Modeling Internet Security Investments
Tackling Topological Information Uncertainty

Ranjan Pal[1] and Pan Hui[2]

[1] University of Southern California, USA,
`rpal@usc.edu`
[2] Deutsch Telekom Laboratories, Berlin, Germany,
`pan.hui@telekom.de`

Abstract. Modern distributed communication networks like the Internet are characterized by nodes (Internet users) interconnected with one another via communication links. In this regard, the security of individual nodes depend not only on their own efforts, but also on the efforts and underlying connectivity structure of neighboring network nodes. By the term 'effort', we imply the amount of investments made by a user in security mechanisms like antivirus softwares, firewalls, etc., to improve his security. However, often due to the large magnitude of such networks, it is not always possible for nodes to have complete effort and connectivity structure information about all their neighbor nodes. Added to this is the fact that in many applications, the Internet users are selfish and are not willing to co-operate with other users on sharing effort information. In this paper, we adopt a non-cooperative game-theoretic approach to analyze individual user security in a communication network by accounting for both, the partial information that a network node possess about its underlying neighborhood connectivity structure and security investment of its neighbors, as well as the presence of positive externalities arising from efforts exerted by neighboring nodes. We analyze the strategic interactions between Internet users on their security investments in order to investigate the equilibrium behavior of nodes and show (i) the existence of monotonic symmetric Bayesian Nash equilibria of efforts and (ii) better connected Internet users choose lower efforts to exert but earn higher utilities than less connected peers with respect to security improvement when user utility functions exhibit strategic substitutes, i.e, are submodular. Our results extend previous work with respect to tackling topological information uncertainty, and provide useful insights to Internet users on appropriately (from improving payoffs perspective) investing in security mechanisms under realistic environments of effort and topological information uncertainty, in order to improve system security and welfare. We also discuss the implications of our results on the parameters of risk management techniques like *cyber-insurance*, and compare the user investment behavior in the incomplete information case with the case when users have increased topological information of their network.

Keywords: security, externality, uncertainty, Bayesian Nash equilibria

1 Introduction

The Internet has become a fundamental and integral part of our daily lives. Billions of people are using the Internet for various types of applications that demand different levels of security. For example, commercial and government organizations run applications that require a high level of security, since security breaches would lead to large financial damage and loss of public reputation. Another example of a high security application in the Internet is maintaining user anonymity through a censorship-resistant network. On the other hand, an ordinary individual for instance generally uses a computing device for purposes that do not demand strict security requirements. However, all these applications are running on a network, that was built under assumptions, some of which are no longer valid for today's applications, e.g., that all users on the Internet can be trusted and that the computing devices connected to the Internet are static objects. Today, the Internet comprises of both good and malicious users. The malicious users perform illegal activities, are able to aspect many users in a short time period, and at the same time reduce their chances of being discovered. To overcome security related issues, Internet users invest in security mechanisms such as anti-virus solutions and firewalls.

It is commonsense information that due to Internet connectivity, the security strength of an Internet user[3] is dependent on the security strength of other users, especially neighboring users. Thus, from an individual user perspective, two important pieces of information are (i) the amount of security investments of his neighbors in the network and (ii) the knowledge of the underlying connectivity structure of his neighbors. Information on both of these drive optimal user investments. Unfortunately, due to the large magnitude of the Internet, it is not feasible or practical to have exact information about the security investments and connectivity structure of all neighboring Internet users. In addition, most Internet users are selfish in nature and would not be inclined to share investment information with other Internet users. However, users do need to invest properly in security/defense mechanisms to protect themselves as much as possible, in turn improving system security. In this paper, we address the problem of optimal security investments when an individual user is uncertain about both, the underlying network connectivity structure of his neighbors as well as their security investment amounts, and accounts for the network externalities[4] posed by the neighbors when they invest in security mechanisms. We emphasize here that the Internet has a static topology and it is not impossible for users to know the whole topology. However, the size of the Internet is so large that naive users do not care to give efforts to know the topology, and thus a virtual uncertainty arises in their mind regarding complete Internet topology information.

---

[3] An Internet user could be a single individual or an individual organization.

[4] An externality is a positive(negative) effect caused to a user not directly involved in an economic transaction, by other users involved in the transaction. For example, an Internet user investing in security mechanisms benefits all the nodes connected to him and thus creates a positive externality for his neighbors.

In the presence of positive network externalities, we consider models related to two general security scenarios as mentioned in [1]. These scenarios are (i) where the security strength of an individual user depends upon the sum security strength of itself and neighboring individual nodes in the network under operation and (ii) where the security strength of an individual user depends on the strength of the strongest node/s amongst its neighbors. An example of scenario 1 is a peer-to-peer network where an attacker might want to slow down the transfer of a given piece of information, whose transfer speed might depend on the aggregate effort of all relevant nodes concerned. An example of scenario 2 is a censorship-resistant network, where a piece of information will remain available to a public domain as long as atleast one node serving that piece of information is unharmed. Another example of scenario 2 is the flow of traffic between two backbone nodes in the Internet. Modeling each path between two backbone nodes as a node, traffic will flow securely between the backbone as long as there is atleast one node that is unharmed by an attacker, i.e., there exists atleast one path between the backbone nodes. Likewise, there are other examples of applications on the Internet that fit scenarios 1 and 2. We emphasize here that there is another practical scenario as mentioned in [1], viz., one where the security strength of an individual user depends on the strength of the weakest neighboring node. This scenario is mainly an intra-organization scenario, where once a node in an organization is compromised due to a weak password or a security policy, it is easy for an attacker to hack the whole system. However, the information of neighborhood topology structure within an organization may be known to the network users in certainty, whereas in this paper we focus on the case when users have uncertain information about the neighborhood topology structure of the network under operation.

We make the following research contributions in this paper.

1. We present a general model for analyzing individual user security investments in a non co-operative Internet environment. In this regard, we study security investment games where 1) Internet users have incomplete information about the underlying neighboring network connectivity structure as well as on neighborhood security investment amounts and 2) Internet users account for the positive externalities posed by the investments of neighboring Internet users. The novelty of our model over existing security investment models lies in the fact that Internet users in our work account for neighborhood topological information uncertainty in order to decide on their optimal security investments. We discuss the implications of optimal user investments on risk management techniques such as *cyber-insurance*. Our model is based on the work in [27](See Section 3.)

