Optimal Cyber-Insurance Contract Design for Dynamic Risk Management and Mitigation

Rui Zhang and Quanyan Zhu, *Senior Member, IEEE*

***Abstract*— With the recent growing number of cyberattacks and the constant lack of effective defense methods, cyber risks have become ubiquitous in enterprise networks, manufacturing plants, and government computer systems. Cyber insurance provides a valuable approach to transfer the cyber risks to insurance companies and further improve the security status of the insured. The designation of effective cyber-insurance contracts requires considerations from both the insurance market and the dynamic properties of the cyber risks. To capture the interactions between the users and the insurers, we present a dynamic moral-hazard type of principal–agent model incorporated with Markov decision processes, which are used to capture the dynamics and correlations of the cyber risks as well as the user's decisions on the protections. We study and fully analyze a case with a two-state two-action user under linear coverage insurance and further show the risk compensation, Peltzman effect, linear insurance contract principle, and zero-operating profit principle in this case. Numerical experiments are provided to verify our conclusions and further extend to cases of a four-state three-action user under linear coverage insurance and threshold coverage insurance.**

***Index Terms*— Cyber insurance, information asymmetry, Markov decision processes (MDPs), mechanism design, moral hazard, principal–agent problem.**

NOMENCLATURE

t	Time t.
$\mathscr{S}$ and N	Set and number of all possible states.
S_n	State n $(1 \leq n \leq N)$.
s and s_t	State and state at time t $(s, s_t \in \mathscr{S})$.
$\mathscr{X}$	Set of direct losses at all possible states.
X_n	Direct Loss at State S_n.
x and x_t	Direct loss, direct loss at time t.
$p(s_t, s_{t+1})$	Transition probability from s_t to s_{t+1}.
$\mathscr{A}$ and M	Set and number of all possible protections.
A_m	Protection m $(1 \leq m \leq M)$.
a and a_t	Protection and protection at time t $(a, a_t \in \mathscr{A})$.
$p(s_t, a_t, s_{t+1})$	Transition probability from s_t to s_{t+1} under a_t.
$c(a)$	Cost function.
α_s	Stationary state protection at state s $(\alpha_s \in \mathscr{A})$.
Ω	Set of all possible stationary protection policies.
π	Stationary protection policy $(\pi(s) = \alpha_s, \forall s \in \mathscr{S})$.
ρ	Value of transition probabilities.
$\mathscr{R}$	Set of all possible coverage functions.
$r(x)$ and K	Coverage function $(r \in \mathscr{R})$ and premium $(K \in \mathbb{R}_{\geq 0})$.
$r_0(x)$	Zero coverage function $(r_0(x) = 0, \forall x \in \mathbb{R}_{\geq 0})$.
R	Coverage level $(r(x) = Rx)$.
$l(s, a, r)$	Effective loss function.
$V(s, \pi, r)$	Expected cumulative effective loss function.
π_r^*	Optimal stationary protection policy under coverage r.
$\mathscr{S}_{GB}$	Set of two states $(\mathscr{S}_{GB} = \{S_G, S_B\})$.
S_G and S_B	Good state and bad state.
s and s^c	One state and other state $(s, s^c \in \mathscr{S}_{GB}; s^c \neq s)$.
X_G and X_B	Direct losses at good state and bad state.
$\mathscr{A}_{HL}$	Set of two actions $(\mathscr{A}_{HL} = \{A_H, A_L\})$.
A_H and A_L	Strong protection and weak protection.
α_G and α_B	Stationary state protections at good state and bad state.
α_s and α_{s^c}	Stationary state protections.
R_G and R_B	Threshold coverage levels at good state and bad state.

Manuscript received September 27, 2019; revised July 27, 2021 and September 14, 2021; accepted September 30, 2021. This work was supported in part by the National Science Foundation (NSF) under Grant SES-1541164, Grant ECCS-1847056, Grant CNS-2027884, and Grant BCS-2122060; and in part by the Army Research Office (ARO) under Grant W911NF-19-1-0041. *(Corresponding author: Rui Zhang.)*

The authors are with the Department of Electrical and Computer Engineering, New York University, Brooklyn, NY 11201 USA (e-mail: rz885@nyu.edu; qz494@nyu.edu).

Digital Object Identifier 10.1109/TCSS.2021.3117905

I. INTRODUCTION

CYBER risks created by malicious attackers, such as ransomware [1], data breaches [2], and denial of service [3], have become severe threats to the security of important devices and private data in the Internet of Things (IoT) and cyber-physical systems (CPSs) [4]–[6]. For example, the CryptoLocker ransomware attack has caused an estimated loss of $3 million [7]. The 2016 Dyn cyberattack has resulted in the disruption of major Internet platforms and services to large swathes of users in Europe and North America [8].

Although various defense methods, such as firewalls [9], intrusion detection systems [10], and moving-target defenses [11], have been deployed to detect the intrusion attempts and protect the networked devices, they cannot eliminate the cyber risks due to the complexities of cyber

environments [12]. Moreover, cyber threats are becoming stealthier, more strategic, and purposeful as exemplified by the advanced persistent threats such as Stuxnet attacks on the Iranian nuclear power plant in 2009 and the Ukrainian power plant attack in 2015 [13], [14].

Recently emerged cyber insurance provides an economically viable solution to further mitigate the cyber risks and improve network resiliency [15]–[19]. The insured network users could quickly recover from severe cyber incidents since part of the losses has been covered by the insurers. However, such as the classic insurance, the insurers may suffer from offering coverage to reckless users due to the information asymmetry that the insurers cannot directly observe the users' protections [20]–[22].

Moreover, as suggested by the theory of risk compensation in traditional insurance scenarios [23], the users may become less careful against cyberattacks knowing that insurers will cover their losses, for example, users may click more phishing emails, ignore the warnings of upgrading firewalls or systems, and reduce the frequency of scanning viruses or worms. As a result, the users may encounter more severe cyber incidents and the insurers may bear extra cyber risks.

Thus, it is imperative to study cyber-insurance contracts and their impacts on the users' cyber-risk statuses. However, classic risk analysis and insurance frameworks cannot be directly applied to cyber risks and cyber insurance as cyber risks are dynamically evolving and strongly correlated [24]–[27]. For example, an adversary can first launch a node capture attack to compromise the system [28], [29] and then gain the administration to the devices [30], steal private information [31], or inject ransomware worms or viruses [32].

In this article, we capture the correlations and dynamics of the cyber risks as well as the users' decisions on the protections with the Markov decision processes (MDPs) [33], [34]. Different states of the MDP are used to capture the different cyber risks from various sources, such as service failures, attackers, or network connections. The transitions of states capture the connections of different cyber risks, and they are affected by the user's actions of protection at different times.

To further mitigate the cyber risks, the user has a choice of purchasing cyber insurance. After paying a premium, the user could receive financial coverages from the insurer to reimburse his losses caused by various cyber risks, as shown in Fig. 1. The objective of the user is to find an optimal deployment of protections and cyber insurance that minimizes his cyber losses.

A rational user selects a cyber insurance from which he could benefit more, i.e., contracts with a low premium and high coverage. However, an insurer tends to offer an insurance contract that has a high premium and low coverage, as the insurer aims to maximize his operating profit. Moreover, similar to the traditional insurance scenarios, the insurer is not aware of the local protections of the user, and an inappropriate insurance contract could largely damage the insurer's profit.

We address such conflicting interests and the information asymmetry between the user and the insurer with a moral hazard type of principal–agent problem [21], [22], [35], [36].

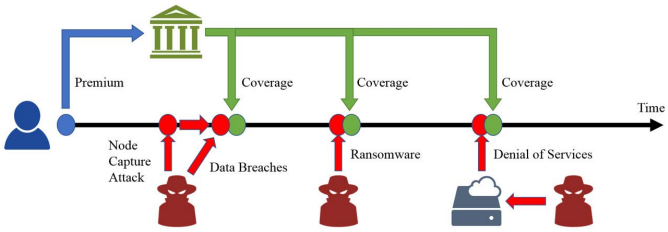

Fig. 1. Cyber-insurance example. The blue, red, and green icons represent user, attacker, and insurer, respectively. A user pays a premium to an insurer to purchase the cyber insurance. Then, the user could receive financial coverages from the insurer to cover part of his losses caused by cyberattacks.

The analysis, as well as the solution of the problem, is important to study the impacts of cyber insurance on the user and design effective insurance contracts. The major contributions of this work are summarized as follows.

1) We integrate MDPs into a moral hazard type of principal–agent model to investigate the impacts of cyber insurance on the user's cyber risks and design effective cyber-insurance contracts for the insurer.
2) We fully characterize a case between a two-state two-action user and a linear coverage insurer. The results of this case indicate that the optimal insurance contracts follow the linear insurance contract principle and zero-operating profit principle. The analysis also demonstrates the existence of risk compensation and the Peltzman effect in cyber insurance.
3) We develop scientific methods incorporating dynamic programming or linear programming for problems involving multiple cyber-risk states, various protection choices, and complex insurance contracts. Our numerical experiments illustrate risk compensation, Peltzman effect, and zero-operating profit principle in cases of a four-state three-action user under linear coverage insurance and threshold coverage insurance.

A. Organization of This Article

The rest of this article is organized as follows. Section II presents the related works. Sections III and IV discuss the user's problem and the insurer's problem, respectively. Section V presents a case study of a linear coverage insurance contract on a two-state two-action user. Sections VI and VII present numerical results and concluding remarks, respectively. Appendixes A, B, and C provide the proofs of the Proposition 2, and Theorem 1, and Proposition 4, respectively. We provide a summary of notations in Nomenclature.

II. Related Works

Recently, with fast-growing types and amounts of networked devices and shortages of effective and state-of-the-art defense methods, cyber insurance has drawn huge attention as it can transfer the unexpected cyber risks to the insurance companies [15]–[19], [27], [37]–[41]. The existing insurance framework could bring useful insights on modeling the cyber insurance [15], [42]. The moral hazard models in the economics literature are good tools to capture the information

asymmetry between the insured and the insurers [20]–[22]. Various frameworks and methodologies have been brought up to investigate cyber-insurance contracts and their impacts on cyber risks.

Several works have studied cyber insurance through market-based approaches by analyzing the supply and demand relations between insurers and insureds [16], [18], [27], [37]. Pal *et al.* [18] have analyzed regulated monopolistic and competitive cyber-insurance markets and showed that cyber insurance can improve the network security, but the insurer can make zero expected profits in monopoly markets. Böhme *et al.* [16], Böhme and Kataria [27], and Böhme [37] have presented several market models of cyber insurance with the consideration of interdependency between cyber risks and information asymmetries between insurers and insureds and showed analytical results on the impacts of cyber insurance to cybersecurity and the viability of a market for cyber insurance.

Game theory has been used to capture the interactions between insurers and insureds of cyber insurance [19], [38], [41]. Laszka *et al.* [41] have used a two-player signaling game to capture the information asymmetry between a potential client and an insurer and further studied incentives for auditing potential clients before cyber-insurance premium calculations. Grossklags *et al.* [38] have presented several security games to capture the decision-making of network users on protections and insurance. The equilibrium analysis shows that users may seek to self-protect themselves at just slightly above the lowest protection level in the weakest target game. Zhang *et al.* [19] have studied the interactions between insureds, attackers, and insurers with a bilevel game-theoretic framework in a networked environment and demonstrated the impacts of network connections to the three types of players.

Most previous works have focused on the information asymmetry and interdependencies of cyber risks, and however, their models have not captured the dynamics and correlations of the cyber risks, which have been studied with different methodologies and models [43]–[47]. Poolsappasit *et al.* [46] have used a Bayesian attack graphs model to analyze the network security risk assessment and mitigation. Kim *et al.* [47] have used a differential epidemic model to capture the spreading of viruses and worms in computer networks. These works aim to reduce the impacts of cyber risks through local protections, such as firewalls [9], intrusion detection [30], or moving-target defenses [11], which cannot fully mitigate the risks of cyberattacks.

