Attack-Aware Cyber Insurance for Risk Sharing in Computer Networks

Yezekael Hayel[1,2]([✉]) and Quanyan Zhu[1]

[1] Polytechnic School of Engineering, New York University, Brooklyn, NY 11201, USA
{yezekael.hayel,quanyan.zhu}@nyu.edu
[2] LIA/CERI, University of Avignon, Avignon, France

Abstract. Cyber insurance has been recently shown to be a promising mechanism to mitigate losses from cyber incidents, including data breaches, business interruption, and network damage. A robust 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 achieve these goals, we first establish a cyber insurance model that takes into account the complex interactions between users, attackers and the insurer. A games-in-games framework nests a zero-sum game in a moral-hazard game problem to provide a holistic view of the cyber insurance and enable a systematic design of robust insurance policy. In addition, the proposed framework naturally captures a privacy-preserving mechanism through the information asymmetry between the insurer and the user in the model. We develop analytical results to characterize the optimal insurance policy and use network virus infection as a case study to demonstrate the risk-sharing mechanism in computer networks.

Keywords: Cyber insurance · Incomplete information game · Bilevel optimization problem · Moral hazards · Cyber attacks

1 Introduction

Cyber insurance is a promising solution that can be used to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. A robust 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 insureds level of self-protection. Different from the traditional insurance paradigm, cyber insurance is used to reduce risk that is not created by nature but by intelligent attacks who deliberately inflict damage on the network. Another important feature of cyber insurance is the uncertainties related to the risk of the attack and the assessment of the damage. To address

---

these challenges, a robust cyber insurance framework is needed to design policies to induce desirable user behaviors and mitigate losses from known and unknown attacks.

In this paper, we propose a game-theoretic model that extends the insurance framework to cyber security, and captures the interactions between users, insurance company and attackers. The proposed game model is established based on a recent game-in-games concept [1] 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 leader-follower game with incomplete information is used to model the interactions between the insurer and the user. The user has a complete information of his action while the insurer cannot directly observe it but indirectly measures the loss as a consequence of his security strategy. The zero-sum game is nested in the incomplete information game to constitute a bilevel problem which provides a holistic framework for designing insurance policy by taking into account the cyber attack models and the rational behaviors of the users.

The proposed framework naturally captures a privacy-preserving mechanism through the information asymmetry between the insurer and the user in the model. The insurance policy designed by the insurer in the framework does not require constant monitoring of users' online activities, but instead, only on the measurement of risks. This mechanism prevents the insurer from acquiring knowledge of users' preferences and types so that the privacy of the users is protected. The major contributions of the paper are three-fold. They are summarized as follows:

(i) We propose a new game-theoretic framework that incorporates attack models, and user privacy.
(ii) We holistically capture the interactions between users, attackers, and the insurer to develop incentive mechanisms for users to adopt protection mechanisms to mitigate cyber risks.
(iii) The analysis of our framework provides a theoretic guideline for designing robust insurance policy to maintain a good network condition.

1.1 Related Works

The challenges of cyber security are not only technical issues but also economic and policy issues [2]. Recently, the use of cyber insurance to enhance the level of security in cyber-physical systems has been studied [3,4]. 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 [5], 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 [6,7] deal with hidden actions from an agent, and aims to address the question: How does a principal design the agent's wage contract in order to maximize his effort? This framework is related to insurance markets, and has been used to model cyber insurance [8] as a solution for mitigate losses from cyber attacks. In addition, in [9], 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.

Other works in the literature such as the robust network framework presented in [10] deal with strategic attacker model over networks. However, the network effect is modeled as a simple influence graph, and the stimulus of the good behavior of the network users is based on a global information known to every player. In [11], the authors propose a generic framework to model cyber-insurance problem. Moreover, the authors compare existing models and explain how these models can fit into their unifying framework. Nevertheless, many aspects, like the attacker model and the network effect, have not been analyzed in depth. In [12], the authors propose a mechanism design approach to the security investment problem, and present a message exchange process through which users converge to an equilibrium where they make investments in security at a socially optimal level. This paper has not yet taken into account both the network effect (topology) and the cyber attacker strategy.

