_u^*} + 1) = \ln(\frac{c_u}{c_a} + 1)$ *at SPE, which is determined by the costs of adopting protections and launching attacks. The ratio is independent of coverage level* s.

Corollary 2 *At SPE, the average direct loss of the user is* $\mathbb{E}(X) = R^* = \ln(\frac{c_u}{c_a} + 1)$, *the average effective loss of the user is* $\mathbb{E}(\xi) = \mathbb{E}((1-s)X) = (1-s)\mathbb{E}(X) = (1-s)R^* = (1-s)\ln(\frac{c_u}{c_a} + 1)$, *the average payment of the insurer to the user is* $\mathbb{E}(sX) = s\mathbb{E}(X) = sR^* = s\ln(\frac{c_u}{c_a} + 1)$.

Corollary 1 indicates the constant SPE ratio of the user and the attacker, which is determined only by the cost parameters c_u and c_a, i.e., the costs for applying certain levels of protections and attacks, respectively. As a result, the SPE risk level of the user is constant, and only determined by the costs as shown in Remark 2. Thus, the average direct loss is constant as shown in Corollary 2. However, when the insurance coverage level s does not satisfy (10), the insurability of a user is not guaranteed, which is shown in the following proposition.

Proposition 2 (Fundamental Limits on Insurability) *Given an insurance coverage level* s *that* $1 - \gamma(1-s)\ln(\frac{c_u}{c_a} + 1) \leq 0$, (p_u^*, p_a^*) *does not satisfy the feasible inequality (4), thus, the average direct loss of the user* $\mathbb{E}(X) \to \infty$, *and the zero-sum game defined in Definition 2 does not admit a SPE. Thus, the user is not insurable, as the insurance policy cannot mitigate his loss. The insurer will not also provide insurance to a user who is not insurable.*

Proposition 3 *Under an insurable scenario, the cost parameter of the user must satisfy* $c_u < c_a(e^{\frac{1}{\gamma(1-s)}} - 1)$, *and the local protection level of the user must satisfy* $p_u > \frac{\gamma(1-s)}{c_a} e^{\frac{1}{\gamma(1-s)}}$.

Proof. The first inequality can be easily achieved from (10). From Appendix A, given the action of the user p_u, the best action of the attacker is $P_a^*(p_u) = \frac{\gamma(1-s)}{c_a} - p_u$. By plugging $P_a^*(p_u)$ into the feasible inequality (4), we can get $p_u > \frac{\gamma(1-s)}{c_a} e^{\frac{1}{\gamma(1-s)}}$. ■

It is important to note that the user must pay a subscription fee $T \in \mathbb{R}_{\geq 0}$ to be insured. The incentive for the user to buy insurance exists when the average loss at equilibrium under the insurance is lower than the loss incurred without insurance. Recall Corollary 2, the average loss of the user with the subscription fee T is $\mathbb{E}(\xi) + T = (1-s)R^* + T$, which is monotonically decreasing on s. When the user is under full coverage, the average loss with the payment T is $\mathbb{E}(\xi) + T\big|_{s=1} = T$. When the user does not subscribe to an insurance, the average loss is $\mathbb{E}(X) = R^*$. Thus, the user has no incentive to insure if the loss under full coverage is higher than that under no insurance, i.e., $T > R^*$. Moreover, for $T \leq R^*$, the user will choose to insure if the average loss under the given coverage level s is lower than under no insurance, i.e., $(1-s)R^* + T \leq R^*$. Therefore, we arrive at the following conditions.

Condition 1 (Individual Rationality (IR-u)) *The subscription fee must satisfy* $T \leq T_{max} := R^* = \ln(\frac{c_u}{c_a} + 1)$*, so that the user prefer to subscribe the insurance.*

Condition 2 (Incentive Compatibility (IC-u)) *For the subscription fee* $T \leq T_{\max}$*, the user will subscribe to the insurance if the coverage level* s *satisfies* $s \geq s_0 = \frac{T}{R^*} = \frac{T}{\ln(\frac{c_u}{c_a}+1)}$.

The user will enroll the insurance only when (IR-u) and (IC-u) constraints are satisfied. Note that when c_u is large and c_a is small, $T_{\max}$ is large and $s_0(T)$ is small, i.e., when the cost of the user to put local protections is large, and the cost of the attacker to conduct cyber-attack is small, the price of the subscription fee is large, but the minimum coverage is low. Note that s_0 is monotonically increasing on T. Specially, when $T = 0$, we have $s = 0$, i.e., the user will accept any coverage level when there is no charge for the insurance premium. Moreover, when $T = T_{\max}$, we have $s = 1$, i.e., the user only accept a full coverage when the subscription fee is the maximum.

3.2 Insurer's Problem

The insurer announces the insurance policy $\{s, T\}$, where s indicates the coverage level, T indicates the subscription fee, and then the user's and the attacker's conflicting interests formulates a zero-sum game, which yields a unique solution as shown in Proposition 1, with the corresponding equilibrium loss as shown in Corollary 2. Note that T is the gross profit of the insurer as he charges it from the user first, but when the user faces a loss $\mathbb{E}(X) = R^*$, the insurer must pay $s\mathbb{E}(X) = sR^*$ to the user. As a result, the operating profit of the insurer can be captured as $T - s\mathbb{E}(X) = T - sR^*$, which must be larger than or equal to 0 so that the insurer will provide the insurance. Thus, we have the following condition.

Condition 3 (Individual Rationality (IR-i)) *The insurer will provide the insurance if* $T - sR^* = T - s\ln(\frac{c_u}{c_a} + 1) \geq 0$.

Recall Proposition 2, the insurer will provide the insurance when the user is insurable, i.e., inequality (10) must be satisfied. Thus, we reach the following proposition that indicates the feasible coverage level.

Condition 4 (Feasibility (F-i)) *The coverage level s is feasible, i.e., the user is insurable, when* $s > 1 - \frac{1}{\gamma\ln(\frac{c_u}{c_a}+1)}$.

With the (IR-u) and (IC-u) constraints for the user and the (IR-i) and (F-i) constraints for the insurer, the insurer's objective to minimize the average effective loss of the user and maximize the operating profit can be captured using the following optimization problem:

$$\begin{aligned} &\min_{\{0\leq s\leq 1, T\geq 0\}} J_i(s,T) := \gamma(1-s)\ln(\tfrac{c_u}{c_a}+1) + c_s(s\ln(\tfrac{c_u}{c_a}+1) - T) \\ &\text{s.t.} \quad \text{(IR-}u\text{)}, \text{(IC-}u\text{)}, \text{(IR-}i\text{)}, \text{(F-}i\text{)}. \end{aligned} \tag{12}$$

Minimizing the first term of the objective function captures the insurer's objective to reduce the loss of the user, while minimizing the second term of the objective function captures the insurer's objective of making a profit. Parameter c_s indicates the trade-off of a safer user and

a larger profit of the insurer. Note that the insurer cannot directly observe the actions of the user and the attacker, but he is aware of the cost parameters c_u and c_a of the actions of the user and the attacker, respectively.

Furthermore, the solution of Problem (12) and the corresponding SPE defined in Definition 2 yields an equilibrium for the bi-level game in Case 1 which can be defined as

Definition 3 *Let $\mathcal{S}_i$ be the action set for the insurer, $\mathcal{S}_u(s)$ and $\mathcal{S}_a(s)$ be the action sets for the user and the attacker given the insurance coverage level, the strategy pair $(p_u^*, p_a^*, \{s^*, T^*\})$ is called a bi-level game Nash equilibrium (BGNE) of the bi-level game in Case 1 defined by the triple $G_1 := \langle \{User, Attacker, Insurer\}, \{\mathcal{S}_u(s), \mathcal{S}_a(s), \mathcal{S}_i\}, K, J_i \rangle$, if $\{s^*, T^*\}$ solves Problem (12) with the BGNE objective function J_i^*, and the strategy pair (p_u^*, p_a^*) is the SPE of the zero-sum game defined in Definition 2 with the equilibrium payoff K^* under the insurance policy $\{s^*, T^*\}$.*

Note that the insurer's Problem (12) is a linear programming problem as the objective function and all the constraints are linear in s and T. Instead of using computational methods to solve this problem, we first observe that (IR-i) and (IC-u) together indicate that the insurance policy s and T must satisfy

$$T = sR^* = s\ln(\frac{c_u}{c_a} + 1). \tag{13}$$

Corollary 3 *Equality (13) indicates the following observations:*

(i) Zero Operating Profit Principle: *The insurer's operating profit is always* 0*, as* $T - sR^* = 0$.

(ii) Linear Insurance Policy Principle: *The insurer can only provide the insurance policy s and T that satisfies (13), so that the user subscribes to the insurance provided by the insurer*

Corollary 3 reveals a zero operating profit principle and a linear insurance policy principle for the insurer. These principles hold in Case 2 and 3 as well. Moreover, the linear insurance policy indicates that the ratio of the subscription fee and the coverage level only depends on the SPE risk R^*, which is determined by the cost parameters seen in Remark 2. It provides a fundamental principle for designing the insurance policy.

As a result, the optimal insurance for the insurer can be summarized using the following proposition.

Proposition 4 *The optimal insurance policy for the insurer is*

$$s^* = 1; \quad T^* = T_{\max} = \ln(\frac{c_u}{c_a} + 1). \tag{14}$$

Proposition 4 shows that a full coverage level and a maximum subscription fee are the optimal insurance policy of the insurer. Together with Proposition 1, we have the following proposition of the BGNE of the bi-level game in Case 1.

Proposition 5 *The bi-level game of Case 1 admits a unique BGNE solution* $(p_u^*, p_a^*, \{s^*, T^*\}) = (0, 0, \{1, \ln(\frac{c_u}{c_a} + 1)\})$. *At the equilibrium, the insurer provides a full coverage for the user and charges a maximum subscription fee from the user. The user and the attacker have no incentives to take actions at the equilibrium as the cost would be too high. The equilibrium also demonstrates that cyber insurance will effectively mitigate the loss.*

4 Case 2: N Nodes-N Users-N Attackers

In this section, we present Case 2(a) and Case 2(b) with N nodes, N users, N attackers and 2 types of insurers, N insurers and 1 insurer over the network. One illustration is shown in Fig. 3(b)(c). We further assume that the network is well-connected, i.e., any two nodes in this network are connected by a path. Note that there exist an user and an attacker at each node $n \in \{1, ..., N\}$. We first formulate the game between the users and the attackers, then

we describe two types of insurers' problems.

4.1 Game of N Zero-Sum Games Between Users and Attackers

In a networked environment, cyber-attacks may affect a node through his neighboring nodes. Typical examples of such cyber-attacks are worms and trojans that propagate into a network of computers one by one, using mail contacts or any application data [33]. At each node n, there exists a zero-sum game between user n and attacker n. Moreover, N zero-sum games at this network induce a network game of N users and N attackers. Let $p_{u,n}$, $p_{u,n}$, s_n, T_n denote the local protection level of the user, the attack level of user, the insurance coverage level and the subscription fee at node $n \in \{1, \cdots, N\}$, respectively.