In this work, we focus on studying the dynamics and correlations of the cyber risks and analyzing the impacts of the cyber insurance to both the insureds and the insurers. Markov models have been applied in various types of insurance to capture dynamic and correlated risks [48]–[50]. Haberman and Pitacco [48] have investigated the disability insurance based on Markov and semi-Markov models; Lambrinoudakis *et al.* [49] have proposed a Markov model to describe the transitions of an information system as a result of a security incident and further utilized it to estimate the premium of the insurance contract against the expected losses from the incident. However, they have not yet considered the fact that the user's decisions on deploying local protections could significantly change the cyber risks and the insurer could face notable losses if it fails to take that into consideration while designing cyber-insurance contracts.

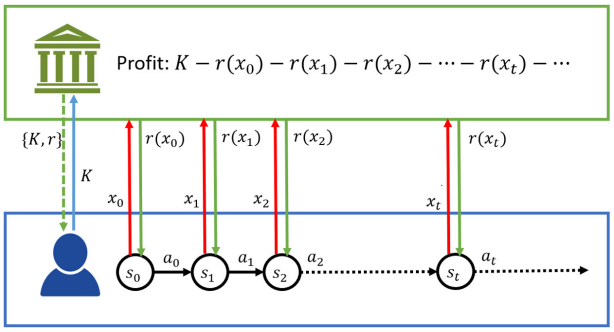

Fig. 2. Illustration of cyber insurance. The dynamics of the user's cyber risks are captured by MDP with s_t denoting the cyber-risk state at time t, which is associated with a direct loss x_t. The user can choose various protections a_t to reduce future losses. The objective of the user is to find the optimal protection sequence $\{a_t\}_{t\geq 0}$, which minimizes his cumulative losses. The user can also purchase cyber insurance to mitigate his losses. The insurer first announces the insurance contract $\{K, r\}$, where K and r indicate the premium and the coverage function, respectively. The user can decide whether to purchase the insurance or not. If the user chooses to purchase the insurance, he must pay a premium K, and when he faces a loss of x, the insurer should provide coverage of $r(x)$ to him. The objective of the insurer is to maximize his profit. Note that the insurer has no information on the user's protection sequences.

We capture the cyber risks as well as the user's deployments of local protections with MDPs, which have been used variously to analyze cybersecurity [51]–[53]. We then use the existing moral hazard type of principal–agent model to capture the interactions between the user and the insurer with incomplete information. The analysis of both the optimal insurance contract and the user's response to it provides useful insights on the designation of the cyber-insurance contracts in the real world.

III. User's Optimal Protection Policies

We use discrete MDPs to capture the evolvements of the user's cyber risks with time, and an illustration is shown in Fig. 2. Let $s_t \in \mathscr{S}$ denote the user's cyber-risk state at time $t \in \mathbb{Z}_{\geq 0}$, where $\mathscr{S} \equiv \{S_n | 1 \leq n \leq N\}$ is the set of all possible cyber-risk states. Different cyber-risk states may incur various types of losses, e.g., data breaches, physical device damages, and compromised financial accounts. In this article, we consider that all types of losses are measurable and can be quantified by monetary direct losses. We assume that each cyber-risk state $S_n \in \mathscr{S}$ is associated with a fixed direct loss $X_n \in \mathbb{R}_{\geq 0}$, and the user's direct loss at time t can be denoted by $x_t \in \mathscr{X}$, where $\mathscr{X} \equiv \{X_n | 1 \leq n \leq N\}$.

The user can adopt different protections, such as firewalls, intrusion detection systems, and moving-target defenses, to reduce the possibilities of entering cyber-risk states that can incur severe losses. Let $a_t \in \mathscr{A}$ denote the protections at time t, where $\mathscr{A} \equiv \{A_m | 1 \leq m \leq M\}$ is the set of all available protections. The transition probability $p(s_t, a_t, s_{t+1})$ denotes the probability that the user goes to state s_{t+1} at time $t+1$ when he is currently in state s_t and adopts protection a_t, which naturally captures the correlations among

different cyber-risk states under different protections. Note that $\sum_{n=1}^{N} p(s_t, a_t, S_n) = 1$ as the user can only enter states within $\mathscr{S}$ at time $t+1$.

We further provide two examples to illustrate the states $\mathscr{S}$ and protections $\mathscr{A}$ of the user.

Example 1: Suppose a customer whose computer faces threats of Ransomware. In this example, the customer has $\mathscr{S} = \{S_1, S_2\}$ and $\mathscr{A} = \{A_1, A_2\}$. States S_1 and S_2 denote that the computer is secure and compromised, respectively. The customer can choose to do nothing A_1 or add firewalls A_2. The computer has a lower probability of facing Ransomware, i.e., entering state S_2, if the customer deploys firewalls. When the computer is compromised, the customer needs to either pay the money or replace the computer, which can be covered if he has purchased cyber insurance.

Example 2: Consider a cloud center who aims to protect itself from the damages caused by potential attackers. In this example, the cloud center has $\mathscr{S} = \{S_1, S_2, S_3\}$ and $\mathscr{A} = \{A_1, A_2, A_3, A_4\}$. State S_1 denotes the situation when it is safe and faces no cyberattacks. However, the cloud center may encounter data breaches and denial of services, which are represented by states S_2 and S_3, respectively. Each state $S_n \in \mathscr{S}$ is associated with a direct loss X_n. For example, at time t, $s_t = S_2$ indicates that the cloud center faces data breaches that inflict X_2 direct losses to it. Especially, the direct loss $X_1 = 0$ at state S_1, which indicates that the cloud center has no loss when it faces no cyberattacks. To defend against these cyberattacks, the cloud center may deploy firewalls, intrusion detection systems, and moving-target defense, which are represented by protections A_2, A_3, and A_4, respectively. Especially, the cloud center can also choose to do nothing, which is denoted as A_1. The cloud center has smaller probabilities of entering states with high losses if he deploys protections, and however, these protections are also costly. The cloud center can also purchase cyber insurance to cover part of its losses and help it recover from cyber incidents. The objective of the cloud center is to find an optimal deployment of protections and cyber insurance such that its future cumulative losses are minimized. Cases involve other cyber risks or protections can be extended through increasing the size of $\mathscr{S}$ and $\mathscr{A}$.

Besides the protections, the user can also mitigate his losses through purchasing cyber insurance. After paying a premium to an insurer, the user could receive a coverage of $r(x_t)$ from the insurer when he faces a direct loss of x_t, where $r : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is the coverage function of the insurance. The objective of the user is to find an optimal sequence of protections $\{a_t\}_{t \in \mathbb{Z}_{\geq 0}}$ that minimizes the expected cumulative effective losses given the initial state $s_0 \in \mathscr{S}$, which can be captured as

$$\min_{\{a_t\}} \mathbb{E}\left\{ \sum_{t=0}^{\infty} \delta^t (x_t - r(x_t) + c(a_t)) \Big| s_0 \right\} \tag{1}$$

where function $c(a_t)$ returns the cost of protection a_t and $\delta \in (0, 1)$ is the discount factor, which indicates that future losses are valued less at time 0.

In this article, we consider that the user decides his protections contingent on his current state. Such feedback strategy allows the user to maintain his security level by adopting the necessary protections that can reduce the losses from cyberattacks and save the costs of protection at the same time. The strategy is usually denoted by a stationary protection policy $\pi : \mathscr{S} \to \mathscr{A}$, e.g., $\pi(S_n) = A_m$ indicates that the user always takes protection A_m at state S_n. As a result, the expected cumulative effective losses of the user under a stationary protection policy can be captured as

$$V(s_0, \pi, r) = \mathbb{E}\left\{ \sum_{t=0}^{\infty} \delta^t (x_t - r(x_t) + c(\pi(s_t))) \Big| s_0 \right\}. \tag{2}$$

The user aims to find an optimal stationary protection policy $\pi_r^* \in \Omega$ that minimizes his expected cumulative effective losses given the coverage function r, and such objective can be captured as

$$\pi_r^* \in \arg\min_{\pi \in \Omega} V(s_0, \pi, r) \tag{3}$$

where Ω denotes the set of all possible stationary policies.

A rational user purchases the insurance only when the expected cumulative effective losses plus the premium under the insurance is lower than the losses without insurance, which can be captured as

$$V(s_0, \pi_r^*, r) + K \leq V(s_0, \pi_{r_0}^*, r_0) \tag{4}$$

where $K \in \mathbb{R}_{\geq 0}$ is the premium of the insurance and r_0 indicates a zero coverage function, i.e., $r_0(X) = 0$ for all $X \in \mathbb{R}_{\geq 0}$, which corresponds to the case when there is no insurance. The fact that the user purchases the insurance only when inequality (4) is satisfied must be considered by the insurer while designing effective insurance contracts.

The optimal protection policy π_r^* could be obtained by solving (3) with either dynamic programming or linear programming [54], and we summarize both approaches in the following.

A. Dynamic Programming Approach

Recall (2), and let us define the loss function $l(s_t, a_t, r) = x_t - r(x_t) + c(a_t)$, which indicates the effective loss at time t under the coverage function r. Note that $l(s_t, a_t, r)$ does not take x_t as variable since the direct loss x_t is uniquely determined by the user's cyber-risk state s_t. Thus, we can express the expected cumulative effective losses as

$$\begin{aligned} V(s_0, \pi, r) &= \mathbb{E}\left\{ \sum_{t=0}^{\infty} \delta^t l(s_t, \pi(s_t), r) | s_0 \right\} \\ &= l(s_0, \pi(s_0), r) + \delta \sum_{s' \in \mathscr{S}} p(s_0, \pi(s_0), s') V(s', \pi, r) \end{aligned} \tag{5}$$

where $l(s_0, \pi(s_0), r)$ and $\delta \sum_{s \in \mathscr{S}} p(s_0, \pi(s_0), s) V(s, \pi, r)$ capture the effective loss at time 0 and the future expected cumulative effective losses, respectively. As a result, given a coverage function r, the optimal protection policy π_r^* can be

found by the following dynamic programming operators [54]:

$$\pi_r^*(s) \in \arg\min_{a\in\mathscr{A}}\left\{ l(s,a,r) + \delta \sum_{s'\in\mathscr{S}} p(s,a,s')V(s',\pi_r^*,r) \right\} \tag{6}$$

$$V(s,\pi_r^*,r) = l(s,\pi_r^*(s),r) + \delta \sum_{s'\in\mathscr{S}} p(s,\pi_r^*(s),s')V(s',\pi_r^*,r). \tag{7}$$

By iterating (6) and (7) for all states $s \in \mathscr{S}$ until no further changes take place, we can achieve π_r^* and $V(s,\pi_r^*,r)$, and the convergence to the optimum is guaranteed [54].

B. Linear Programming Approach

Besides the dynamic programming, we can also use linear programming to solve the user's problem (3) [54]. Let $\eta \in \mathbb{R}^{NM\times 1}$ and $\theta \in \mathbb{R}^{N\times 1}$ denote the prime variable and the dual variable of the linear programming problems, respectively. Let $\mathbf{b} \in \mathbb{R}^{N\times 1}$ denote a column vector of size N with all the elements equal to 1. Let $\mathbf{d} \in \mathbb{R}^{NM\times 1}$ denote a column vector of size NM, which captures the per-state and per-action losses, and the $(N(n-1)+m)$th element of it equals $l(S_n, A_m, r)$, where $1 \le n \le N$ and $1 \le m \le M$. Let matrix $O = E - \delta P$, where matrix $E \in \mathbb{R}^{N\times NM}$ has that $E_{n,N(n-1)+m} = 1$ for $1 \le n \le N$ and $1 \le m \le M$ and all the other elements are 0, and matrix $P \in \mathbb{R}^{N\times NM}$ is the transition probability matrix, where $P_{n',N(n-1)+m} = p(n,a_m,n')$, $1 \le n \le N$, $1 \le n' \le N$, and $1 \le m \le M$. Problem (3) can be reformulated into a linear programming problem in the standard form as [54]

$$\min_{\eta}\ \mathbf{d}^T\eta$$
$$\text{s.t.} O\eta = \mathbf{b}, \eta \ge \mathbf{0}$$

with its dual problem

$$\max_{\theta}\ \mathbf{b}^T\theta$$
$$\text{s.t.} \mathbf{d} - O^T\theta \ge \mathbf{0}.$$

The optimal primal variable η^* represents the optimal state–action frequencies; the optimal dual variable θ^* represents the expected cost-to-go values of the states for the given coverage function r, i.e., $\theta_n^* = V(S_n,\pi_r^*,r)$ for $1 \le n \le N$. After solving the dual problem, we can find the optimal protection policy π_r^* by plugging $V(S_n,\pi_r^*,r)$ into (6).