1.2   Organization of the Paper

The paper is organized as follows. In Sect. 2, we describe the general framework of cyber moral hazard by first introducing the players and the interactions between them, and second, by defining the influence graph that models the network effect. In Sect. 3, we analyze the framework for a class of problems with separable utility functions. In addition, we use a case study to demonstrate the analysis of an insurance policy for the case of virus infection over a large-scale computer networks. The paper is concluded in Sect. 4.

2   Game-Theoretic Model for Cyber Insurance

In this section, we introduce the cyber insurance model between a user i and an insurance company I (Player I). A user i invests or allocates $a_i \in [0, 1]$ resources for his own protection to defense against attacks. When $a_i = 1$, the user employs maximum amount of resources, e.g., investment in firewalls, frequent change of passwords, and virus scan of attached files for defense. When $a_i = 0$, the user does not invest resources for protection, which corresponds to behaviors such as reckless response to phishing emails, minimum investment in cyber protection, or infrequent patching of operating systems. The protection level a_i can also

be interpreted as the probability that user i invokes a protection scheme. User i can be attacked with probability $q_i \in [0, 1]$. The security level of user i, Z_i, depends on a_i and q_i. To capture the dependency, we let $Z_i = p_i(a_i, q_i)$, where $p_i : [0, 1]^2 \to \mathbb{R}_+$ is a continuous function that quantifies the security level of user i. An insurance company cannot observe the action of the user, i.e., the action a_i if user i. However, it can observe a measurable risk associated with the protection level of user i. We let a random variable X_i denote the risk of user i that can be observed by the insurance company, described by

$$X_i := \mathcal{G}_i(Z_i, \theta_i), \tag{1}$$

where θ_i is a random variable with probability density function g_i that captures the uncertainties in the measurement or system parameters. The risk X_i can be measured in dollars. For example, a data breach due to the compromise of a server can be a consequence of low security level at the user end [13]. The economic loss of the data breach can be represented as random variable X_i measured in dollars. 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_i. The information structure of the model is depicted in Fig. 1.
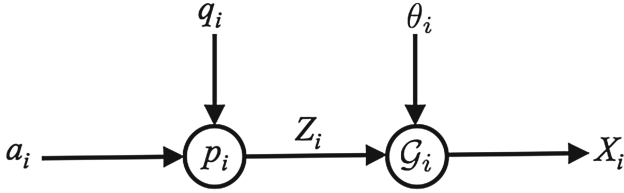

Fig. 1. Illustration of the information structure of the two-person cyber insurance system model: user i determines protection level a_i and an attacker chooses attack probability q_i. The security level Z_i is assessed using function p_i. The cyber risk X_i for user i is measured by the insurance company.

Note that the insurer cannot directly observe the actions of the attack and the user. Instead, he can measure an outcome as a result of the action pair. This type of framework falls into a class of moral hazard models proposed by Holmstrom in [6,7]. One important implication of the incomplete information of the insurer is on privacy. The user's decision a_i can often be related to personal habits and behaviors, which can be used to infer private information (e.g., online activities and personal preferences). This framework naturally captures a privacy-preserving mechanism in which the insurer is assumed to be uncertain about the user and his type. Depending on the choice of random variable θ_i, the level of uncertainties can vary, and hence θ_i can be used to determine the level of privacy of a user.

Player I measures the risk and pays the amount $s_i(X_i)$ for the losses, where $s_i : \mathbb{R}_+ \to \mathbb{R}_+$ is the payment function that reduces the risk of the user i if he is insured by Player I. Hence the effective loss to the user is denoted by $\xi_i = X_i - s_i(X_i)$, and hence user i aims to minimize a cost function U_i that depends on ξ_i, a_i and q_i given by $U_i(\xi_i, a_i, q_i)$, where $U_i : \mathbb{R}_+ \times [0,1]^2 \to \mathbb{R}_+$ is a continuous function monotonically increasing in ξ and q_i, and decreasing in a_i. The function captures the fact that a higher investment in the protection and careful usage of the network on the user side will lead to a lower cost, while a higher intensity of attack will lead to a higher cost. Therefore, given payment policy s_i, the interactions between an attacker and a defender can be captured by a zero-sum game in which the user minimizes U_i while the attacker maximizes it:

$$\text{(UG-1)} \quad \min_{a_i \in [0,1]} \max_{q_i \in [0,1]} \mathbb{E}[U_i(\xi_i, a_i, q_i)]. \tag{2}$$

