Security Adoption in Heterogeneous Networks: the Influence of Cyber-insurance Market

Zichao Yang John C.S. Lui
Computer Science & Engineering Department
The Chinese University of Hong Kong

Abstract—**Hosts (or nodes) in the Internet often face epidemic risks such as virus and worms attack. Despite the awareness of these risks and the importance of network/system security, investment in security protection is still scare, and hence epidemic risk is still prevalent. Deciding whether to invest in security protection is an *interdependent process*: security investment decision made by one node can affect the security risk of others, and therefore affect their decisions also. The first goal of this paper is to understand how "network externality" and "nodes heterogeneity" may affect security adoption. Nodes make decisions on security investment by evaluating the epidemic risk and the expected loss. We characterize it as a *Bayesian network game* in which nodes only have the local information, e.g., the number of neighbors, and minimum common information, e.g., degree distribution of the network. Our second goal is to study a new form of risk management, called *cyber-insurance*. We investigate how the presence of competitive insurance market can affect the security adoption and show that if the insurance provider can observe the protection level of nodes, the insurance market is a positive incentive for security adoption if the protection quality is not very high. We also find that cyber-insurance is more likely to be a good incentive for nodes with higher degree. Conversely, if the insurance provider cannot observe the protection level of nodes, we verify that partial insurance can be a non-negative incentive, improving node's utility though not being an incentive.**

I. Introduction

Network security is a major problem in communication networks. One of its most common manifestations is in form of virus, worms and bonnet spreading, which we call the *epidemic risk*. In these epidemic risks, hosts (or nodes) which are infected become the sources of new infections, and adversaries can use these compromised nodes to generate new attacks. Epidemic risk is highly damaging, e.g., the Code Red worm [22] has infected thousands of computers and induced huge financial loss. To counter this risk, there have been great efforts in both the research and industrial fronts to come up with techniques and tools (i.e., anti-virus software, intrusion detection systems, firewalls etc) to detect virus/worms. Despite the sophistication of these tools, security protection adoption is relatively low, making epidemic risk still prevalent.

Note that a node's decision of whether to adopt some security measures is not a simple individual and independent process, but rather, *depends* on the decisions of many other nodes in the network. Nodes which decide not to invest in security protection, also put other nodes at security risk. This *network externality effect* caused by the spreading of epidemic influences the degree of adoption of security measure. *Our first contribution in this paper is to model the network externality effect and node heterogeneity on security adoption by studying a network of interconnected nodes where the virus/worms can propagate.*

Modeling such decision and security problem requires the combination of epidemic theory and game theory. While extensive studies in traditional literatures have been dedicated to epidemic theory [4] [23], few works have addressed the problems of strategic behavior of security investment. In a realistic situation, nodes which make decision in security investment usually do not have complete information about the network topology or knowledge of other nodes. As a result, it is difficult for them to accurately evaluate the epidemic risk and other nodes' influence on itself. In this paper, we model the security investment as a *Bayesian network game* where nodes only have the local information of their degree and the minimum common information of network's degree distribution. In contrast to graphical game [24], in which complete topology is given and analysis is complicated, Bayesian network game has an elegant tradeoff in incorporating partial topology information while making the analysis tractable.

By using Bayesian network game, *we show how heterogeneous nodes, characterized by their degree, can estimate their epidemic risk and make decisions on security investment with incomplete information*. We show that nodes with higher degree are more likely to be infected by epidemic. The secure measure is less effective for node with higher degree in terms of the reduction in infection probability. Nodes with higher degrees are more sensitive to externality, i.e., they are more likely to be affected by other's decision. However, the final adoption fraction of nodes with different degrees also strongly depends on their relative loss from epidemic.

While protection measures may limit the spread of virus/worms, another way to manage the epidemic risk is to transfer the risk to a third-party, which is called *cyber-insurance* [14]: nodes pay certain premium to insurance companies in return for compensation in the virus outbreaks. The two main challenges in cyber-insurance are: *adverse selection* and *moral hazard* [12], [14]. The problem of adverse selection arises when the insurance provider cannot distinguish between high and low risk nodes. The combination of self-protection and insurance raises the problem of moral hazard, in which nodes covered by insurance may take fewer secure measures, or even falsify their loss. Moral hazard happens when the insurance provider cannot observe the protection level of nodes. In this paper, we address the moral hazard problem which is especially serious in cyber-insurance. In this paper, we investigate the effect of cyber-insurance on security adoption under competitive insurance market. *Our second contribution is to show the conditions under which cyber-insurance is an incentive, with and without moral hazard.* We find that cyber-insurance without moral hazard is an incentive for security adoption if the initial secure condition is bad and the quality of secure measure is not very high. Moreover, cyber-insurance is more likely to be an incentive for nodes with high degree. We verify that partial insurance coverage can be a non-negative incentive for secure adoption with moral hazard.

This is the outline of our paper. In Section II, we present the epidemic and security investment models. In Section III, we show how heterogeneous nodes can determine their infection probability and decide on proper security investment. In Section IV, we investigate the effect of insurance market, both with and without moral hazard, on security adoption. Validations and performance evaluations are presented in Section V. Section VI gives related work and Section VII concludes.

II. Mathematical Models

In here, we present the mathematical models on how nodes make decision on security investment. Our models include: (a) *epidemic model*: to characterize the spread of virus or malware in a network, (b) *investment model*: to characterize node's decision in security investment, and (c) *Bayesian network game*: given the epidemic and investment models, how nodes make decision under the incomplete information setting.

Epidemic Model: The interaction relation of N nodes is denoted by the undirected graph $G = (V, E)$ with the vertex set V, $|V| = N$ and the edge set E. For $i, j \in V$, if $(i, j) \in E$, then nodes i and j are neighbors and we use $i \sim j$ to denote this relationship. Let $S = \{\mathit{healthy}, \mathit{infected}\}$ represents the set of states each node can be in. If node i is infected (healthy), then $S_i = 1$ ($S_i = 0$). Each infected node can contaminate its neighbors independently with probability q. Note that this is similar to the *bond percolation process* [23] in which every edge is occupied with probability q. Each node has an *initial state* of being infected or not. This can represent whether the node has been attacked by the adversary. Let us denote it by s_i where $s_i = 1$ if node i is initially infected and $s_i = 0$ otherwise. Hence, at the steady state, a node is infected either because it is initially infected, or it contracts virus from its infected neighboring nodes. The final state of node i can be expressed in the following recursive equation:

$$1 - S_i = (1 - s_i) \prod_{\forall j: j \sim i} (1 - \theta_{ji} S_j) \qquad \forall i \in V, \qquad (1)$$

where θ_{ji} is a random variable indicating whether the edge (i, j) is occupied or not. According to previous discussion, θ_{ji} is a Bernoulli random variable with $\Pr(\theta_{ji} = 1) = q$. Now, given the network topology G and the probabilities of infection, every node can evaluate the probability that it will eventually be infected. Since an infected node will incur some financial loss, hence, a node needs to decide whether to invest in self-protection to reduce the potential financial loss. Let us present the model to help a node in making such a decision.

Investment Model: Node i has an initial wealth $w_i \in \mathbb{R}_+$. A node's utility $u_i(w)$ is a function of wealth $w \in \mathbb{R}_+$. We consider nodes are *risk averse*, i.e., the utility function is strictly increasing and concave in w, i.e., $u_i'(w) > 0$ and $u_i''(w) < 0$. Fig. 1 depicts a risk averse utility function. In this paper, we consider the *constant relative risk averse* utility function commonly used in the economic literature [5]:

$$u(w) = \frac{w^{1-\sigma}}{1-\sigma}, \quad 0 < \sigma < 1, \qquad (2)$$

where σ is a parameter for the degree of risk aversion. The condition $0 < \sigma < 1$ is added to ignore the case of $\sigma = 1$ and also for tractability of analysis later on. For node i, the utility function is given by the above utility function with parameter σ_i. If node i is infected, then it will incur a financial loss of $l_i \in \mathbb{R}_+$. For node i, the expected utility is as shown in Fig. 1. D is the initial utility point, E is the utility point after getting infected. C is the expected utility. To reduce the potential financial loss, a node can consider some self-protection measures or purchasing insurance. In the first part of this paper, we consider the case of self-protection. In the second part of this paper, we consider both cases and study the influence of insurance market on security protection.

