On Differentiating Cyber-Insurance Contracts *A Topological Perspective*

Ranjan Pal
University of Southern California
Email: rpal@usc.edu

Pan Hui
HKUST and Deutsch Telekom Laboratories
Email: pan.hui@telekom.de

***Abstract*—Recent literature on cyber-insurance has stressed the importance of discriminating network users on insurance contracts for the following reasons: (i) preventing adverse selection, (ii) partly internalizing the negative externalities of interdependent security, (iii) achieving maximum social welfare, (iv) helping a risk-averse insurer to distribute costs of holding safety capital among its clients, and (v) insurers sustaining a fixed amount of profit per contract. Thus, an important problem is studying ways to appropriately execute the user discrimination process. In this paper we take a network topological perspective and propose a technique (mechanism) to pertinently contract discriminate insured network users. We mathematically show that the Bonacich/Eigenvector centralities of network users is an appropriate parameter for differentiating insurance clients.**

***Keywords:* cyber-insurance; contract discrimination; centrality**

I. Introduction

The cyberspace has become a fundamental and an integral part of our daily lives. Billions of people nowadays are using the electronic medium for various types of applications. However, all these applications are running on networks, that were built under assumptions, some of which are no longer valid for today's applications, e,g., that all users on a given network can be trusted and that there are no malicious elements propagating in it. On the contrary, the infrastructure, the users, and the services offered on computer networks today are all subject to a wide variety of risks. These risks include distributed denial of service attacks, intrusions of various kinds, eavesdropping, hacking, phishing, worms, viruses, spams, etc. In order to counter the threats posed by the risks, network users[1] have traditionally resorted to antivirus and anti-spam softwares, firewalls, intrusion-detection systems (IDSs), 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 currently centered around developing and deploying tools and techniques to detect threats and anomalies in order to protect the cyber infrastructure and its users from the negative impact of the anomalies.

In the past one and half decade, risk 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, it is impossible to achieve a perfect/near-perfect cyber-security protection [2][8]. The impossibility arises primarily due to the following eight reasons: (i) non-existence of sound technical solutions, (ii) varied intentions behind network attacks, (iii) misaligned incentives between network users, security product vendors, and regulatory authorities, (iv) externalities and the free-riding problem, (v) customer lock-in and first mover effects of vulnerable security products, (vi) difficulty to measure risks, (vii) the problem of a lemons market [1], and (viii) liability shell games played by product vendors. In view of the above mentioned inevitable barriers to 100% risk mitigation, the need arises for alternative methods of risk management in cyberspace. In this regard, security researchers in the recent past have identified *cyber-insurance* as a potential tool for effective risk management.

Cyber-insurance is a technique via which network user risks are transferred to an insurance company (e.g., ISP, cloud provider.), in return for a fee, i.e., the *insurance premium*. Proponents of cyber-insurance believe that in the *long run*[2], cyber-insurers would have a better estimate of risk values by covering different types of risks and this in turn would entail the design of insurance contracts that would shift appropriate amounts of self-defense[3] liability on the clients, thereby making the cyberspace more robust. Cyber-insurance will also lead to a market solution that will be aligned with economic incentives of cyber-insurers, users (individuals/organizations), policy makers, and security software vendors, i.e., the cyber-insurers will earn profit from appropriately pricing premiums, network users will seek to hedge potential losses by jointly buying insurance and investing in self-defense mechanisms, the policy makers would ensure the increase in overall network

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

[2] A certain amount of time, not necessarily large.

[3] Self-defense implies the efforts by a network user to secure his system through technical solutions such as anti-virus and anti-spam softwares, firewalls, using secure operating systems, etc.,

978-3-901882-50-0 ©2013 IFIP

security, and the software vendors could go ahead with their first-mover and lock-in strategies as well as experience an increase in their product sales.