Here, the expectation is taken with respect to the statistics of θ_i. The minimax problem can also be interpreted as a worst-case solution for a user who deploys best security strategies by anticipating the worst-case attack scenarios. From the attacker side, he aims to maximize the damage under the best-effort protection of the user, i.e.,

$$\text{(UG-2)} \quad \max_{q_i \in [0,1]} \min_{a_i \in [0,1]} \mathbb{E}[U_i(\xi_i, a_i, q_i)]. \tag{3}$$

The two problems described by (UG-1) and (UG-2) constitute a zero-sum game on at the user level. For a given insurance policy s_i, user i chooses protection level $a_i^* \in A_i(s_i)$ with the worst-case attack $q_i^* \in Q_i(s_i)$. Here, A_i and Q_i are set-valued functions that yield a set of saddle-point equilibria in response to s_i, i.e., a_i^* and q_i^* satisfy the following

$$\mathbb{E}[U_i(\xi_i, a_i^*, q_i)] \le \mathbb{E}[U_i(\xi_i, a_i^*, q_i^*)] \le \mathbb{E}[U_i(\xi_i, a_i, q_i^*)], \tag{4}$$

for all $a_i, q_i \in [0,1]$. In addition, in the case that $A_i(s_i)$, and $Q_i(s_i)$ are singleton sets, the zero-sum game admits a unique saddlepoint equilibrium strategy pair (a_i^*, q_i^*) for every s_i. We will use a shorthand notation val to denote the value of the zero-sum game, i.e.,

$$\mathbb{E}[U_i(\xi_i, a_i^*, q_i^*)] = \text{val}[\mathbb{E}[U_i(\xi_i, a_i, q_i)], \tag{5}$$

and arg val to denote the strategy pairs that achieve the game value, i.e.,

$$(a_i^*, q_i^*) \in \text{arg val}[\mathbb{E}[U_i(\xi_i, a_i, q_i)]. \tag{6}$$

The outcome of the zero-sum game will influence the decision of the insurance company in choosing payment rules. The goal of the insurance company is twofold. One is to minimize the payment to the user, and the other is to reduce the risk of the user. These two objectives well aligned if the payment policy s_i is an increasing function in X_i, and we choose cost function $V(s_i(X_i))$, where $V : \mathbb{R}_+ \to \mathbb{R}_+$ is a continuous and increasing function. Therefore, with

these assumptions, Player I aims to find an optimal policy among a class of admissible policies $\mathcal{S}_i$ to solve the following problem:

$$(\text{IP}) \quad \min_{s_i \in \mathcal{S}_i} \quad \mathbb{E}[V(s_i(X_i))]$$

$$\text{s.t.} \quad \text{Saddle-Point (6)}.$$

This problem is a bilevel problem in which the insurance company can be viewed as the leader who announces his insurance policy, while the user behaves as a follower who reacts to the insurer. This relationship is depicted in Fig. 2. One important feature of the game here is that the insurer cannot directly observe the action a_i of the follower, but its state X_i. This class of problem differs from the classical complete information Stackelberg games and the signaling games where the leader (or the sender) has the complete information whereas the follower (or the receiver) has incomplete information. In this case the leader (the insurance company) has incomplete information while the follower (the user) has complete information. The game structure illustrated in Fig. 2 has a games-in-games structure. A zero-sum game between a user and a defender is nested in a bilevel game problem between a user and the insurer.