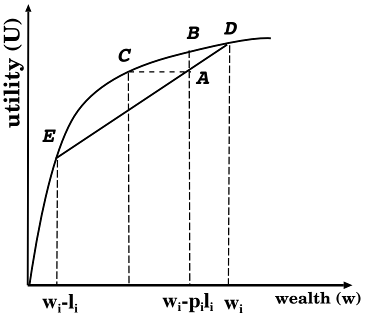


Fig. 1: Risk-averse utility function

A node's investment in self-protection can reduce the probability of being infected initially. For the amount of investment x, the probability of being infected initially is $p(x)$, which is a continuous differentiable decreasing function of x. In particular, we assumed the effort of security investment is separable with the wealth, which is a feature though restrictive, now standard in the literature [27]. If node i invests x_i in secure protection, the expected utility is

$$p_i u_i(w_i - l_i) + (1 - p_i) u_i(w_i) - x_i, \qquad (3)$$

where p_i is the *final* probability that node i will be infected. p_i contains two parts: the probability of being infected initially, given by $p(x_i)$ and the probability of getting infected from neighbor nodes. For simplicity of analysis, we assume that the choice of node i regarding security self-protection is a binary decision: either the node invests unit amount with a cost of c_i, or it does not invest at all. We use the action set $A = \{\mathcal{S}, \mathcal{N}\}$ to denote the behavior, where $\mathcal{S}$ denotes taking secure measure and $\mathcal{N}$ otherwise. If it decides to invest, the node can still be infected with probability p^-. Otherwise, it will be infected with probability p^+. Obviously we have $0 < p^- < p^+ < 1$. Let $a = (a_1, ..., a_i, ..., a_N)= (a_i, a_{-i})$ be an *action profile*. Given the action profile a_{-i} of other nodes, node i makes the decision by maximizing its expected utility. If node i takes action $\mathcal{N}$, the expected utility is:

$$p_i(\mathcal{N}, a_{-i})u_i(w_i - l_i) + (1 - p_i(\mathcal{N}, a_{-i}))u_i(w_i) \quad (4)$$

where $p_i(\mathcal{N}, a_{-i})$ is the final probability of node i being infected when it initially did not adopt security protection. On the other hand, the expected utility of a node which initially subscribed to security protection (or action $\mathcal{S}$) is:

$$p_i(\mathcal{S}, a_{-i})u_i(w_i - l_i) + (1 - p_i(\mathcal{S}, a_{-i}))u_i(w_i) - c_i \quad (5)$$

where $p_i(\mathcal{S}, a_{-i})$ is the final probability of a node being infected when it initially subscribed to some self-protection measures with cost of c_i. Note that $p_i(\mathcal{S}, a_{-i})$ and $p_i(\mathcal{N}, a_{-i})$ are functions of p^- and p^+, and the contagion probability q.

Each node needs to consider whether it should subscribe to some self-protection measures. The decision is based on the cost of investing in security measure, as well as the risk loss of being infected. The decision is non-trivial because one has to consider the *network externality effect*. In particular, node i will choose to invest in security protection if and only if

$$c_i < (p_i(\mathcal{N}, a_{-i}) - p_i(\mathcal{S}, a_{-i}))(u_i(w_i) - u_i(w_i - l_i)) \quad (6)$$

Note that the inequality is a function of a_{-i}, and this shows that a node's decision is based on the action of other nodes.

Bayesian Network Game: According to Inequality (6), each node needs to have the complete information of the network topology G so as to make the proper decision. However, it is almost impossible in practice for each node to have the complete information of G. Instead, each node can only have some *local information* on G, i.e., a node may only know its neighbors, and some cases, only knows the number of neighbors it is to interact with. Secondly, it is impossible to know the exact loss of other nodes in a large network.

In here, we assume that nodes only have the *minimum common information*, that is, the knowledge of the degree distribution of G, as well as the distribution of financial loss of nodes caused by virus. Assume that the degree distribution of the graph is $\{p_k\}_{\underline{K}}^{\overline{K}}$, where $\overline{K}$ is the maximum degree and $\underline{K}$ is the minimum degree. In this paper, we consider the *asymptotic case* that N, the number of nodes, tends to infinity and the degree distribution converges to the fixed probability distribution $\{p_k\}_{\underline{K}}^{\overline{K}}$. For nodes with degree k, the loss distribution is given by the CDF $F_k(l)$. We assume that the cost of secure measure is the same for all nodes which have the same degree and we denoted this as c_k. Furthermore, these nodes have the same utility function u_k and the same initial wealth w_k. Nodes make decision on security investment based on the information of degree and loss. According to the discussion in the investment model, a node should know the probability of getting infected before deciding on security investment. Since nodes do not have the complete information, they should estimate these probabilities based on the limited common information. Next, we derive this infected probability using the *local mean field technique* [1].

III. Analysis for Strategic Security Adoption

Let's show how nodes make decisions on security investment and how to determine the final security protection level.

A. General Case

Determining the final infection probability for a node is a difficult problem because of the complex network structure. In this work, we assume that a node only knows the degree distribution and consider the network topology as a *random graph* [23] with a given degree distribution $\{p_k\}_{\underline{K}}^{\overline{K}}$. Thus, nodes do not need to know the full network topology G to determine the final infection probability. Although real networks are not random graphs [23] and they have some characteristics, e.g., high clustering coefficient, community structure etc, that are not possed by random graph, recent study [20] has shown that random graph is very often accurate for real network. Thus, it is reasonable to assume that the network topology is random graph, especially here we consider incomplete information case.

Each node can compute its the final infection probability using the following methodology.

Estimating the Probability: A node can calculate its final infection probability by constructing a *local mean field tree* [1]. Fig. 2 illustrates the local mean field of node i which has degree k. For simplicity of illustration, let say that none of these nodes will take secure measure, i.e., the initial infection probability is p^+ for all nodes in this subsection. We will show how to relax this in later section.

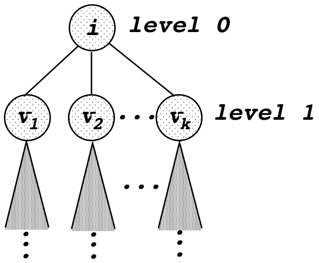


Fig. 2: Local mean field tree for node i with degree k

The children of node i in the local mean field tree are denoted as $v_c, c \in [1, k]$. The triangle under each child node v_c denotes another tree structure. Based on the results in [1], for any node i, the local topology of a large random graph G can be modeled as a tree rooted at node i with high probability. In other words, we transform G to a tree rooted at node i (or local mean field of node i). Node i can be independently influenced by each subtree rooted at v_c. For every subtree rooted at v_c, it consists of its subtrees. Using this *recursive* structure, we derive the total infection probability that other nodes in G can impose on node i.

First we divide nodes into levels. The root node i is at the zero level. The neighbors of node i is at the first level and so on. Let Y_j be the final state of node $j, j \neq i$, *conditioned on its parent in the tree structure is not infected*, and y_j be the initial state of node j. For the root node i, we use S_i to denote its final state and s_i to denote its initial state, then we have

$$1 - S_i = (1 - s_i) \prod_{\forall j: j \sim i} (1 - \theta_{ji} Y_j). \qquad (7)$$

The above equation indicates the root node i is either initially infected, or it can be infected by its neighbors. The state of its neighbors conditioned on that the root node i is not infected is also determined by the state of the children of the neighbors in the tree structure, or one can express it recursively as:

$$1 - Y_j = (1 - y_j) \prod_{\forall l: l \to j} (1 - \theta_{lj} Y_l) \quad j \neq i, \qquad (8)$$

where $l \to j$ denotes that l is a child of j in the tree structure. To solve Eq. (8), we need to know the degree distribution of a child node. This degree distribution can be expressed as:

$$\tilde{p}_k = \frac{k p_k}{\sum_{k=\underline{K}}^{\overline{K}} k p_k} = \frac{k p_k}{\bar{d}},$$

where $\bar{d}$ is the average degree of nodes in G. The number of edges of a child excluding the edge connecting to its parents is called the *excess degree* [23]. Let $\underline{K}' = \max\{0, \underline{K}-1\}$ and $\overline{K}' = \max\{0, \overline{K}-1\}$. The excess degree distribution of a child is

$$q_k = \tilde{p}_{k+1} = \frac{(k+1) p_{k+1}}{\bar{d}}, \quad k \in [\underline{K}', \overline{K}']. \qquad (9)$$

From [1], if nodes are at the same level of the tree structure, then their states are independent of each other. Let $\rho_n, n \geq 1$ be the probability that a node at the n^{th} level is infected conditioned on its parent is not infected. By Eq. (8), we have

$$1 - \rho_n = (1 - p^+) \sum_{k=\underline{K}'}^{\overline{K}'} q_k (1 - q\rho_{n+1})^k.$$

ρ_1 is the average probability that a child node of the root node i will be infected conditioned on the root node is not infected. When we scale up the network (or let $n \to \infty$), define $\rho \triangleq \lim_{n \to \infty} \rho_1$, then ρ is determined by the solution of the fixed point equation

$$1 - \rho = (1 - p^+) \sum_{k=\underline{K}'}^{\overline{K}'} q_k (1 - q\rho)^k.$$

By Eq. (7), for a node with degree k, the infection probability under the condition of incomplete information is

$$\phi_k = 1 - (1 - p^+)(1 - q\rho)^k. \qquad (10)$$

Security Adoption: In the previous subsection, we show how a node can compute the infection probability with incomplete information. The calculation is based on the assumption that none of the nodes take secure adoption, so that the initially infection probability is p^+. In here, we show how to use this infection probability for strategy selection. Let λ_k be the fraction of nodes with degree k which take action $\mathcal{S}$. Then by applying the method shown above, we have

Proposition *1: If λ_k fraction of the nodes with degree k take secure measure, ρ is given by the unique solution of the fixed point equation in $[0,1]$:*

$$\rho = 1 - \sum_{k=\underline{K}'}^{\overline{K}'} q_k (1 - p^+ + \lambda_{k+1}(p^+ - p^-))(1 - q\rho)^k. \qquad (11)$$

For a node with degree k, if it decides to take secure measure, then by Eq. (10), the infection probability is

$$\phi_k(\mathcal{S}, \lambda_{\underline{K}}, ..., \lambda_{\overline{K}}) = 1 - (1 - p^-)(1 - q\rho)^k. \qquad (12)$$

If it does not invest in protection measure, the probability for this node to get infected is

$$\phi_k(\mathcal{N}, \lambda_{\underline{K}}, ..., \lambda_{\overline{K}}) = 1 - (1 - p^+)(1 - q\rho)^k. \qquad (13)$$

The infection probability reduction for a node with degree k is

$$\phi_k(\mathcal{N}) - \phi_k(\mathcal{S}) = (p^+ - p^-)(1 - q\rho)^k. \qquad (14)$$

Note that this infection probability reduction decreases as degree increases. This implies that higher degree nodes have *less incentive* to invest in protection measure.