IV. Insurer's Optimal Insurance Contracts

In this section, we present and analyze the insurer's problem of designing cyber-insurance contracts. An illustration of the interactions between the user and the insurer is shown in Fig. 2. Note that the insurer first announces the insurance contract $\{K,r\}$, and the user then makes the decision of purchasing the insurance based on the expected cumulative effective losses under that insurance contract. If the user chooses to purchase the insurance, the insurer instantly earns a profit of K at time 0, but the insurer is required to pay the coverage of $r(x_t)$ when the user faces a loss of x_t at time t. As a result, the insurer's operating profit can be captured as $K - \mathbb{E}\{\sum_{t=0}^{\infty}\delta^t r(x_t)|s_0\}$, where $\mathbb{E}\{\sum_{t=0}^{\infty}\delta^t r(x_t)|s_0\}$ denotes the expected cumulative coverage provided by the insurer to the user. The objective of the insurer is to find an optimal insurance contract $\{K^*,r^*\}$ that maximizes his operating profit. As a result, the insurer's problem can be captured as

$$\max_{\{K,r\}}\quad K - \mathbb{E}\left\{\sum_{t=0}^{\infty}\delta^t r(x_t)\big|s_0\right\}$$
$$\text{s.t.}\quad K - \mathbb{E}\left\{\sum_{t=0}^{\infty}\delta^t r(x_t)\big|s_0\right\} \ge 0 \tag{8a}$$
$$V(s_0,\pi_r^*,r) + K \le V(s_0,\pi_{r_0}^*,r_0). \tag{8b}$$

Constraint (8a) captures the insurer's individual rationality that he chooses not to provide the insurance if he has a negative profit. Constraint (8b) captures the user's individual rationality on purchasing the insurance and it comes from inequality (4).

By solving problem (8), the insurer can find an optimal insurance contract, which maximizes his operating profit and is acceptable by the user. After combining the user's problem and the insurer's problem, the interactions of the user and the insurer can be captured by the following principal–agent problem:

$$\max_{\{K,r\}}\ K - \mathbb{E}\left\{\sum_{t=0}^{\infty}\delta^t r(x_t)\big|s_0\right\}$$
$$\text{s.t.}\ \ K - \mathbb{E}\left\{\sum_{t=0}^{\infty}\delta^t r(x_t)\big|s_0\right\} \ge 0 \tag{9a}$$
$$V(s_0,\pi_r^*,r) + K \le V(s_0,\pi_{r_0}^*,r_0) \tag{9b}$$
$$\pi_r^* \in \arg\min_{\pi\in\Omega} V(s_0,\pi,r). \tag{9c}$$

Problem (9) is an optimization problem nested with various suboptimization problems. The solution of Problem (9) captures both the user's objective of minimizing his expected cumulative effective losses and the insurer's objective of maximizing his own profit with the consideration of the user's rational choice of purchasing the insurance. To find the solution of problem (9), we can first solve the user's problem (3) and obtain the optimal protection policies π_r^* and the corresponding losses $V(s_0,\pi_r^*,r)$ to the coverage function r and then achieve $\{K^*,r^*\}$ by solving the insurer's problem (8).

We can simplify the insurer's problem (8) by exploring the expected cumulative effective losses and the optimal protection policies as discussed in the following.

A. Insurer's Problem: Simplifications and Direct Conclusions

We first notice that the expected cumulative coverage is equal to the expected cumulative direct losses minus the expected cumulative effective losses, i.e.,

$$\begin{aligned}
&\mathbb{E}\left\{\sum_{t=0}^{\infty}\delta^t r(x_t)|s_0\right\} \\
&\quad= \mathbb{E}\left\{\sum_{t=0}^{\infty}\delta^t\big(x_t + c(\pi_r^*(s_t))\big)|s_0\right\} \\
&\qquad- \mathbb{E}\left\{\sum_{t=0}^{\infty}\delta^t\big(x_t - r(x_t) + c(\pi_r^*(s_t))\big)|s_0\right\} \\
&\quad= V(s_0,\pi_r^*,r_0) - V(s_0,\pi_r^*,r)
\end{aligned}$$

where $V(s_0, \pi_r^*, r_0)$ can be interpreted as the expected cumulative effective losses given the optimal protection policy π_r^* and the zero coverage function r_0. Thus, Problem (8) can be rewritten as follows:

$$\begin{aligned} &\max_{\{K,r\}} K - \big(V(s_0, \pi_r^*, r_0) - V(s_0, \pi_r^*, r)\big) \\ &\text{s.t.} \quad K - \big(V(s_0, \pi_r^*, r_0) - V(s_0, \pi_r^*, r)\big) \geq 0 \qquad (10a) \\ &\qquad V(s_0, \pi_r^*, r) + K \leq V(s_0, \pi_{r_0}^*, r_0). \qquad (10b) \end{aligned}$$

Constraint (10b) indicates that the maximum premium that can be charged by the insurer for a coverage function r is

$$K_{\max} = V(s_0, \pi_{r_0}^*, r_0) - V(s_0, \pi_r^*, r). \qquad (11)$$

The user chooses not to purchase the insurance with a premium $K > K_{\max}$ because the losses and the premium under the insurance are higher than the losses without insurance.

As a result, problem (8) is equivalent to the following problem after letting K be equal to $K_{\max}$ and plugging (11) into its objective function and constraint:

$$\begin{aligned} &\max_{r \in \mathscr{R}} V(s_0, \pi_{r_0}^*, r_0) - V(s_0, \pi_r^*, r_0) \\ &\text{s.t.} \ V(s_0, \pi_{r_0}^*, r_0) - V(s_0, \pi_r^*, r_0) \geq 0 \qquad (12) \end{aligned}$$

where $\mathscr{R}$ denotes the set of all possible coverage functions, and the constraint indicates that the profit of the insurer cannot be negative. After solving (12), we can find the optimal coverage function r^*, and then, the optimal premium can be computed through (11). Similarly, the principal–agent problem (9) can also be rewritten as

$$\begin{aligned} &\max_{r \in \mathscr{R}} \ V(s_0, \pi_{r_0}^*, r_0) - V(s_0, \pi_r^*, r_0) \\ &\text{s.t.} \ \ V(s_0, \pi_{r_0}^*, r_0) - V(s_0, \pi_r^*, r_0) \geq 0 \qquad (13a) \\ &\qquad \pi_r^* \in \arg\min_{\pi \in \Omega} V(s_0, \pi, r). \qquad (13b) \end{aligned}$$

Comparing (8) and (9), we only need to find the optimal protection policies π_r^* to obtain the optimal insurance contract $\{K^*, r^*\}$ through (12) and (13).

One useful insight regarding the operating profit could be obtained without solving (12) or (13), which is summarized in the following remark and proposition.

Remark 1: Any coverage function r that yields $\pi_r^* = \pi_{r_0}^*$, i.e., the user has the same optimal protection policy between the case under the coverage function r and the case under no insurance, is a feasible solution with the corresponding premium $K = V(s_0, \pi_{r_0}^*, r_0) - V(s_0, \pi_r^*, r) = V(s_0, \pi_{r_0}^*, r_0) - V(s_0, \pi_{r_0}^*, r) \geq 0$ as $V(s_0, \pi_{r_0}^*, r) \leq V(s_0, \pi_{r_0}^*, r_0)$, and the insurer has a zero-operating profit under that insurance contract as $V(s_0, \pi_{r_0}^*, r_0) - V(s_0, \pi_r^*, r_0) = V(s_0, \pi_{r_0}^*, r_0) - V(s_0, \pi_{r_0}^*, r_0) = 0$.

Proposition 1: Any insurance contract $\{K, r\}$ that yields $\pi_r^* = \pi_{r_0}^*$ and meets (11) is optimal for the insurer, and the insurer has a zero-operating profit under that contract.

Proof: The operating profit of the insurer has that $V(s, \pi_{r_0}^*, r_0) - V(s, \pi_r^*, r_0) \leq 0$ from (13b), i.e., $\pi_{r_0}^* \in \arg\min_{\pi \in \Omega} V(s, \pi, r_0)$. Thus, the maximum profit that the insurer can achieve is 0. As a result, if the user has $\pi_r^* = \pi_{r_0}^*$ under an insurance contract $\{K, r\}$, this contract is feasible from Remark 1 and it is also optimal. □

Remark 1 indicates that the insurer has a zero-operating profit when the user has the same protection policies with or without insurance, which explains market neutrality. Proposition 1 indicates that the insurance contract in Remark 1 is optimal for the insurer. We denote this conclusion as the zero-operating profit principle.

V. Case Study: Two-State Two-Action User and Linear Coverage Insurer

In this section, we present a representative case where the user has two states and two actions and the insurer provides the linear coverage. Analysis of this case provides structural insights into the insurance contracts. Recall Section III that the user in this case has the set of states $\mathscr{S}_{GB} \equiv \{S_G, S_B\}$, where S_G and S_B indicate good state and bad state, respectively. The losses that associated with the states can be further identified as X_G and X_B. The difference between the good state and the bad state is that the user has lower losses at the good state than that at the bad state, i.e., $0 \leq X_G < X_B$.

To reduce the losses, the user can choose to take strong protection A_H or weak protection A_L; in other words, the user has the action set $\mathscr{A}_{HL} = \{A_H, A_L\}$. We further use shorthand notations C_H and C_L to represent the costs of protections A_H and A_L, respectively, i.e., $c(A_H) = C_H$ and $c(A_L) = C_L$. The differences between strong protection and weak protection can be identified in detail as follows.

1) $p(s, A_H, S_B) < p(s, A_L, S_B), \forall s \in \mathscr{S}_{GB}$, which indicates that the user has a higher probability of going to the bad state when he has a weak protection.
2) $p(s, A_L, S_G) < p(s, A_H, S_G), \forall s \in \mathscr{S}_{GB}$, which indicates that the user has a higher probability of going to the good state when he has strong protection.
3) $0 \leq C_L < C_H$, which indicates that the cost of a strong protection is higher than the cost of a weak protection.

These differences capture the fact that a strong protection can make the user more secure, but its cost is also higher.

With two states and two actions, the user has only four possible stationary protection policies, i.e., $\Omega = \{\Pi_{HH}, \Pi_{HL}, \Pi_{LH}, \Pi_{LL}\}$, where the following conditions hold.

1) $\Pi_{HH}(S_G) = A_H$ and $\Pi_{HH}(S_B) = A_H$.
2) $\Pi_{HL}(S_G) = A_H$ and $\Pi_{HL}(S_B) = A_L$.
3) $\Pi_{LH}(S_G) = A_L$ and $\Pi_{LH}(S_B) = A_H$.
4) $\Pi_{LL}(S_G) = A_L$ and $\Pi_{LL}(S_B) = A_L$.

An optimal protection policy $\pi^* \in \Omega$ can be achieved by solving Problem (3), which minimizes the user's expected cumulative effective losses.

Besides protection, the user can also purchase insurance to further mitigate his losses. We consider that the insurer offers a linear coverage with $R \in [0, 1]$ denoting the coverage level of the insurance, i.e., $r(x) = Rx$. Especially, $R = 0$ and $R = 1$ indicate no coverage and full coverage, respectively.

Methods in Sections III and IV can be used to find the optimal protection policy of the user and the optimal insurance contract for the insurer. Since there are only two states and two actions for the user, we can find them analytically.