It is also important to note that user i pays Player I a subscription fee $T \in \mathbb{R}_{++}$ to be insured. The incentive for user i to buy insurance is when the average cost at equilibrium under the insurance is lower the cost incurred without insurance. Therefore, user i participates in the insurance program when

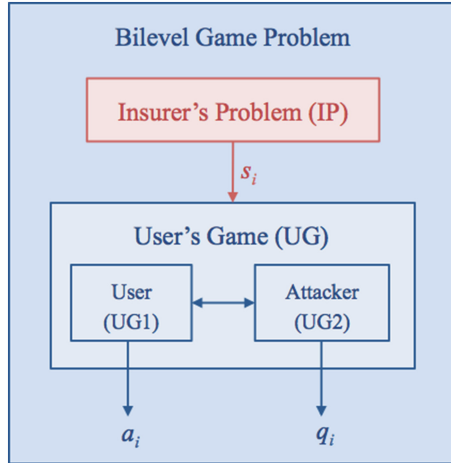$$\mathbb{E}[U_i(\xi_i, a_i^*, q_i^*)] \geq T. \tag{7}$$

Fig. 2. The bilevel structure of the two-person cyber insurance game. The problem has a games-in-games structure. The user and the attacker interact through a zero-sum game while the insurer and the user interact in a bilevel game in which the user has complete information but the leader does not.

It can bee seen that the insurance policy plays an important role in the partic-
ipation decision of the user. If the amount of payment from the insurer is low,
then the user tends not to be insured. On the other hand, if the payment is high,
then the risk for the insurer will be high and the user may behave recklessly in
the cyber space, as have been shown in Peltzman's effect [14].

3   Analysis of the Cyber Insurance Model

The formal framework introduced in Sect. 2 provides the basis for analysis and
design of cyber insurance to reduce risks for the Internet users. One challenge in
the analysis of the model comes from the information asymmetry between the
user and the insurer, and the information structure illustrated in Fig. 1. Since the
cost functions in (UG-1), (UG-2), and (IP) are expressed explicitly as a function
of X_i, the optimization problems can be simplified by taking expectations with
respect to the sufficient statistics of X_i. Let f_i be the probability density function
of X_i. Clearly, f_i is a transformation from the density function g_i (associated with
the random variable θ_i) under the mapping $\mathcal{G}_i$. In addition, f_i also depends on the
action pair (a_i, q_i) through the variable Z_i. Therefore, we can write $f_i(x_i; a_i, q_i)$
to capture the parametrization of the density function. To this end, the insurer's
bilevel problem (IP) can be rewritten as follows:

$$(\text{IP'}) \quad \min_{s_i \in \mathcal{S}_i} \qquad \int_{x_i \in \mathbb{R}_+} V(s_i(x_i)) f_i(x_i, a_i^*, q_i^*) dx_i$$

$$\text{s.t.} \quad (a_i^*, q_i^*) = \arg \operatorname{val} \left[\int_{x_i \in \mathbb{R}_+} U_i(x_i - s_i(x_i), a_i, q_i) f_i(x_i, a_i, q_i) dx_i \right].$$

Under the regularity conditions (i.e., continuity, differentiability and measur-
ability), the saddle-point solution (a_i^*, q_i^*) can be characterized by the first-order
conditions:

$$\int_{x_i \in \mathbb{R}_+} \left[\frac{\partial U_i}{\partial a_i}(x_i - s_i(x_i), a_i, q_i) f_i(x_i; a_i, q_i) \right.$$

$$\left. + U_i(x_i - s_i(x_i), a_i, q_i) \frac{\partial f_i}{\partial a_i} f_i(x_i; a_i, q_i) \right] dx_i = 0, \tag{8}$$

and

$$\int_{x_i \in \mathbb{R}_+} \left[\frac{\partial U_i}{\partial q_i}(x_i - s_i(x_i), a_i, q_i) f_i(x_i; a_i, q_i) \right.$$

$$\left. + U_i(x_i - s_i(x_i), a_i, q_i) \frac{\partial f_i}{\partial q_i} f_i(x_i; a_i, q_i) \right] dx_i = 0, \tag{9}$$