The risk level R_n of node n does not depend only on the user's action $p_{u,n}$ and the attacker's action $p_{a,n}$ at this node, but also on all the other players' actions at other nodes due to the network effects. Thus, we assume that for user n, his risk level R_n is given by:

$$R_n := r_n(p_{u,n}, p_{a,n}) + \eta \sum_{m=1}^{N} w_{mn} R_m.$$

Note that the first term denotes the local risk level caused by the actions of user n and attacker n. Following a similar definition of the local risk level in (1), $r_n(p_{u,n}, p_{a,n}) = \ln(\frac{p_{a,n}}{p_{u,n}} + 1)$. The second term denotes the risk level caused by network effects. Note that w_{mn} indicates the probability that an attack on node m leads to an attack on node n, and $0 \leq \eta \leq 1$ indicates the scalability parameter of the network effect that models the attenuation of an attack from a neighboring node. The closer is η to 1, the stronger is the network effect between the nodes. Indeed, the network effect increases the risk level of the users, which leads to a negative impact on the cyber-security. Typically, we have

$$w_{nn} = 0, \sum_{n=1}^{N} w_{mn} = 1, \quad \forall n = 1, ..., N, \tag{15}$$

meaning that node n does not contaminate itself, and an attack on node m generates an

attack to node n with probability w_{mn}. Thus, the vector of risk levels $\mathbf{R} = [R_1, ..., R_N]^T$ can be expressed by $\mathbf{R} = \mathbf{r} + \eta \mathbf{W}^T \mathbf{R}$, where $\mathbf{r} = [r_1(p_{u,1}, p_{a,1}), ..., r_1(p_{u,N}, p_{a,N})]^T$ and $\mathbf{W}^T$ is the transpose of matrix $\mathbf{W}$. Note that $\mathbf{W}$ is a right irreducible stochastic matrix with all diagonal elements being 0. Thus, we have $(\mathbf{I}_N - \eta \mathbf{W}^T)\mathbf{R} = \mathbf{r}$. Note that $\mathbf{I}_N$ is the identity matrix of size N. Furthermore, we have the following useful facts.

Proposition 6 *Let $\mathbf{W}^* = (\mathbf{I}_N - \eta \mathbf{W}^T)^{-1}$ if the inverse exists, we have*

(i) The inverse of $\mathbf{I}_N - \eta \mathbf{W}^T$ always exists.

(ii) $\mathbf{W}^*$ is a nonnegative matrix with $w^*_{nn} > 1, w^*_{nm} \geq 0, \forall n, m \in \{1, ..., N\}$ and $m \neq n$.

(iii) $\mathbf{1}_N^T \mathbf{W}^* = \frac{1}{1-\eta} \mathbf{1}_N^T$, where $\mathbf{1}_N$ is a column vector of size N with every elements being 1. As a result, $\sum_{m=1}^N w^*_{mn} = \frac{1}{1-\eta}, \forall n \in \{1, ..., N\}$, i.e, the sum of each column of $\mathbf{W}^*$ are the same and constant, which is equal to $\frac{1}{1-\eta}$.

Proof. See Appendix D. ■

With this result, we have $\mathbf{R} = \mathbf{W}^* \mathbf{r}$. The risk level for all node n, due to network effect, is then given by:

$$R_n(p_{u,n}, p_{a,n}; p_{u,-n}, p_{a,-n}) = \sum_{m=1}^{N} w^*_{nm} r_m(p_{u,m}, p_{a,m}), \quad \forall n = 1, ..., N.$$

Note that $p_{u,-n} = \{p_{u,1}, ..., p_{u,n-1}, p_{u,n+1}, ...p_{u,N}\}, p_{a,-n} = \{p_{a,1}, ..., p_{a,n-1}, p_{a,n+1}, ...p_{a,N}\}$. When there is no network effect, i.e., $\mathbf{W} = \mathbf{0}_N$, we have $\mathbf{W}^* = \mathbf{I}_N$, as a result, $R_n(p_{u,n}, p_{a,n}; p_{u,-n}, p_{a,-n}) = r_n(p_{u,n}, p_{a,n})$, i.e., the zero-sum game at each node is equivalent to Case 1. Due to the network effect, the average damage $\mathbb{E}[X_n] = \sum_{m=1}^N w^*_{nm} r_m(p_{u,m}, p_{a,m}) > r_n(p_{u,n}, p_{a,n})$, because $w^*_{nn} > 1$ and $w^*_{nm} \geq 0$ for $n \neq m$. It means that the network effect has a negative impact as expected. As nodes are connected, the level of risk will increase.

At each node n, the conflicting interests of the user n and the attacker n constitute a zero-sum game. Different from Case 1, the risk level at each node are coupled with the risk levels of the other nodes, and thus, the average effective loss is dependent on the actions

taken by other nodes. Following a similar reasoning of Case 1 in Section 3, we can formulate the minimax or max-min problem at each node n with

$$K_n(p_{u,n}, p_{a,n}, s_n; p_{u,-n}, p_{a,-n}) := \gamma_n(1-s_n)\sum_{m=1}^{N} w^*_{nm} r_m(p_{u,m}, p_{a,m}) + c_{u,n}p_{u,n} - c_{a,n}p_{a,n}, \quad (16)$$

$$\mathcal{S}_{u,a,n} := \left\{ (p_{u,n}, p_{a,n}) \middle| 1-\gamma_n(1-s_n)\left(w^*_{nn}\ln(\frac{p_{a,n}}{p_{u,n}}+1) + \sum_{m\neq n} w^*_{nm}\ln(\frac{p_{a,m}}{p_{u,m}}+1)\right) > 0 \right\}. \quad (17)$$

The first term of the objective function K_n captures the average effective loss given an insurance coverage level s_n, a local protection level $p_{u,n}$ and an attack level $p_{a,n}$. The second and third terms indicate the cost of user n and attacker n, respectively, with $c_{u,n} \in \mathbb{R}_{>0}$ and $c_{a,n} \in \mathbb{R}_{>0}$ being the cost parameters of user n and attacker n, respectively. (17) indicates the feasible set of node n. Note that the feasible inequality in (17) are coupled with other nodes.

Furthermore, the zero-sum game between user n and attacker n at node n yields a saddle-point equilibrium which can be defined as follows.

Definition 4 *At node $n \in \{1, ..., N\}$, given the actions of players $(p_{u,-n}, p_{a,-n})$ and the corresponding risk levels R_{-n} at other nodes, and the network parameters η, $\mathbf{W}^*$, let $\mathcal{S}_{u,n}(s_n)$ $\mathcal{S}_{a,n}(s_n)$, and $\mathcal{S}_{u,a,n}(s_n)$ be the action sets for user n and attacker n given an insurance coverage level s_n, then the strategy pair $(p^*_{u,n}, p^*_{a,n})$ is a saddle-point equilibrium (SPE-n) of the zero-sum game at node n defined by the triple $G_{z,n} := \langle \{User_n, Attacker_n\}, \{\mathcal{S}_{u,n}(s_n), \mathcal{S}_{a,n}(s_n), \mathcal{S}_{u,a,n}(s_n)\}, K_n \rangle$, if*

$$K_n(p^*_{u,n}, p_{a,n}, s_n; p_{u,-n}, p_{a,-n}) \leq K_n(p^*_{u,n}, p^*_{a,n}, s_n; p_{u,-n}, p_{a,-n}) \leq K_n(p_{u,n}, p^*_{a,n}, s_n; p_{u,-n}, p_{a,-n}), \quad (18)$$

$\forall p_{u,n} \in \mathcal{S}_{u,n}(s_n), p_{a,n} \in \mathcal{S}_{a,n}(s_n), (p_{u,n}, p_{a,n}) \in \mathcal{S}_{u,a,n}(s_n)$, *where K_n and $\mathcal{S}_{u,a,n}(s_n)$ is the objective function and the feasible set defined in (16) and (17), respectively.*

Furthermore, the strategy pairs $\{(p^*_{u,n}, p^*_{a,n})\}_{n\in\{1,...,N\}}$ is a saddle-point equilibrium (SPE-

N) of the game of N zero-sum games at each node if for every $n \in \{1, ..., N\}$,

$$K_n(p^*_{u,n}, p_{a,n}, s_n; p^*_{u,-n}, p^*_{a,-n}) \leq K_n(p^*_{u,n}, p^*_{a,n}, s_n; p^*_{u,-n}, p^*_{a,-n}) \leq K_n(p_{u,n}, p^*_{a,n}, s_n; p^*_{u,-n}, p^*_{a,-n}). \tag{19}$$

The definition indicates that if a pair $(p^*_{u,n}, p^*_{a,n})$ at node n satisfies (18), then it is a SPE-n of the zero-sum game between user n and attacker n. Note that $(p^*_{u,n}, p^*_{a,n})$ also depends on the actions of other players at other nodes. The definition also indicates that the game of N zero-sum games in this network admits a SPE-N if all the strategy pairs $(p^*_{u,n}, p^*_{a,n})$ at every node satisfy (19).

Proposition 7 *At node* $n \in \{1, ..., N\}$, *given the actions of players* $(p_{u,-n}, p_{a,-n})$ *and the corresponding risk level* R_{-n} *at other nodes, and the network parameters* η, $\mathbf{W}^*$, *if an insurance coverage level* s_n *satisfies*

$$1 - \gamma_n(1 - s_n)\left(\ln(\frac{c_{u,n}}{c_{a,n}} + 1) + \sum_{m \neq n} w^*_{nm} \ln(\frac{p_{a,m}}{p_{u,m}} + 1)\right) > 0, \tag{20}$$

there exists a unique SPE-n to the zero-sum game defined in Definition 4, given by

$$p^*_{u,n} = \frac{\gamma_n(1-s_n)w^*_{nn}}{c_{u,n}+c_{a,n}}, \quad p^*_{a,n} = \frac{c_{u,n}\gamma_n(1-s_n)w^*_{nn}}{c_{a,n}(c_{u,n}+c_{a,n})}. \tag{21}$$

Furthermore, if $\{s_n\}_{n\in\{1,...,N\}}$ *satisfy*

$$1 - \gamma_n(1 - s_n)\left(\sum_{m=1}^{N} w^*_{nm} \ln(\frac{c_{u,m}}{c_{a,m}} + 1)\right) > 0, \quad \forall n \in \{1, ..., N\}, \tag{22}$$

there exists a unique SPE-N to the game of N zero-sum games defined in Definition 4, which is the same as (21), $\forall n \in \{1, ..., N\}$.

Proof. See Appendix B. ■

Proposition 7 indicates the SPE-n of the zero-sum game between the user and the attacker at each node. The SPE-n at each node does not depend on the actions of players at other

nodes. With the increase of the insurance coverage, both the user and the attacker will take weaker actions. Comparing Proposition 7 with Proposition 1 for Case 1, we note that the equilibrium solution in Case 2 naturally incorporates w^*_{nn}, demonstrating the network impact on the security of each node. Since $w^*_{nn} > 1$, $p^*_{u,n} > p^*_u, p^*_{a,n} > p^*_a$, it can be seen that the users and the attackers take stronger protection and attack actions, respectively, when nodes are networked. Proposition 7 also indicates the SPE-N of the game of N zero-sum games. Following similar steps in Case 1, we have the following theorem regarding the SPE-n and SPE-N.