A. User's Optimal Protection Policy

We first introduce several notations to simplify representations. Since the user has only two states S_G and S_B, we use $s^c \neq s$ to denote the other state for a given state $s \in \mathscr{S}_{GB}$. Since the user adopts a stationary protection policy, i.e., he has fixed protections at each state, we identify his state protections as α_G and α_B for the good state and the bad state, respectively. We further define the action-dependent expected cumulative effective loss function as follows:

$$\overline{V}(s, \alpha_s; \alpha_{s^c}, R) = l(s, \alpha_s, R) + \delta p(s, \alpha_s, S_G)\overline{V}(S_G, \alpha_G; \alpha_B, R) + \delta p(s, \alpha_s, S_B)\overline{V}(S_B, \alpha_B; \alpha_G, R). \quad (14)$$

Remark 2: For a protection policy π that has $\pi(S_G) = \alpha_G$ and $\pi(S_B) = \alpha_B$, the expected cumulative effective loss function (5) is equivalent to the action-dependent expected cumulative effective loss function (14), i.e.,

$$V(S_G, \pi, R) = \overline{V}(S_G, \pi(S_G); \pi(S_B), R) = \overline{V}(S_G, \alpha_G; \alpha_B, R)$$
$$V(S_B, \pi, R) = \overline{V}(S_B, \pi(S_B); \pi(S_G), R) = \overline{V}(S_B, \alpha_B; \alpha_G, R).$$

As a result, the dynamic programming operators (6) and (7) can be written as

$$\pi_R^*(S_G) \in \arg\min_{\alpha_G \in \mathscr{A}_{HL}} \overline{V}(S_G, \alpha_G; \pi_R^*(S_B), R) \quad (15)$$

$$\pi_R^*(S_B) \in \arg\min_{\alpha_B \in \mathscr{A}_{HL}} \overline{V}(S_B, \alpha_B; \pi_R^*(S_G), R) \quad (16)$$

where

$$\overline{V}(S_G, \alpha_G; \alpha_B, R) = l(S_G, \alpha_G, R) + \delta p(S_G, \alpha_G, S_G)\overline{V}(S_G, \alpha_G; \alpha_B, R) + \delta p(S_G, \alpha_G, S_B)\overline{V}(S_B, \alpha_B; \alpha_G, R) \quad (17)$$

$$\overline{V}(S_B, \alpha_B; \alpha_G, R) = l(S_B, \alpha_B, R) + \delta p(S_B, \alpha_B, S_G)\overline{V}(S_G, \alpha_G; \alpha_B, R) + \delta p(S_B, \alpha_B, S_B)\overline{V}(S_B, \alpha_B; \alpha_G, R). \quad (18)$$

Both (17) and (18) are linear equations on $\overline{V}(S_G, \alpha_G; \alpha_B, R)$ and $\overline{V}(S_B, \alpha_B; \alpha_G, R)$, and thus, we can solve them together and achieve

$$\overline{V}(S_G, \alpha_G; \alpha_B, R) = \frac{(1 - \delta p(S_B, \alpha_B, S_B))l(S_G, \alpha_G, R) + \delta p(S_G, \alpha_G, S_B)l(S_B, \alpha_B, R)}{I_p(\alpha_G, \alpha_B)} \quad (19)$$

$$\overline{V}(S_B, \alpha_B; \alpha_G, R) = \frac{\delta p(S_B, \alpha_B, S_G)l(S_G, \alpha_G, R) + (1 - \delta p(S_G, \alpha_G, S_G))l(S_B, \alpha_B, R)}{I_p(\alpha_G, \alpha_B)} \quad (20)$$

where

$$I_p(\alpha_G, \alpha_B) = \Big(1 - \delta p(S_G, \alpha_G, S_G)\Big)\Big(1 - \delta p(S_B, \alpha_B, S_B)\Big) - \delta^2 p(S_G, \alpha_G, S_B)p(S_B, \alpha_B, S_G). \quad (21)$$

As a result, we can find π_R^* by solving (15) and (16) with (19) and (20), respectively. Since there are only two protection choices A_H and A_L, we can find the optimal protection policy by comparing the action-dependent expected cumulative effective losses under A_H and A_L.

Lemma 1: The optimal protection policy π_R^* given the coverage level R can be summarized as follows.

1) $\pi_R^* = \Pi_{LL}$ if and only if $\overline{V}(S_G, A_H; A_L, R) \geq \overline{V}(S_G, A_L; A_L, R)$ and $\overline{V}(S_B, A_H; A_L, R) \geq \overline{V}(S_B, A_L; A_L, R)$.
2) $\pi_R^* = \Pi_{LH}$ if and only if $\overline{V}(S_G, A_H; A_H, R) \geq \overline{V}(S_G, A_L; A_H, R)$ and $\overline{V}(S_B, A_H; A_L, R) < \overline{V}(S_B, A_L; A_L, R)$.
3) $\pi_R^* = \Pi_{HL}$ if and only if $\overline{V}(S_G, A_H; A_L, R) < \overline{V}(S_G, A_L; A_L, R)$ and $\overline{V}(S_B, A_H; A_H, R) \geq \overline{V}(S_B, A_L; A_H, R)$.
4) $\pi_R^* = \Pi_{HH}$ if and only if $\overline{V}(S_G, A_H; A_H, R) < \overline{V}(S_G, A_L; A_H, R)$ and $\overline{V}(S_B, A_H; A_H, R) < \overline{V}(S_B, A_L; A_H, R)$.

Proof: The user chooses a protection policy with lower expected cumulative effective losses in both good state and bad state. □

We consider that the user always takes A_L when $\overline{V}(s, A_H; \alpha_{s^c}, R) = \overline{V}(s, A_L; \alpha_{s^c}, R)$. We can further simplify the comparisons in Lemma 1 as shown in the following proposition.

Proposition 2: Let us define function $h : \mathscr{S} \times \mathscr{A} \times \mathscr{R} \to \mathbb{R}$ as

$$h(s, \alpha_{s^c}, R) = (1 - R)\delta\big(p(s, A_H, s^c) - p(s, A_L, s^c)\big)(X_{s^c} - X_s) + (1 - \delta + \delta p(S_B, \alpha_{s^c}, S_G) + \delta p(S_G, \alpha_{s^c}, S_B))(C_H - C_L)$$

the optimal protection policy π_R^* can be summarized as follows.

1) $\pi^* = \Pi_{LL}$ if and only if $h(S_G, A_L, R) \geq 0$ and $h(S_B, A_L, R) \geq 0$.
2) $\pi^* = \Pi_{LH}$ if and only if $h(S_G, A_H, R) \geq 0$ and $h(S_B, A_L, R) < 0$.
3) $\pi^* = \Pi_{HL}$ if and only if $h(S_G, A_L, R) < 0$ and $h(S_B, A_H, R) \geq 0$.
4) $\pi^* = \Pi_{HH}$ if and only if $h(S_G, A_H, R) < 0$ and $h(S_B, A_H, R) < 0$.

Proof: See Appendix A. □

Thus, we could obtain the optimal protection policy of the user by analyzing $h(s, \alpha_{s^c}, R)$, and we further have the following observation on it.

Proposition 3: Function $h(s, \alpha_{s^c}, R)$ is linearly increasing on the coverage level R.

Proof: We can see that $h(s, \alpha_{s^c}, R)$ is linear on R with a slope of $-\delta(p(s, A_H, s^c) - p(s, A_L, s^c))(X_{s^c} - X_s)$. From the properties of protections and direct losses, we have $p(S_G, A_H, S_B) - p(S_G, A_L, S_B) < 0$, $X_B - X_G > 0$, $p(S_B, A_H, S_G) - p(S_B, A_L, S_G) > 0$, and $X_G - X_B < 0$. As a result, $-\delta(p(s, A_H, s^c) - p(s, A_L, s^c))(X_{s^c} - X_s) > 0$ and $h(s, \alpha_{s^c}, R)$ is linearly increasing on R. □

Before we obtain the optimal protection policy π_R^*, we note the following proposition regarding the uniqueness of π_R^*.

Theorem 1: The optimal protection policy π_R^* is unique.

Proof: See Appendix B. □

With Lemma 1, Proposition 3, and Theorem 1, we can obtain the optimal protection policies of the user with respect to the coverage level as stated in the following proposition.

Proposition 4: Let us define the value of transition probabilities as

$$\rho = p(S_B, A_H, S_G) + p(S_G, A_H, S_B) - p(S_B, A_L, S_G) - p(S_G, A_L, S_B). \quad (22)$$

The user's optimal protection policies with respect to the insurer's coverage level can be summarized with the following cases, as also shown in Fig. 3.

Case 1: If $h(S_G, A_L, 0) \geq 0$ and $h(S_B, A_L, 0) \geq 0$, the optimal protection policies $\pi_R^* = \Pi_{LL}$ for $R \in [0, 1]$.

Case 2: If $h(S_G, A_L, 0) < 0$ and $h(S_B, A_H, 0) \geq 0$, we have $\rho < 0$ in this case. The optimal protection policies $\pi_R^* = \Pi_{HL}$ for $R \in [0, R_G)$ and $\pi_R^* = \Pi_{LL}$ for $R \in [R_G, 1]$, where

$$R_G = 1 - \frac{(1-\delta+\delta p(S_B, A_L, S_G)+\delta p(S_G, A_L, S_B))(C_H - C_L)}{\delta(p(S_G, A_L, S_B) - p(S_G, A_H, S_B))(X_B - X_G)}.$$

Case 3: If $h(S_G, A_H, 0) \geq 0$ and $h(S_B, A_L, 0) < 0$, we have $\rho > 0$ in this case. The optimal protection policies $\pi_R^* = \Pi_{LH}$ for $R \in [0, R_B)$ and $\pi_R^* = \Pi_{LL}$ for $R \in [R_B, 1]$, where

$$R_B = 1 - \frac{(1-\delta+\delta p(S_G, A_L, S_B)+\delta p(S_B, A_L, S_G))(C_H - C_L)}{\delta(p(S_B, A_H, S_G) - p(S_B, A_L, S_G))(X_B - X_G)}.$$

Case 4: If $h(S_G, A_H, 0) < 0$ and $h(S_B, A_H, 0) < 0$, then the following conditions hold.

1) *Case 4(a):* If $\rho < 0$, $\pi_R^* = \Pi_{HH}$ for $R \in [0, R_B)$, $\pi_R^* = \Pi_{HL}$ for $R \in [R_B, R_G)$, and $\pi_R^* = \Pi_{LL}$ for $R \in [R_G, 1]$, where

$$R_G = 1 - \frac{(1-\delta+\delta p(S_B, A_L, S_G)+\delta p(S_G, A_L, S_B))(C_H - C_L)}{\delta(p(S_G, A_L, S_B) - p(S_G, A_H, S_B))(X_B - X_G)},$$
$$R_B = 1 - \frac{(1-\delta+\delta p(S_G, A_H, S_B)+\delta p(S_B, A_H, S_G))(C_H - C_L)}{\delta(p(S_B, A_H, S_G) - p(S_B, A_L, S_G))(X_B - X_G)}.$$

2) *Case 4(b):* If $\rho > 0$, $\pi_R^* = \Pi_{HH}$ for $R \in [0, R_G)$, $\pi_R^* = \Pi_{LH}$ for $R \in [R_G, R_B)$, and $\pi_R^* = \Pi_{LL}$ for $R \in [R_B, 1]$, where

$$R_G = 1 - \frac{(1-\delta+\delta p(S_B, A_H, S_G)+\delta p(S_G, A_H, S_B))(C_H - C_L)}{\delta(p(S_G, A_L, S_B) - p(S_G, A_H, S_B))(X_B - X_G)},$$
$$R_B = 1 - \frac{(1-\delta+\delta p(S_G, A_L, S_B)+\delta p(S_B, A_L, S_G))(C_H - C_L)}{\delta(p(S_B, A_H, S_G) - p(S_B, A_L, S_G))(X_B - X_G)}.$$

3) Case 4(c): If $\rho = 0$, $\pi_R^* = \Pi_{HH}$ for $R \in [0, R_s)$ and $\pi_R^* = \Pi_{LL}$ for $R \in [R_s, 1]$, where

$$R_s = R_G = 1 - \frac{(1-\delta+\delta p(S_B, A_H, S_G)+\delta p(S_G, A_H, S_B))(C_H - C_L)}{\delta(p(S_G, A_L, S_B) - p(S_G, A_H, S_B))(X_B - X_G)}$$
$$= R_B = 1 - \frac{(1-\delta+\delta p(S_G, A_H, S_B)+\delta p(S_B, A_H, S_G))(C_H - C_L)}{\delta(p(S_B, A_H, S_G) - p(S_B, A_L, S_G))(X_B - X_G)}.$$

Proof: See Appendix C. □

We can see from Proposition 4 that the user tends to take weak protections with the increase of the coverage level in all cases, and this reckless behavior is often referred to as the risk compensation [23]. One critical impact of the risk compensation is the Peltzman effect as shown in the following theorem.