In addition, with the assumption that f_i and U_i are both strictly convex in
a_i and strictly concave in q_i, the zero-sum game for a given s_i admits a unique

saddle-point equilibrium [15]. Using Lagrangian methods from vector-space optimization [16], we can form a Lagrangian function with multipliers $\lambda_i, \mu_i \mathbb{R}_+$ as follows:

$$
\begin{aligned}
\mathcal{L}(s_i, \mu_i, a_i, q_i; \lambda_i, \mu_i) = &\int_{x_i \in \mathbb{R}_+} V(s_i(x_i)) f_i(x_i, a_i, q_i) dx_i + \\
&\lambda_i \int_{x_i \in \mathbb{R}_+} \left[\frac{\partial U_i}{\partial a_i}(x_i - s_i(x_i), a_i, q_i) f_i(x_i; a_i, q_i) \right. \\
&\left. + U_i(x_i - s_i(x_i), a_i, q_i) \frac{\partial f_i}{\partial a_i} f_i(x_i; a_i, q_i) \right] dx_i + \\
&\mu_i \int_{x_i \in \mathbb{R}_+} \left[\frac{\partial U_i}{\partial q_i}(x_i - s_i(x_i), a_i, q_i) f_i(x_i; a_i, q_i) \right. \\
&\left. + U_i(x_i - s_i(x_i), a_i, q_i) \frac{\partial f_i}{\partial q_i} f_i(x_i; a_i, q_i) \right] dx_i.
\end{aligned}
$$

The insurer's bilevel problem can thus be rewritten as a one-level optimization problem with Lagrange function $\mathcal{L}$:

$$
\text{(IP')} \quad \max_{\lambda_i, \mu_i} \min_{s_i \in \mathcal{S}_i, a_i \in [0,1], q_i \in [0,1]} \mathcal{L}(s_i, \mu_i, a_i, q_i; \lambda_i, \mu_i).
$$

Generally speaking, this Lagrangian is not simple to study but, as we see in the next section, several assumptions of the utility functions will help us to obtain the characterization of the optimal payment policies for the insurer.

3.1 Separable Utilities

One main assumption about player utility function is that it is separable into his variables, i.e.:

$$
\forall i \in \{1, \ldots, N\}, \quad U_i(\xi_i, a_i, q_i) = H_i(\xi_i) + c_i(a_i, q_i).
$$

In fact, the protection investment a_i induces a direct cost $c_i(a_i, q_i)$ on user i. This cost function is strictly increasing in a_i. Moreover, each player is typically risk-averse, and H_i is assumed to be increasing and concave. We give general results considering this particular case of separable utilities.

Following the first-order conditions (8) for user i, we obtain

$$
\int_{x_i \in \mathbb{R}_+} \left[H_i(x_i - s_i(x_i)) \frac{\partial f_i}{\partial a_i}(x_i; a_i, q_i) + \frac{\partial c_i}{\partial a_i}(a_i, q_i) f_i(x_i; a_i, q_i) \right] dx_i = 0.
$$

As we have $\frac{\partial c_i}{\partial a_i}(a_i, q_i) > 0$, the last equality is equivalent to:

$$
\frac{H_i(x_i - s_i(x_i))}{-\frac{\partial c_i}{\partial a_i}(a_i, q_i)} \frac{\partial f_i}{\partial a_i}(x_i; a_i, q_i) = f_i(x_i; a_i, q_i)
$$

Similarly, following (9), we obtain

$$\int_{x_i \in \mathbb{R}_+} \left[H_i(x_i - s_i(x_i)) \frac{\partial f_i}{\partial q_i}(x_i; a_i, q_i) + \frac{\partial c_i}{\partial q_i}(a_i, q_i) f_i(x_i; a_i, q_i) \right] dx_i = 0,$$

and arrive at

$$\frac{H_i(x_i - s_i(x_i))}{-\frac{\partial c_i}{\partial q_i}(a_i, q_i)} \frac{\partial f_i}{\partial q_i}(x_i; a_i, q_i) = f_i(x_i; a_i, q_i).$$

Therefore, we arrive at the following proposition:

Proposition 1. *The saddle-point strategy pair* (a_i, q_i) *satisfies the following relationship for every* $x_i \in \mathbb{R}_+$:

$$\frac{\frac{\partial f_i(x_i; a_i, q_i)}{\partial a_i}}{\frac{\partial f_i(x_i; a_i, q_i)}{\partial q_i}} = \frac{\frac{\partial c_i(a_i, q_i)}{\partial a_i}}{\frac{\partial c_i(a_i, q_i)}{\partial q_i}} \tag{10}$$

It can be seen that the saddle-point strategy pair depends on the state x_i. For different risk, the user will invest accordingly to protect his computer system.