Corollary *1: ρ, given by the solution of fixed point Eq. (11), has a unique solution in $[0,1]$, and $\rho(\lambda_{\underline{K}}, ..., \lambda_{\overline{K}})$ is a decreasing function of λ_k, $\forall k \in [\underline{K}, \overline{K}]$.*

Proof: Let

$$g(\rho, \lambda_{\underline{K}}, ..., \lambda_{\overline{K}}) = 1 - \sum_{k=\underline{K}'}^{\overline{K}'} q_k (1 - p^+ + \lambda_{k+1}(p^+ - p^-))(1 - q\rho)^k.$$

Obviously, $g(\rho, \lambda_{\underline{K}}, ..., \lambda_{\overline{K}})$ is an increasing function of ρ.

$$g(0, \lambda_{\underline{K}}, ..., \lambda_{\overline{K}}) = 1 - \sum_{k=\underline{K}'}^{\overline{K}'} q_k (1 - p^+ + \lambda_{k+1}(p^+ - p^-)) > 0,$$

$$g(1, \lambda_{\underline{K}}, ..., \lambda_{\overline{K}}) = 1 - \sum_{k=\underline{K}'}^{\overline{K}'} q_k (1 - p^+ + \lambda_{k+1}(p^+ - p^-))(1 - q)^k < 1.$$

We can see that the fixed point equation $\rho = g(\rho)$ has at least one solution. Taking the second order derivative with respect to ρ, we have

$$g_{\rho\rho} = -\sum_{k=\underline{K}'}^{\overline{K}'} q_k (1 - p^+ + \lambda_{k+1}(p^+ - p^-)) k(k-1)(1 - q\rho)^{k-2} q^2 < 0,$$

$g(\rho)$ is a concave function. Let ρ^* be one of the solutions, i.e., $\rho^* = g(\rho^*)$. Then by concavity of $g(\rho)$, $g_\rho(\rho^*) < 1$. Otherwise, $g(\rho^*) = g(0) + \int_0^{\rho^*} g_\rho(\rho) d\rho > \rho^*$. Then for $0 < \rho < \rho^*$, $g(\rho) > \rho$, for $\rho^* < \rho < 1$, $g(\rho) < \rho$. As a result, the fixed point equation $\rho = g(\rho, \lambda_{\underline{K}}, ..., \lambda_{\overline{K}})$ has a unique solution in $[0,1]$.

Let $\lambda_k^1 < \lambda_k^2$, and $\rho_1 = g(\rho_1, \lambda_k^1)$ and $\rho_2 = g(\rho_2, \lambda_k^2)$. Since $g(\rho, \lambda_k)$ is a decreasing function of λ_k for all $k \in [\underline{K}, \overline{K}]$

and $\lambda_k^1 < \lambda_k^2$, we have $g(\rho_2, \lambda_k^1) > g(\rho_2, \lambda_k^2) = \rho_2$. Using the result above, we can get $\rho_1 > \rho_2$. As a result, the solution of $\rho = g(\rho, \lambda_k)$ is a decreasing function of λ_k, $\forall k \in \left[\underline{K}, \overline{K}\right]$. ■

Remark: Combining Corollary 1 with Eq. (14), we see that the reduction in infection probability by taking security measure increases as other nodes adopt security measure. This shows the *network externality effect*, i.e., the value of security measure increases as more nodes invest in self-protection.

Sensitivity Analysis: Nodes with different degrees have different sensitivity to the externality effect. Define $\widetilde{\phi}_k = \phi_k(\mathcal{N}) - \phi_k(\mathcal{S}) = (p^+ - p^-)(1 - q\rho)^k$. Assume ρ decreases by a small amount $\Delta\rho$, then $\Delta\widetilde{\phi}_k = (p^+ - p^-)(1 - q\rho)^{k-1}kq\Delta\rho$, and the relative change is given by $\frac{\Delta\widetilde{\phi}_k}{\widetilde{\phi}_k} = \frac{kq\Delta\rho}{(1-q\rho)}$, which indicates that nodes with degree k are k times as sensitive to the network externality effect as nodes with degree 1.

A node with degree k will invest if and only if the utility with secure measure is higher than that without secure measure, or

$$\begin{aligned} c_k <&(\phi_k(\mathcal{N}) - \phi_k(\mathcal{S}))(u_k(w_k) - u_k(w_k - l)) \\ =& (p^+ - p^-)(1 - q\rho)^k(u_k(w_k) - u_k(w_k - l)) \end{aligned}$$

Note that the loss distribution of nodes with degree k is $F_k(l)$. Since the infection probability varies with the fraction of security adopters, we consider the *self-fulfilling expectations equilibrium* [7] in analyzing the final adoption extent. Nodes form a shared expectation that the fraction of the nodes has adopted security measure and if each of them makes decision based on this expectation, then the final fraction is indeed the initial expectation.

Let l_k^* be the minimum value that satisfies the above inequality in the equilibrium, then λ_k^*, the fraction of node of degree k taking the secure measure, is given by the equation $\lambda_k^* = 1 - F_k(l_k^*)$. Summarizing the previous analysis, we have the following proposition.

Proposition *2: Nodes with degree k will take the secure measure if their loss is greater than l_k^*. The final fraction of nodes with degree k that invest in self-protection is λ_k^*. l_k^* and λ_k^* are solutions of the following fixed point equations:*

$$\lambda_k^* = 1 - F_k(l_k^*), \tag{15}$$

$$c_k = (p^+ - p^-)(1 - q\rho^*)^k(u_k(w_k) - u_k(w_k - l_k^*)), \tag{16}$$

where ρ^* is given by the solution of the following equation

$$\rho^* = 1 - \sum_{k=\underline{K}'}^{\overline{K}'} q_k(1 - p^+ + \lambda_{k+1}^*(p^+ - p^-))(1 - q\rho^*)^k. \tag{17}$$

Corollary *2: Fixed point equations (15)–(17) has at least one solution.*

Proof: We prove the corollary using iteration method. Given a set of $\lambda_k^t, k \in [\underline{K}, \overline{K}]$, we update it as follows. First, we solve ρ^t by substituting λ_k^t in Eq. (17) and get an updated fraction λ_k^{t+1} by Eq. (15) and (16). We start from $\lambda_k^0 = 0$ and do the iteration. Obviously $\lambda_k^1 \geq \lambda_k^0 = 0$. If there does not exist k such that $\lambda_k^1 > \lambda_k^0$, then $\lambda_k^* = 0$ is an equilibrium point. Otherwise, with Corollary 1, it is easy to prove that $\rho^{t+1} \leq \rho^t$ and $\lambda_k^{t+1} \geq \lambda_k^t$ by induction. During the iteration process, λ_k^t is non-decreasing with t and is bounded with $\lambda_k^t \leq 1$. So λ_k^t will converge to the minimum equilibrium point given by the solutions of the fixed point equations in Proposition 2. ■

The above proof also shows the dynamics of the adoption process. Initially, $\lambda_k^0 = 0$, based on this belief nodes make decisions. Then they update the belief and continue to update their decision. The above proof shows the convergence of this dynamic process.

Corollary *3: The equilibrium points given by fixed point equations (15)–(17) are monotone, i.e., if $\mathbf{\Lambda}^{*1} = (\lambda_{\underline{K}}^{*1}, ..., \lambda_k^{*1}, ..., \lambda_{\overline{K}}^{*1})$ and $\mathbf{\Lambda}^{*2} = (\lambda_{\underline{K}}^{*2}, ..., \lambda_k^{*2}, ..., \lambda_{\overline{K}}^{*2})$ are two equilibrium points, then we have either $\mathbf{\Lambda}^{*1} \geq \mathbf{\Lambda}^{*2}$ or $\mathbf{\Lambda}^{*1} \leq \mathbf{\Lambda}^{*2}$ and there exists at least one $k \in [\underline{K}, \overline{K}]$ such that $\lambda_k^{*1} \neq \lambda_k^{*2}$.*

Proof: We prove the above corollary by contradiction. Assume there exist k_1 and k_2 such that $\lambda_{k_1}^{*1} < \lambda_{k_1}^{*2}$ and $\lambda_{k_2}^{*1} > \lambda_{k_2}^{*2}$. By $\lambda_{k_1}^{*1} < \lambda_{k_1}^{*2}$ and Eq. (15) and (16), we have $\rho^{*1} > \rho^{*2}$. Since $\rho^{*1} > \rho^{*2}$, by similar analysis, we can conclude $\lambda_{k_2}^{*1} \leq \lambda_{k_2}^{*2}$, which contradicts $\lambda_{k_2}^{*1} > \lambda_{k_2}^{*2}$. ■

The above corollaries prove the existence and monotonicity of equilibrium points. In the following, we study the *multiplicity* and *monotonicity* of the equilibrium points by considering a special case.