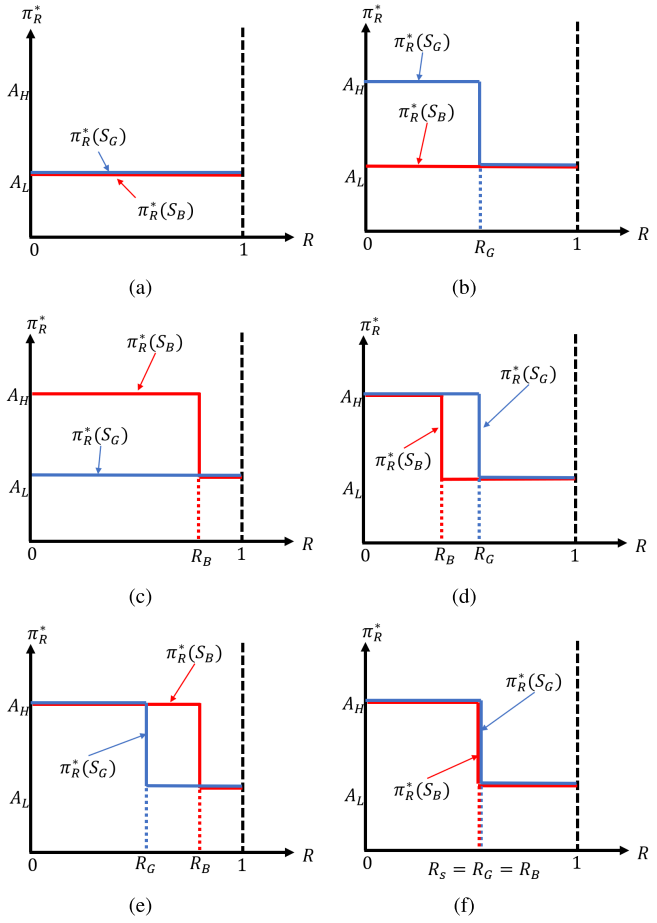

Fig. 3. All possible cases of the user's optimal protection policies with respect to the insurer's coverage level. A detailed discussion is provided in Proposition 4. (a) Case 1. (b) Case 2. (c) Case 3. (d) Case 4(a). (e) Case 4(b). (f) Case 4(c).

Theorem 2 (Peltzman Effect): The user faces higher cyber risks under cyber insurance. Such phenomena exists in the following cases.

1) $R \in [R_G, 1]$ in Cases 2 and 4(b).
2) $R \in [R_B, 1]$ in Cases 3 and 4(a).
3) $R \in [R_s, 1]$ in Case 4(c).

Proof: We only need to prove that the user has higher expected cumulative direct losses in these cases. Let $V_d(s, \pi)$ and $V_c(\pi)$ denote the expected cumulative direct losses and the expected cumulative costs given the initial state s and the protection policy π. We have that $V_d(s, \pi) + V_c(\pi) = V(s, \pi, 0)$. Recall that the optimal protection policy π_0^* without insurance has $V(s, \pi_0^*, 0) \leq V(s, \pi, 0)$ for $\pi \in \Omega$; thus, when the user has a different optimal protection policy $\pi_R^* \neq \pi_0^*$ given the coverage level R, we have $V(s, \pi_0^*, 0) \leq V(s, \pi_R^*, 0)$. As a result, we can achieve $V_d(s, \pi_0^*) + V_c(\pi_0^*) \leq V_d(s, \pi_R^*) + V_c(\pi_R^*)$. Note that $V_c(\pi_0^*) > V_c(\pi_R^*)$ in these cases as $V_c(\Pi_{HH}) > V_c(\Pi_{HL}) > V_c(\Pi_{LL})$ and $V_c(\Pi_{HH}) > V_c(\Pi_{LH}) > V_c(\Pi_{LL})$ from $C_H > C_L$. Thus, we have $V_d(s, \pi_0^*) < V_d(s, \pi_R^*)$ and the user faces higher cyber risks. □

B. Optimal Insurance Contract

Recall Section IV that, the insurer's problem (12) in this case can be written as follows:

$$\max_{R\in[0,1]} \ \tau(R) = V(S_G, \pi_0^*, 0) - V(S_G, \pi_R^*, 0)$$
$$\text{s.t. } \tau(R) \geq 0 \tag{23}$$

where $\tau(R)$ denotes the operating profit of the insurer if he provides a coverage level of R. Note that S_G in $\tau(R)$ indicates that the initial state of the user is the good state.

Proposition 5: The optimal insurance contract $\{K^*, R^*\}$ for each case in Proposition 4 can be summarized as follows.

1) *Case 1:* $R^* \in [0, 1]$ and $K^* = R^* k(S_G, A_L; A_L)$.
2) *Case 2:* $R^* \in [0, R_G]$ and $K^* = R^* k(S_G, A_H; A_L)$.
3) *Case 3:* $R^* \in [0, R_B]$ and $K^* = R^* k(S_G, A_L; A_H)$.
4) *Case 4(a):* $R^* \in [0, R_B]$ and $K^* = R^* k(S_G, A_H; A_H)$.
5) *Case 4(b):* $R^* \in [0, R_G]$ and $K^* = R^* k(S_G, A_H; A_H)$.
6) *Case 4(c):* $R^* \in [0, R_s]$ and $K^* = R^* k(S_G, A_H; A_H)$.

Here,

$$k(S_G, \alpha_G; \alpha_B) = \frac{(1-\delta p(S_B, \alpha_B, S_B))X_G + \delta p(S_G, \alpha_G, S_B)X_B}{I_p(\alpha_G, \alpha_B)}. \tag{24}$$

For all the cases, the operating profit under the optimal insurance contract is 0, i.e., $\tau(R^*) = 0$.

Proof: We can obtain the optimal insurance contract for all cases using the results from Proposition 1. In Case 1, any coverage level $R^* \in [0, 1]$ is optimal, and the associated premium $K^* = V(S_G, \Pi_{LL}, 0) - V(S_G, \Pi_{LL}, R) = \overline{V}(S_G, A_L; A_L, 0) - \overline{V}(S_G, A_L; A_L, R) = R^* k(S_G, A_L; A_L)$, where $k(S_G, A_L; A_L)$ comes from (27) in Appendix A. Similarly, we can obtain the optimal insurance contracts in Cases 2–4. □

We can see from the optimal insurance contracts that the premium is linear on the coverage level, which can be summarized as the linear insurance contract principle. Moreover, all the optimal insurance contracts lead to a zero-operating profit for the insurer, which indicates a zero-operating profit principle. The optimal insurance contracts usually provide limited coverage levels. When the coverage level is high, the user tends to act recklessly, which induces high risks and high direct losses of the user as shown in Theorem 2, and the insurer is required to cover the extra losses caused by that, which induces a negative profit of him. As a result, the insurer chooses not to provide the insurance to the user in that case.

VI. Numerical Examples

In this section, we first present numerical experiments on a two-state two-action user and a linear coverage insurer to verify our previous analytical results. We then present numerical experiments on a four-state three-action user with a linear coverage insurer and a threshold coverage insurer.

A. Two-State Two-Action User and Linear Coverage Insurer

In this section, we aim to verify our analysis on the two-state two-action user and the linear coverage insurer with numerical experiments. We assume that the user has $\delta = 0.9$, $X_G = 0$, $X_B = 10$, $C_L = 0$, $C_H = 1$, $p(S_G, A_L, S_B) = p(S_G, A_L, S_G) = 0.5$, $p(S_B, A_L, S_G) = p(S_B, A_L, S_B) = 0.5$, $p(S_G, A_H, S_B) = 1 - p(S_G, A_H, S_G) = 0.2$, and $p(S_B, A_H, S_G) = 1 - p(S_B, A_H, S_B) = 0.6$. We can achieve that $\rho = -0.20$, $h(S_G, A_H, 0) = -1.88$, $h(S_G, A_L, 0) = -1.70$, $h(S_B, A_H, 0) = -0.08$, and $h(S_B, A_L, 0) = 0.10$. Thus, the user's optimal protection policies can be described as Case 4(a) in Proposition 4. The optimal insurance contract $\{K^*, R^*\}$ has $R^* \in [0, R_B]$ and $K^* = R^* k(S_G, A_H; A_H)$, where $R_B = 0.0889$ and $k(S_G, A_H; A_H) = 21.9512$ from Proposition 5.

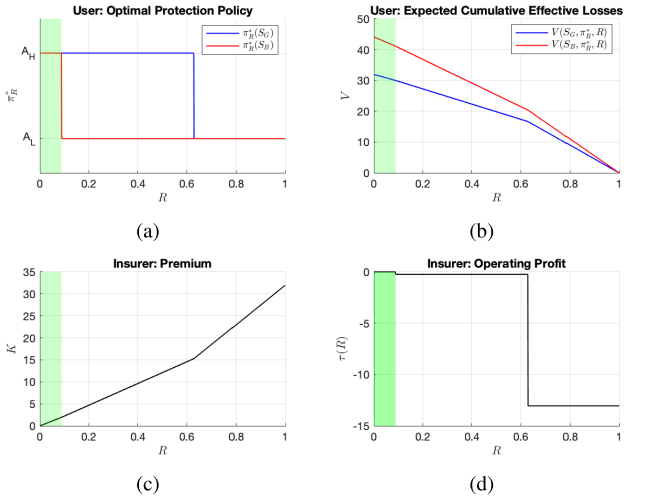

Fig. 4. Two-state two-action user and threshold coverage insurer. The green area denotes the region of optimal insurance contracts.

With the dynamic programming approach or linear programming approach in Section III, we can compute the optimal protection policies and the expected cumulative effective losses of the user, as shown in Fig. 4(a) and (b). We can further calculate the premium and the operating profit of the insurer, as shown in Fig. 4(c) and (d). We can see that the numerical results coincide with our analytical results.

B. Four-State Three-Action User and Linear Coverage Insurer

In this section, we consider a more complicated example where the user has four states and three actions, and the insurer provides linear coverage. We show that our model can be used to analyze the interactions between the user and the insurer in a numerical way.

We assume that the user's states can be identified as S_G, $S_{B,1}$, $S_{B,2}$, and $S_{B,3}$ with the state losses $X_G = 0$, $X_{B,1} = 4$, $X_{B,2} = 8$, and $X_{B,3} = 16$, respectively. S_G indicates the good state, while $S_{B,i}$ indicates the bad states with i capturing the level of the damage. The user can take no protection A_0, weak protection A_L, or strong protection A_H, and the costs of them can be identified as $c(A_0) = 0$, $c(A_L) = 0.3$, and $c(A_H) = 0.6$, respectively. Different actions have different impacts on the transition probabilities. For convenience, we summarize the transition probabilities in (25), shown at the bottom of the next page.

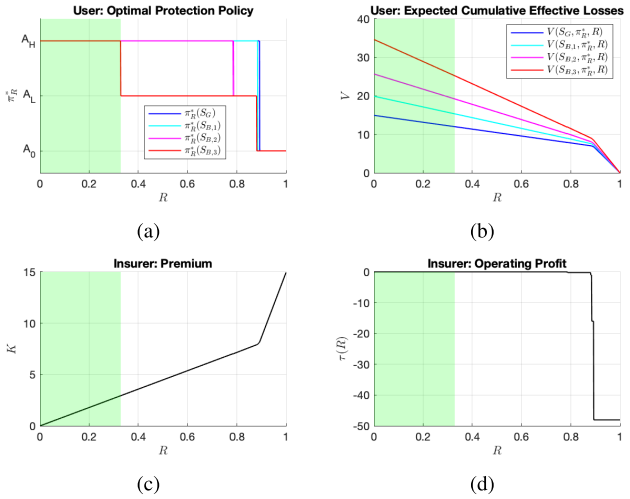

Fig. 5. Four-state three-action user and linear coverage insurer. The green area denotes the region of optimal insurance contracts.