3.2   Case Study: Cyber Insurance Under Infection Dynamics

We consider a possible virus or worm that propagates into a network. Each computer can be infected by this worm and we assume that if a node is infected, it induces a time window in which the node is vulnerable to serious cyber-attacks. The propagation dynamics follow a Susceptible-Infected-Susceptible (SIS) type infection dynamics [17] such that the time duration a node is infected follows an exponential distribution with parameter γ that depends on a and q. Note that we remove index i for the convenience of notations. Indeed, when a computer is infected, it is vulnerable to serious cyber-attacks. These can cause an outbreak of the machine and of the network globally. We thus assume that the parameter γ is increasing in a (resp. decreasing in q) meaning that more protection (resp. more attacks) reduces (resp. increases) the remaining time the node/computer is infected. Then, the action of the node decreases his risk whereas the action of the attacker increases the risk. We make also the following assumptions:

- The cost function is convex, i.e., the user is absolute risk-averse: $\forall \xi$, $H(\xi) = e^{r\xi}$;
- The cost function $c(a, q) = a - q$ is bi-linear;
- X follows an exponential distribution with parameter $\gamma(a, q)$, i.e., $X \sim \exp(\gamma(a, q))$. This random variable may represent the time duration a node is infected under an SIS epidemic process.
- The insurance policy is assumed to be linear in X, i.e., sX, where $s \in [0, 1]$. Hence the residual risk to the user is $\xi = (1 - s)X$.

Without loss of generality, we denote γ as a single constant when the notation does not lead to confusion. We thus have the following density function for the outcome:

$$\forall x \in \mathbb{R}_+, \quad f(x|a,q) = \gamma(a,q)e^{-\gamma(a,q)x}.$$

Then, we obtain

$$\forall x \in \mathbb{R}_+, \quad f_a(x|a,q) = \gamma_a e^{-\gamma x}\left(1 - \gamma x\right),$$

where by abuse of notation we denote $\gamma := \gamma(a,q)$ and $\gamma_a := \frac{\partial \gamma}{\partial a}(a,q)$. The average amount of damage is $\mathbb{E}(X) = \frac{1}{\gamma(a,q)} := \frac{q}{a}$. The expected utility of the node is given by:

$$\mathbb{E}U(X,a,q) = \int_0^\infty \left[H(x - sx) + c(a,q)\right] f(x|a,q)dx,$$

$$= c(a,q) + \int_0^\infty H(x(1-s))f(x|a,q)dx,$$

$$= c(a,q) + \frac{a}{q}\int_0^\infty e^{rx(1-s) - x\frac{a}{q}}dx,$$

$$= a - q + \frac{a}{q}\int_0^\infty e^{x[r(1-s) - \frac{a}{q}]}dx,$$

We assume that $a > qr(1-s)$ then:

$$\mathbb{E}U(X,a,q) = a - q + \frac{a}{a - qr(1-s)}.$$

We can observe that the optimal protection level of the node depends in a non-linear fashion of the cyber-attack level. For a given action of the attacker q and a contract s, the best action $a^*(s,q)$ for the node protection level is:

$$a^*(s,q) = \arg\min_a \mathbb{E}U(X,a,q) = q(1-s)r + \sqrt{q(1-s)r}.$$

Given the best protection, we can obtain the saddle point solution:

$$a^* = q^* = \frac{r(1-s)}{(1 - r(1-s))^2}.$$

If a player does not subscribe to cyber insurance, i.e., $s = 0$, then his best action becomes

$$a^*(0) = qr + \sqrt{qr}.$$

Hence, its expected cost is:

$$\mathbb{E}U^0 = \frac{a^*(0)}{a^*(0) - qr} + a^*(0) = qr + 2\sqrt{qr} + 1 = (1 + \sqrt{qr})^2.$$