B. Analysis of Node Heterogeneity: Two Types Case

To provide more insight on how different nodes can influence each other, let us consider a special case where there are two types of nodes: nodes with low degree k_L and nodes with high degree k_H, $k_H > k_L$. We assume that the cost of self-protection for low degree nodes is c_L and the loss due to being infected is l_L. On the other hand, if $k = k_H$, the cost of self-protection is c_H and the loss is l_H. Note that in Proposition 2, we did not explicitly impose any restriction on the CDF $F_k(l)$. So Proposition 2 still applies to the case when the loss is the same for all node with given degree.

Nodes will invest in self-protection if their utility with investment is greater than that without investment, hence

$$\lambda_L = \Pr((\phi_L(\mathcal{N}) - \phi_L(\mathcal{S}))(u_L(w_L) - u_L(w_L - l_L)) \geq c_L),$$
$$\lambda_H = \Pr((\phi_H(\mathcal{N}) - \phi_H(\mathcal{S}))(u_H(w_H) - u_H(w_H - l_H)) \geq c_H).$$

Note that the probabilities $\phi_L(\mathcal{S})$, $\phi_L(\mathcal{N})$ and $\phi_H(\mathcal{S})$, $\phi_H(\mathcal{N})$ are functions of λ_L and λ_H. We can compare the utilities to determine the fraction of users that will invest in self-protection. Define $\Delta u_L(l_L) \triangleq u_L(w_L) - u_L(w_L - l_L)$ and $f_L(\lambda_L, \lambda_H) \triangleq (\phi_L(\mathcal{N}) - \phi_L(\mathcal{S})) = (p^+ - p^-)(1 - q\rho)^{k_L}$. For $k = k_L$, the utility gap is

$$f_L(\lambda_L, \lambda_H)\Delta u_L(l_L) - c_L,$$

where $f_L(\lambda_L, \lambda_H)$ is the reduction in probability for nodes being finally infected if they invest in self-protection. Similarly, for $k = k_H$, define $\Delta u_H(l_H) \triangleq u_H(w_H) - u_H(w_H - l_H)$ and $f_H(\lambda_L, \lambda_H) \triangleq (\phi_H(\mathcal{N}) - \phi_H(\mathcal{S})) = (p^+ - p^-)(1 - q\rho)^{k_H}$, the utility gap is :

$$f_H(\lambda_L, \lambda_H)\Delta u_H(l_H) - c_H,$$

By corollary 1, $f_L(\lambda_L, \lambda_H)$ and $f_H(\lambda_L, \lambda_H)$ are increasing functions in λ_L and λ_H, which indicates that λ_L and λ_H degenerate to indicator functions. In other words, either no nodes will invest in self-protection, or all of them will invest in self-protection.

Nodes can decide whether to make investment or not by comparing the expected profit of investment $f_L(\lambda_L, \lambda_H)\Delta u_L(l_L)$ $(f_H(\lambda_L, \lambda_H)\Delta u_H(l_H))$ with the cost c_L (c_H) for nodes with low (high) degree. We compare $f_L(\lambda_L, \lambda_H)$ with $c_L/\Delta u_L(l_L)$ and $f_H(\lambda_L, \lambda_H)$ with $c_H/\Delta u_H(l_H)$. There are four cases to consider:

Case 1: If $f_L(0,0) > c_L/\Delta u_L(l_L), f_H(0,0) > c_H/\Delta u_H(l_H)$, then there is a unique equilibrium point $(\lambda_L^*, \lambda_H^*) = (1,1)$ where all nodes will invest in self-protection. Even if initially none of the nodes invest in self-protection, the profit of investment exceeds the cost regardless of the degree of nodes and eventually, all nodes will purchase self-protection tools.

Case 2: If $f_L(0,0) > c_L/\Delta u_L(l_L), f_H(0,0) < c_H/\Delta u_H(l_H)$, then all nodes with degree $k = k_L$ will invest in self-protection because the profit of investment for low degree nodes exceeds the cost, while the profit is smaller than the cost for high degree nodes.

- If $f_H(1,0) > c_H/\Delta u_H(l_H)$, then all nodes with degree k_H will invest in self-protection. The profit of investment for nodes with high degree increases since nodes with low degree will do the investment. Hence, the investment in security by nodes with degree k_L will incentivize nodes with degree k_H to invest also. There is a unique equilibrium point $(\lambda_L^*, \lambda_H^*) = (1,1)$.
- If $f_H(1,0) < c_H/\Delta u_H(l_H) < f_H(1,1)$, there exists a *tipping point* λ_H^T, such that $f_H(1, \lambda_H^T) = \frac{c_H}{\Delta u_H(l_H)}$. This implies that if we can offer self-protection to λ_H^T fraction of nodes with degree k_H for free, then this will incentivize all nodes with high degree to invest. There are two equilibrium points $(\lambda_L^*, \lambda_H^*) = (1,0)$ and $(\lambda_L^*, \lambda_H^*) = (1,1)$.
- If $c_H/\Delta u_H(l_H) > f_H(1,1)$, all nodes with degree k_H will not perform self-protection. There is only one equilibrium point $(\lambda_L^*, \lambda_H^*) = (1,0)$.

Case 3: If $f_L(0,0) < c_L/\Delta u_L(l_L)$, $f_H(0,0) > c_H/\Delta u_H(l_H)$, then all nodes with degree k_H will take self-protection measure.

- If $f_L(0,1) > c_L/\Delta u_L(l_L)$, then all nodes with degree k_L will invest in self-protection. In this case, the investment in security by nodes with degree k_H will incentivize nodes with degree k_L to invest in self-protection. There is only one equilibrium point $(\lambda_L^*, \lambda_H^*) = (1,1)$.
- If $f_L(0,1) < c_L/\Delta u_L(l_L) < f_L(1,1)$, there exists a *tipping point* λ_L^T, such that $f_L(\lambda_L^T, 1) = c_L/\Delta u_L(l_L)$. There are two equilibrium points $(\lambda_L^*, \lambda_H^*) = (0,1)$ and $(\lambda_L^*, \lambda_H^*) = (1,1)$.
- If $c_L/\Delta u_L(l_L) > f_L(1,1)$, all nodes with degree k_L will not invest in self-protection. There is only one equilibrium point $(\lambda_L^*, \lambda_H^*) = (0,1)$.

Case 4: If $f_L(0,0) < c_L/\Delta u_L(l_L) < f_L(1,1), f_H(0,0) < c_H/\Delta u_H(l_H) < f_H(1,1)$, then there exists a *tipping point* λ_L^T and λ_H^T. There are two equilibrium points $(\lambda_L^*, \lambda_H^*) = (0,0)$ and $(\lambda_L^*, \lambda_H^*) = (1,1)$.

IV. Analysis for Cyber-insurance Market

In here, we consider *cyber-insurance* and analyze its impact on security adoption.

A. Supply of Insurance

Let's say the insurance provider offers insurance at the price of $\pi < 1$. Nodes which buy insurance at the premium of πX from the insurance provider will be compensated X for the loss incurred if they are infected. Given the price π, node will choose to buy the amount of insurance that maximizes its utility. Define $\phi_k(\mathcal{S})(\phi_k(\mathcal{N}))$ as the probability that a node with degree k will be infected if it subscribes (does not subscribe) to a secure measure. In this paper, we consider cyber-insurance without adverse selection, in which the insurance provider can observe the degree of a node, hence the risk type of a node (high degree indicates high risk level). Thus, in the following, we drop the subscript k where the meaning is clear for general presentation. A node will choose the amount of insurance that maximizes

$$U(\pi, X) = \phi u(w - l + (1-\pi)X) + (1-\phi)u(w - \pi X) - x, \quad (18)$$

where x is the wealth spent on security protection. When a node chooses $\mathcal{N}$, ϕ becomes $\phi(\mathcal{N})$, $x = 0$. When a node chooses $\mathcal{S}$, ϕ becomes $\phi(\mathcal{S})$, $x = c$. Assume the insurance provider is risk neutral, so they only care about the expected wealth. If a node buys X amount of insurance, then the profit of the insurance is $(\pi - \phi)X$. In here, we consider a competitive market so the insurance provider has to offer the insurance at the price $\pi = \phi$, or the *actuarially fair price* [8].