Theorem 1 *The following facts of SPE-n and SPE-N in Case 2 holds.*

(i) Peltzman Effect*: When s_n is higher, the SPE-n $p^*_{u,n}$ of user n tends to be smaller.*

(ii) Invariability of The SPE-n Ratio*: The SPE-n satisfies $p^*_{u,n}c_{u,n} = p^*_{a,n}c_{a,n}$. Specially, $\frac{p^*_{a,n}}{p^*_{u,n}} = \frac{c_{u,n}}{c_{a,n}}$, if $p^*_{u,n}, p^*_{a,n} \neq 0$.*

(iii) Constant Cost Determined SPE-N Risk*: User n has a constant SPE-N risk level $R^*_n = \sum_{m=1}^N w^*_{nm}\ln(\frac{p^*_{a,m}}{p^*_{u,m}} + 1) = \sum_{m=1}^N w^*_{nm}\ln(\frac{c_{u,m}}{c_{a,m}} + 1)$.*

(iv) At the SPE-N of the game of N zero-sum games, the average direct loss of user n is $\mathbb{E}(X_n) = R^*_n$, the average effective loss of user n is $\mathbb{E}(\xi_n) = (1 - s_n)R^*_n$, the expected payment of the insurer to user n is $\mathbb{E}(s_nX_n) = s_nR^*_n$.

Theorem 1 indicate similar results to Remark 1, Corollary 1, Remark 2 and Corollary 2 of Case 1. Note that the average loss at node n not only depends on the actions of the user and the attacker at this node, but also player's actions at other nodes, which is different from Corollary 2 of Case 1. Thus, the average loss at each node is larger than the average loss of Case 1 due to the network effects. Moreover, the expected payment of the insurer is also higher.

Following similar steps in Case 1, we reach the following proposition on insurability.

Proposition 8 (Fundamental Limits on Insurability) *Given an insurance coverage level* s_n *that* $1-\gamma_n(1-s_n)\left(\sum_{m=1}^{N} w_{nm}^{*}\ln(\frac{c_{u,m}}{c_{a,m}}+1)\right)\leq 0$, $(p_{u,n}^{*}, p_{a,n}^{*})$ *does not satisfy (22), thus, the average direct loss of user* n $\mathbb{E}(X_n)\to\infty$, *and the game of* N *zero-sum games defined in Definition 4 does not admit an SPE-*N. *Thus, user* n *is not insurable, as the insurance policy cannot mitigate his loss. Insurers will not also provide insurance to users who are not insurable.*

Each user must pay the insurer a subscription fee T_n to be insured. The average effective loss of user n at SPE-N with subscription fee T_n is $(1-s_n)R_n^{*}+T_n=(1-s_n)\sum_{m=1}^{N} w_{nm}^{*}\ln(\frac{c_{u,m}}{c_{a,m}}+1)+T_n$, which is monotonically decreasing in s_n. Follow similar steps in Condition 1 and Condition 2, and we have the following condition.

Condition 5 *User* n *will subscribe to the insurance if the following conditions are satisfied.*

(i) Individual Rationality (IR-u,n)*: The subscription fee must satisfy*

$$T_n\leq T_{\max,n}:=R_n^{*}=\sum_{m=1}^{N} w_{nm}^{*}\ln(\frac{c_{u,m}}{c_{a,m}}+1).$$

(ii) Incentive Compatibility (IC-u,n)*: For the subscription fee* $T_n\leq T_{\max,n}$, *user* n *will subscribe to the insurance if the coverage level* s_n *satisfies* $s_n\geq s_{0,n}(T_n)=\frac{T_n}{R_n^{*}}=\frac{T_n}{\sum_{m=1}^{N} w_{nm}^{*}\ln(\frac{c_{u,m}}{c_{a,m}}+1)}$.

Compared with Condition 1 and Condition 2 in Case 1, $T_{\max,n}$ is larger and $s_{0,n}(T)$ is smaller due to network effects. This fact indicates that the user will accept a higher subscription fee and a lower coverage level from the insurer as the network effect can increase the average loss of the user. In the following subsections, we consider two types of insurers: the case with a centralized insurer and the case with a fully distributed one.

4.2 Problem of N Insurers

In this subsection, we consider that the network contains N insurers with each node has 1 insurer who aims to minimize the effective loss of user n at this node and maximize his

operating profit. Note that the gross profit of insurer n is T_n, and the average payment to user n is $s_n R_n^* = s_n \sum_{m=1}^{N} w_{nm}^* \ln(\frac{c_{u,m}}{c_{a,m}} + 1)$ from Theorem 1, thus, with similar steps in Condition 3 and Condition 4, we reach the following conditions for insurers.

Condition 6 *Insurer n will provide the insurance to user n when the following conditions are satisfied.*

(i) Individual Rationality (IR-i, n)*: The insurance policy at node n must satisfy*

$$T_n - s_n R_n^* = T_n - s_n \sum_{m=1}^{N} w_{nm}^* \ln(\frac{c_{u,m}}{c_{a,m}} + 1) \geq 0.$$

(ii) Feasibility (F-i, n)*: The coverage level at node n must be feasible, i.e., $s_n > 1 - \frac{1}{\gamma\left(\sum_{m=1}^{N} w_{nm}^* \ln(\frac{c_{u,m}}{c_{a,m}}+1)\right)}$.*

With (IR-u,n) and (IC-u,n) constraints for user n, and (IR-i,n) and (F-i, n) constraints for insurer n, the insurer's objective can be captured as the following linear programming problem.

$$\begin{aligned} \min_{\{0 \leq s_n \leq 1, T_n \geq 0\}} \; & J_{i,n}(s_n, T_n) := \gamma_n (1 - s_n) \sum_{m=1}^{N} w_{nm}^* \ln(\frac{c_{u,m}}{c_{a,m}} + 1) + c_{s,n}(s_n \sum_{m=1}^{N} w_{nm}^* \ln(\frac{c_{u,m}}{c_{a,m}} + 1) - T_n) \\ \text{s.t.} \quad & (\text{IR-}u, n), (\text{IC-}u, n), (\text{IR-}i, n), (\text{F-}i, n). \end{aligned} \tag{23}$$

The first and the second terms of the objective function indicate the average effective loss of user n under the coverage s_n and the operating profit of insurer n. Note that parameter $c_{s,n}$ indicates the trade-off of a safer user n and a larger profit of insurer n.

Furthermore, the solution of Problem (23) and the corresponding SPE-N defined in Definition 4 yield an equilibrium for the bi-level game in Case 2(a) which can be defined as

Definition 5 *Let $\mathcal{S}_{i,n}$ be the action set for insurer n, $\mathcal{S}_{u,n}(s_n)$ and $\mathcal{S}_{a,n}(s_n)$ be the action sets for user n and attacker n given the insurance coverage level, the strategy pairs $(p_{u,n}^*, p_{a,n}^*, \{s_n^*, T_n^*\})_{n \in \{1,\ldots,N\}}$ is called a bi-level game Nash equilibrium (BGNE-N) of the bi-level game in Case 2(a) defined by the triple $G_{2(a)} := \langle \{Users, Attackers, Insurers\}, \{\{\mathcal{S}_{u,n}(s_n)\}, \{\mathcal{S}_{a,n}(s_n)\},$ if $\{s_n^*, T_n^*\}$ solves Problem (23) with the BGNE-N objective function $J_{i,n}^*$, and the strategy*

pair $(p^*_{u,n}, p^*_{a,n})$ *is the SPE-N of the game of N zero-sum games defined in Definition 4 with the equilibrium payoff* K^*_n *under the insurance policy* $\{s^*_n, T^*_n\}$.

Note that (IR-i,n) and (IC-u,n) together indicate that s_n and T_n must satisfy

$$T_n = s_n R^*_n = s_n \sum_{m=1}^{N} w^*_{nm} \ln\left(\frac{c_{u,m}}{c_{a,m}} + 1\right). \tag{24}$$

Corollary 4 *Equality (24) indicates the following observations:*

(i) Zero Operating Profit Principle: *The operating profit of insurer n is always* 0, *as* $T_n - s_n R^*_n = 0$.

(ii) Linear Insurance Policy Principle: *The insurer n can only provide the insurance policy* s_n *and* T_n *that satisfies (24), so that user n subscribes to the insurance provided by the insurer n.*

With (24), the optimal insurance for insurer n is summarized in the following proposition.

Proposition 9 *The optimal insurance policy for insurer n is*

$$s^*_n = 1; \quad T^*_n = T_{n,\max} = \sum_{m=1}^{N} w^*_{nm} \ln\left(\frac{c_{u,m}}{c_{a,m}} + 1\right). \tag{25}$$

Together with Proposition 7, we have the following proposition of the BGNE-N of the bi-level game for Case 2(a).

Proposition 10 *The bi-level game of Case 2(a) between N users, N attackers and N insurers at a network with N nodes admits a unique BGNE-N solution at each node* $(p^*_{u,n}, p^*_{a,n}, \{s^*_n, T^*_n\})$ $= (0, 0, \{1, \sum_{m=1}^{N} w^*_{nm} \ln(\frac{c_{u,m}}{c_{a,m}} + 1)\})$. *At the equilibrium, insurer n provides a full coverage for user n and charges a maximum subscription fee from user n. User n and attacker n take no actions. The equilibrium demonstrates that cyber insurance will effectively mitigate the loss.*

4.3 Problem of 1 Insurer

In this subsection, we consider that the network contains only 1 insurer with the aim to minimize the effective loss of all the users and maximize his operating profit. Following similar steps in Condition 6, we arrive at the following condition for the insurer.

Condition 7 *The insurer will provide the insurance to each user when the following conditions are satisfied.*

(i) Individual Rationality (IR-i)*: The insurance policy at each node n must satisfy* $\sum_{n=1}^{N}(T_n - s_n R_n^*) = \sum_{n=1}^{N}(T_n - s_n \sum_{m=1}^{N} w_{nm}^* \ln(\frac{c_{u,m}}{c_{a,m}} + 1)) \geq 0$.

(ii) Feasibility (F-i)*: The coverage level at each node n must be feasible as the item (ii) in Condition 6.*

Thus, the insurer's objective can be captured as the following linear programming problem,

$$\begin{aligned} \min_{\{s_n, T_n\}} & \sum_{n=1}^{N} \gamma_n (1 - s_n) \sum_{m=1}^{N} w_{nm}^* \ln(\tfrac{c_{u,m}}{c_{a,m}} + 1) + \sum_{n=1}^{N} c_{s,n}(s_n \sum_{m=1}^{N} w_{nm}^* \ln(\tfrac{c_{u,m}}{c_{a,m}} + 1) - T_n) \\ \text{s.t.} \quad & (\text{IR-}u, n), (\text{IC-}u, n), (\text{IR-}i), (\text{F-}i). \end{aligned} \tag{26}$$

Compared to Problem (23), the insurer's objective in Problem (26) is to minimize the global average effective loss of all the users at every node, and maximize the global operating profit. The rationality constraint for the insurer also takes into account of all the users. Moreover, the rationality constraints of the insurer and the incentive compatibility constraints of the users have the following properties.

Theorem 2 *(IC-u, n) and (IR-i) indicate the following observations:*

(i) Zero Operating Profit Principle: *The operating profit of insurer n is always* 0*, as* $T_n - s_n R_n^* = 0$.