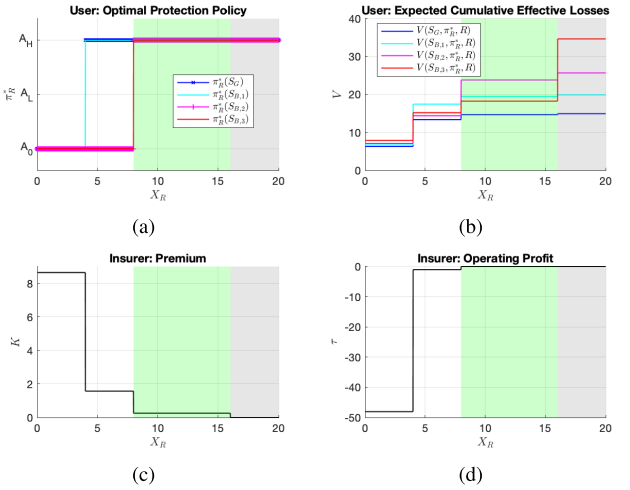

Fig. 6. Four-state three-action user and threshold coverage insurer. The green area denotes the region of optimal insurance contracts.

The user has a larger probability of going to the good state and a smaller probability of going to the bad state with better protections. We then take the following transition probabilities in this example:

$$P_{A_0} = \begin{bmatrix} 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0.25 & 0.25 & 0.25 \end{bmatrix},$$

$$P_{A_L} = \begin{bmatrix} 0.4 & 0.3 & 0.2 & 0.1 \\ 0.4 & 0.3 & 0.2 & 0.1 \\ 0.4 & 0.3 & 0.2 & 0.1 \\ 0.4 & 0.3 & 0.2 & 0.1 \end{bmatrix},$$

$$P_{A_H} = \begin{bmatrix} 0.8 & 0.2 & 0.0 & 0.0 \\ 0.7 & 0.2 & 0.1 & 0.0 \\ 0.6 & 0.2 & 0.1 & 0.1 \\ 0.5 & 0.2 & 0.2 & 0.1 \end{bmatrix}.$$

Let $\delta = 0.9$, and the optimal protection policies and the expected cumulative effective losses of the user are shown in Fig. 5(a) and (b). We can see from Fig. 5(a) and (b) that the user decreases his protections with the increase of the coverage level, and the user also has lower expected cumulative effective losses with higher coverage levels. The premium and the operating profit of the insurer are shown in Fig. 5(c) and (d). We can see that with the increase of the coverage level, the premium is linearly increasing. Moreover, the maximum operating profit that can be achieved by the insurer is 0. We can also observe that the optimal insurance contract tends to provide limited coverage levels, and higher coverage levels can lead to negative operating profits of the insurer. Thus, the risk compensation, the zero-operating profit principle, and the linear insurance contract principle still hold in this example.

C. Four-State Three-Action User and Threshold Coverage Insurer

In this section, we consider a threshold coverage insurance and show its impact on the four-state three-action user and the insurer.

We use the same settings for the user as in Section VI-B. The threshold insurance contract has two coverage levels $R_0 = 0$ and $R_1 = 0.9$, which are distinguished by a threshold $X_R \in [0, 20]$. When the loss of the user $x \leq X_R$, the insurer provides no coverage $R_0 x$; otherwise, the insurer provides a coverage $R_1 x$. A lower X_R indicates that the insurance has a higher coverage for smaller losses. The objective of the insurer is to maximize his operating profit by finding the optimal threshold X_R^* and the associated premium K^*.

The optimal protection policies and the expected cumulative effective losses of the user are shown in Fig. 6(a) and (b), and we can see from them that the user decreases his protections with the decrease of the threshold X_R, which indicates that the user tends to act recklessly knowing that the insurer provides a high coverage even he has a small loss from cyber risks. Moreover, we can see that the premium is a staircase function on the threshold X_R, and it decreases with the increase of X_R, which shows that the insurer charges a higher premium to provide a higher coverage level. The maximum operating profit that can be achieved by the insurer is 0. As a result, this example shows the similar risk compensation and zero-operating profit principle as in the previous examples. Note that the gray area has $X_R > X_{B,3}$, i.e., the insurer provides no coverage for the user at any states, which is equivalent to the case when there is no insurance.

$$P_a = \begin{bmatrix} p(S_G, a, S_G) & p(S_G, a, S_{B,1}) & p(S_G, a, S_{B,2}) & p(S_G, a, S_{B,3}) \\ p(S_{B,1}, a, S_G) & p(S_{B,1}, a, S_{B,1}) & p(S_{B,1}, a, S_{B,2}) & p(S_{B,1}, a, S_{B,3}) \\ p(S_{B,2}, a, S_G) & p(S_{B,2}, a, S_{B,1}) & p(S_{B,2}, a, S_{B,2}) & p(S_{B,2}, a, S_{B,3}) \\ p(S_{B,3}, a, S_G) & p(S_{B,3}, a, S_{B,1}) & p(S_{B,3}, a, S_{B,2}) & p(S_{B,3}, a, S_{B,3}) \end{bmatrix} \quad (25)$$

VII. Conclusion

In this article, we have presented a dynamic moral-hazard type of principal–agent model to study cyber insurance and its impacts on cybersecurity. The dynamics and correlations of the cyber risks have been modeled by MDPs where the user aims to find the optimal protection policy to mitigate the impacts of cyberattacks. We have studied and fully analyzed a case where the user has two states and two actions, and the insurer provides linear coverage insurance. We have further demonstrated the Peltzman effect that the user has higher cyber risks under insurance due to risk compensation, i.e., the user tends to act more recklessly knowing he is protected. We have presented the linear insurance contract principle and the zero-operating profit principle of the optimal cyber-insurance contract. Numerical experiments have been used to corroborate our results and further demonstrate the case study with a four-state three-action user and his interactions with linear coverage insurance and threshold coverage insurance. The risk compensation and the zero-operating profit principle have been shown to hold in these cases. One direction of future research is the investigation of cyber-insurance contracts over complex networks, such as scale-free and small-world networks with dynamic cyber risks.

Appendix A
Proof of Proposition 2

To simplify the notation in this proof, we define the discounted transition probabilities as

$$\widehat{p}(s,\alpha_s,s) = 1-\delta p(s,\alpha_s,s)$$
$$\widehat{p}(s,\alpha_s,s^c) = \delta p(s,\alpha_s,s^c).$$

Remark 3: The following facts hold for $\widehat{p}$.

1) $\widehat{p}(S_G,\alpha_G,S_G) - \widehat{p}(S_G,\alpha_G,S_B) = \widehat{p}(S_B,\alpha_B,S_B) - \widehat{p}(S_B,\alpha_B,S_G) = 1-\delta$.
2) If $\delta = 1$, we have $\widehat{p}(S_G,\alpha_G,S_G) = \widehat{p}(S_G,\alpha_G,S_B)$ and $\widehat{p}(S_B,\alpha_B,S_B) = \widehat{p}(S_B,\alpha_B,S_G)$.

Thus, (21) can be written as

$$I_p(\alpha_G,\alpha_B) = \widehat{p}(S_G,\alpha_G,S_G)\widehat{p}(S_B,\alpha_B,S_B) - \widehat{p}(S_G,\alpha_G,S_B)\widehat{p}(S_B,\alpha_B,S_G).$$

Remark 4: The following facts hold for I_p.

1) $I_p(\alpha_G,\alpha_B) = (1-\delta+\widehat{p}(S_G,\alpha_G,S_B))(1-\delta+\widehat{p}(S_B,\alpha_B,S_G)) - \widehat{p}(S_G,\alpha_G,S_B)\widehat{p}(S_B,\alpha_B,S_G) = (1-\delta)^2 + (1-\delta)(\widehat{p}(S_G,\alpha_G,S_B)+\widehat{p}(S_B,\alpha_B,S_G)) > 0$ when $0 \le \delta < 1$.
2) $I_p(A_H,\alpha_B) - I_p(A_L,\alpha_B) = (1-\delta)(\widehat{p}(S_G,A_H,S_B) - \widehat{p}(S_G,A_L,S_B))$.
3) $I_p(\alpha_G,A_H) - I_p(\alpha_G,A_L) = (1-\delta)(\widehat{p}(S_B,A_H,S_G) - \widehat{p}(S_B,A_L,S_G))$.

The action-dependent expected cumulative effective losses (19) and (20) can be rewritten as follows:

$$\overline{V}(s,\alpha_s;\alpha_{s^c},R) = (1-R)k(s,\alpha_s;\alpha_{s^c}) + b(s,\alpha_s;\alpha_{s^c}) \quad (26)$$

where

$$k(s,\alpha_s;\alpha_{s^c}) = \frac{\widehat{p}(S_B,\alpha_B,s^c)X_G + \widehat{p}(S_G,\alpha_G,s^c)X_B}{I_p(\alpha_G,\alpha_B)} \quad (27)$$

$$b(s,\alpha_G;\alpha_{s^c}) = \frac{\widehat{p}(S_B,\alpha_B,s^c)c(\alpha_G) + \widehat{p}(S_G,\alpha_G,s^c)c(\alpha_B)}{I_p(\alpha_G,\alpha_B)}. \quad (28)$$

Note that

$$\begin{aligned}
&k(S_G,A_H;\alpha_B) - k(S_G,A_L;\alpha_B)\\
&= \frac{\widehat{p}(S_B,\alpha_B,S_B)X_G + \widehat{p}(S_G,A_H,S_B)X_B}{I_p(A_H,\alpha_B)} - \frac{\widehat{p}(S_B,\alpha_B,S_B)X_G + \widehat{p}(S_G,A_L,S_B)X_B}{I_p(A_L,\alpha_B)}\\
&= \frac{\widehat{p}(S_B,\alpha_B,S_B)I_p(A_L,\alpha_B)X_G + \widehat{p}(S_G,A_H,S_B)I_p(A_L,\alpha_B)X_B}{I_p(A_H,\alpha_B)I_p(A_L,\alpha_B)} - \frac{\widehat{p}(S_B,\alpha_B,S_B)I_p(A_H,\alpha_B)X_G + \widehat{p}(S_G,A_L,S_B)I_p(A_H,\alpha_B)X_B}{I_p(A_H,\alpha_B)I_p(A_L,\alpha_B)}\\
&= \frac{\widehat{p}(S_B,\alpha_B,S_B)(I_p(A_L,\alpha_B) - I_p(A_H,\alpha_B))X_G}{I_p(A_H,\alpha_B)I_p(A_L,\alpha_B)} + \frac{\widehat{p}(S_G,A_H,S_B)I_p(A_L,\alpha_B)X_B - \widehat{p}(S_G,A_L,S_B)I_p(A_H,\alpha_B)X_B}{I_p(A_H,\alpha_B)I_p(A_L,\alpha_B)}\\
&= \frac{(1-\delta)\widehat{p}(S_B,\alpha_B,S_B)(\widehat{p}(S_G,A_L,S_B) - \widehat{p}(S_G,A_H,S_B))X_G}{I_p(A_H,\alpha_B)I_p(A_L,\alpha_B)} + \frac{(1-\delta)\widehat{p}(S_B,\alpha_B,S_B)(\widehat{p}(S_G,A_H,S_B) - \widehat{p}(S_G,A_L,S_B))X_B}{I_p(A_H,\alpha_B)I_p(A_L,\alpha_B)}\\
&= \frac{(1-\delta)\widehat{p}(S_B,\alpha_B,S_B)(\widehat{p}(S_G,A_L,S_B) - \widehat{p}(S_G,A_H,S_B))(X_G - X_B)}{I_p(A_H,\alpha_B)I_p(A_L,\alpha_B)}
\end{aligned} \quad (29)$$

where the fourth equality is achieved by plugging Remark 41) and 2). Similarly, we can achieve that

$$\begin{aligned}
&k(S_B,A_H;\alpha_G) - k(S_B,A_L;\alpha_G)\\
&= \frac{(1-\delta)\widehat{p}(S_G,\alpha_G,S_G)(\widehat{p}(S_B,A_H,S_G) - \widehat{p}(S_B,A_L,S_G))(X_G - X_B)}{I_p(\alpha_G,A_H)I_p(\alpha_G,A_L)}
\end{aligned} \quad (30)$$

$$\begin{aligned}
&b(S_G,A_H;\alpha_B) - b(S_G,A_L;\alpha_B)\\
&= \frac{(1-\delta)\widehat{p}(S_B,\alpha_B,S_B)(\widehat{p}(S_B,\alpha_B,S_B) + \widehat{p}(S_G,\alpha_B,S_B))(C_H - C_L)}{I_p(A_H,\alpha_B)I_p(A_L,\alpha_B)}
\end{aligned} \quad (31)$$

$$\begin{aligned}
&b(S_B,A_H;\alpha_G) - b(S_B,A_L;\alpha_G)\\
&= \frac{(1-\delta)\widehat{p}(S_G,\alpha_G,S_G)(\widehat{p}(S_G,\alpha_G,S_G) + \widehat{p}(S_B,\alpha_G,S_G))(C_H - C_L)}{I_p(\alpha_G,A_H)I_p(\alpha_G,A_L)}.
\end{aligned} \quad (32)$$