Lemma *1: When the insurance is offered at the actuarially fair price, the optimal insurance coverage is a full insurance coverage, i.e., a node will buy insurance amount l, which is equal to the loss. The maximal expected utility is* $\max_X U(\phi, X) = u(w - \phi l) - x$, *i.e., when a node chooses $\mathcal{N}$, the maximal expected utility is $u(w - \phi(\mathcal{N})l)$, when a node chooses $\mathcal{S}$, the maximal expected utility is $u(w - \phi(\mathcal{S})l) - c$.*

Proof: A node will optimize

$$U(\phi, X) = \phi u(w - l + (1-\phi)X) + (1-\phi)u(w - \phi X) - x. \quad (19)$$

Taking the derivative of $U(\phi, X)$ with respect to X, we have

$$U'(\phi,X) = \phi(1-\phi)\left[u'(w - l + (1-\phi)X) - u'(w - \phi X)\right].$$

Since $u(w)$ is an increasing and concave function, $u'(w)$ is a decreasing and positive function. When $X < l$, $U'(\phi, X) > 0$; when $X > l$, $U'(\phi, X) < 0$. The expected utility is maximized at $X = l$, the optimal expected utility is $u(w - \phi l) - x$. ∎

In Fig. 1, the expected utility without insurance market is point C, i.e., nodes feel that they lose more than the expected wealth loss because of the risk averson. With insurance market, the expected utility improves from point C to point B.

Lemma *2: When the insurance is offered at price $\pi > \phi$, the optimal insurance coverage is partial insurance coverage, i.e., a node will buy insurance coverage less than l. The maximal expected utility is $u(w-\phi l-\delta(\phi,\pi))-x$., where $\delta(\phi,\pi) > 0$.*

Proof: Similar to the proof of Lemma 1, a node optimizes

$$U(\pi,X)=\phi u(w-l+(1-\pi)X)+(1-\phi)u(w-\pi X)-x.$$

The first order differentiation of $U(\pi,X)$ is

$$U'(\pi,X)=\phi(1-\pi)u'(w-l+(1-\pi)X)-(1-\phi)\pi u'(w-\pi X).$$

It is easy to verify that $U'(\pi,l) < 0$ since $\pi > \phi$. The second order derivative is

$$\begin{aligned}U''(\pi,X)=&\phi(1-\pi)^2u''(w-l+(1-\pi)X)\\&+(1-\phi)\pi^2u''(w-\pi X).\end{aligned}$$

Since $u(w)$ is concave, $u''(w) < 0$, it follows that $U''(\pi,X) < 0$. $U(\pi,X)$ is a concave function of X. Also, $U'(\pi,l) < 0$, so the optimal solution is smaller than l. As a result, the optimal insurance converge is partial coverage. Let the optimal expected utility be $u(w-\phi l-\delta(\phi,\pi))-x$. Since $U(\phi,X)>U(\pi,X)$, $u(w-\phi l)-x=\max_X U(\phi,X)>\max_X U(\pi,X) = u(w-\phi l-\delta(\phi,\pi))-x$, we can get $\delta(\phi,\pi) > 0$. ∎

Remark: Lemma 1 shows that the expected utility with insurance market is $u(w-\phi l)-x > \phi u(w-l)+(1-\phi)u(w)-x$. The utility of a node is *improved* by the insurance market with the fair price. But if the contract is at an unfair price, the utility improvement is smaller according to Lemma 2.

One problem with the combination of insurance and self-protection is *moral hazard*, which happens when the insurance provider cannot observe the protection level of a node. Insurance coverage may discourage the node to take self-protection measure to prevent the losses from happening, or even to encourage nodes to cause the loss and make insurance claims. In here, we examine the effect of the insurance market on the self-protection level. We consider the two cases, one is without moral hazard, where the insurance provider can observe the protection level of a node, the other is with moral hazard, where insurance provider does not have any information about the protection level of a node. Without the moral hazard, the insurance provider can discriminate against the nodes with protection measure and those without protection measure. We investigate whether the insurance market will help to incentivize nodes to take secure measure. For the case with moral hazard, we investigate whether insurance provider can design contracts so that insurance market is not a negative incentive, where nodes can still take protection measure.

B. Cyber-insurance Without Moral Hazard

Security Adoption with Cyber-insurance Market: Because the insurance provider can observe the protection level of a node, the insurance provider will offer insurance price of $\phi(\mathcal{S})$ (or $\phi(\mathcal{N})$) for those nodes with (or without) security protection. According to Lemma 1, nodes will buy the full insurance regardless of its protection level. As a result, the expected utility for nodes without protection is $u(w-\phi(\mathcal{N})l)$ and the expected utility for nodes with protection is $u(w-\phi(\mathcal{S})l)-c$. Thus, with insurance market, a node will invest in security protection if and only if

$$c < g(l,\rho) \triangleq u(w-\phi(\mathcal{S})l)-u(w-\phi(\mathcal{N})l).$$

Note that $g(l,\rho)$ is a function of ρ because $\phi(\mathcal{S})$ and $\phi(\mathcal{N})$ can be expressed in ρ.

Lemma *3: The function $g(l,\rho) \triangleq u(w-\phi(\mathcal{S})l)-u(w-\phi(\mathcal{N})l)$ increases with respect to the loss l.*

Proof: Substituting $u(w)$ with $\frac{w^{1-\sigma}}{1-\sigma}$, we can get the first order derivative of $g(l,\rho)$:

$$g_l = -\frac{\phi(\mathcal{S})}{(w-\phi(\mathcal{S})l)^\sigma}+\frac{\phi(\mathcal{N})}{(w-\phi(\mathcal{N})l)^\sigma} \tag{20}$$

It is easy to verify that $g_l > 0$ since $\phi(\mathcal{N}) > \phi(\mathcal{S})$. ∎

Lemma *4: The function $g(l,\rho) \triangleq u(w-\phi(\mathcal{S})l)-u(w-\phi(\mathcal{N})l) = u(w-(1-(1-p^-)(1-q\rho)^k)l)-u(w-(1-(1-p^+)(1-q\rho)^k)l)$ is decreasing with respect to ρ.*

Proof: Similarly, taking the first order derivative we can get:

$$\begin{aligned}g_\rho = lkq(1-q\rho)^{k-1}[&(1-p^+)(w-l+(1-p^+)(1-q\rho)^kl)^{-\sigma}\\&-(1-p^-)(w-l+(1-p^-)(1-q\rho)^kl)^{-\sigma}]\end{aligned}$$

It is easy to verify that function $h(p) \triangleq (1-p)(w-l+(1-p)(1-q\rho)^kl)^{-\sigma}$ decreases with p. Thus, $h(p^+) < h(p^-)$ and $g_\rho < 0$. ∎

Lemma 3 indicates that nodes with higher loss are more likely to invest in security. From Lemma 4 we know that positive network externality still exists even in the presence of insurance market. Similar to the analysis in Sec. III, we can arrive in the following proposition regarding the adoption fraction with insurance market:

Proposition *3: With insurance market, nodes with degree k will take the secure measure if their loss is greater than $l_k^{*\mathtt{I}}$. The final fraction of nodes with degree k that will invest in self-protection is $\lambda_k^{*\mathtt{I}}$. $l_k^{*\mathtt{I}}$ and $\lambda_k^{*\mathtt{I}}$ are solutions of the following fixed point equations:*

$$\lambda_k^{*\mathtt{I}} = 1-F_k(l_k^{*\mathtt{I}}), \tag{21}$$

$$c_k = u_k(w_k-\phi(\mathcal{S})l_k^{*\mathtt{I}})-u_k(w_k-\phi(\mathcal{N})l_k^{*\mathtt{I}}), \tag{22}$$

where $\rho^{*\mathtt{I}}$ is given by the solution of the following equation

$$\rho^{*\mathtt{I}} = 1-\sum_{k=\underline{K}'}^{\overline{K}'} q_k(1-p^+ + \lambda_{k+1}^{*\mathtt{I}}(p^+-p^-))(1-q\rho^{*\mathtt{I}})^k. \tag{23}$$

Previous corollaries following Proposition 2 on the existence and monotonicity of equilibrium points also hold here. Comparing Proposition 3 with Proposition 2, we can recognize the only difference lies in Eq. (22) and Eq. (16). Buying insurance improves node's utility, and hence changes their decision on security protection as well. In the following, we examine the effect of insurance market on security adoption. An overall and detailed analysis needs calculating out all the equilibrium points and comparing the equilibrium points specified by the two propositions. which is quite complicated. Instead, we examine the effect from the local point of view, but still provide enough insight.

Incentive Analysis: According to previous analysis, a node will take secure measure if

$$c < c_{NI} \triangleq (\phi(\mathcal{N}) - \phi(\mathcal{S}))(u(w) - u(w-l)), \tag{24}$$

where c_{NI} is the threshold without insurance market. With insurance market, nodes will take secure measure if and only if

$$c < c_I \triangleq u(w - \phi(\mathcal{S})l) - u(w - \phi(\mathcal{N})l), \tag{25}$$

where c_I denotes the threshold with insurance market.

In order for insurance market to be a good incentive for self-protection, we should have $c_{NI} < c_I$, i.e.,

$$\begin{aligned} c_I - c_{NI} = {} & u(w - \phi(\mathcal{S})l) + \phi(\mathcal{S})(u(w) - u(w-l)) \\ & - [u(w - \phi(\mathcal{N})l) + \phi(\mathcal{N})(u(w) - u(w-l))] > 0. \end{aligned}$$

Define $r(p) \triangleq u(w - pl) + p(u(w) - u(w-l))$, then the above condition becomes $r(\phi(\mathcal{S})) > r(\phi(\mathcal{N}))$. Next we investigate under what condition the above inequality will hold. Consider the function $r(p)$, we have the following lemma.