(ii) Linear Insurance Policy Principle: *The insurer can only provide the insurance policy s_n and T_n that satisfy (24), so that the user n subscribes to the insurance.*

Proof. From the constraint (IC-u,n), we have

$$\begin{aligned}\sum_{n=1}^{N}(T_n - s_n\sum_{m=1}^{N} w_{nm}^{*}\ln(\tfrac{c_{u,m}}{c_{a,m}}+1)) &\leq \sum_{n=1}^{N}(T_n - s_{0,n}\sum_{m=1}^{N} w_{nm}^{*}\ln(\tfrac{c_{u,m}}{c_{a,m}}+1)) \\ &\leq \sum_{n=1}^{N}(T_n - \tfrac{T_n}{\sum_{m=1}^{N} w_{nm}^{*}\ln(\frac{c_{u,m}}{c_{a,m}}+1)}\sum_{m=1}^{N} w_{nm}^{*}\ln(\tfrac{c_{u,m}}{c_{a,m}}+1)) \leq 0.\end{aligned}$$

Together with (IR-i) constraint, we have $\sum_{n=1}^{N}(T_n - s_n\sum_{m=1}^{N} w_{nm}^{*}\ln(\frac{c_{u,m}}{c_{a,m}}+1)) = 0$, which indicates that the profit of the insurer is 0. Moreover, with (IR-u,n), the fact that the sum of all non-positive terms equal to 0 shows that $T_n - s_n\sum_{m=1}^{N} w_{nm}^{*}\ln(\frac{c_{u,m}}{c_{a,m}}+1) = 0$, which is the same as (24). ■

Note that Theorem 2 admits the same relation between the subscription fee and the coverage level as in Corollary 4. The insurer cannot achieve better by controlling all the nodes. Thus, the optimal insurance policy for 1 insurer at each node is the same as the optimal insurance policy for N insurers at each node, which is shown in Proposition 9. As a result, together with Proposition 7, the bi-level game of Case 2(b) admits an equilibrium where the insurer provides a full coverage for user n and charges a maximum subscription fee from user n, user n and attacker n take no actions.

5 Case 3: N Nodes-1 User-1 Attacker-1 Insurer

In this section, we consider the same network with N nodes in Section 4. Note that in this network there exist only one user, one attacker and one insurer. This setting differs from Section 3 and Section 4 in that the user and the attacker consider the network as a system.

5.1 Zero-Sum Game between User and Attacker

The user aims to reduce the average effective losses of all the nodes while the attacker aims to maximize the losses. The local protection levels and the attack levels can be represented as $\{p_{u,n}\}_{n\in\{1,\ldots,N\}}$ and $\{p_{a,n}\}_{n\in\{1,\ldots,N\}}$, respectively. The insurance policy can be represented by coverage levels $\{s_n\}_{n\in\{1,\ldots,N\}}$ and subscription fee T. Recall (16) and (17), by following a

similar step in Section 4, we can describe the zero-sum game with:

$$K\left(\{p_{u,n}\}_{n\in\{1,...,N\}},\{p_{a,n}\}_{n\in\{1,...,N\}},\{s_n\}_{n\in\{1,...,N\}}\right)=\sum_{n=1}^{N}K_n(p_{u,n},p_{a,n},s_n;p_{u,-n},p_{a,-n}),\quad(27)$$

$$\mathcal{S}_{u,a}:=\left\{\left(\{p_{u,n}\}_{n\in\{1,...,N\}},\{p_{a,n}\}_{n\in\{1,...,N\}}\right)\middle|(p_{u,n},p_{a,n})\in\mathcal{S}_{u,a,n}\right\}.\quad(28)$$

where K_n and $\mathcal{S}_{u,a,n}$ come from (16) and (17), respectively. Note that (28) indicates the feasible set of the user. Furthermore, the zero-sum game yields a saddle-point equilibrium which can be defined as follows.

Definition 6 *Given the network parameters $\eta,\mathbf{W}^*$, let $\mathcal{S}_{u,n}(\{s_n\})$, $\mathcal{S}_{a,n}(\{s_n\})$ and $\mathcal{S}_{u,a,n}(\{s_n\})$ be the action sets for the user and the attacker given the insurance coverage level $\{s_n\}$ at each node n. Then the strategy pair $\left(\{p^*_{u,n}\}_{n\in\{1,...,N\}},\{p^*_{a,n}\}_{n\in\{1,...,N\}}\right)$ is a saddle-point equilibrium (SPE) of the zero-sum game defined by the triple $G_z:=\langle\{User,Attacker\},\{\mathcal{S}_{u,n}(s_n),\mathcal{S}_{a,n}(s_n),\mathcal{S}_{u,a,n}(\{s_n\})\}_{n\in}$ if*

$$K\left(\{p^*_{u,n}\},\{p_{a,n}\},\{s_n\}\right)\le K\left(\{p^*_{u,n}\},\{p^*_{a,n}\},\{s_n\}\right)\le K\left(\{p_{u,n}\},\{p^*_{a,n}\},\{s_n\}\right),\quad(29)$$

where K is the objective function from (27).

Proposition 11 *Given network parameters $\eta,\mathbf{W}^*$, if $1-\gamma_n(1-s_n)\sum_{m=1}^{N}w^*_{nm}\ln(\frac{c_{u,m}}{c_{a,m}}+1)>0,\forall n\in\{1,...,N\}$, the SPE of the zero-sum game is $\left(\{p^*_{u,n}\}_{n\in\{1,...,N\}},\{p^*_{a,n}\}_{n\in\{1,...,N\}}\right)$, where*

$$p^*_{u,n}=\frac{\sum_{m=1}^{N}\gamma_m(1-s_m)w^*_{mn}}{c_{u,n}+c_{a,n}},\quad p^*_{a,n}=\frac{c_{u,n}\sum_{m=1}^{N}\gamma_m(1-s_m)w^*_{mn}}{c_{a,n}(c_{u,n}+c_{a,n})},\quad\forall n\in\{1,...,N\}.\quad(30)$$

Proof. See Appendix C. ■

Proposition 11 provides a closed-form SPE of the zero-sum game between an user and an attacker in a network with N nodes. Compared to Proposition 1 for Case 1, the equilibrium defense and attack actions in Proposition 11 are stronger with network effects. Compared to Proposition 7 for N users and N attackers case, the equilibrium actions in Proposition 11

with are coupled with other nodes' insurance policies $\{s_m\}$, network parameters $\{w^*_{mn}\}$, and $\{\gamma_m\}$. Thus, the user and the attacker spend more efforts at each node.

Theorem 3 *The following facts of SPE in Case 3 hold.*

(i) Peltzman Effect*: When s_n is higher, the SPE of the user at node n $p^*_{u,n}$ tend to be smaller.*

(ii) Invariability of The SPE Ratio*: The SPE satisfies $p^*_{u,n}c_{u,n} = p^*_{a,n}c_{a,n}$. Specially, $\frac{p^*_{a,n}}{p^*_{u,n}} = \frac{c_{u,n}}{c_{a,n}}$ if $p^*_{u,n}, p^*_{a,n} \neq 0$.*

(iii) Constant Cost Determined SPE Risk*: At node n, the user has a constant SPE risk level* $R^*_n = \sum_{m=1}^N w^*_{nm}\ln(\frac{p^*_{a,m}}{p^*_{u,m}} + 1) = \sum_{m=1}^N w^*_{nm}\ln(\frac{c_{u,m}}{c_{a,m}} + 1)$.

(iv) At the SPE, the average direct loss of the user is $\mathbb{E}(\sum_{n=1}^N X_n) = \sum_{n=1}^N \mathbb{E}(X_n) = \sum_{n=1}^N R^*_n$, the average effective loss of the user is $\mathbb{E}(\sum_{n=1}^N \xi_n) = \sum_{n=1}^N \mathbb{E}(\xi_n) = \sum_{n=1}^N R^*_n$, the expected payment of the insurer to the user is $\mathbb{E}(\sum_{n=1}^N s_n X_n) = \sum_{n=1}^N s_n R^*_n$.

This theorem gives similar conclusions as Remark 1, Corollary 1, Remark 2 and Corollary 2 of Case 1 and Theorem 1 in Case 2. Furthermore, we have the following conditions that the user will subscribe to the insurance.

Condition 8 *The user will subscribe to the insurance if the following conditions are satisfied.*

(i) Individual Rationality (IR-u)*: The subscription fee must satisfy* $T \leq T_{\max} := \sum_{n=1}^N R^*_n = \sum_{n=1}^N \sum_{m=1}^N w^*_{nm}\ln(\frac{c_{u,m}}{c_{a,m}} + 1)$.

(ii) Incentive Compatibility (IC-u)*: For the subscription fee $T \leq T_{\max}$, the user will subscribe to the insurance if the coverage level s_n satisfies $\sum_{n=1}^N \sum_{m=1}^N s_n w^*_{nm}\ln(\frac{c_{u,m}}{c_{a,m}} + 1) \geq T$.*

Compared to Case 2, $T_{\max} = \sum_{n=1}^N T_{\max,n}$, but s_n depends on the insurance coverage levels in other nodes.

5.2 Insurer's Problem

Similar to Section 4.C, insurer in Case 3 aims to minimize the average effective loss of the network, but the insurer charges a single subscription fee T to the only user of the network. Following similar steps in Section 4.C, we arrive the following conditions for the insurer.

Condition 9 *The insurer will provide the insurance to the user when the following conditions are satisfied.*

(i) Individual Rationality (IR-i)*: The insurance policy must satisfy*

$$T - \sum_{n=1}^{N} s_n R_n^* = T - \sum_{n=1}^{N} s_n \sum_{m=1}^{N} w_{nm}^* \ln\left(\frac{c_{u,m}}{c_{a,m}} + 1\right) \geq 0.$$

(ii) Feasibility (F-i)*: The coverage level at each node n must be feasible as the item (ii) in Condition 6.*

As a result, the insurer's objective can be captured as the following linear programming problem:

$$\begin{aligned} \min_{\{\{s_n\},T\}} \; & J_i(\{s_n\}, T) := \sum_{n=1}^{N} \gamma_n (1 - s_n) \sum_{m=1}^{N} w_{nm}^* \ln\left(\frac{c_{u,m}}{c_{a,m}} + 1\right) + c_s\left(\sum_{n=1}^{N} \sum_{m=1}^{N} s_n w_{nm}^* \ln\left(\frac{c_{u,m}}{c_{a,m}} + 1\right) - T\right) \\ \text{s.t.} \quad & (\text{IR-}u), (\text{IC-}u), (\text{IR-}i), (\text{F-}i). \end{aligned} \tag{31}$$

Furthermore, the solution of Problem (31) and the corresponding SPE defined in Definition 6 yield an equilibrium for the bi-level game in Case 3 which can be defined as

Definition 7 *Let $\mathcal{S}_i$ be the action set for the insurer, $\mathcal{S}_u(\{s_n\})$ and $\mathcal{S}_a(\{s_n\})$ be the action sets for the attacker and the user given the insurance coverage levels, the strategy pair $(\{p_{u,n}^*\}, \{p_{a,n}^*\}, \{\{s_n^*\}, T^*\})$ is called a bi-level game Nash equilibrium (BGNE) of the bi-level game in Case 3 defined by the triple $G_3 := \langle \{User, Attacker, Insurer\}, \{\mathcal{S}_u(\{s_n\}), \mathcal{S}_a(\{s_n\}), \mathcal{S}_i\}, K, J_i \rangle$, if $\{\{s_n^*\}, T^*\}$ solves Problem (31) with the BGNE function $J_{i,n}^*$, and the strategy pair $(p_{u,n}^*, p_{a,n}^*)$ is the SPE of the zero-sum game defined in Definition 6 with the equilibrium payoff K^* under the insurance policy $\{\{s_n^*\}, T^*\}$.*

Note that (IR-i) and (IC-u) together indicate that s_n and T must satisfy

$$T = \sum_{n=1}^{N} s_n R_n^* = \sum_{n=1}^{N} s_n \sum_{m=1}^{N} w_{nm}^* \ln(\frac{c_{u,m}}{c_{a,m}} + 1). \tag{32}$$

Theorem 4 *(IC-u) and (IR-i) indicate the following observations:*

(i) Zero Operating Profit Principle: *The operating profit of the insurer is always* 0*, as* $T - \sum_{n=1}^{N} s_n R_n^* = 0$.