As a result, we have

$$\begin{aligned}
&\overline{V}(S_G,A_H;\alpha_B,R) - \overline{V}(S_G,A_L;\alpha_B,R)\\
&\quad = (1-R)(k(S_G,A_H;\alpha_B) - k(S_G,A_L;\alpha_B))\\
&\qquad + b(S_G,A_H;\alpha_B) - b(S_G,A_L;\alpha_B)\\
&\quad = \frac{(1-\delta)\widehat{p}(S_B,\alpha_B,S_B)}{I_p(A_H,\alpha_B)I_p(A_L,\alpha_B)}h(S_G,\alpha_B,R)
\end{aligned} \quad (33)$$

$$\begin{aligned}
&\overline{V}(S_B,A_H;\alpha_G,R) - \overline{V}(S_B,A_L;\alpha_G,R)\\
&\quad = \frac{(1-\delta)\widehat{p}(S_G,\alpha_G,S_G)}{I_p(\alpha_G,A_H)I_p(\alpha_G,A_L)}h(S_B,\alpha_G,R)
\end{aligned} \quad (34)$$

where $h(s,\alpha_{s^c},R)$ has been defined in Proposition 2. Since $1-\delta > 0$, $\widehat{p}(s,\alpha_s,s) > 0$, and $I_p(\alpha_s,\alpha_{s^c}) > 0$, we have that $\overline{V}(s,A_H;\alpha_{s^c},R) < \overline{V}(s,A_L;\alpha_{s^c},R)$ if $h(s,\alpha_{s^c},R) < 0$ and $\overline{V}(s,A_H;\alpha_{s^c},R) \ge \overline{V}(s,A_L;\alpha_{s^c},R)$ if $h(s,\alpha_{s^c},R) \ge 0$. Proposition 2 holds.

APPENDIX B
PROOF OF THEOREM 1

Recall the value of transition probabilities ρ from (22) in Proposition 4. Besides Proposition 3, we note that $h(s, \alpha_{s^c}, R)$ has the following extra facts:

$$\begin{aligned} &h(S_G, A_H, R) - h(S_G, A_L, R) \\ &= h(S_B, A_H, R) - h(S_B, A_L, R) = \rho\delta(C_H - C_L) \end{aligned} \tag{35}$$

$$\begin{aligned} &h(S_G, A_H, R) - h(S_B, A_H, R) \\ &= h(S_G, A_L, R) - h(S_B, A_L, R) = \rho\delta(1-R)(X_B - X_G) \end{aligned} \tag{36}$$

$$\begin{aligned} &h(S_G, A_H, R) - h(S_B, A_L, R) \\ &= \rho\delta((C_H - C_L) + (1-R)(X_B - X_G)) \end{aligned} \tag{37}$$

$$\begin{aligned} &h(S_B, A_H, R) - h(S_G, A_L, R) \\ &= \rho\delta((C_H - C_L) - (1-R)(X_B - X_G)). \end{aligned} \tag{38}$$

If $\pi_R^* = \Pi_{HL}$, we have $h(S_G, A_L, R) < 0$ and $h(S_B, A_H, R) \geq 0$ from Proposition 2. Thus, $\pi_R^* \neq \Pi_{LL}$ and $\pi_R^* \neq \Pi_{HH}$. Similarly, if $\pi_R^* = \Pi_{LH}$, we have $\pi_R^* \neq \Pi_{LL}$ and $\pi_R^* \neq \Pi_{HH}$; if $\pi_R^* = \Pi_{LL}$, we have $\pi_R^* \neq \Pi_{LH}$ and $\pi_R^* \neq \Pi_{HL}$; if $\pi_R^* = \Pi_{HH}$, we have $\pi_R^* \neq \Pi_{LH}$ and $\pi_R^* \neq \Pi_{HL}$. Thus, to prove the uniqueness of π_R^*, we only need to prove that $\pi_R^* = \Pi_{LH}$ and $\pi_R^* = \Pi_{HL}$ cannot exist at the same time and $\pi_R^* = \Pi_{LL}$ and $\pi_R^* = \Pi_{HH}$ cannot exist at the same time.

If $\pi_R^* = \Pi_{LH}$ and $\pi_R^* = \Pi_{HL}$ at the same time, we have $h(S_G, A_H, R) \geq 0$, $h(S_B, A_L, R) < 0$, $h(S_G, A_L, R) < 0$, and $h(S_B, A_H, R) \geq 0$ from Proposition 2, which indicates that $\rho > 0$ from (37) as $h(S_G, A_H, R) > h(S_B, A_L, R)$ and $\rho\delta((C_H - C_L) - (1-R)(X_B - X_G)) > 0$ from (38) as $h(S_G, A_L, R) < h(S_B, A_H, R)$. Thus, we can achieve that $(C_H - C_L) > (1-R)(X_B - X_G)$. However,

$$\begin{aligned} &h(S_G, A_L, R) \\ &= (1-R)\delta(p(S_G, A_H, S_B) - p(S_G, A_L, S_B))(X_B - X_G) \\ &\quad + (1 - \delta + \delta p(S_B, A_L, S_G) + \delta p(S_G, A_L, S_B))(C_H - C_L) \\ &> (1-R)\delta(p(S_G, A_H, S_B) - p(S_G, A_L, S_B))(X_B - X_G) \\ &\quad + (1 - \delta + \delta p(S_B, A_L, S_G) \\ &\qquad + \delta p(S_G, A_L, S_B))(1-R)(X_B - X_G) \\ &= (1-R)(X_B - X_G)(1 - \delta + \delta p(S_G, A_H, S_B) \\ &\qquad\qquad + \delta p(S_B, A_L, S_G)) \\ &> 0 \end{aligned} \tag{39}$$

which violates $h(S_G, A_L, R) < 0$. As a result, $\pi_R^* = \Pi_{LH}$ and $\pi_R^* = \Pi_{HL}$ cannot exist at the same time.

If $\pi_R^* = \Pi_{LL}$ and $\pi_R^* = \Pi_{HH}$ at the same time, we have $h(S_G, A_L, R) \geq 0$, $h(S_B, A_L, R) \geq 0$, $h(S_G, A_H, R) < 0$, and $h(S_B, A_H, R) < 0$, which indicates that $\rho < 0$ from (35) and $\rho\delta((C_H - C_L) - (1-R)(X_B - X_G)) < 0$ from (38). Thus, we can achieve that $(C_H - C_L) - (1-R)(X_B - X_G) > 0$. However,

$$\begin{aligned} &h(S_B, A_H, R) \\ &= (1-R)\delta(p(S_B, A_H, S_G) - p(S_B, A_L, S_G))(X_G - X_B) \\ &\quad + (1 - \delta + \delta p(S_B, A_H, S_G) + \delta p(S_G, A_H, S_B))(C_H - C_L) \\ &> (1-R)\delta(p(S_B, A_H, S_G) - p(S_B, A_L, S_G))(X_G - X_B) \\ &\quad + (1 - \delta + \delta p(S_B, A_H, S_G) \\ &\qquad + \delta p(S_G, A_H, S_B))(1-R)(X_B - X_G) \\ &= (1-R)(X_B - X_G)(1 - \delta + \delta p(S_G, A_H, S_B) \\ &\qquad\qquad + \delta p(S_B, A_L, S_G)) \\ &> 0 \end{aligned}$$

which violates $h(S_B, A_H, R) < 0$. As a result, $\pi_R^* = \Pi_{LL}$ and $\pi_R^* = \Pi_{HH}$ cannot exist at the same time. Thus, Theorem 1 holds.

APPENDIX C
PROOF OF PROPOSITION 4

There are only four possible protection policies Π_{LL}, Π_{HL}, Π_{LH}, and Π_{HH}. Thus, the optimal protection policy π_0^* without insurance has only four cases: Cases 1–4 as presented in Proposition 4, which are determined by $h(s, \alpha_{s^c}, 0)$ in Proposition 2. As a result, we only need to prove the trends of π_R^* with respect to R in different cases.

We first note that when $R = 1$, we have $h(S_G, \alpha_B, 1) > 0$ and $h(S_B, \alpha_G, 1) > 0$, which indicates that $\pi_{R=1}^* = \Pi_{LL}$. Moreover, if the user has $\pi_{\widehat{R}}^* = \Pi_{LL}$ for a coverage level of $\widehat{R} \in [0, 1]$, we have $h(S_G, A_L, \widehat{R}) \geq 0$ and $h(S_B, A_L, \widehat{R}) \geq 0$ from Proposition 2. Since $h(s, \alpha_{s^c}, R)$ is linearly increasing on R as shown in Proposition 3, we have $h(S_G, A_L, R) \geq 0$ and $h(S_B, A_L, R) \geq 0$ for $R \geq \widehat{R}$, which indicates that $\pi_R^* = \Pi_{LL}$ for $R \geq \widehat{R}$. Thus, we can conclude that $\pi_R^* = \Pi_{LL}$ when R is sufficiently large and the user chooses not to change his policy with the increase of R once he achieves $\pi_R^* = \Pi_{LL}$ for all cases.

To prove Cases 2–4, recall the value of transition probabilities ρ from (22). If $\rho < 0$, we have $h(S_G, A_H, R) < h(S_B, A_L, R)$ from (37). However, when $\pi_R^* = \Pi_{LH}$, we have $h(S_G, A_H, R) \geq 0$ and $h(S_B, A_L, R) < 0$ from Proposition 2, which violates $h(S_G, A_H, R) < h(S_B, A_L, R)$. Thus, we have $\pi_R^* \neq \Pi_{LH}$ if $\rho < 0$. As a result, Cases 2 and 4(a) have $\rho < 0$ and the user has $\pi_R^* \neq \Pi_{LH}$ in these cases. Since $h(S_B, A_H, 0) \geq 0$ when $\pi_0^* = \Pi_{HL}$ in Case 2 and $h(S_B, A_H, R)$ is linearly increasing on R, $h(S_B, A_H, R) \geq 0$ for $R \in [0, 1]$. Thus, the user has $\pi_R^* \neq \pi_{HH}$ in Case 2, and Case 2 holds. The threshold R_G is achieved by solving $h(S_G, A_L, R) = 0$. Case 4(a) holds from Case 2, and the thresholds R_G and R_B are achieved by solving $h(S_G, A_L, R) = 0$ and $h(S_B, A_H, R) = 0$, respectively.

If $\rho > 0$ and $\pi_R^* = \Pi_{HL}$, we have $h(S_G, A_L, R) < 0$ and $h(S_B, A_H, R) \geq 0$ from Proposition 2, and thus, $h(S_B, A_H, R) - h(S_G, A_L, R) = \rho\delta((C_H - C_L) - (1-R)(X_B - X_G)) > 0$ from (38), which indicates that $(C_H - C_L) - (1-R)(X_B - X_G) > 0$. However, we could obtain that $h(S_G, A_L, R) > 0$ following similar arguments as in (39), which violates $h(S_G, A_L, R) < 0$. Thus, we have $\pi_R^* \neq \Pi_{HL}$ if $\rho > 0$. As a result, Cases 3 and 4(b) have $\rho > 0$ and the user has $\pi_R^* \neq \Pi_{HL}$ in these cases. Since $h(S_G, A_H, R) \geq 0$ when $\pi_0^* = \Pi_{LH}$ in Case 3 and $h(S_G, A_H, R)$ is linearly increasing on R, $h(S_G, A_H, R) \geq 0$ for $R \in [0, 1]$. Thus, the user has $\pi_R^* \neq \pi_{HH}$ in Case 3, and Case 3 holds. The threshold R_B is achieved by

solving $h(S_B, A_L, R) = 0$. Case 4(b) holds from Case 3, and the thresholds R_B and R_G are achieved by solving $h(S_B, A_L, R) = 0$ and $h(S_G, A_H, R) = 0$, respectively.