2. We formulate our user security investment problems as Bayesian games of incomplete information and show the existence of a *monotonic symmetric Nash equilibrium* of user investments in these games. The results related to equilibrium show that under incomplete neighboring network topology information, better connected users choose lower efforts to exert and earn

higher payoffs than lesser connected peers when user utility functions exhibit strategic substitutes, i.e., are submodular. We also show the existence of monotonic symmetric equilibria in games of increased topological information and compare user investment behaviors in such games with those in which there is uncertainty regarding complete topological information. We discuss the implications of equilibria on the 'free-riding' behavior of Internet users. (See Section 4.)

2 Related Work

There have been few works related to security investments in the Internet. In this section, we give a brief overview of related work on Internet security investments. We divide the related work into the following three subdivisions:

2.1 Joint Investments in Cyber-Insurance and Self-Protection

The authors in [2][3] have analyzed self-protection[5] investments in Internet security under the presence of cyber-insurance, which is a form of a third-party risk transfer. These papers are based on the inter-dependent risk model in [9]. Under the assumption of users having complete network topology information of neighbors, the works show that (i) cyber-insurance incentivizes users to invest in self-protection, (ii) cyber-insurance entails optimal user investments both in insurance and in self-protection, and (iii) co-operation amongst Internet users result in higher user self-protection investments when compared to the case when users do not co-operate. However, attractive though the concept may seem, cyber-insurance may not be a market reality due to factors such as inter-dependent security, correlated risks, and information asymmetry between the insurer and the insured [4][5]. In addition, it is also infeasible for Internet users to have complete network topology information of their neighbors.

2.2 Investments In Self-Protection and/or Self-Insurance

For non cyber-insurance environments, in a recent series of works [7][6], the authors show that Internet users invest sub-optimally in self-protection measures under selfish environments when compared to the case when user co-operation is allowed. They account for positive network externalities posed by the security investments of Internet users but base their results by assuming users having complete network topology information of neighbors. However, as we have discussed previously, in a large network such as the Internet, having complete network topology information is infeasible. In addition, all the mentioned related works do not model the well-known security games mentioned in [1], that are in general played between attackers and defenders (non malicious Internet users) when externalities are present in a network. In this regard, the works in

---

[5] Protection using anti-virus and antispam softwares, firewalls, etc.

[11][12][8] [13] tackle the problem of optimal security investments (self-protection and self-insurance) and model the cited security games mentioned in [1], but do not account for any uncertainty of information that a user has regarding the underlying neighboring network topology, or regarding the security investments of other users. In a different type of investment work, the authors in [14] derive optimal liability schemes for increasing software security, where liability schemes are different types of investments by a vendor of a security software to prevent zero-day attacks. However, their work has no relation with the topological elements of a network, i.e., they do not model the network topology in evaluating the probability of zero-day attacks.

2.3   Tackling Information Uncertainty

The authors in [15][16][17][18][19] address certain challenges posed by information uncertainty related to security threats, response mechanisms, and associated expected losses and costs. As a set of contributions, the latter set of papers (i) derive bounds for the ratio of Internet user utilities with and without perfect information on risk parameters, (ii) model uncertainty in risk parameters like user security investments (self-protection and self-insurance), probability of attack, probability of risk propagation, as probability distributions, and (iii) propose Bayesian games of incomplete information to address the strategic interaction amongst Internet users under uncertain environments of risk information and analyze Nash equilibria in the games with their practical applications. However, the works do not consider network topology to be a parameter when users make a decision on their security investments.

In this paper, we advance previous research in security investments by jointly modeling (i) externalities due to user security investments (only self-protection), (ii) the fact that users have uncertain information regarding the connectivity structure of their neighboring nodes, and (iii) user uncertainty about security investments of their neighbors, to arrive at optimal user security investments. Thus, the novelty of our paper over existing security investment models lies in the fact that Internet users in our work account for neighborhood topological information uncertainty in order to decide on their optimal security investments.

3   Modeling Network Security Investment Games

In this section, we propose a general model for analyzing user network security investments using a game-theoretic approach when topological information needs to be accounted for. First, we model the user interaction network in the Internet. Second, we describe the utility/payoff function of the Internet users as a function of their strategies/actions, which are nothing but the security investments of users. Finally, we explain the information structure of Internet users with respect to the underlying connectivity structure of their neighbors and their security investments, and highlight the games of investments that result from the information structure.

3.1 Network Structure

We consider a set $N = \{1, ..., n\}$ of n Internet users, where the connections between them form a graph $G = (V, E)$, where $v_{ij} = 1$ (edge weight between nodes (users) i and j) if the utility of user i is affected by the security investment of user j, i being not equal to j, and 0 otherwise. Let $N_i(v) = \{j | v_{ij} = 1\}$ denote the set of all the one hop neighbors of i, where $v \in \{0, 1\}^{n \times n}$ is a matrix of connections amongst nodes. We also consider the k-hop neighbors of node i and denote the set by $N_i^k(v)$. This set consists of all the nodes that are within k-hops of node i, where $k \geq 1$. Inductively, we have the following relationships between $N_i^k(v)$ and $N_i(v)$:

$$N_i^1(v) = N_i(v). \tag{1}$$

$$N_i^k(v) = N_i^{k-1}(v) \cup (\cup_{j \, \epsilon \, N_i^{k-1}(v)} N_j(v)). \tag{2}$$

We represent the degree of a node i by d_i, where d_i equals $|N_i(v)|$. In this paper, we assume that each user has perfect knowledge about his own degree but does not have complete information about the degrees of his neighbors. (More on degree information structure in Section 3.3.)