(ii) Linear Insurance Policy Principle: *The insurer can only provide the insurance policy* s_n *and* T_n *that satisfies (32), so that the user subscribes to the insurance provided by the insurer.*

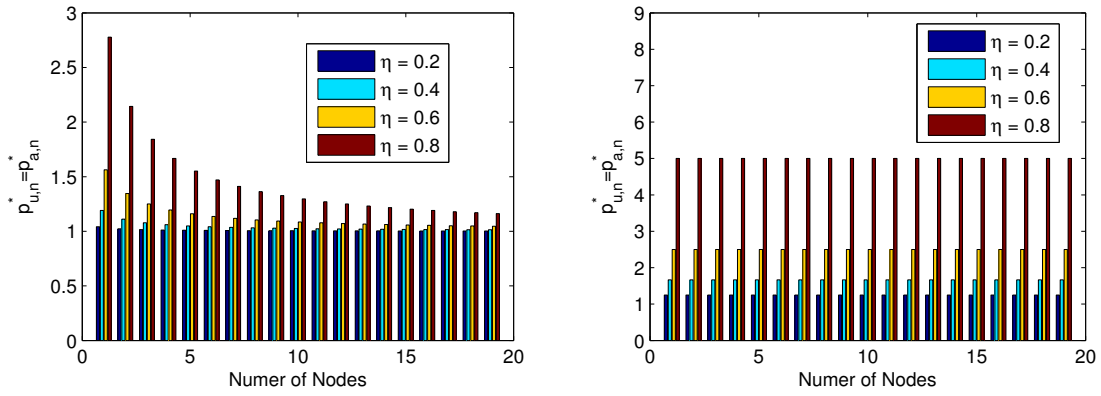
As a result, the optimal insurance policy for the insurer can be shown in the following proposition.

Proposition 12 *The optimal insurance policy for the insurer is*

$$s_n^* = 1, \forall n \in \{1, ..., N\}; \quad T^* = T_{\max} = \sum_{n=1}^{N} \sum_{m=1}^{N} w_{nm}^* \ln(\frac{c_{u,m}}{c_{a,m}} + 1). \tag{33}$$

Together with Proposition 11, we have the following proposition of the equilibrium solution of the bi-level game in Case 3.

Proposition 13 *The bi-level game of Case 3 admits a BGNE* $(\{p_{u,n}^*\}, \{p_{a,n}^*\}, \{\{s_n^*\}, T^*\})$ $= (\{0\}, \{0\}, \{\{1\}, \sum_{n=1}^{N} \sum_{m=1}^{N} w_{nm}^* \ln(\frac{c_{u,m}}{c_{a,m}} + 1)\})$. *The insurer provides a full coverage for every node and charges a maximum subscription fee from the user. The user and the attacker take no actions at the equilibrium. The equilibrium demonstrates that cyber insurance will effectively mitigate the loss.*



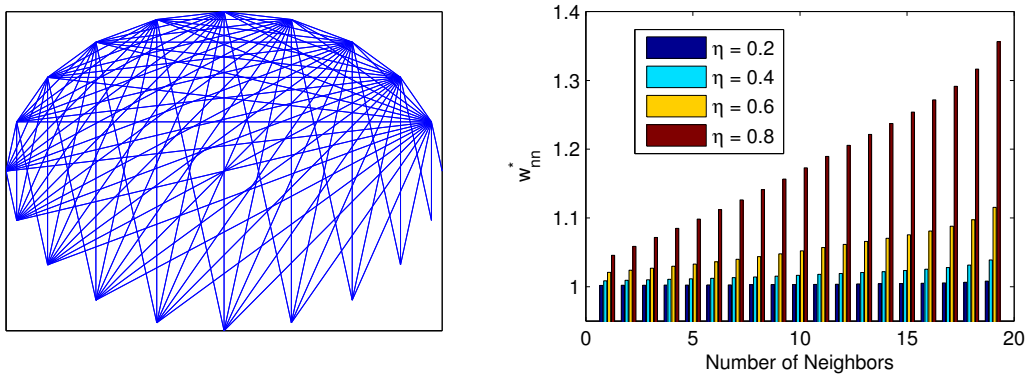
(a) N Nodes-N Users-N Attackers (b) N Nodes-1 User-1 Attacker

Figure 5: Saddle-point local protection level and attack level at node n in a fully connected network with N nodes. Each node has the same γ_n, s_n, $c_{u,n}$ and $c_{a,n}$, and they have $\frac{\gamma_n(1-s_n)}{c_{u,n}+c_{a,n}} = 1$. η denotes the discount rate of the network effects.

6 Numerical Experiments

In this section, we present numerical examples to demonstrate network effects on the cyber insurance. Consider a fully connected network with N nodes. The risk level of the nodes are coupled. We assume that the probability that an attack on node n can create an adversarial impact on node $m \neq n$ is the same for all nodes in the network. Hence, we have $\mathbf{W} = \{w_{nm}\}$, where $w_{nn} = 0$ and $w_{nm} = \frac{1}{N-1}$, $\forall n, m \in \{1, ..., N\}, n \neq m$. We also consider that each node has the same γ_n, s_n, $c_{u,n}$ and $c_{a,n}$ that $\frac{\gamma_n(1-s_n)}{c_{u,n}+c_{a,n}} = \frac{c_{u,n}\gamma_n(1-s_n)}{c_{a,n}(c_{u,n}+c_{a,n})} = 1$. Thus, the insurance policy satisfies $s_n = 1 - \frac{c_{u,n}+c_{a,n}}{\gamma_n}$. Therefore, the SPE-$N$ of the user and the attacker at node n in N Nodes-N Users-N Attackers case can be described as $p^*_{u,n} = p^*_{a,n} = w^*_{nn}$, the SPE of the user and the attacker in Case 3 can be found as $p^*_{u,n} = p^*_{a,n} = \sum_{m=1}^{N} w^*_{mn}$. Note that w^*_{nn} and w^*_{nm} comes from Proposition 6 with $\mathbf{W}^* = (\mathbf{I}_N - \eta \mathbf{W}^T)^{-1}$, with η being the attenuation of damage when an attack propagates from a neighboring node. A larger η indicates that an attack on one node has a more significant impact on other nodes. Moreover, when $w^*_{nn} = 1$ and $w^*_{nm} = 0$, both cases have $p^*_{u,n} = p^*_{a,n} = 1$, i.e., the results of Case 1.

Fig. 5 shows that, with a larger discount rate η, the equilibrium local protection level of the user and the attack level of the attacker are higher, indicating that the user and the



(a) Network (b) w^*_{nn}

Figure 6: The value of w^*_{nn} for nodes with different numbers of neighbors under different η. The network has 20 nodes.

attacker are required to spend more efforts when the network effect is strong. Moreover, as the number of nodes increases, the results of Case 2(a) an Case 2(b) satisfy $p^*_{u,n} = p^*_{a,n} \to 1$, i.e., Case 1, while in the Case 3, $p^*_{u,n} = p^*_{a,n} = \frac{1}{1-\eta}$, which is independent of the size of the network, and it corroborates the result of (iii) in Proposition 6. From Proposition 11, note that since $\sum_{m=1}^{N} w^*_{mn} = \frac{1}{1-\eta}$, the value of w^*_{nn} describes the level of dependence of user's decision on attacker and insurer's decisions at the node. When w^*_{nn} is large, the user and the attacker's decisions tend to be less affected by the network effects, specially the insurer's decisions on other nodes.

In the next experiments, we consider the case when each node has different degrees. Note all the other variables are the same for each node. From Fig. 6, since w^*_{nn} increases with respect to η, the local protection level and attack level are high when η is large. Note that w^*_{nn} also increases with respect to the number of neighbors. Thus, users and attackers at nodes with more neighbors are required to spend more efforts at the equilibrium in Case 2(a) and 2(b). Since $\sum_{m=1}^{N} w^*_{mn} = \frac{1}{1-\eta}$, the user and the attackers' actions at nodes with more neighbors depend less on the the insurance coverage levels at other nodes in Case 3.

7 Dynamic Insurance

The main focus of the paper has been on the static analysis of the bi-level game-theoretic framework for cyber insurance problem. In this section, we will extend the static problem to a dynamic setting with a network of users and attackers.

7.1 Risk-Sensitive Cyber-Insurance

Consider a network with N users. The state of user i is denoted by $x_i(t) \in \mathcal{X}_i \subset \mathbb{R}_+$ which models the risk level that evolves over time. Let $x = \{x_i\}_{i=1}^N$ be the state vector of all users. Since users are connected by a network, the dynamics of the risk levels of the users are described by the following linear Itô stochastic differential equation:

$$dx(t) = (A(t)x(t) + B(t)u(t))dt + \sqrt{\varepsilon}D(t)d\mathcal{B}(t), \tag{34}$$

where $A(t) \in \mathbb{R}^{N\times N}$ is the state transition matrix; $B(t) \in \mathbb{R}^{N\times N}$ is the input matrix; $u(t) = \{u_i\}_{i=1}^N \in U := \prod_{i=1}^N U_i \subset \mathbb{R}^N$ is the control input; ϵ is a small positive number; $D(t) \in \mathbb{R}^{N\times N}$ is the volatility matrix; $\{\mathcal{B}(t), t \geq 0\}$ is a standard M-dimensional Brownian motion process with $\mathcal{B}(0) = 0$ with probability 1. Note that matrix A captures the network topology of the network. If two nodes are connected, then $A_{ij} \neq 0$. Each user can control their risk by employing defense mechanisms such as frequently changing passwords and adopting anti-virus software. The control law determined by each user can be generally described by $u_i(t) = \mu_i(I_i(t), t)$, where $\mu_i \in \Gamma_i$ is a class of policies that depend on the information structure $I_i(t)$ of user i. For example, when $I_i = \{x_i(t)\}$, a user can only observe his own risk state and the control policy is given by $u_i = \mu_i^{\mathrm{D}}(x_i)$, where $\mu_i^D \in \Gamma_i^{\mathrm{D}}$ is a distributed control policy and Γ_i^{D} denotes all the admissible control policies of this type. Similarly, when $I_i = \{x(t)\}$, a user can observe the state of the entire network. The control policy given by $u_i = \mu_i^{\mathrm{S}}(x), \mu_i^{\mathrm{S}} \in \Gamma_i^{\mathrm{S}}$ is a perfect-state feedback policy, and Γ_i^{S} denotes all the admissible control policies of this type.