If the player decides to be insured, then $s > 0$, i.e., part of his damage is covered and he has to pay a flat rate T for the participation. Then, his best action becomes $a^*(s)$ that depends on his coverage level s, and his expected cost is:

$$EU^s = \frac{a^*(s)}{a^*(s) - qr(1-s)} + a^*(s) + T = qr(1-s) + 2\sqrt{qr(1-s)} + 1 + T,$$

$$= (1 + \sqrt{qr(1-s)})^2 + T.$$

Proposition 2. *If the cyber insurance is too expensive, i.e. $T \geq T_{\max} := qr + 2\sqrt{qr}$, then the player will not subscribe to the cyber insurance independent of the coverage level s.*

Sketch of Proof. This proposition comes from the equivalence of $EU^1 \geq EU^0$ with $T \geq qr + 2\sqrt{qr}$. In this case, independent of the coverage level s, we have $EU^s \geq EU^0$, which implies that the node will not choose to pay the cyber insurance for any coverage level s.

Proposition 3. *For the subscription fee $T < qr + 2\sqrt{qr}$, there exists a minimum coverage $s^0(T)$ such that, for any coverage level $s \in [s^0(T), 1]$, the player will subscribe to the cyber-insurance. This minimum coverage is equal to:*

$$s^0(T) = 1 - \left(\frac{\sqrt{(1 + \sqrt{qr})^2 - T} - 1}{\sqrt{qr}} \right)^2.$$

Sketch of Proof. The function EU^s is strictly decreasing in s and $\lim_{s \to 0} EU^s > EU^0$. If $T < qr + 2\sqrt{qr}$, then $EU^1 < EU^0$. Hence, for a given $T < qr + 2\sqrt{qr}$, there exists a unique $s^0(T)$ such that $EU^{s^0(T)} = EU^0$. Moreover, for any $s \in [s^0(T), 1]$, we have $EU^s < EU^0$, then the player will subscribe to cyber insurance. By comparing the expressions of the expected utility functions, we obtain the following solution:

$$s^0(T) = 1 - \left(\frac{\sqrt{(1 + \sqrt{qr})^2 - T} - 1}{\sqrt{qr}} \right)^2.$$

We observe in Fig. 3 that for a same price T, for the node to subscribe to insurance, the level of cyber attack has to be sufficiently high. If we consider a competition framework in which the cyber insurer cannot change its price T, then for a fixed price, a higher cyber attack level leads to less minimum coverage accepted by the node. This shows that cyber attack plays an important role in insurance policy as it increases the willingness of the users to be insured.

The loss probability is defined as the probability that the damage covered by the insurance exceeds the price paid by the subscriber. We then define this loss of profit by $L(T) := \mathbb{P}(s^0(T)X(s^0(T)) > T)$, and obtain the following expression of the loss as:

$$L(T) = \exp\left(-\frac{q(1 - s^0(T))r + \sqrt{q(1 - s^0(T))r}}{qs^0(T)}T\right).$$

As we can see in Fig. 4, the loss is not monotone in the price, and a small price does not guarantee a profit (no loss) for the insurance company. One goal of the extended version of this work is to study the property of this loss depending on T.
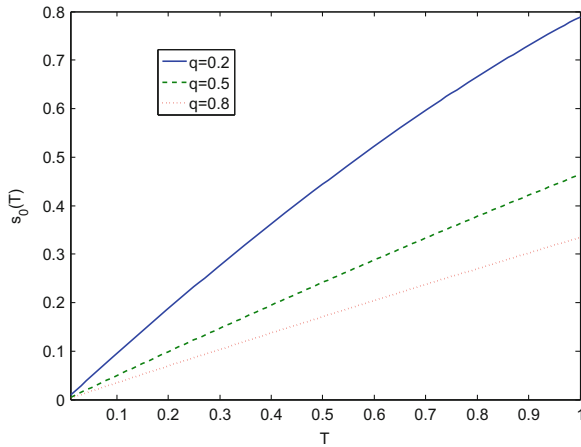