3.2 User Strategies and Payoffs

In this paper we consider two types of non co-operative security investment games concerning the case when Internet users have incomplete information on the topology of their neighbors and their security investments: (1) *sum of efforts game* - the users are selfish and invest to maximize their own utilities, with the security strength of an individual user depending on the sum of security investments of himself and his neighboring individual nodes and 2) *best-shot game* - the users are selfish and invest to maximize their own utilities, with the security strength of an individual user network depending on the security investments of the most robust node/s amongst his neighbors. In both these types of games, each Internet user is a player and his strategy is the amount of security investment he makes. We assume here that the strategy/action of each user i is x_i and lies in the *compact*[6] set $[0, 1]$. We model the utility/payoff to each user i as U_i, which is a function of the security investments made by himself and his one hop neighbors. Thus, $U_i = U_i(x_i, \overrightarrow{x}_{N_i(v)})$, where $\overrightarrow{x}_{N_i(v)}$ is the vector of security investments of the one hop neighbors of user i. From the structure of user utility functions, we observe that two players having the same degree will have the same utility function. We also model the concept of a positive externality as it forms an integral part of game analyses. A positive externality to a user from its one hop neighbors results when the latter invest in security, thereby improving the individual security strength of the user. We represent the concept mathematically in the following manner: we say that a payoff function exhibits positive externalities if for each U_i and for all $\overrightarrow{x} \geq \overrightarrow{x}', U_i(x_i, \overrightarrow{x}) \geq U_i(x_i, \overrightarrow{x}')$, where $\overrightarrow{x}$ and $\overrightarrow{x}'$ are the vectors of security investments of one hop neighbors of user i.

---

[6] In mathematical analysis, a compact set is one that is closed and bounded.

In scenarios where the security strength of a user i depends on the sum of investments of himself and other neighboring users, i.e., as in a *sum-of-efforts* game, we mathematically formulate i's utility/payoff function as follows:

$$U_i(x_1, ..., x_{d_i}) = f\left(x_i + \lambda \sum_{j=1}^{d_i} x_j\right) - c(x_i), \tag{3}$$

where $f(\cdot)$ is a non-decreasing function of $\overrightarrow{x}$, $c(x_i)$ is the cost incurred by user i for putting in effort x_i to make his system more robust, and λ is a real scalar quantity which determines the magnitude of the positive externality experienced by user i due to the security investments made by his one-hop neighbors.

The situation where the security strength of a user depends on the investments made by the strongest neighbor/s, i.e., as in a *best-shot game*, can be modeled as a *special case* of the situation where user security strength depends on the sum of the security investments of his neighbors. We first note that from user i's perspective, the strongest-neighbor situation implies that as long as there is a neighboring node/s that is secure, user i is safe. In Section 1 we have already cited censorship resistant networks and Internet backbone networks to be examples of networks where the former situation might arise leading to a best-shot game. We had also given an example of how the best-shot scenarios arising in these networks can be modeled as a graph to reflect the 'user-neighbor' concept. Once we have modeled a best-shot scenario as a graph, we fix the strategy space of individual users to $\{0, 1\}$ and make $f(0) = 0$ and $f(y) = 1$ for all $y \geq 1$. A binary strategy space of $\{0, 1\}$ implies that each user decides either to invest or not to invest. If a user or any of his neighbors invest, the former is safe, else he is not. We observe that the 'sum of investments' game gets converted to a best-shot game. In this case user i's payoff follows the following equation:

$$U_i(x_i, (\overrightarrow{x}, 0)) = U_i(x_i, \overrightarrow{x}), \ \forall (x_i, \overrightarrow{x}) \, \epsilon \, [0, 1]^{d_i+1}. \tag{4}$$

Equation (4) implies that adding a link to a neighbor who invests zero amount in security mechanisms is equivalent to not having the neighbor. This fact captures the intuition of a best-shot game.

In this paper we assume the utility functions of players in both the game types to be of the *strategic substitute* type exhibiting *positive externalities*. We say that a utility/payoff function exhibits strategic substitutes or is *submodular* if it exhibits the property of decreasing differences, i.e., $U_i(x_i, \overrightarrow{x}) - U_i(x'_i, \overrightarrow{x}) \leq U_i(x_i, \overrightarrow{x}') - U_i(x'_i, \overrightarrow{x}')$. The practical interpretation of a strategic substitute as applicable to this paper is that an increase in the security investments of a user's neighbors reduces the marginal utility of the user, thus de-incentivizing him from investing. This happens due to the positive externality a neighbor exerts on the user through his own investments.

3.3 Information Structure

In this paper we assume that each Internet user (player) knows his own degree[7] but does not have perfect information regarding the degree of his neighbors. It has already been shown by Newman in [20] that nodes (Internet users) in an Internet like network exhibit degree correlations[8]. In this regard, we account for the degree correlations between the neighboring nodes of a user i in our model, i.e., when a user decides on his strategy, he accounts for the amount of information he has on the degree of his neighbors. Information on degree correlations is important as it guides a user to making better security investments when compared to the situation when he has no information about the correlations. For example, a user having the knowledge that his neighbors are connected to a high number of nodes would invest differently than he would if he knows that his neighbors are connected to few nodes.

Let the degrees of the neighbors of user i be the vector $\overrightarrow{d}_{N_i(v)}$, whose dimension is d_i. We assume that user i does not know the vector $\overrightarrow{d}_{N_i(v)}$ but has information regarding its probability distribution, i.e., he knows the value of $P(\overrightarrow{d}_{N_i(v)}|d_i)$. We assume that each player in the network under consideration begins with *ex-ante symmetrical beliefs* and *common priors* regarding the degree of his neighbors. The players may end up with different positions in a network and conditional beliefs, but these beliefs are only updated based on their realized position (their own degree) and not on their identities. Thus, arises a family of conditional distributions, $\mathbf{C} \equiv \{[P(\overrightarrow{d}|d)]_{\overrightarrow{d} \, \epsilon \, N^d}\}_{d \, \epsilon \, N}$, where $\overrightarrow{d}$ is a vector of degrees of the neighbors of a node and d is the degree of a given node.

We model the strategic interactions between the players of the network as a *Bayesian game of incomplete information*. The type space of the Bayesian game is the user knowledge on the potential degrees of his neighboring players. The strategy for each player is his security investment conditioned on the knowledge of the degrees of his neighbors, and the payoff function for each player is as defined in Section 3.2, which depends on the game being a sum of investments game or a best-shot game. Assuming that S is the set of possible investments a user could make, the strategy for player i is a mapping $\gamma_i : \{0, 1, ..., n-1\} \rightarrow \Omega(S)$, where $\Omega(S)$ is the set of distribution functions on S.

We already noted that for a player, his conditional distributions concerning the neighbors' degrees can vary with his own degree. According to our model, players may have different number of neighbors, and the degrees of the neighbors are correlated with each other due to the well-known result in [20]. Thus, the dimension of the vector of degrees of its neighbors may vary from player

---

[7] We restrict ourselves to having perfect knowledge *only* about a node's own degree because (i) no user has zero knowledge about the Internet topology, which is static, and thus we decide to model partial knowledge of a user, and (ii) for simplicity of analysis we just assume one level of complete information with regard to the neighbors of a node.