Lemma 5: *$r(p)$ is a concave function of p, there exists a unique p^* that maximizes $r(p)$.*

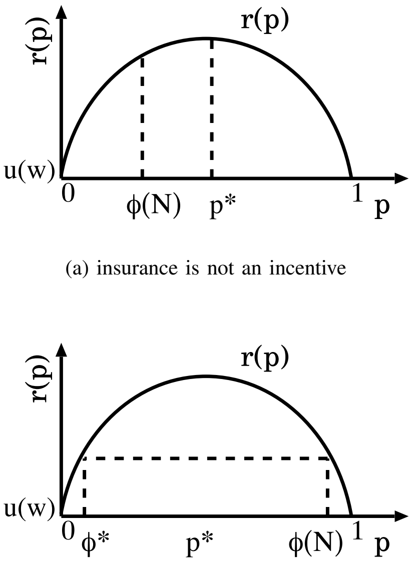
Proof: Substituting $u(w)$ with $\frac{w^{1-\sigma}}{1-\sigma}$, we can derive the second order derivative of $r(p)$:

$$r''(p) = -\sigma l^2 (w - pl)^{-\sigma - 1},$$

Since $r''(p) < 0$, $r(p)$ is a concave function with respect to p. Because $r(0) = r(1) = u(w)$, there exists a unique optimal point $p^* \in (0, 1)$ that maximizes $r(p)$. ■

Proposition 4: *If the initial infection probability $\phi(\mathcal{N})$ is greater than p^* and the quality of self-protection is not too high, i.e., $\phi(\mathcal{N}) - \phi(\mathcal{S})$ is bounded, insurance will be a good incentive for self-protection.*

Proof: We want $r(\phi(\mathcal{S})) > r(\phi(\mathcal{N}))$ conditioned on $\phi(\mathcal{N}) > \phi(\mathcal{S})$. Let ϕ^* be the minimum value such that $r(\phi^*) = r(\phi(\mathcal{N}))$. If $\phi(\mathcal{N})$ is smaller than the optimal value p^*, as shown in Fig. 3a, then $\phi^* = \phi(\mathcal{N})$. In this case, it is impossible for insurance to be an incentive for self-protection. Otherwise if $\phi(\mathcal{N})$ is bigger than the optimal value p^*, then $\phi^* < \phi(\mathcal{N})$. In this case, if $\phi^* < \phi(\mathcal{S}) < \phi(\mathcal{N})$, then insurance market will be a good incentive for self-protection. The feasible region of $\phi(\mathcal{S})$ is shown in Fig. 3b. ■



(a) insurance is not an incentive

(b) insurance is an incentive

Fig. 3: Thresholds of $\phi(S)$

Fig. 3a shows the case where $\phi(\mathcal{N})$ is smaller than the optimal value p^* that maximizes $r(p)$. In this case, it is impossible for insurance to be an incentive. In Fig. 3b, $\phi(\mathcal{N})$ is greater than p^*. If $\phi(\mathcal{S})$ is within the region $[\phi^*, \phi(\mathcal{N})]$, then insurance is a good incentive for security adoption. From Fig. 3b, we can see that insurance will be more likely to be an incentive with large $\phi(\mathcal{N})$ and small $\phi(\mathcal{N}) - \phi(\mathcal{S})$. Hence, if the initial secure situation is bad and the protection quality of secure measure is not too high, then insurance market is a positive incentive for self-protection; otherwise, insurance market is a negative incentive, i.e., if a node adopts secure measure without insurance, it may decide not to adopt secure measure with insurance market.

We can study the effect of cyber-insurance on nodes with *different degrees* based on above analysis. For $k_1 < k_2$, we have $\phi_{k_1}(\mathcal{S}) < \phi_{k_2}(\mathcal{S})$, $\phi_{k_1}(\mathcal{N}) < \phi_{k_2}(\mathcal{N})$ and $\phi_{k_1}(\mathcal{N}) - \phi_{k_1}(\mathcal{S}) < \phi_{k_2}(\mathcal{N}) - \phi_{k_2}(\mathcal{S})$. In other words, nodes with higher degree have higher initial infection probability and the protection measure will be less effective to nodes with higher degree. As a result, insurance market will be more likely to be an incentive for nodes with higher degree. (A quantitative conclusion needs to examine the influence of wealth and loss difference for nodes with different degrees.)

Whether insurance will be an incentive greatly depends on the parameters. Generally speaking, cyber-insurance can be a positive insurance for all nodes, a negative insurance for all nodes and a negative incentive for low degree nodes, but a positive incentive for high degree nodes. We provide extensive numerical results in the Section V to demonstrate the above cases.

C. Cyber-insurance with Moral Hazard

With moral hazard, insurance provider cannot observe the protection level of the nodes. As a result, insurance contract cannot be differentiated for nodes with different protection level. Instead, with the insurance contracts given, nodes will choose the behavior that maximizes their expected utility.

It is possible that nodes will choose not to invest in self-protection if the insurance can cover part of the loss. In this case, insurance is a negative incentive for self-protection. In here, we investigate whether it is possible to design a contract that is *not* a negative incentive for self-protection.

In a competitive insurance market, the only possible equilibrium is that the insurance provider offers the contracts at the price $\phi(\mathcal{S})$ ($\phi(\mathcal{N})$) and the nodes choose (not) to invest in self-protection. If the price is at $\phi(\mathcal{S})$, but nodes choose not to invest in self-protection, then the expected profit of the provider $(\phi(\mathcal{S}) - \phi(\mathcal{N}))X < 0$. The provider will not offer such insurance since it will lead to a loss. On the other hand, if the insurance provider sells the contracts at the price of $\phi(\mathcal{N})$, but nodes choose to invest in self-protection, then the expected profit is $(\phi(\mathcal{N}) - \phi(\mathcal{S}))X > 0$. Since the market is competitive, the positive profit will lead to competition and the insurance provider who offers contracts at $\phi(\mathcal{S})$ will survive.

We first consider the case when insurance provider can offer the full insurance coverage. Nodes can choose the optimal amount of insurance coverage. First, we consider the $\mathcal{N}$-*equilibrium*, i.e., contracts are sold at $\phi(\mathcal{N})$ and nodes choose $\mathcal{N}$. If the insurance provider offers the price at $\phi(\mathcal{N})$, nodes will decide to choose $\mathcal{N}$ if the expected utility with $\mathcal{N}$ is greater. By Lemma 1, if nodes choose $\mathcal{N}$, they will buy the full coverage of insurance. The expected utility is $u(w - \phi(\mathcal{N})l)$. If nodes choose $\mathcal{S}$, then by Lemma 2, the maximal expected utility is $u(w - \phi(\mathcal{S})l - \delta(\phi(\mathcal{S}), \phi(\mathcal{N}))) - c$. So nodes will choose $\mathcal{N}$ if $c > c_{NE} = u(w - \phi(\mathcal{S})l - \delta(\phi(\mathcal{S}), \phi(\mathcal{N}))) - u(w - \phi(\mathcal{N})l)$, where c_{NE} is the threshold for $\mathcal{N}$-equilibrium.

Next, we consider the $\mathcal{S}$-*equilibrium*, i.e., contracts are sold at the price of $\phi(\mathcal{S})$ and nodes choose $\mathcal{S}$. If nodes choose $\mathcal{N}$, the optimal expected utility is $\max_X U_{\mathcal{N}}(\phi(\mathcal{S}), X) \geq U_{\mathcal{N}}(\phi(\mathcal{S}), l) = u(w - \phi(\mathcal{S})l)$. If nodes choose $\mathcal{S}$, by Lemma 1, the optimal expected utility is $u(w - \phi(\mathcal{S})l) - c < u(w - \phi(\mathcal{S})l)$. So nodes will choose $\mathcal{N}$ if full insurance coverage can be offered. In other words, $\mathcal{S}$-equilibrium does not exist under full insurance coverage. Full coverage insurance is never an incentive for security adoption with moral hazard. The reason why full coverage insurance is not an incentive is that if nodes get infected, loss will be covered fully regardless whether they take secure measure or not by paying the same premium. As a result, the investment on security protection is not necessary. One solution to the moral hazard problem is partial coverage against loss [26]. Partial insurance can incentivize nodes to invest in self-protection by exposing them to certain risk loss.