If $\rho = 0$, we have $h(S_G, A_H, R) = h(S_G, A_L, R) = h(S_B, A_H, R) = h(S_B, A_L, R)$ from (35) to (38). However, Π_{LH} and Π_{HL} indicate that $h(S_G, A_H, R) \geq 0 > h(S_B, A_L, R)$ and $h(S_G, A_L, R) < 0 \leq h(S_B, A_H, R)$, respectively. Thus, we have $\pi_R^* \neq \Pi_{HH}$ and $\pi_R^* \neq \Pi_{LL}$ if $\rho = 0$. As a result, Case 4(c) has $\rho = 0$ and the user has $\pi_R^* \neq \Pi_{HL}$ and $\pi_R^* \neq \Pi_{LH}$. Thus, Case 4(c) holds, and the thresholds R_G and R_B are achieved by solving $h(S_G, A_H, R) = 0$ and $h(S_B, A_H, R) = 0$, respectively.

REFERENCES

[1] G. O'Gorman and G. McDonald, *Ransomware: A Growing Menace*. Tempe, AZ, USA: Symantec Corporation, 2012.

[2] S. Romanosky, D. Hoffman, and A. Acquisti, "Empirical analysis of data breach litigation," *J. Empirical Legal Stud.*, vol. 11, no. 1, pp. 74–104, Mar. 2014.

[3] L. Apiecionek, J. M. Czerniak, and H. Zarzycki, "Protection tool for distributed denial of services attack," in *Proc. Int. Conf., Beyond Databases, Archit. Struct.*, 2014, pp. 405–414.

[4] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, p. 25, 2013.

[5] Y. Zhang, C. Xu, S. Yu, H. Li, and X. Zhang, "SCLPV: Secure certificateless public verification for cloud-based cyber-physical-social systems against malicious auditors," *IEEE Trans. Comput. Social Syst.*, vol. 2, no. 4, pp. 159–170, Dec. 2015.

[6] S. Li, S. Zhao, Y. Yuan, Q. Sun, and K. Zhang, "Dynamic security risk evaluation via hybrid Bayesian risk graph in cyber-physical social systems," *IEEE Trans. Comput. Social Syst.*, vol. 5, no. 4, pp. 1133–1141, Dec. 2018.

[7] L. Kelion, "Cryptolocker ransomware has 'infected about 250,000 PCs,"' *BBC News Technol.*, 2013. Accessed: 2016. [Online]. Available: http://www.bbc.com/news/technology-25506020

[8] S. Hilton, "Dyn analysis summary of Friday October 21 attack," *Dyn. Blog. Dyn. News*, 2016. [Online]. Available: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[9] W. R. Cheswick, S. M. Bellovin, and A. D. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker*. Reading, MA, USA: Addison-Wesley, 2003.

[10] C. H. Rowland, "Intrusion detection system," U.S. Patent 6 405 318, Jun. 11, 2002.

[11] S. Jajodia, A. K. Ghosh, V. Subrahmanian, V. Swarup, C. Wang, and X. S. Wang, *Moving Target Defense II: Application of Game Theory and Adversarial Modeling*, vol. 100. New York, NY, USA: Springer, 2012.

[12] V. Kumar, J. Srivastava, and A. Lazarevic, *Managing Cyber Threats: Issues, Approaches, and Challenges*, vol. 5. New York, NY, USA: Springer, 2006.

[13] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[14] A. Beelitz and D. M. Merkl-Davies, "Using discourse to restore organisational legitimacy: 'CEO-speak' after an incident in a German nuclear power plant," *J. Bus. Ethics*, vol. 108, no. 1, pp. 101–120, 2012.

[15] 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, pp. 1–46.

[16] R. Böhme and G. Schwartz, "Modeling cyber-insurance: Towards a unifying framework," in *Proc. WEIS*, 2010, pp. 1–36.

[17] N. Shetty, G. Schwartz, M. Felegyhazi, and J. Walrand, "Competitive cyber-insurance and internet security," *Econ. Inf. Secur. Privacy*, pp. 229–247, 2010.

[18] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will cyber-insurance improve network security? A market analysis," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2014, pp. 235–243.

[19] R. Zhang, Q. Zhu, and Y. Hayel, "A bi-level game approach to attack-aware cyber insurance of computer networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 3, pp. 779–794, Mar. 2017.

[20] M. Rothschild and J. Stiglitz, "Equilibrium in competitive insurance markets: An essay on the economics of imperfect information," in *Uncertainty in Economics*. Amsterdam, The Netherlands: Elsevier, 1978, pp. 257–280.

[21] B. Holmstrom, "Moral hazard and observability," *Bell J. Econ.*, vol. 10, no. 1, pp. 74–91, 1979.

[22] B. Holmstrom, "Moral hazard in teams," *Bell J. Econ.*, pp. 324–340, 1982.

[23] F. Ewold, "Insurance and risk," in *The Foucault Effect: Studies in Governmentality*. Chicago, IL, USA: Univ. Chicago Press, 1991, pp. 197–210.

[24] S. Xu, "Cybersecurity dynamics," in *Proc. Symp. Bootcamp Sci. Secur. (HotSoS)*, 2014, p. 14.

[25] D. Fava, J. Holsopple, S. J. Yang, and B. Argauer, "Terrain and behavior modeling for projecting multistage cyber attacks," in *Proc. 10th Int. Conf. Inf. Fusion*, Jul. 2007, pp. 1–7.

[26] S. Cheung, U. Lindqvist, and M. W. Fong, "Modeling multistep cyber attacks for scenario recognition," in *Proc. DARPA Inf. Survivability Conf. Expo.*, vol. 1, 2003, pp. 284–292.

[27] R. Böhme and G. Kataria, "Models and measures for correlation in cyber-insurance," in *Proc. WEIS*, 2006, pp. 1–26.

[28] P. Tague and R. Poovendran, "Modeling node capture attacks in wireless sensor networks," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 1221–1224.

[29] P. Tague, M. Li, and R. Poovendran, "Mitigation of control channel jamming under node capture attacks," *IEEE Trans. Mobile Comput.*, vol. 8, no. 9, pp. 1221–1234, Sep. 2009.

[30] A. K. Jones and R. S. Sielken, "Computer system intrusion detection: A survey," Comput. Sci. Tech. Rep., 2000, pp. 1–25.

[31] S. Romanosky, R. Telang, and A. Acquisti, "Do data breach disclosure laws reduce identity theft?" *J. Policy Anal. Manage.*, vol. 30, no. 2, pp. 256–286, 2011.

[32] A. Gazet, "Comparative analysis of various ransomware virii," *J. Comput. Virol.*, vol. 6, no. 1, pp. 77–90, Feb. 2008.

[33] M. L. Puterman, *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. Hoboken, NJ, USA: Wiley, 2014.

[34] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci. (HICSS)*, 2010, pp. 1–10.

[35] S. J. Grossman and O. D. Hart, "An analysis of the principal-agent problem," in *Foundations of Insurance Economics*. Dordrecht, The Netherlands: Springer, 1992, pp. 302–340.

[36] J.-J. Laffont and D. Martimort, *The Theory of Incentives: The Principal-Agent Model*. Princeton, NJ, USA: Princeton Univ. Press, 2009.

[37] R. Böhme, "Cyber-insurance revisited," in *Proc. WEIS*, 2005, pp. 1–22.

[38] J. Grossklags, N. Christin, and J. Chuang, "Secure or insure: A game-theoretic analysis of information security games," in *Proc. 17th Int. Conf. World Wide Web (WWW)*, 2008, pp. 209–218.

[39] D. K. Tosh, S. Shetty, S. Sengupta, J. P. Kesan, and C. A. Kamhoua, "Risk management using cyber-threat information sharing and cyber-insurance," in *Proc. Int. Conf. Game Theory Netw.* Cham, Switzerland: Springer, 2017, pp. 154–164.

[40] J. P. Kesan and C. M. Hayes, "Strengthening cybersecurity with cyberinsurance markets and better risk assessment," *Minnesota Law Rev.*, vol. 102, p. 191, 2017.

[41] A. Laszka, E. Panaousis, and J. Grossklags, "Cyber-insurance as a signaling game: Self-reporting and external security audits," in *Proc. 9th Conf. Decis. Game Theory Secur. (GameSec)*. Cham, Switzerland: Springer, 2018, pp. 508–520.

[42] I. Ehrlich and G. S. Becker, "Market insurance, self-insurance, and self-protection," *J. Political Economy*, vol. 80, no. 4, pp. 623–648, Jul. 1972.

[43] W. Stallings, *Network and Internetwork Security: Principles and Practice*, vol. 1. Englewood Cliffs, NJ, USA: Prentice-Hall, 1995.

[44] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, Jun. 2004.

[45] Q. Zhu, C. Fung, R. Boutaba, and T. Basar, "GUIDEX: A game-theoretic incentive-based mechanism for intrusion detection networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 11, pp. 2220–2230, Dec. 2012.

[46] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic security risk management using Bayesian attack graphs," *IEEE Trans. Dependable Secur. Comput.*, vol. 9, no. 1, pp. 61–74, Jan. 2012.

[47] J. Kim, S. Radhakrishnan, and S. K. Dhall, "Measurement and analysis of worm propagation on internet network topology," in *Proc. 13th Int. Conf. Comput. Commun. Netw.*, 2004, pp. 495–500.

[48] S. Haberman and E. Pitacco, *Actuarial Models for Disability Insurance*. Boca Raton, FL, USA: CRC Press, 1999.
[49] C. Lambrinoudakis, S. Gritzalis, P. Hatzopoulos, A. N. Yannacopoulos, and S. Katsikas, "A formal model for pricing information systems insurance contracts," *Comput. Standards Interfaces*, vol. 27, no. 5, pp. 521–532, Jun. 2005.
[50] K. K. Aase, "A Markov model for the pricing of catastrophe insurance futures and spreads," *J. Risk Insurance*, pp. 25–49, 2001.
[51] Y. Wu, B. Wang, and K. J. R. Liu, "Optimal defense against jamming attacks in cognitive radio networks using the Markov decision process approach," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2010, pp. 1–5.
[52] D. Shen, G. Chen, E. Blasch, and G. Tadda, "Adaptive Markov game theoretic data fusion approach for cyber network defense," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2007, pp. 1–7.
[53] Y. Liu and S. Hu, "Cyberthreat analysis and detection for energy theft in social networking of smart homes," *IEEE Trans. Comput. Social Syst.*, vol. 2, no. 4, pp. 148–158, Dec. 2015.
[54] J. Filar and K. Vrieze, *Competitive Markov Decision Processes*. New York, NY, USA: Springer, 2012.

Rui Zhang received the B.S. degree in optical information science and technology from Wuhan University, Wuhan, China, in 2014, and the Ph.D. degree in electrical engineering from New York University, Brooklyn, NY, USA, in 2020.

His research interests include cybersecurity, adversarial machine learning, cyber insurance, and optimal transport.

Dr. Zhang was a recipient of the Runner Up Best Student Paper Award at the International Conference on Information Fusion in 2015.

Quanyan Zhu (Senior Member, IEEE) received the B.Eng. degree (Hons.) in electrical engineering from McGill University, Montreal, QC, Canada, in 2006, the M.A.Sc. degree from the University of Toronto, Toronto, ON, Canada, in 2008, and the Ph.D. degree from the University of Illinois at Urbana–Champaign (UIUC), Urbana, IL, USA, in 2013.

From 2013 to 2014, he was a Postdoctoral Research Associate at the Department of Electrical Engineering, Princeton University, Princeton, NJ, USA. He is currently an Associate Professor at the Department of Electrical and Computer Engineering, New York University, Brooklyn, NY, USA. His current research interests include resilient and secure interdependent critical infrastructures, the Internet of Things, cyber-physical systems, machine learning, and network optimization and control.

Dr. Zhu was a recipient of many awards, including the NSF CAREER Award, the NSERC Canada Graduate Scholarship (CGS), the Mavis Future Faculty Fellowships, and the NSERC Postdoctoral Fellowship (PDF). He was a recipient of best paper awards at the 5th International Conference on Resilient Control Systems and the 18th International Conference on Information Fusion. He spearheaded and chaired the INFOCOM Workshop on Communications and Control on Smart Energy Systems (CCSES), the Midwest Workshop on Control and Game Theory (WCGT), and the 7th Conference on Decision and Game Theory for Security (GameSec).