[8] Newman show through empirical studies that technological and Internet networks exhibit negative degree correlation whereas social networks exhibit positive degree correlation.

to player. In order to address correlation amongst vectors of different dimensions, we adopt the technique of 'affiliation' from the domain of statistics [21]. Affiliation is used to track the correlation patterns of groups of random variables, given the complicated interdependencies that might be present between them. A positive affiliation indicates that higher levels of one variable (in this case a player's degree) implies higher levels of all other variables (in this case a player's neighbors' degrees). On the other hand, a negative affiliation indicates that higher levels of one variable implies lower levels of other variables. Next, we mathematically describe affiliation as appropriate to our work.

Mathematical Description of Affiliation: Given a player i with degree d_i, enumerate the degrees of i's neighbors as $\overrightarrow{d}_{N_i(v)} = (d_1, \ldots, d_{d_i})$. Now consider a function $F : \{0, 1, \ldots, n-1\}^m \to R$, where $m \leq d_i$. Let the following relation hold:

$$E_{P(\cdot | d_i)}[F] = \sum_{\overrightarrow{d}_{N_i(v)}} P(\overrightarrow{d}_{N_i(v)} | d_i) F(d_1, \ldots, d_m). \tag{5}$$

In Equation (5) we fix a subset $m \leq d_i$ of user i's neighbors, and then take the expectation of F operating on their degrees. We say that the family of distributions $\mathbf{C}$ exhibits positive affiliation if, for all $k' > k$, and any non-decreasing $F : \{0, 1, \ldots, n-1\}^k \to R$, we have

$$E_{P(\cdot | k')}[F] \geq E_{P(\cdot | k)}[F], \tag{6}$$

and $\mathbf{C}$ exhibits negative affiliation if

$$E_{P(\cdot | k')}[F] < E_{P(\cdot | k)}[F], \tag{7}$$

for all $k' > k$, and any non-decreasing $F : \{0, 1, \ldots, n-1\}^k \to R$. The concept of affiliation simply implies that higher degrees for a given player are correlated with higher of lower degree (depending on whether the affiliation is positive or negative) of all her neighbors.

Practical Implications of Optimal Security Investments: As mentioned in [2], cyber-insurance incentivizes Internet users to invest in self-defense investments. However, self-defense investments have a direct impact on insurance premiums as high investments would result in lesser premiums for a user and low investments would lead to a user paying higher premiums. We will discuss more on the relation between premium amounts and user welfare in Section 4.

4 Game Analysis

In this section, we analyze the *symmetric* Bayesian game of incomplete information played between the users of the network under operation. In any symmetric game, the player payoffs for playing a particular strategy depend only on the strategies of other players and not on who is playing the strategies. In our game, symmetric equilibrium implies that players with the same network characteristic, i.e., network degree, choose the same strategy in a Bayesian Nash equilibrium.

The primary reasons why we consider only symmetric equilibria are (i) the network formation mechanism is anonymous and the population (ex., as in the Internet) is very large, and (ii) the payoff function is strictly concave in its own actions. Under these two conditions, all users of any given degree face the same decision problem and due to the nature of their utility functions choose an unique optimal strategy. We investigate the *existence*, *uniqueness*, and *monotonicity* of our game equilibria. In studying monotonicity of equilibria, we investigate the changes in the best response investment magnitude of a user when other users in the network increase/decrease their best response investment amounts. We also investigate the effect of the increase/decrease in user degrees on the equilibria of the game. We initially give a mathematical definition of our Bayesian game and follow it up with the analysis and practical implications of our game equilibria.

4.1   Game Definition

Consider a player (Internet user) i having degree d_i in a *sum-of-efforts game* or a *best-shot game*. Each player chooses a security investment amount from the set S as its strategy, where S is as defined in Section 3.3. Let $d\rho_{-i}(\overrightarrow{\gamma}, d_i)$ be the probability density over $x_{N_i(v)} \epsilon S^{d_i}$ induced by the beliefs $P(\cdot|d_i)$ held by player i over the degrees of his neighbors, combined with the strategies played via $\overrightarrow{\gamma}$, the vector of strategies of other users in the network. Let

$$EU_i(x_i, \overrightarrow{\gamma}, d_i) = \int_{x_{N_i(v)} \epsilon S^{d_i}} U_i(x_i, x_{N_i(v)}) d\rho_{-i}(\overrightarrow{\gamma}, d_i), \qquad (8)$$

where $EU_i(x_i, \overrightarrow{\gamma}, d_i)$ is the expected utility/payoff of player i with degree d_i and investment x_i when other players choose strategy $\overrightarrow{\gamma}$. The *Bayesian Nash equilibrium* of the game is a strategy vector that *maximizes* the expected utility of each player in the network [22][23]. We note here that the above formulation of a Bayesian game is valid only for continuous payoff functions, which can arise for non-discrete strategy sets. The case for discrete sets has been analyzed by [27]. What is important from this paper's point of view is to relate network structure and user utilities to the Nash equilibria results, which in turn requires us to relate user strategies (security investments) to their degrees. In this regard, we next provide some basic definitions related to our problem model. which would be used in the analysis of game equilibria.

Definition 1. A strategy $\overrightarrow{\gamma}$ is monotonically increasing in player degrees if $\overrightarrow{\gamma}(d')$ first-order stochastically dominates[9] $\overrightarrow{\gamma}(d)$ for each $d' > d$. Similarly,

---

[9] Let X and Y be two random variables representing risks. Then X is said to be smaller than Y in first order stochastic dominance, denoted as $X \leq_{ST} Y$ if the inequality $VaR[X; p] \leq VaR[Y; p]$ is satisfied for all $p \epsilon [0, 1]$, where $VaR[X; p]$ is the value at risk and is equal to $F_X^{-1}(p)$. First order stochastic dominance implies dominance of higher orders. We adopt the stochastic dominant approach to comparing risks because a simple comparison between various moments of two distributions may not be enough for a correct prediction about the dominance of one distribution over another.

a strategy $\overrightarrow{\gamma}$ is monotonically decreasing in player degrees if the domination relationship is reversed, for each $d' > d$.