In this section, we consider that risk-sensitive users who aim to minimize the following exponentiated cost functional.

$$J(\mu; t, x) = \delta \log \mathbb{E}\left\{\exp(\frac{1}{\delta})\left[q(x(t_f)) + \int_t^{t_f} g(\hat{t}, x(\hat{t}), u(\hat{t}))d\hat{t}\right]\right\}, \tag{35}$$

where $\delta > 0$ is the risk-sensitivity index for the users. Here, we assume that q and g are nonnegative, q is uniformly bounded on $[0, t_f]$, and g is uniformly bounded on $[0, t_f] \times \mathbb{R}^N \times U$. We further assume that $q(x(t_f)) := x'(t_f)Q_f x(t_f)$, where $Q_f \in \mathbb{R}^{N\times N}$, and

$$g(\hat{t}, x(\hat{t}), u(\hat{t})) = x'(t)Q(t)x(t) + u'(t)u(t),$$

where $Q(t) \in \mathbb{R}^{N\times N}$. The linear-quadratic structure of the problem lead to the following risk-sensitive optimal perfect-state feedback control:

$$u^*(t) = \mu^*(t; x) = -B'(t)Z(t)x, \quad 0 \le t \le t_f, \tag{36}$$

where $Z(\cdot)$ is the nonnegative definite solution of the generalized Riccati differential equation (RDE):

$$\begin{gathered} \dot{Z} + A'Z + ZA + Q - Z(BB' - (1/\gamma^2)DD')Z = 0, \\ Z(t_f) = Q_f. \end{gathered} \tag{37}$$

Note that $\gamma = \sqrt{\frac{\delta}{2\varepsilon}}$. Moreover, the value function is thus denoted by

$$V(t; x) = \inf_{\mu} J(\mu; t, x) = x'Z(t)x + l^{\varepsilon}(t), \quad t \ge 0, \tag{38}$$

where $l^{\varepsilon}(t) = \varepsilon \int_t^{t_f} Tr\left[Z(\hat{t})D(\hat{t})D'(\hat{t})\right] d\hat{t}$.

The users aim to further mitigate the risks of cyber-attacks with cyber insurance. Note that the user pays a premium to the insurer and the insurer will then provide a coverage policy $s : \mathbb{R}^N \to \mathbb{R}$ at time t_f. Here, we assume that the policy takes a quadratic form

$s(x(t_f)) = x'(t_f)Sx(t_f)$, where $S \in \mathbb{R}^{N\times N}$ is a semi-positive definite matrix and $x(t_f)$ is the final state of the users. The insurance policy is parametrized by S and it can take different forms depending on whether the insurance is centralized or distributed.

As a result, the risk-sensitive cost functional with cyber insurance becomes

$$J^I(\mu; t, x|S) = \delta \log \mathbb{E}\left\{\exp(\frac{1}{\delta})\left[q(x(t_f)) - s(x(t_f)) + \int_t^{t_f} g(\hat{t}, x(\hat{t}), u(\hat{t}))d\hat{t}\right]\right\}. \tag{39}$$

The optimal control input then becomes

$$u^*(t) = \mu^*(t; x) = -B'(t)\widehat{Z}(t)x, \quad 0 \le t \le t_f, \tag{40}$$

and the value function is

$$V^I(t; x) = \inf_{\mu} J^I(\mu; t, x) = x'\widehat{Z}(t)x + l^{\varepsilon}(t), \quad t \ge 0, \tag{41}$$

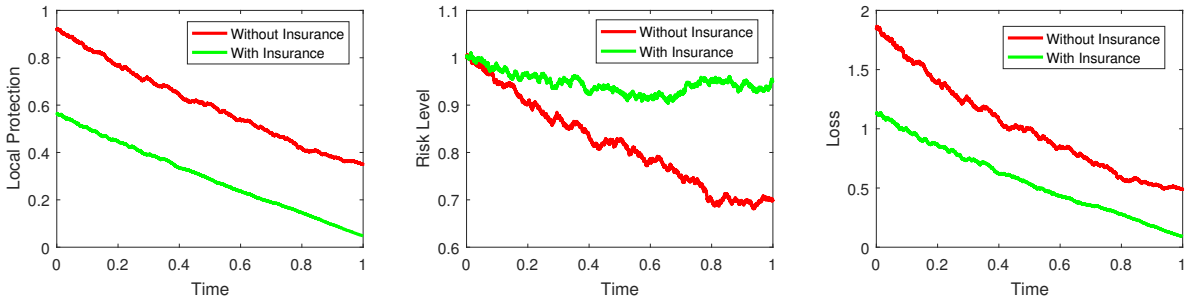
where $l^{\varepsilon}(t) = \varepsilon \int_t^{t_f} Tr\left[\widehat{Z}(\hat{t})D(\hat{t})D'(\hat{t})\right] d\hat{t}$, and $\widehat{Z}$ is given by:

$$\begin{gathered}\dot{\widehat{Z}} + A'\widehat{Z} + \widehat{Z}A + Q - \widehat{Z}(BB' - (1/\gamma^2)DD')\widehat{Z} = 0, \\ \widehat{Z}(t_f) = Q_f - S.\end{gathered} \tag{42}$$

Note that the only difference between (37) and (42) is the final value of Z, and when $S = \mathbf{0}$, (40) and (42) are the same as (36) and (37), respectively.

Equations (40), (41) and (42) capture the behavior of a risk-sensitive user under cyber insurance. Note that the user only subscribes the insurance when the cost under insurance is lower than the cost under no insurance. Let $W \in \mathbb{R}_+$ denote the subscription fee, and then we have that the user will subscribe the insurance when

$$V^I(t; x) + W \le V(t; x). \tag{43}$$



(a) Local protection. (b) Risk level. (c) Loss.

Figure 7: Continuous-time Risk-sensitive User.

Thus, the insurer's problem is given by

$$\begin{aligned} \min_{\{S,W\}} \ & \mathbb{E}\left\{f(x(t_f)) + s(x(t_f))\right\} - W \\ \text{s.t.} \ \ & V^I(t;x) + W \leq V(t;x). \end{aligned} \tag{44}$$

Here, f is the cost of the network to the insurer if the state of the terminal state of users are x_{t_f}. Note that minimizing $f(x(t_f))$ captures the insurer's intention to minimize the loss of the user, and minimizing $s(x(t_f)) - W$ captures the insurer's objective to maximize his profit. The constraint captures the incentive compatibility of the user. The individual rationality constraints have been implicitly built into the value function V^I of optimization problem (44). The solution $\{S^*, W^*\}$ to Problem (44) is the optimal insurance policy with which the insurer makes a profit and the user mitigates his loss.

Example: Consider that there is only one user at this network with $A = 0.1$, $B = 0.5$, $D = 0.1$, $Q = 1$, $Q_f = 1$. At time $t = 0$, the user has risk level $x_0 = 1$. The insurer provides the insurance coverage level $s = 0.8$. Numerical results are shown in Fig. 7. We can see from the figure that the user tends to take lower local protection levels when he subscribes to the insurance, which is referred as Peltzman effect. As a result, the risk level of the user becomes higher under the insurance. However, the effective loss of the user is lower as the insurer covers part of the loss.

7.2 Markov Decision Process Cyber-Insurance

Let $s_t \in \mathcal{S}$ denote the state of the user at time t, with $\mathcal{S} = \{G, B\}$. For $t \geq 0$, if $s_t = G$, the user is in a good state with a lower loss, otherwise, the user is in a bad state with a higher loss. To avoid high total losses, the user aims to stay at good state as often as possible. We further define the action set of the user $\mathcal{A} = \{a_H, a_L\}$. By taking action $a_t = a_H$, the user has a high local protection level; otherwise, the user has a low local protection level. Let $p^a_{s,s'} = Pr(s_{t+1} = s' | s_t = s, a_t = a)$ denotes the probability that action a in state s at time t will lead to state s' at time $t+1$. Note that $p^{a_H}_{s_G,s_G} + p^{a_H}_{s_G,s_B} = 1$, $p^{a_H}_{s_B,s_G} + p^{a_H}_{s_B,s_B} = 1$, $p^{a_L}_{s_G,s_G} + p^{a_L}_{s_G,s_B} = 1$, $p^{a_L}_{s_B,s_G} + p^{a_L}_{s_B,s_B} = 1$. Furthermore, we make the following assumptions on $p^a_{s,s'}$:

- $p^{a_H}_{s_G,s_B} < p^{a_H}_{s_G,s_G}$, i.e., the probability that a user returns to a bad state is lower than the probability that the user stays at a good state when the user has a high local protection level at a good state.

- $p^{a_H}_{s_B,s_B} < p^{a_H}_{s_B,s_G}$, i.e., the probability that a user stays at a bad state is lower than the probability that the user returns to a good state when the user has a high local protection level at a bad state.

- $p^{a_L}_{s_G,s_B} > p^{a_L}_{s_G,s_G}$, i.e., the probability that a user returns to a bad state is greater than the probability that the user stays at a good state when the user has a low local protection level at a good state.

- $p^{a_L}_{s_B,s_B} > p^{a_L}_{s_B,s_G}$, i.e., the probability that a user stays at a bad state is greater than the probability that the user returns to a good state when the user has a low local protection level at a bad state.

Let $\{x_t\}_{t=0}^{\infty}$ denote the sequence of random losses. Let $\{y_t := x_t + c_t\}_{t=0}^{\infty}$ denote the sequence of random total losses, where c_t indicates the cost of the user taking local protections at time

t. We further assume that $c_t = c(a_t)$, where a_t is the level of the local protection at time t. We impose the following assumption on $c(a)$:

- $c(a_H) > c(a_L)$, i.e., taking high local protection level costs more.

The key objective of Markov Decision Process (MDP) is to find a policy for the user: a set function $\pi = \{\pi_{s_G}, \pi_{s_B}\}$ that specifies the action π_s that the user will choose when in state s. The goal of the problem is to find a policy π that will minimize the expected discounted sum over an infinite horizon:

$$\sum_{t=0}^{\infty} \gamma^t y^{\pi_{s^t}}(s^t, s^{t+1}),$$

where $y^{\pi_{s^t}}(s^t, s^{t+1}) = x^{\pi_{s^t}}(s^t, s^{t+1}) + c(\pi_{s^t})$ represents the total loss at time t, incurred to the user who is in state s^t and takes action π_{s^t}. γ is the discounted rate, where $\gamma \geq 0$ and is assumed to be strictly less than 1. Here, we focus on optimal stationary policy, or policy that can be written as a function of s only, that is, π is independent of time t as described above.