Consider the $\mathcal{S}$-equilibrium, insurance provider offers contract at price $\phi(\mathcal{S})$ and the maximal insurance coverage is W. We already showed $W < l$. In a partial insurance contract, a node cannot decide the amount of coverage by maximizing its utility. If a node chooses $\mathcal{N}$, its maximal expected utility is

$$\begin{aligned} U_{\mathcal{N}}(\phi(\mathcal{S}), W) =& \phi(\mathcal{N})u(w - l + (1 - \phi(\mathcal{S}))W) \\ &+ (1 - \phi(\mathcal{N}))u(w - \phi(\mathcal{S})W). \end{aligned} \tag{26}$$

If a node chooses $\mathcal{S}$, its maximal expected utility is

$$\begin{aligned} U_{\mathcal{S}}(\phi(\mathcal{S}), W) =& \phi(\mathcal{S})u(w - l + (1 - \phi(\mathcal{S}))W) \\ &+ (1 - \phi(\mathcal{S}))u(w - \phi(\mathcal{S})W) - c. \end{aligned} \tag{27}$$

The S-equilibrium exists if and only if

$$\begin{aligned} \Delta(W) =& U_{\mathcal{S}}(\phi(\mathcal{S}), W) - U_{\mathcal{N}}(\phi(\mathcal{S}), W) \\ =& (\phi(\mathcal{N}) - \phi(\mathcal{S}))(u(w - l + (1 - \phi(\mathcal{S}))W) \\ &- u(w - \phi(\mathcal{S})W)) - c \geq 0. \end{aligned} \tag{28}$$

It is easy to find out that $\Delta(W)$ is a strictly decreasing function of W. We want to find out whether there exits W such that $W \in [0, l]$ and $\Delta(W) \geq 0$. From previous analysis, we know $\Delta(l) < 0$, i.e., when full insurance is offered, nodes will choose $\mathcal{N}$. If $W = 0$, it indicates no insurance is provided. $\Delta(0)$ is the expected utility gap when no insurance is provided. If $\Delta(0) < 0$, i.e., nodes will not invest in self-protection without insurance market, it is impossible to find out W such that $\Delta(W) > 0$ due to the monotonicity of $\Delta(W)$. Thus, cyber-insurance can never be a positive incentive for self-protection. However, if $\Delta(0) > 0$, i.e., nodes will invest in self-protection without insurance market, we can always find such W such that $\Delta(W) = 0$ since $\Delta(W)$ is a continuous function of W. As a result, the maximal insurance coverage which can be offered by the insurance provider so that $\mathcal{S}$-equilibrium is possible is:

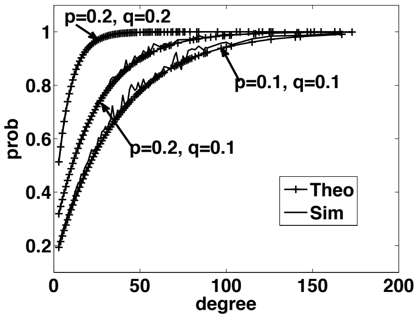
$$W_{max} = \arg\{\Delta(W) = 0\}. \tag{29}$$

In the competitive insurance market without moral hazard, the expected utility of nodes who choose $\mathcal{S}$ with insurance market is $u(w - \phi(\mathcal{S})l) - c$. With moral hazard, the maximal insurance coverage is W_{max}. Then the maximal expected utility for nodes choosing $\mathcal{S}$ is $U_{\mathcal{S}}(\phi(\mathcal{S}), W_{max})$. Since $W_{max} < l$, we have $U_{\mathcal{S}}(\phi(\mathcal{S}), W_{max}) < u(w - \phi(\mathcal{S})l) - c$. In other words, nodes' welfare is hurt by the moral hazard. If the insurance provider offers full insurance, nodes will, on the contrary, choose $\mathcal{N}$. Partial insurance with maximal contract W_{max} will make it worthwhile for nodes for invest in self-protection.

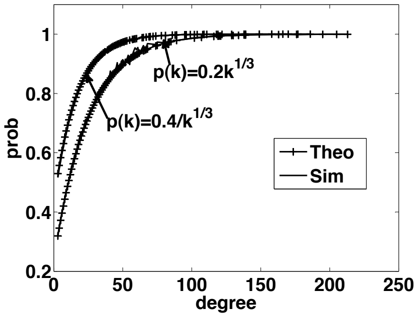
V. Simulation & Numerical Results

We present simulation and numerical results to investigate the influence of various parameters in this section.

Validating Final Infection Probability: We consider a large graph with power-law degree distribution [9]. We want to verify the accuracy of using the mean field on these power law graphs. We use the popular *Generalized Linear Preference (GLP)* method to generate power law graphs [6]. Parameters were selected so that the power law exponent $\gamma = -3$. We generate graphs with $10,000$ nodes and approximately $30,000$ edges. The minimum degree is 3 and the maximum degree is approximately 200. First, we verify the case when all the nodes have the same probability of being infected initially. The result is shown in Fig. 4a. Initially, every node is infected with the same probability p and every edge is occupied with probability q. We calculate the probability that nodes with certain degree is infected. Fig. 4a shows the simulation verifies the theoretical results. One can also observe that the infection probability is an increasing function of node's degree. When the p and q increases, the infection probability also increases.



(a) homogeneous infection prob.



(b) heterogeneous infection prob.

Fig. 4: Determine final infection prob. via local mean field

Next, Fig. 4b shows the infection probability of nodes with different degrees under different initial infection probability. For both curves, q is set to be 0.1. For the curve above, we set the initial probability for nodes with degree k to be $p(k) = 0.4/k^{\frac{1}{3}}$. The probability decreases with degree. For the curve below, we set the initial infection probability to be $p(k) = 0.2k^{\frac{1}{3}}$. The probability increases with degree. From the figure, we see that the local mean field technique is very accurate and the theoretical results accurately match with simulation results.

Security Adoption: Let us investigate how parameters can influence the fraction of nodes with different degrees in adopting secure measures. We consider a graph G with power law distribution with $\gamma = -3$, minimum and maximum degree are 3 and 13. Here maximum degree is set small for the convenience of selecting other parameters. For example, with very large maximum degree, even a small q will make the infection probability $\phi_k(\mathcal{N})$ or $\phi_k(\mathcal{S})$ very big because of the power relationship. However, our results still apply when the maximum degree is large.

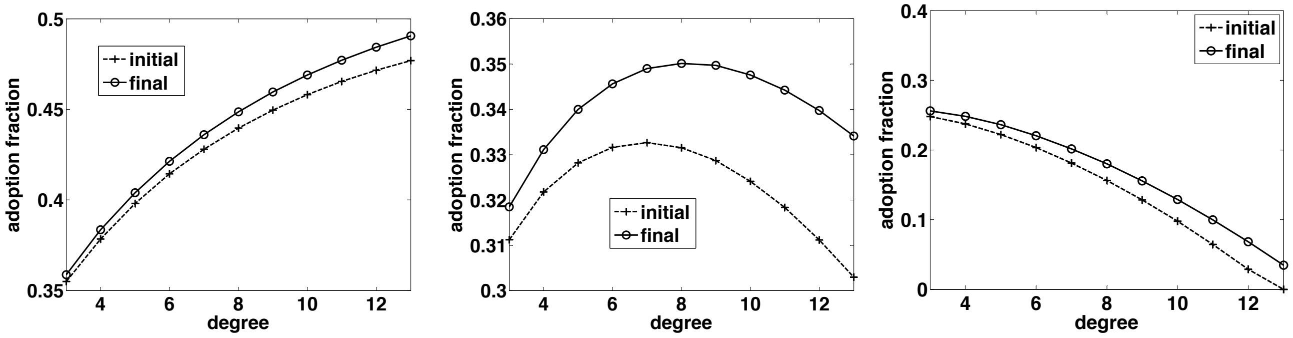
We set the degree of risk of aversion of the utility function $\sigma = 0.5$, the same for all node. The initial wealth of nodes with degree k is $w_k = 10 * k + 50$. The loss follows uniform distribution from 0 to half of the initial wealth. The cost of secure measure of all nodes is $c = 0.3$. Initially, all nodes without (with) secure measure are infected initial with probability $p^+ = 0.3$ ($p^- = 0.2$). Having fixed the above parameters, we choose to change the q to calculate the fraction of adoptors with different degrees because nodes with different degree are mainly differentiated via the term $(1 - q\rho)^k$, in which q plays an important role. We want to examine the effect of heterogeneity by seting different q.

We show the initial fraction and final fraction of adoption in Fig. 5. Here the initial fraction means that every node assumes that other nodes will not adoption secure measure and makes its decision on this assumption. Final fraction means the fraction given by the minimum equilibrium point in Proposition 2. Due to the positive externality effect, final fraction is greater than initial fraction. We plot them to examine the externality effect. From Fig. 5a to Fig. 5c, we set q to be $0.05, 0.10$ and 0.15 respectively. The figures show that the adoption fraction of nodes with every degree decreases as q increases. This indicates that the spreading effectiveness can inhibit adoption of secure measure. In Fig. 5a, the adoption fraction increases with degree, in Fig. 5b, the adoption fraction initially increases with degree, then decreases with degree, while in Fig. 5c , the adoption fraction decreases with degree. Comparing these three figures, we see that there is no general rule regarding the fraction of adoptors as a function of the degree. It greatly depends on the parameters. However, we can see in all figures that the gap between the final adoption fraction and the initial adopt fraction increases with degree, indicating nodes with higher degree will be incentivized better than nodes with lower degree. This agrees with our previous result that higher degree nodes are more sensitive to the externality effect.