Definition 2. For a given player i, we say that his expected utility function exhibits degree substitutability if

$$EU_i(x_i, \overrightarrow{\gamma}, d_i) - EU_i(x'_i, \overrightarrow{\gamma}, d_i) \leq EU_i(x_i, \overrightarrow{\gamma}, d'_i) - EU_i(x'_i, \overrightarrow{\gamma}, d'_i), \quad (9)$$

where $x_i > x'_i$, $d_i > d'_i$, and $\overrightarrow{\gamma}$ is non-increasing. Similarly for a given player i, we say that his expected utility function exhibits degree complementarity if

$$EU_i(x_i, \overrightarrow{\gamma}, d_i) - EU_i(x'_i, \overrightarrow{\gamma}, d_i) \geq EU_i(x_i, \overrightarrow{\gamma}, d'_i) - EU_i(x'_i, \overrightarrow{\gamma}, d'_i), \quad (10)$$

where $x_i > x'_i$, $d_i > d'_i$, and $\overrightarrow{\gamma}$ is non-decreasing.

We observe that the concepts of degree substitutability and complementarity are in relation to the marginal expected utilities of a player with increase in his degree. Degree substitutability states that if a high strategy (security investment) is less attractive than a low strategy, for a player of some degree, then the same is true for a player of a higher degree, when the strategy being played by other players is non-increasing. Similarly, degree complementarity states that if a high strategy is more attractive than a low strategy, for a player of some degree, then the same is true for a player of a higher degree, when the strategy being played by other players is non-decreasing. In a recent work, [24] have shown as sufficient conditions that when Equation 4 holds, the user utility functions exhibit strategic substitutes, and the neighbor affiliation of **C** is negative, degree substitution arises. However, the authors did not state these conditions as necessary to ensure degree substitutability. In our work, we only assume the sufficient conditions while considering degree substitutability because the payoff functions for the players in the sum-of-efforts and best-shot games exhibit the strategic substitute property. *We emphasize here that it is yet to be proved through theory or experiments that the the topology of the Internet at the user level exhibits degree substitutes. We assume in this paper that there exists a negative degree of neighbor affiliation (like in the case of degree correlations at the router level [20]) for the Internet at the user level. The analysis case for positive affiliation is an important open problem and is left for future work.*

4.2 Game Equilibria Results

In this section we state the results related to equilibria of our proposed Bayesian game of security investments, and analyze various practical implications of our results. As mentioned earlier, given a symmetric environment; i.e., players participate in a symmetric Bayesian game of security investments, we analyze *symmetric equilibria*. Apart from the reasons previously mentioned on why we address only symmetric game equilibria, asymmetric behavior seems relatively unintuitive, and difficult to explain in a one-shot interaction [25].

Lemma 1. *There exists a symmetric equilibrium in our proposed security investment game when user utility functions exhibit strategic susbstitutes, and the*

equilibrium is non-increasing, i.e., monotone decreasing.

Proof. In our game the players (Internet users) have identical strategy set S. The utility functions of each player is the same, and each player's beliefs about the degrees of its neighbors are ex-ante symmetric. Given that action set is compact and the utility/payoff function of users are continuous, there exists a mixed strategy Nash equilibrium of the Bayesian game [22][23]. Regarding monotonicity of equilibria, we use the degree substitute property to show that a player would play a monotone best-reply if the rest of the players play monotone strategies. Thus, the monotone strategies form a compact and convex set, and by the results in [28] there exists a monotonic equilibrium. **Q.E.D.**

Implications of Lemma 1: The degree substitutes property ensures that there is a game equilibrium that is monotonically decreasing. From a user point of view this implies that his investments monotonically decrease with increase in his own degree, which further implies low user investments on being well connected, leading to a free-riding problem. Assuming the existence of cyber-insurance markets, this problem can be tackled to incentivize well-connected users to invest optimally [2]. Under mandatory cyber-insurance, well-connected users would either pay high premiums or would invest more to avoid high premiums. In the case when there are multiple symmetric Nash equilibria (this case does not arise in best-shot games, It has been shown in [27] that best-shot Bayesian games have a *unique* pure strategy symmetric Nash equilibria which is monotone decreasing) that are *non-monotone*, it may prove good for overall network security because well connected users might put in more investment efforts even if it has high degree, in turn paying less insurance premiums. On the other hand, we cannot be sure if low degree users would exert high investment efforts for non-monotone equilibria.

Lemma 2. *Given that (1) $U_i(x_i, (\overrightarrow{x}, 0)) = U_i(x_i, \overrightarrow{x})$, $\forall (x_i, \overrightarrow{x}) \, \epsilon \, S^{d_i+1}$, for each player i and (2) degrees of neighboring nodes of users are independent, then strategic substitutes of user utility functions result in every symmetric equilibrium of our proposed Bayesian game of security investments being monotone decreasing.*

Proof. Let $\overrightarrow{\gamma}^*$ be the strategy played in equilibrium. Consider any $d \, \epsilon \, \{0, 1, ..., n\}$ and let $x_d = inf[\mathbf{supp}(\gamma_d^*)]$. If $x_d = 1$, then $x_{d'} \leq x_d$ for all $x_{d'} \, \epsilon \, \mathbf{supp}(\gamma_{d'}^*)$ for $d' > d$. Now let us assume $x_d < 1$. Then for any $x > x_d$, Equation 4 holding, and user utility functions exhibiting strategic substitutes, we have for player i

$$A \leq B. \tag{11}$$

Here

$$A = U_i(x, x_{dn_1}, ..., x_{dn_d}, x_s) - U_i(x_d, x_{dn_1}, ..., x_{dn_d}, x_s)$$

and

$$B = U_i(x, x_{dn_1}, ..., x_{dn_d}) - U_i(x_d, x_{dn_1}, ..., x_{dn_d})$$

, where $x_s \geq 0$. Given the assumption of stochastically independent neighbor degree distributions, we have

$$EU_i(x, \overrightarrow{\gamma}^*, d+1) - EU_i(x_d, \overrightarrow{\gamma}^*, d+1) < EU_i(x, \overrightarrow{\gamma}^*, d) - EU_i(x_d, \overrightarrow{\gamma}^*,). \quad (12)$$

Now we also know that for all x

$$EU_i(x, \overrightarrow{\gamma}^*, d) - EU_i(x_d, \overrightarrow{\gamma}^*, d) \leq 0. \quad (13)$$