Fig. 3. Minimum coverage s_0 depending on the price T and cyber-attack level q with a risk-averse coefficient $r = 2$.
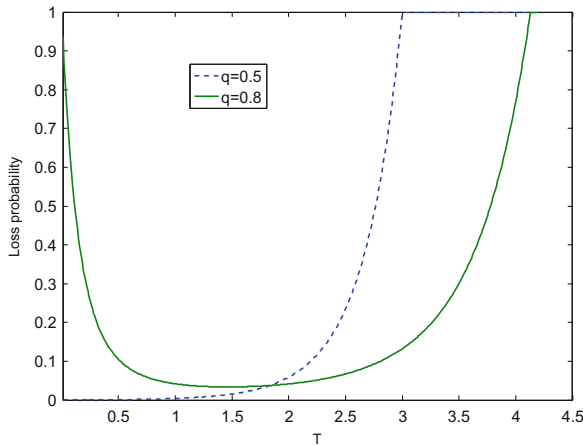

Fig. 4. Loss probability depending on the price T.

4   Conclusion

In this paper, we describe a game-theoretic framework for studying cyber insurance. We have taken into account complex interactions between users, insurer and attackers. The framework incorporates attack models, and naturally provides privacy-preserving mechanisms through the information asymmetry between the players. This work provides a first step towards a holistic understanding of cyber insurance and the design of optimal insurance policies. We would extend this framework to capture network effects, and address the algorithmic and design issues in cyber insurance.

References

1. Zhu, Q., Başar, T.: Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems. IEEE Control Syst. **35**(1), 46–65 (2015)
2. Anderson, R., Moore, T.: The economics of information security. Science **314**, 610–613 (2006)
3. Kesan, J., Majuca, R., Yurcik, W.: Cyber-insurance as a market-based solution to the problem of cybersercurity: a case study. In: Proceedings of WEIS (2005)
4. Lelarge, M., Bolot, J.: A local mean field analysis of security investments in networks. In: Proceedings of ACM NetEcon (2008)
5. Pal, R., Golubchik, L., Psounis, K., Hui, P.: Will cyber-insurance improve network security? a market analysis. In: Proceedings of INFOCOM (2014)
6. Hölmstrom, B.: Moral hazard and observability. Bell J. Econ. **10**(1), 74–91 (1979)
7. Holmstrom, B.: Moral hazard in teams. Bell J. Econ. **13**(2), 324–340 (1982)
8. Lelarge, M., Bolot, J.: Cyber insurance as an incentive for internet security. In: Proceedings of WEIS (2008)
9. Acemoglu, D., Malekian, A., Ozdaglar, A.: Network security and contagion. Perform. Eval. Rev. **42**(3) (2014)
10. Goyal, S., Vigier, A.: Attack, defense and contagion in networks. Rev. Econ. Stud. **81**(4), 1518–1542 (2014)
11. Böhme, R., Schwartz, G.: Modeling cyber-insurance: towards a unifying framework. In: Proceedings of WEIS (2010)
12. Naghizadeh, P., Liu, M.: Voluntary participation in cyber-insurance markets. In: Proceedings of WEIS (2014)
13. Raymond Law Group: Protecting the individual from data breach. In: The National LawReview (2014)
14. Peltzmann, S.: The effects of automobile safety regulation. J. Polit. Econ. **83**(4), 677–726 (1975)
15. Başar, T., Olsder, G.J.: Dynamic Noncooperative Game Theory, vol. 200. SIAM, Philadelphia (1995)
16. Luenberger, D.G.: Optimization by Vector Space Methods. Wiley, New York (1997)
17. Bailey, N.T.J., et al.: The Mathematical Theory of Infectious Diseases and its Applications. Charles Griffin & Company Ltd., London (1975). 5a Crendon Street, High Wycombe, Bucks HP13 6LE