Influence of Cyber-insurance: We claim in previous section that insurance can be a negative incentive for all nodes, a positive incentive for all nodes and a negative incentive for low degree nodes but a positive incentive for high degree nodes. We demonstrate these cases through numerical results. In Fig. 6a, we set the parameters $p^+ = 0.3$, $p^- = 0.2$ and $q = 0.02$. We see that the fraction of nodes which adopt the secure measure without insurance market is greater than that with insurance market. This is because the infection probability without secure measure is low. In Fig. 6b, we set the parameters $p^+ = 0.8$, $p^- = 0.7$ and $q = 0.02$. As the figure shows, insurance market is a positive incentive. In this case, the infection probability without secure measure is high and the protection quality is low. In Fig. 6c, we set the parameters $p^+ = 0.8$, $p^- = 0.7$ and $q = 0.15$. In contrast to Fig. 6a, q is greater, making the infection probability for low degree nodes small while for high degree nodes big. Thus insurance is a negative incentive for low degree nodes, but a positive incentive for high degree nodes.

VI. Related Work

Recently there has been growing research in the economic of information security [2], [3]. Several models are proposed to study the strategic behavior of security investment. Some models consider the security investment game without incorporating the effect of network topology, i.e., [10], [11], [15]. Others assume that the graph topology is given. These works combine the epidemic theory with game theory. The authors in [25] combine the N-intertwined epidemic model

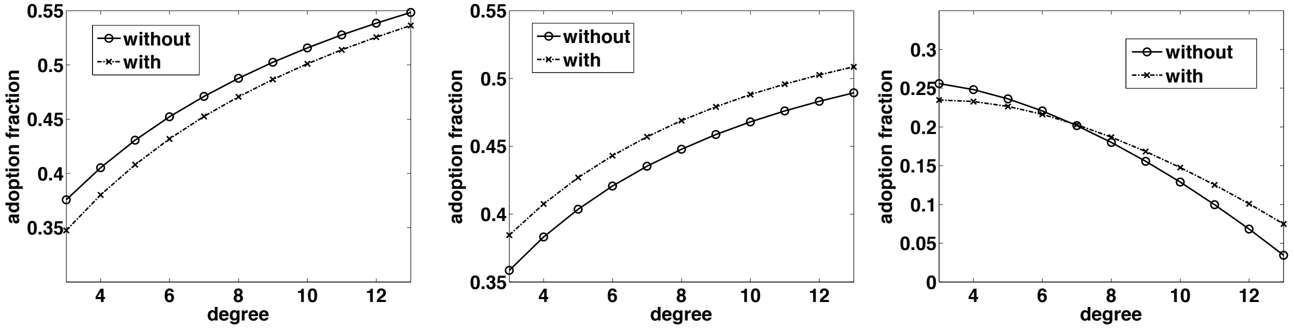


(a) $q = 0.05$

(b) $q = 0.10$

(c) $q = 0.15$

Fig. 5: Externality effect on nodes with different degrees



(a) negative incentive

(b) positive incentive

(c) negative & positive incentive

Fig. 6: Effect of cyber-insurance on security adoption

with game theory and model nodes' strategic behavior. The model is based on complete information of topology. In [13], [21], the level of security is determined by weights assigned to a topology and no infection process is modeled. [16], [17] are the closely related to our work. The network topology is modeled as a Poisson random graph while real networks are with power law degree distribution. They assume that all nodes are the same to examine the average effect and do not consider the interaction among those nodes. Node heterogeneity, an important characteristic in real networks, is not considered. We generalize their work to consider the interaction of nodes by studying a Bayesian network game. Our modeling result provides significant insight on the influence of heterogeneity. [28] is our previous extended abstract in considering network heterogeneity, which is defined by setting degree thresholds to divide the nodes into classes. This work generalizes previous work and also considers the effect of cyber-insurance.

Insurance was studied in the economic literature long time ago [8] [26]. But these literatures lack to consider many characteristics specific to computer network, such as the interdependence of security, heterogeneity considered in this work. Cyber-insurance was proposed to manage security risk [19] but is only modeled recently [14], [18], [27]. A key concern is whether cyber-insurance is an incentive for security adoption. In [18], the authors do not consider the heterogeneity in modeling cyber-insurance. Moreover, they only model the full coverage insurance. However, we consider heterogeneity and show that cyber-insurance is more likely to be an incentive for node with higher degree. We also consider partial insurance and verify that it can be a non-negative incentive. [27] assume the effort on security protection is continuous and do not consider the network topology.

VII. **Conclusion and Future Work**

Modeling strategic behavior in security adoption helps us to understand what are the factors that could result in under investment. We formulate the security adoption with node heterogeneity as a Bayesian network game and determine the security adoption level. We also investigate the effect of cyber-insurance on protection level. We establish the conditions under which cyber-insurance is a positive incentive without moral hazard. Under the situation of moral hazard, we verify that partial insurance can be a non-negative incentive.

However, the model is still simple and there are several directions in which the paper can be improved. The first is to consider that the effort on security investment is continuous, which is more practical. The second direction is to incorporating the strategic behavior of adversaries, which can overcome the weakness of our paper by assuming that all the nodes have the same probability of being attacked. One interesting research direction is to incorporate the strategic behavior of adversary and see how it may impact adoption on security measures and cyber-insurance. We also hope to get the real data on the parameters defined in our paper, which we artificially set in the simulation, to verify our model.

References

[1] D. Aldous and A. Bandyopadhyay. A survey of max-type recursive distributional equations. *The Annals of Applied Probability*, 15(2):1047–1110, 2005.

[2] R. Anderson. Why information security is hard-an economic perspective. In *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*, pages 358–365. IEEE, 2001.

[3] R. Anderson and T. Moore. The economics of information security. *Science*, 314(5799):610, 2006.

[4] A. Barrat, M. Barthlemy, and A. Vespignani. *Dynamical processes on complex networks*. Cambridge University Press, 2008.

[5] R. Böhme and G. Schwartz. Modeling cyber-insurance: Towards a unifying framework. In *Proceedings of the Workshop on the Economics of Information Security WEIS, Harvard University, Cambridge (June 2010)*. Citeseer.

[6] T. Bu and D. Towsley. On distinguishing between internet power law topology generators. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 638–647. IEEE, 2002.

[7] D. Easley and J. Kleinberg. *Networks, crowds, and markets: Reasoning about a highly connected world*. Cambridge Univ Pr, 2010.

[8] I. Ehrlich and G. Becker. Market insurance, self-insurance, and self-protection. *The Journal of Political Economy*, 80(4):623–648, 1972.

[9] M. Faloutsos, P. Faloutsos, and C. Faloutsos. On power-law relationships of the internet topology. In *ACM SIGCOMM Computer Communication Review*, volume 29, pages 251–262. ACM, 1999.

[10] J. Grossklags, N. Christin, and J. Chuang. Secure or insure?: a game-theoretic analysis of information security games. In *Proceeding of the 17th international conference on World Wide Web*, pages 209–218. ACM, 2008.

[11] G. Heal and H. Kunreuther. The vaccination game. *Center for Risk Management and Decision Process Working Paper*, 2005.

[12] B. Hillier. *The economics of asymmetric information*. Palgrave Macmillan, 1997.

[13] L. Jiang, V. Anantharam, and J. Walrand. Efficiency of selfish investments in network security. In *Proceedings of the 3rd international workshop on Economics of networked systems*, pages 31–36. ACM, 2008.

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

[15] H. Kunreuther and G. Heal. Interdependent security. *Journal of Risk and Uncertainty*, 26(2):231–249, 2003.

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

[17] M. Lelarge and J. Bolot. Network externalities and the deployment of security features and protocols in the internet. In *Proceedings of the 2008 ACM SIGMETRICS international conference on Measurement and modeling of computer systems*, pages 37–48. ACM, 2008.

[18] M. Lelarge and J. Bolot. Economic incentives to increase security in the internet: The case for insurance. In *INFOCOM 2009, IEEE*, pages 1494–1502. IEEE, 2009.

[19] G. Medvinsky, C. Lai, and B. Neuman. Endorsements, licensing, and insurance for distributed system services. In *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, pages 170–175. ACM, 1994.

[20] S. Melnik, A. Hackett, M. Porter, P. Mucha, and J. Gleeson. The unreasonable effectiveness of tree-based theory for networks with clustering. *Physical Review E*, 83(3):036112, 2011.

[21] R. Miura-Ko, B. Yolken, N. Bambos, and J. Mitchell. Security investment games of interdependent organizations. In *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*, pages 252–260. IEEE, 2008.

[22] D. Moore, C. Shannon, et al. Code-red: a case study on the spread and victims of an internet worm. In *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*, pages 273–284. ACM, 2002.

[23] M. Newman. *Networks: an introduction*. Oxford Univ Pr, 2010.

[24] N. Nisan. *Algorithmic game theory*. Cambridge Univ Pr, 2007.

[25] J. Omic, A. Orda, and P. Van Mieghem. Protecting against network infections: A game theoretic perspective. In *INFOCOM 2009, IEEE*, pages 1485–1493. IEEE, 2009.

[26] S. Shavell. On moral hazard and insurance. *The Quarterly Journal of Economics*, 93(4):541, 1979.

[27] N. Shetty, G. Schwartz, M. Felegyhazi, and J. Walrand. Competitive cyber-insurance and internet security. *Economics of Information Security and Privacy*, pages 229–247, 2010.

[28] Z. Yang and J. Lui. Investigating the effect of node heterogeneity and network externality on security adoption.