Performance Evaluation 74 (2014) 1–17

Contents lists available at ScienceDirect

Performance Evaluation

journal homepage: www.elsevier.com/locate/peva

Security adoption and influence of cyber-insurance markets in heterogeneous networks☆

Zichao Yang, John C.S. Lui*

Department of Computer Science and Engineering, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong

ARTICLE INFO

Article history:
Received 1 August 2012
Received in revised form 25 May 2013
Accepted 24 October 2013
Available online 5 December 2013

Keywords:
Self-protection
Security adoption
Heterogeneous networks
Bayesian network game
Cyber-insurance

ABSTRACT

Hosts (or nodes) in the Internet often face epidemic risks such as virus and worm 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 contribution of this paper is to provide a fundamental understanding on how "network externality" with "node 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 a 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.

1. Introduction

Network security is a major problem in communication networks. One of its most common manifestations is in form of virus, worms and botnet 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 [1] 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, only a small percentage of hosts adopt some form of security protection, making epidemic risk still prevalent. In this paper, instead of discussing the technology side of security, we discuss the security adoption in economic language. We argue that it may better explain the low adoption level of security products.

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

☆ An earlier conference version appeared in [37].

* Corresponding author.
E-mail addresses: zcyang@cse.cuhk.edu.hk (Z. Yang), cslui@cse.cuhk.edu.hk (J.C.S. Lui).

0166-5316/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.peva.2013.10.003

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 provide a theoretical understanding on how network externality effect with node heterogeneity may influence security adoption in a network of interconnected nodes (i.e., the Internet).* The externality effect with heterogeneity has significant implication for a policy maker aiming to boost the security level in that by subsidizing early adopters, later adopters will naturally follow.

Modeling such decision and security problem requires the combination of epidemic theory and game theory. While extensive studies in the traditional literature have been dedicated to epidemic theory [2,3], 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 [4], in which complete topology is given and analysis is complicated, we show that using the Bayesian network game, one can elegantly tradeoff using partial topology information while making analysis tractable.

By using the 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, making the secure measure less effective for nodes with higher degree in terms of the reduction in infection probability. Moreover, nodes with higher degrees are more sensitive to externality, i.e., they are more likely to be affected by others' decision. The final adoption fraction of nodes with different degrees 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* [5]: 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* [5,6]. 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. We investigate the effect of cyber-insurance on security adoption under a 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 paper is outlined as follows. In Section 2, we present the epidemic and security investment models. In Section 3, we show how heterogeneous nodes can determine their infection probability and decide on proper security investment. In Section 4, we investigate the effect of the insurance market, both with and without moral hazard, on security adoption. Validations and performance evaluations are presented in Section 5. Section 6 gives related work. Finally, in Section 7, we briefly summarize and discuss several ways in which our model could be improved.

2. Mathematical models

Let us first present the mathematical models on how nodes make decision on security investment. The model mainly derives from that of [7,8] with some modification. 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. We summarize some of the notations in Table 1 for reference.

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 $S = \{healthy, infected\}$ represent 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* [3] 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:

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

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 $\Pr(\theta_{ji} = 1) = q$. Since an infected node will incur some financial loss, a node needs to