Let $\mathbf{v}$ denotes the value vector which contains the loss-to-go for all states. Furthermore, an optimal policy $(\mathbf{v}^*, \pi^*)$ is then a fixed point of the following minimum loss operator:

$$\pi^*_{s_G} := \arg\min_{a \in \mathcal{A}} \left\{ p^a(s_G, s_G) \left(y^a(s_G, s_G) + \gamma v^*_{s_G} \right) + p^a(s_G, s_B) \left(y^a(s_G, s_B) + \gamma v^*_{s_B} \right) \right\}$$

$$\pi^*_{s_B} := \arg\min_{a \in \mathcal{A}} \left\{ p^a(s_B, s_G) \left(y^a(s_B, s_G) + \gamma v^*_{s_G} \right) + p^a(s_B, s_B) \left(y^a(s_B, s_B) + \gamma v^*_{s_B} \right) \right\}$$

$$v^*_{s_G} := p^{\pi^*_{s_G}}(s_G, s_G) \left(y^{\pi^*_{s_G}}(s_G, s_G) + \gamma v^*_{s_G} \right) + p^{\pi^*_{s_G}}(s_G, s_B) \left(y^{\pi^*_{s_G}}(s_G, s_B) + \gamma v^*_{s_B} \right)$$

$$v^*_{s_B} := p^{\pi^*_{s_B}}(s_B, s_G) \left(y^{\pi^*_{s_B}}(s_B, s_G) + \gamma v^*_{s_G} \right) + p^{\pi^*_{s_B}}(s_B, s_B) \left(y^{\pi^*_{s_B}}(s_B, s_B) + \gamma v^*_{s_B} \right)$$

Using dynamic programming, we can find π^* and $\mathbf{v}^*$.

Lemma 1 *Let*

$$P_\pi = \begin{bmatrix} p^{\pi_{s_G}}(s_G, s_G) & p^{\pi_{s_B}}(s_B, s_G) \\ p^{\pi_{s_G}}(s_G, s_B) & p^{\pi_{s_B}}(s_B, s_B) \end{bmatrix}$$

and

$$\mathbf{y}_\pi = \begin{bmatrix} p^{\pi_{s_G}}(s_G, s_G) y^{\pi_{s_G}}(s_G, s_G) + p^{\pi_{s_G}}(s_G, s_B) y^{\pi_{s_G}}(s_G, s_B) \\ p^{\pi_{s_B}}(s_B, s_G) y^{\pi_{s_B}}(s_B, s_G) + p^{\pi_{s_B}}(s_B, s_B) y^{\pi_{s_B}}(s_B, s_B) \end{bmatrix}.$$

Then, the optimal policy $(\mathbf{v}^*, \pi^*)$ *satisfies*

$$(I - \gamma P_{\pi^*}^T)\mathbf{v}^* = \mathbf{y}_{\pi^*}. \tag{45}$$

The MDP problem can also be reformulated as a linear programming (LP) problem:

$$\begin{aligned} &\max_{\beta} \mathbf{1}^T \beta \\ &\text{s.t.} \quad \left((P \odot (X + C))^T \mathbf{1}\right) - (E - \gamma P)^T \beta \geq \mathbf{0}, \end{aligned} \tag{46}$$

where $\odot$ is the Hadamard product, i.e., entry-wise product, and

$$P = \begin{bmatrix} p^{a_H}(s_G, s_G) & p^{a_L}(s_G, s_G) & p^{a_H}(s_B, s_G) & p^{a_L}(s_B, s_G) \\ p^{a_H}(s_G, s_B) & p^{a_L}(s_G, s_B) & p^{a_H}(s_B, s_B) & p^{a_L}(s_B, s_B) \end{bmatrix},$$

$$X = \begin{bmatrix} x^{a_H}(s_G, s_G) & x^{a_L}(s_G, s_G) & x^{a_H}(s_B, s_G) & x^{a_L}(s_B, s_G) \\ x^{a_H}(s_G, s_B) & x^{a_L}(s_G, s_B) & x^{a_H}(s_B, s_B) & x^{a_L}(s_B, s_B) \end{bmatrix},$$

$$C = \begin{bmatrix} c(a_H) & c(a_L) & c(a_H) & c(a_L) \\ c(a_H) & c(a_L) & c(a_H) & c(a_L) \end{bmatrix},$$

$$E = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

The solution of the linear programming problem (46) denotes the optimal cost-to-go, i.e., $\beta^* = [\beta_1^*, \beta_2^*]^T = \mathbf{v}^*$. The optimal policy can then be achieved by solving the following

problems:

$$\pi^*_{s_G} := \arg\min_{a\in\mathcal{A}} \{p^a(s_G, s_G)\,(y^a(s_G, s_G) + \gamma\beta^*_1) + p^a(s_G, s_B)\,(y^a(s_G, s_B) + \gamma\beta^*_2)\}$$

$$\pi^*_{s_B} := \arg\min_{a\in\mathcal{A}} \{p^a(s_B, s_G)\,(y^a(s_B, s_G) + \gamma\beta^*_1) + p^a(s_B, s_B)\,(y^a(s_B, s_B) + \gamma\beta^*_2)\}$$

The user aims to mitigate the loss by subscribing to the insurance. By paying a subscription fee at the initial time, the user will receive a coverage from the insurer when he faces losses. We further assume that the subscription fee is a constant T and the coverage is a function of the losses:

$$r(X) : \mathbb{R}^{2\times 4} \to \mathbb{R}^{2\times 4}.$$

As a result, the user's problem with the insurance can be captured as follows:

$$\begin{aligned} &\max_{\beta} \mathbf{1}^T\beta \\ &\text{s.t.} \quad \left((P \odot (X - r(X) + C))^T\mathbf{1}\right) - (E - \gamma P)^T\beta \geq \mathbf{0}, \end{aligned} \tag{47}$$

Note that when function $r(X) = \mathbf{0}_{2\times 4}$ for any given losses X, i.e., there is no coverage, Problem (47) is equivalent to Problem (46).

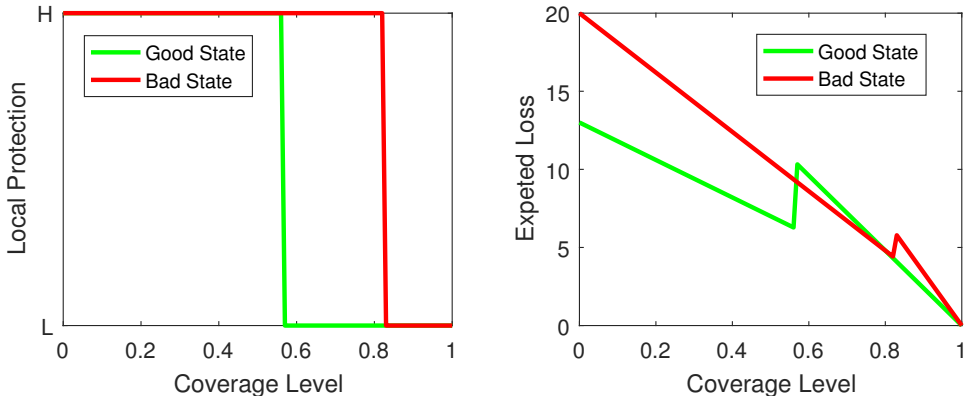
Problem (47) captures the user's behavior under insurance. Note that the user subscribes to the insurance only when the loss with the insurance is lower than the loss without the insurance. Thus, the user will purchase the insurance when

$$\beta^r_1 + T \leq \beta^0_1 \text{ and } \beta^r_2 + T \leq \beta^0_2 \tag{48}$$

where β_1, β_2 come from (46) and β^r_1, β^r_2 come from (47).

Note that the insurer will provide the insurance only when he can make a profit from it. The profit of the insurer can be captured as follows:

$$\mathbf{T} - (I - \gamma P^T_{\pi^*})^{-1} r(\mathbf{x}_{\pi^*})$$



(a) Local protection. (b) Total Loss.

Figure 8: Markov decision process.

where $(I - \gamma P_{\pi^*}^T)^{-1} r(\mathbf{x}_{\pi^*})$ denotes the covered losses of the user paid by the insurer. Thus, the insurer will provide the insurance when the following condition holds:

$$\mathbf{T} - (I - \gamma P_{\pi^*}^T)^{-1} r(\mathbf{x}_{\pi^*}) \geq \mathbf{0}. \tag{49}$$

As a result, the insurer's objective of maximizing the total profit can be described as follows:

$$\begin{aligned} &\max_{r,\mathbf{T}} \mathbf{1}^T \left(\mathbf{T} - (I - \gamma P_{\pi^*}^T)^{-1} r(\mathbf{x}_{\pi^*}) \right) \\ &\text{s.t.} \\ &\mathbf{T} - (I - \gamma P_{\pi^*}^T)^{-1} r(\mathbf{x}_{\pi^*}) \geq \mathbf{0}; \\ &\beta^r + \mathbf{T} \leq \beta^0. \end{aligned} \tag{50}$$

The solution $\{\mathbf{T}^*, r^*\}$ to Problem (50) is the optimal insurance policy with which the insurer makes a profit and the user mitigates his loss.

Example: We present a numerical example in Fig. 8. We can see from Fig. (a) that with the increase of the coverage level, the user tends to take a low local protection level at both states, which shows the Peltzman effect where the user acts riskily when he is protected by the insurance. From Fig. (b) we can see that the expected total loss decreases with the increase of the coverage level. Note that when the user changes his local protection level

from high to low, the loss increases. Yet as a result, the loss decreases again as the insurer provides more coverage.

8 Discussions

In this paper, we have described a bi-level game-theoretic framework for studying cyber insurance of computer networks. We have taken into account complex interactions between users, insurers, and attackers. The framework captures the information asymmetry between users and the insurers through the moral-hazard type of principal-agent model and incorporates the attack and defense behaviors of the users and the adversaries as zero-sum games. The developed framework and enables the analysis of the design of cyber insurance as an additional layer of mitigation scheme in networks. We have studied four cases and have completely characterized their equilibrium solutions. Our analysis has provided a fundamental limit on the insurability of the users, and predicted the Peltzman effect. We have shown further that the subscription fee of the insurance policy is a linear function of the coverage level, and the zero operating profit principle of the insurer at the equilibrium. Our numerical experiments have shown that for a fully connected network, with the increase of the number of nodes, the saddle-point equilibrium solutions of the user and the attacker exhibits less on network effects. We have also shown that users and attackers at nodes with more neighbors are required to put more local efforts in the decentralized case while these nodes exhibit weaker network effects in centralized one. We have included a generalization of the bi-level game framework into dynamic settings in which the risk of the nodes evolves over time. One direction of future research is the investigation of insurance policy over complex networks such as scale-free and small-world networks.

Appendix

A. Proof of Proposition 1

Consider the minimax problem in (6), for a given insurance policy s and action of the user p_u, $\frac{\partial K(p_u,p_a,s)}{\partial p_a} = 0$ gives the best action of the attacker: $p_a^*(p_u) = \frac{\gamma(1-s)}{c_a} - p_u$. As a result, $K(p_u, p_a^*(p_u), s) = \gamma(1-s)\ln(\frac{\gamma(1-s)}{c_a p_u}) + c_u p_u - \gamma(1-s) + c_a p_u$, and the derivative of it with respect to p_u: $\frac{\partial K(p_u,p_a^*(p_u),s)}{\partial p_u} = c_u + c_a - \frac{\gamma(1-s)}{p_u} = 0$, which gives the best action of the user, $p_u^* = \frac{\gamma(1-s)}{c_u+c_a}$. By plugging p_u^* into $p_a^*(p_u)$, we can obtain $p_a^* = \frac{c_u\gamma(1-s)}{c_a(c_u+c_a)}$. Following similar steps, the max-min problem in (6) admits the same solution. Thus, the minimax problem and the max-min problem have the same saddle-point solution, which is unique. Note that the solution is feasible only when it satisfies the feasible constraint (4). Thus, we have $1 - \gamma(1-s)\ln(\frac{p_a^*}{p_u^*} + 1) = 1 - \gamma(1-s)\ln(\frac{c_u}{c_a} + 1) > 0$.