Thus, we have for all $x > x_d$

$$EU_i(x, \overrightarrow{\gamma}^*, d+1) - EU_i(x, \overrightarrow{\gamma}^*, d+1) < 0, \quad (14)$$

which implies γ_d^* first order stochastically dominates γ_{d+1}^*. Iterating our argument, we arrive at the conclusion that γ_d^* first order stochastically dominates $\gamma_{d'}^*$ whenever $d' > d$. **Q.E.D.**

Implications of Lemma 2: Lemma 2 states the conditions under which all symmetric equilibria are monotone, and gives an insight on the topology of the network that could result in all symmetric equilibria being monotone. Lemma 1 only guarantees the existence of a single monotone equilibria when the network topology exhibits degree substitutes. Lemma 2 states that under independence of neighbor degree nodes (ex., as in a *Erdos-Renyi* random graph) every symmetric equilibria is monotone decreasing. However, topologies such as the Erdos-Renyi graph do not represent the Internet. Assuming every equilibrium would be monotone decreasing with respect to the Internet topology, it would enable cyber-insurance markets to flourish (provided that markets exist and cyber-insurance is made mandatory for Internet users). Thus, for user-level Internet topologies and for multiple non-monotone symmetric equilibria, the overall network security strength explanation follows as per the explanation in Lemma 1.

Lemma 3. *Suppose $U_i(x_i, (\overrightarrow{x}, 0)) = U_i(x_i, \overrightarrow{x}), \forall (x_i, \overrightarrow{x}) \epsilon S^{d_i+1}$, for each player i. If $\mathbf{C}$ is negatively affiliated and user utility functions exhibit strategic substitutes, then in every monotonically decreasing symmetric equilibrium of security investment of our proposed Bayesian game, the expected utilities of players are non-decreasing in degree.*

Proof. Let $\overrightarrow{\gamma}^*$ be an equilibrium strategy. Suppose that $x_d \epsilon \mathbf{supp}(\gamma_k^*)$ and $x_{d+1} \epsilon \mathbf{supp}(\gamma_{d+1}^*)$. Equation 4 implies that

$$U_i(x_d, x_{dn_1}, ..., x_{dn_d}, 0) = U_i(x_d, x_{dn_1}, ..., x_{dn_d}), \quad (15)$$

for all $x_{dn_1}, ..., x_{dn_d}$. Now since the user utilities exhibit positive externalities, it is true for all $x > 0$ that

$$U_i(x_d, x_{dn_1}, ..., x_{dn_d}, x) = U_i(x_d, x_{dn_1}, ..., x_{dn_d}). \quad (16)$$

Now for negative neighbor affiliation, we have

$$EU_i(x_d, \overrightarrow{\gamma}^*, d+1) \leq EU_i(x_d, \overrightarrow{\gamma}^*, d). \quad (17)$$

Since, γ_{d+1}^* is a best response in the network game, and that $x_{d+1} \, \epsilon \, supp(\gamma_{d+1}^*)$, we have

$$EU_i(x_{d+1}, \overrightarrow{\gamma}^*, d+1) \leq EU_i(x_d, \overrightarrow{\gamma}^*, d+1). \tag{18}$$

Thus, our result is proved. **Q.E.D.**

Implications of Lemma 3. Lemma 3 provides the relation between network degrees of users and their equilibrium payoffs, and identifies the conditions under which payoffs increase/decrease with network degree. Assuming that the Internet at the user level has negative neighbor degree affiliation, the lemma states that players with more neighbors exert lesser investment efforts and earn higher payoffs as compared to their less connected peers. In general, the lemma provides intuitions about user investments in games exhibiting strategic substitutes. Given that there exist markets for cyber-insurance and that insurance is made compulsory for Internet users, the overall network security strength explanation follows as per the explanation in Lemma 1.

4.3   The Case of Increased Topological Information

In this section, we investigate player investment behavior when he has more information regarding the network topology than just knowing his own degree and the conditional distributions of the degrees of his neighbors. Our goal is to compare user behavior regarding security investments between the 'less information' and 'more information' cases. We consider the case where players apart from knowing his own degree also knows the degrees of his neighbors. In the case when a player has *complete information* about the network topology, it has been shown in [26] that multiple pure strategy Nash equilibria may result (not necessarily monotone).

For the ease of exposition, we consider the simple comparison setting where the degrees of neighbors of a user are stochastically independent. This assumption also implies the independence of the degrees of neighbors of neighbors. Recall from Lemma 2 that under degree independence and the strategic substitute property of user utility functions, *all* symmetric Nash equilibria of the Bayesian game are monotonic decreasing. However, an interesting trend to study is whether all equilibria are monotone when the ''level of topological information' increases. Note that in the case of increased topology information, the type space of each player in the Bayesian game is of the form $(d_i; dn_{i1}, ..., dn_{id_i})$, where d_i is the degree of player i and $\{dn_i\}$'s are the degrees of i's neighbors. We have the following lemma regarding user behavior in the increased topological information scenario, i.e., the scenario where a user in addition to his own degree also knows the degree of his neighbors.

Lemma 4. *Suppose* $U_i(x_i, (\overrightarrow{x}, 0)) = U_i(x_i, \overrightarrow{x})$, $\forall (x_i, \overrightarrow{x}) \, \epsilon \, S^{d_i+1}$, *for each player i. When user utility functions exhibit strategic substitutes and neighbor degrees are stochastically independent, our proposed Bayesian game of security investments has at least one symmetric equilibrium that is monotone decreasing.*

Proof. The proof of this lemma follows from the same logic as that in Lemma 1, i,e., the best-response of a player to a monotone decreasing strategy by all other players is monotone decreasing, given that the set of monotone strategies is convex and compact. The latter condition guarantees the existence of equilibrium. The proof details follow a similar method as proposed in Proposition 10 of [24]. **Q.E.D**

Implications of Lemma 4. The lemma states does not guarantee the existence of every symmetric equilibrium being monotone decreasing, when compared to Lemma 2. Thus, with increasing information, the flourishing of cyber-insurance markets and increments in overall network security might follow the same trends as in the case when users had less information.