B. Proof of Proposition 7

Notice that at node n, for a given insurance coverage s_n and players' actions at other nodes $(p_{u,-n}, p_{a,-n})$, the minimax-problem with the objective function (16) is equivalent as solving the following problem

$$\min_{p_{u,n}\in\mathcal{S}_{u,n}(s_n)} \max_{p_{a,n}\in\mathcal{S}_{a,n}(s_n)} \gamma_n(1-s_n)w_{nn}^* r_n(p_{u,n}, p_{a,n}) + c_{u,n}p_{u,n} - c_{a,n}p_{a,n}.$$

The other terms have been removed as they do not depend on the decision variables $(p_{u,n}, p_{a,n})$. Following similar steps in Appendix A, the minimax problem yields (21). Similarly, the max-min problem yields the same solution. Thus, the zero-sum game between the user and the attacker at node n admits the unique saddle-point solution shown in Proposition 7.

C. Proof of Proposition 11

We use similar methods in Appendix A and B to prove Proposition 11. Note that there is no coupling between $p_{u,n}$ and $p_{a,n}$ in the utility function. Thus, for a given insurance policy $\{s_n\}$ and the actions of the user $\{p_{u,n}\}$, the max-problem for the attacker with decision variables $\{p_{a,n}\}$ is equivalent to solving N sub-max-problems, which can be described as follows:

$$\max_{p_{a,n}\in\mathcal{S}_{a,n}(\mathbf{s})} r_n(p_{u,n},p_{a,n}) \sum_{m=1}^{N} \gamma_m(1-s_m)w_{mn}^* - c_{a,n}p_{a,n}. \tag{51}$$

Similarly, given the actions of the attacker $\{p_{a,n}\}$, the min-problem for the user with decision variables $\{p_{u,n}\}$ is equivalent to solving N sub-min-problems, which can be described as follows:

$$\min_{p_{u,n}\in\mathcal{S}_{u,n}(\mathbf{s})} r_n(p_{u,n},p_{a,n}) \sum_{m=1}^{N} \gamma_m(1-s_m)w_{mn}^* + c_{u,n}p_{u,n}. \tag{52}$$

Following similar steps in Appendix A and Appendix B, we can achieve the unique SPE in Proposition 11.

D. Proof of Proposition 6

Since the network is well-connected and $w_{nn}=0, \sum_{n=1}^{N} w_{mn}=1, \forall 1,...,N$, we have that $\mathbf{W}$ is a right irreducible stochastic matrix with all diagonal elements being 0, and $\mathbf{W}\mathbf{1}_N=\mathbf{1}_N$, where $\mathbf{1}_N$ is a column vector of size N with all elements equal to 1. Thus, $\mathbf{W}$ has an eigenvalue of 1 associated with an eigenvector $\mathbf{1}_N$.

Based on the Perron-Frobenius Theorem (Section 8, [34]), the largest absolute eigenvalue of an irreducible stochastic matrix is 1, and then we have that the spectral radius $\rho(\mathbf{W})=1$. Thus, $\rho(\eta\mathbf{W}^T)=\eta\in(0,1)$. As a result, $\widetilde{\mathbf{W}}=\mathbf{I}_N-\eta\mathbf{W}^T$ is a $n\times n$ non-singular M-matrix. Since the inverse of a non-singular M-matrix A always exists and $A^{-1}\geq 0$ (F_{15}, [35]), $\widetilde{\mathbf{W}}^{-1}$ exists and $\mathbf{W}^*=\widetilde{\mathbf{W}}^{-1}\geq 0$. Thus, Proposition 6(i) holds.

Furthermore, the Neumann Series $(\mathbf{I}_N - \eta\mathbf{W}^T)^{-1} = \sum_{k=0}^{\infty}(\eta\mathbf{W}^T)^k$ converges as $\rho(\eta\mathbf{W}^T) = \eta < 1$ (7.10.9, [34]). Thus, $\mathbf{W}^* = \sum_{k=0}^{\infty}(\eta\mathbf{W}^T)^k = \mathbf{I}_N + (\eta\mathbf{W}^T) + (\eta\mathbf{W}^T)^2 + \cdots$. As a result, $w^*_{nn} > 1, \forall n \in \{1, ..., N\}$. Since we have already proved that $\mathbf{W}^* = \widetilde{\mathbf{W}}^{-1} \geq 0$, Proposition 6(ii) holds.

To prove Proposition 6(iii), we first consider that $(\mathbf{I}_N - \eta\mathbf{W})\mathbf{1}_N = \mathbf{I}_N\mathbf{1}_N - \eta\mathbf{W}\mathbf{1}_N = \mathbf{1}_N - \eta\mathbf{1}_N = (1-\eta)\mathbf{1}_N$. By multiplying both sides by $(\mathbf{I}_N - \eta\mathbf{W})^{-1}$, we have $\mathbf{1}_N = (1-\eta)(\mathbf{I}_N - \eta\mathbf{W})^{-1}\mathbf{1}_N$. Note that $(\mathbf{I}_N - \eta\mathbf{W})^{-1} = ((\mathbf{I}_N - \eta\mathbf{W}^T)^T)^{-1} = ((\mathbf{I}_N - \eta\mathbf{W}^T)^{-1})^T = \mathbf{W}^{*T}$, thus, $\mathbf{1}_N = (1-\eta)\mathbf{W}^{*T}\mathbf{1}_N$, i.e., $\mathbf{1}_N^T\mathbf{W}^* = \frac{1}{1-\eta}\mathbf{1}_N^T$. Thus, Proposition 6(iii) holds.

References

[1] W. R. Cheswick, S. M. Bellovin, and A. D. Rubin, *Firewalls and Internet security: repelling the wily hacker*. Addison-Wesley Longman Publishing Co., Inc., 2003.

[2] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," tech. rep., Technical report Chalmers University of Technology, Goteborg, Sweden, 2000.

[3] S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, *Moving target defense: creating asymmetric uncertainty for cyber threats*, vol. 54. Springer Science & Business Media, 2011.

[4] V. Kumar, J. Srivastava, and A. Lazarevic, *Managing cyber threats: issues, approaches, and challenges*, vol. 5. Springer Science & Business Media, 2006.

[5] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, "The economic impact of cyber-attacks," Congressional Research Service, Library of Congress, 2004.

[6] R. Anderson and T. Moore, "The economics of information security," *Science*, vol. 314, no. 5799, pp. 610–613, 2006.

[7] Q. Zhu, C. Fung, R. Boutaba, and T. Başar, "Guidex: A game-theoretic incentive-based mechanism for intrusion detection networks," *Selected Areas in Communications, IEEE Journal on*, vol. 30, no. 11, pp. 2220–2230, 2012.

[8] C. Kreibich and J. Crowcroft, "Honeycomb: creating intrusion detection signatures using honeypots," *ACM SIGCOMM computer communication review*, vol. 34, no. 1, pp. 51–56, 2004.

[9] Q. Duan, E. Al-Shaer, and H. Jafarian, "Efficient random route mutation considering flow and network constraints," in *Communications and Network Security (CNS), 2013 IEEE Conference on*, pp. 260–268, IEEE, 2013.

[10] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems," *Control Systems, IEEE*, vol. 35, no. 1, pp. 46–65, 2015.

[11] S. Peltzman, "The effects of automobile safety regulation," *The Journal of Political Economy*, pp. 677–725, 1975.

[12] J. Kesan, R. Majuca, and W. Yurcik, "Cyberinsurance as a market-based solution to the problem of cybersecurity: a case study," in *Proc. WEIS*, 2005.

[13] M. Lelarge and J. Bolot, "A local mean field analysis of security investments in networks," in *Proceedings of the 3rd international workshop on Economics of networked systems*, pp. 25–30, ACM, 2008.

[14] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will cyber-insurance improve network security? a market analysis," in *INFOCOM, 2014 Proceedings IEEE*, pp. 235–243, IEEE, 2014.

[15] B. Hölmstrom, "Moral hazard and observability," *The Bell journal of economics*, pp. 74–91, 1979.

[16] B. Holmstrom, "Moral hazard in teams," *The Bell Journal of Economics*, pp. 324–340, 1982.

[17] J. Bolot and M. Lelarge, "Cyber insurance as an incentivefor internet security," in *Managing information risk and the economics of security*, pp. 269–290, Springer, 2009.

[18] D. Acemoglu, A. Malekian, and A. Ozdaglar, "Network security and contagion," tech. rep., National Bureau of Economic Research, 2013.

[19] R. Miura-Ko, B. Yolken, J. Mitchell, and N. Bambos, "Security decision-making among interdependent organizations," in *Computer Security Foundations Symposium, 2008. CSF'08. IEEE 21st*, pp. 66–80, IEEE, 2008.

[20] J. Raiyn *et al.*, "A survey of cyber attack detection strategies," *International Journal of Security and Its Applications*, vol. 8, no. 1, pp. 247–256, 2014.

[21] P. Tague and R. Poovendran, "Modeling node capture attacks in wireless sensor networks," in *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*, pp. 1221–1224, IEEE, 2008.

[22] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "Dos attacks in mobile ad hoc networks: A survey," in *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*, pp. 535–541, IEEE, 2012.

[23] C. Tankard, "Advanced persistent threats and how to monitor and deter them," *Network security*, vol. 2011, no. 8, pp. 16–19, 2011.

[24] C. E. Shannon, "Communication theory of secrecy systems*," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[25] S. Shavell, *On moral hazard and insurance*. Springer, 1979.

[26] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys (CSUR)*, vol. 45, no. 3, p. 25, 2013.

[27] E. Altman, K. Avrachenkov, and A. Garnaev, "A jamming game in wireless networks with transmission cost," in *Network Control and Optimization*, pp. 1–12, Springer, 2007.

[28] F. P. Kelly, A. K. Maulloo, and D. K. Tan, "Rate control for communication networks: shadow prices, proportional fairness and stability," *Journal of the Operational Research society*, pp. 237–252, 1998.

[29] L. D. Minkova, "Insurance risk theory," *Lecture notes, TEMPUS Project SEE doctoral studies in mathematical sciences*, 2010.

[30] M. Finkelstein, *Failure rate modelling for reliability and risk*. Springer Science & Business Media, 2008.

[31] K. Balakrishnan, *Exponential distribution: theory, methods and applications*. CRC press, 1996.

[32] P. Christoffersen and D. Pelletier, "Backtesting value-at-risk: A duration-based approach," *Journal of Financial Econometrics*, vol. 2, no. 1, pp. 84–108, 2004.

[33] S. Qing and W. Wen, "A survey and trends on internet worms," *Computers & Security*, vol. 24, no. 4, pp. 334–346, 2005.

[34] C. D. Meyer, *Matrix analysis and applied linear algebra*, vol. 2. Siam, 2000.

[35] R. J. Plemmons, "M-matrix characterizations. i—nonsingular m-matrices," *Linear Algebra and its Applications*, vol. 18, no. 2, pp. 175–188, 1977.