A Note on Multiplicity of Nash Equilibria. We observe that our games might have multiple symmetric Nash equilibria, and that the chances of having multiple equilibria increases with the increase in the amount of topological information [27]. There are two important practical implications of this behavior: (i) it is difficult for a player to choose the *best* equilibrium as computing a single Nash equilibria is PPAD-complete [29], and (ii) there might be multiple cyber-insurance contracts for the multiple equilibria, and due to the intractability of computing any Nash equilibria, let alone the best equilibria, clients might go for a contract that either 'over-prices' or 'under-prices' them with regard to insurance premiums, thus leading to chances of market failure. Thus we observe a flip side to having more information on the network topology. However, in most practical cases (approximately 95% of the time) Nash equilibria is reached in polynomial time. Added to this is the fact that having more information on a large network is infeasible and therefore more chances that users will be involved in a game having a single or less number of Nash equilibria.

5 Cyber-Insurance - A Brief Note

In this section we give a brief overview of the need for cyber-insurance in Internet security since we draw practical implications of our model results with respect to this risk management technique.

The Internet has become a fundamental and an integral part of our daily lives. Billions of people nowadays are using the Internet for various types of applications. However, all these applications are running on a network, that was built under assumptions, some of which are no longer valid for today's applications, e,g., that all users on the Internet can be trusted and that there are no malicious elements propagating in the Internet. On the contrary, the infrastructure, the users, and the services offered on the Internet today are all subject to a wide variety of risks. These risks include denial of service attacks, intrusions of various kinds, hacking, phishing, worms, viruses, spams, etc. In order to counter the threats posed by the risks, Internet users[10] have traditionally

---

[10] The term 'users' may refer to both, individuals and organizations.

resorted to antivirus and anti-spam softwares, firewalls, and other add-ons to reduce the likelihood of being affected by threats. In practice, a large industry (companies like *Symantec, McAfee,* etc.) as well as considerable research efforts are centered around developing and deploying tools and techniques to detect threats and anomalies in order to protect the Internet infrastructure and its users from the resulting negative impact.

In the past one and half decade, protection techniques from a variety of computer science fields such as cryptography, hardware engineering, and software engineering have continually made improvements. Inspite of such improvements, recent articles by Schneier [30] and Anderson [31][32] have stated that it is impossible to achieve a 100% Internet security protection. The authors attribute this impossibility primarily to four reasons:

- New viruses, worms, spams, and botnets evolve periodically at a rapid pace and as a result it is extremely difficult and expensive to design a security solution that is a panacea for all risks.
- The Internet is a distributed system, where the system users have divergent security interests and incentives, leading to the problem of 'misaligned incentives' amongst users. For example, a rational Internet user might well spend $20 to stop a virus trashing its hard disk, but would hardly have any incentive to invest sufficient amounts in security solutions to prevent a service-denial attack on a wealthy corporation like an Amazon or a Microsoft [33]. Thus, the problem of misaligned incentives can be resolved only if liabilities are assigned to parties (users) that can best manage risk.
- The risks faced by Internet users are often correlated and interdependent. A user taking protective action in an Internet like distributed system creates positive externalities [9] for other networked users that in turn may discourage them from making appropriate security investments, leading to the 'free-riding' problem [8][7][34][6].
- Network externalities affect the adoption of technology. Katz and Shapiro [35] have determined that externalities lead to the classic S-shaped adoption curve, according to which slow early adoption gives way to rapid deployment once the number of users reaches a critical mass. The initial deployment is subject to user benefits exceeding adoption costs, which occurs only if a minimum number of users adopt a technology; so everyone might wait for others to go first, and the technology never gets deployed. For example DNSSEC, and S-BGP are secure protocols that have been developed to better DNS and BGP in terms of security performance. However, the challenge is getting them deployed by providing sufficient internal benefits to adopting entities.

In view of the above mentioned inevitable barriers to 100% risk mitigation, the need arises for alternative methods of risk management in the Internet. Anderson and Moore [32] state that microeconomics, game theory, and psychology will play as vital a role in effective risk management in the modern and future Internet, as did the mathematics of cryptography a quarter century ago. In this regard, *cyber-insurance* is a psycho-economic-driven risk-management technique, where risks are transferred to a third party, i.e., an insurance company, in return for a fee, i.e.,

the *insurance premium*. The concept of cyber-insurance is growing in importance amongst security engineers. The reason for this is three fold: (i) ideally, cyber-insurance increases Internet safety because the insured increases self-defense as a rational response to the reduction in insurance premium [36][37][38][39], a fact that has also been mathematically proven by the authors in [40][2], (ii) in the IT industry, the mindset of 'absolute protection' is slowly changing with the realization that absolute security is impossible and too expensive to even approach while adequate security is good enough to enable normal functions - the rest of the risk that cannot be mitigated can be transferred to a third party [41], and (iii) cyber-insurance will lead to a market solution that will be aligned with economic incentives of cyber-insurers and users (individuals/organizations) - the cyber-insurers will earn profit from appropriately pricing premiums, whereas users will seek to hedge potential losses. In practice, users generally employ a simultaneous combination of retaining, mitigating, and insuring risks [42].

6 Conclusion

In this paper we proposed a security investment model for the Internet in which Internet users account for the positive externality posed to them by other Internet users and make security investments under situations when they do not have complete information about the underlying connecting topology of his neighbors and their security investments. Our model is based on a game-theoretic approach and we showed (i) the existence of symmetric monotone Bayesian Nash equilibria of efforts and (ii) better connected nodes choose lower efforts to exert but earn higher utilities with respect to security improvement when user utility functions exhibit strategic substitutes. Our results provided ways for Internet users to appropriately invest in security mechanisms under realistic environments of information uncertainty. Our results also clarified how the basic strategic features of the game - as manifest in the substitutes property - combine with different patterns of degree association to shape network behavior and user payoffs. We also stated the implications of our results to successfully realizing risk management schemes such as cyber-insurance, in practice. Finally, we compared between user investment behaviors in 'low information' and 'increased information' scenarios. As a part of future work, we plan to investigate security investments under an asymmetric environment, i.e., a game environment in which user payoffs depend not only on the strategy of other users but also on the identity of the users.

References

1. Varian. H.: System Reliability and Free Riding. ACM ICEC. (2003)
2. Lelarge. M., Bolot. J.: Economic Incentives to Increase Security in the Internet: The Case for Insurance. IEEE INFOCOM. (2009)
3. Pal. R., Golubchik. L.: Analyzing Self-Defense Investments In The Internet Under Cyberinsurance Coverage. IEEE ICDCS. (2010)
4. Bohme. R., Schwartz. G.: Modeling Cyberinsurance: Towards A Unifying Framework. WEIS. (2010)

5. Shetty. N., Schwarz. G., Feleghyazi. M., Walrand. J.: Competitive Cyberinsurance and Internet Security. WEIS. (2009)
6. Omic. J., Orda. A., Mieghem. V. P.: Protecting Against Network Infections: A Game-Theoretic Perspective. IEEE INFOCOM. (2009)
7. Jiang. L., Ananthram. V., Walrand. J.: How Bad are Selfish Investments in Network Security. IEEE Transactions On Networking. (2010)
8. Grossklags. J., Christin. G., Chuang. J.: Security and Insurance Management in Networks with Heterogenous Agents. ACM EC. (2008)
9. Kunreuther. H., Heal. G.: Interdependent Security. Journal of Risk and Uncertainty, 26. (2002)
10. Varian. H. R.: Microeconomic Analysis. Norton. (1992)
11. Fultz. N., Grossklags. J.: Blue versus Red: A Model of Distributed Security Attacks. International Conference on Financial Cryptography and Data Security. (2009)
12. Grossklags. J., Christin. N., Chuang. J.: Secure or Insure ? A Game-Theoretic Analysis of Information Security Games. WWW. (2008)
13. Grossklags. J., Christin. N., Chuang. J.: Security Investments(Failures) in Five Economic Environments.
14. Terrence. A., Tunca. I. T.: Who Should Be Responsible for Software Security? Management Science 57(5). (2011)
15. Grossklags. J., Johnson. B.: Uncertainty In Weakest-Link Security Game. GameNets. (2009)
16. Grossklags. J., Johnson. B., Christin. N.: The Price of Uncertainty in Security Games. Economics of Information Security and Privacy. (2010)
17. Grossklags. J., Johnson. B., Christin. N.: When Information Improves Information Security. Financial Cryptography and Data Security. (2010)
18. Johnson. B., Grossklags. J., Christin. N., Chuang. J.: Are Security Experts Useful? Bayesian Nash Equilibria for Network Security Games with Limited Information. ESORICS. (2010)
19. Johnson. B., Grossklags. J., Christin. N., Chuang. J.: Uncertainty In Interdependent Security Games. GameSec. (2010)
20. Newman. M. E. J.: Assortative Mixing in Networks. Phy.Rev.Lett. 89. (2002)
21. Esary. J. D., Proschan F., Walkup. W.: Association of Random Variables With Applications. Annals of Mathematical Statistics. 38(5). (1967)
22. Fudenberg. D., Tirole. J.: Game Theory. MIT Press. (1991)
23. Osborne. M. J., Rubinstein. A.: A Course in Game Theory. MIT Press. (1994)
24. Galeotti. A., Goyal. S., Jackson. M. O., Vega-Redondo. F., Yariv. L.: Network Games. Review of Economic Studies. 77(1). (2010)
25. Kreps. D.: Game Theory and Economic Modelling. Oxford University Press. (1990)
26. Bramoulle. K., Kranton. R.: Strategic Experimentation in Networks. Journal of Economic Theory. 135(1). (2007)
27. Galeotti. A., Goyal. S., Jackson. M. O., Vega-Redondo. F., Yariv. L.: Network Games. Technical Report. (2006)
28. Milgrom. P., Shannon. C.: Monotone Comparative Statics. Econometrica. 62. (1994)
29. Daskalakis. C.; Goldberg. P. W., Papadimitrou. C. H.: The Complexity of Computing A Nash Equilibrium. SIAM Journal of Computing. 39(1). (2009)
30. Schneier, B.: Secrets and Lies: Digital Security in a Networked World. John Wiley and Sons. (2001)
31. Anderson, R.: Why Information Security is Hard - An Economic Perspective. Annual Computer Security Applications Conference. (2001)

32. Anderson. R., Moore. T.: Information Security Economics and Beyond. Information Security Summit. (2008)
33. Varian. H.: Managing Online Security Risks. The New York Times, June, 1. (2000)
34. Ko-Miura. A. R., Yolken. B., Bambos. N., Mitchell. J.: Security Investment Games of Interdependent Organizations. Allerton. (2008)
35. Katz. M., Shapiro. C.: Network Externalities, Competition, and Compatibility. The American Economic Review. 75(3). (1985)
36. Kesan. J., Majuca. R., Yurcik. W.: The Economic Case for Cyber-Insurance: In Securing Privacy in the Internet Age. Stanford University Press. (2005)
37. Kesan. J., Majuca. R., Yurcik. W.: Cyberinsurance As A Market-Based Solution To The Problem of Cyber-Security: A Case Study. WEIS. (2005)
38. Scheier. B.: Its The Economics Stupid. WEIS. (2002)
39. Yurcik. W., Doss. D.: Cyberinsurance: A Market Solution To The Internet Security Market Failure. WEIS. (2002)
40. Lelarge. M., Bolot. J.: Cyberinsurance As An Incentive for Internet Security. WEIS. (2008)
41. Majuca. R. P., Yurcik. W., Kesan. J. P.: The Evolution of Cyberinsurance. Information Systems Frontier. (2005)
42. Schneier. B.: Insurance and the Computer Industry. Communications of the ACM. 44(3). 2001
43. Honeyman. P., Schwarz. G. Interdependence of Reliability and Security. WEIS. (2007)
44. Neumann. J. V., Morgenstern. O.: Theory of Games and Economic Behavior. Princeton University Press. (2009)
45. Mascollel. A., Winston. M. D., Green. J. R.: Microeconomic Theory. Oxford University Press. (1985)
46. Hau. A.: When is A Coinsurance-Type Insurance Policy Inferior or Even Giffen. Journal of Risk and Insurance. 75(2). (2008)
47. Lelarge. M., Bolot. J.: A Local Mean Field Analysis of Security Investments in Networks. ACM NetEcon. (2008)
48. Lelarge. M., Bolot. J.: Network Externalities and The Deployment of Security Features and Protocols in the Internet. ACM SIGMETRICS. (2008)
49. Internet Wikipedia Source. Information Asymmetry.
50. Pal. R., Golubchik. L.: Pricing and Investments in Internet Security. Arxiv. (2011)