A. Research Motivation

Recent research on cyber-insurance has stressed on the need to contract discriminate network users due to the following reasons [6][8][3][10]:

- *Preventing adverse selection* - conditioned on the fact that cyber-insurers can observe or stochastically estimate the security investment of their clients, premium discrimination (in the form of fines and rebates) will mitigate the adverse selection problem.
- *Partly internalizing the negative externalities of interdependent security* - users who do not invest pertinent amounts in network security pose increased risk to others in the network and would pay more for insurance than a user who invests considerable amounts in security and generates positive network externalities.
- *Achieving maximum social welfare* - one of the ways in which a social planner (e.g., a monopolistic cyber-insurer) could maximize social welfare is by premium discriminating clients (in the form of fines and rebates). The insurer provides a contract to a client based on the condition that when the latter files a claim and is found to invest non-considerable amounts in security, he needs to pay a fine atop his premium. The converse holds true for a user who is found to invest considerable amounts in security, i.e., he gets a rebate.
- *Distributing costs of holding safety capital* - in a correlated risk environment such as the Internet, an insurer cannot afford to be risk-neutral as there are chances it might go bankrupt due to expected aggregate losses in a period being more than what it could afford to compensate. As a result it might hold a safety capital for a certain cost and make sure that the cost is distributed amongst the clients in an appropriate manner. This would lead to contract differentiation amongst its clients.
- *Insurer profits* - in imperfectly competitive, regulated markets insurers can afford to earn a fixed amount of profit per contract through premium loading. The amount of profit per user contract would vary from user to user leading to overall contract differentiation amongst the users.

B. Research Contribution

In this paper we propose a technique (mechanism) based on the topological location of users that allows cyber-insurers to appropriately contract discriminate their clients. We mathematically justify via a game-theoretic analysis that network users invest in proportion to their Bonacich/Eigenvector centralities under the Nash equilibrium (and in turn generate proportional amount of network externalities), and as a result cyber-insurance contracts should be discriminated based on a user's network centrality.

To the best of our knowledge, this is the first work to consider ways to appropriately differentiate cyber-insurance contracts amongst network users.

II. System Model

We consider a single cyber-insurer providing full or partial of coverage to its clients at certain premiums. The premium and coverage values per client is set after a claim is filed by the latter. We assume that the insurer can either observe or stochastically learn the security investment amount of its clients while deciding on the (premium, coverage) pair. We do not model the insurance parameters in this work, and only consider the pre-insurance buying stage, i.e., the stage where the network users invest in self-defense mechanisms.

Each network user (insurance client + non-insured user) is risk-averse and invests in self-defense mechanisms to a certain extent. Each user also possess a *Von Neumann-Morgenstern* utility function $u(\cdot)$ that is twice continuously differentiable, and is an increasing function of the self-defense investments of all users in the network. A network user is a part of a static communication network N of n nodes. The edges (links) of the network are assumed to have weights l_{ij} denoting the externality effect of node j's investments on node i. Network N is characterized by the weighted $n \times n$ matrix $\mathbf{L}$ with non-negative entries l_{ij}. We assume here that $\mathbf{L}$ is a column stochastic matrix, i.e.,$\sum_i l_{ij} = 1, \forall j$, with $l_{ii} = 0$ for all i. In this paper we will deal with centrality aspects of a communication network when relating network topology effects with contract differentiation parameters. Node centrality is a standard graph theoretic measure to evaluate the relative importance a node (user) has on the overall graph/network. In this work, node centrality maps to the externality effects a node investment has on other network nodes considering his own topological location. For the purposes of analysis, we adopt the *eigenvector* and *Bonacich* centrality measures [4] in this paper, which are popular centrality standards in graph theory. Both these measures assign relative importance scores to all nodes in a network based on the concept that connections to high-scoring nodes contribute more to the centrality score of the node in question than equal connections to low-scoring nodes, which is likely the case when we consider externality effects due to self-defense investments made by a user in a certain network location. We assume here that a cyber-insurer has complete information about the network topology. An example of such a cyber-insurer could be an ISP or any third-party insurance provider who buys topological information from an ISP.

III. Mechanism and Its Justification

In this section, we first define the statement of our mechanism that enables a cyber-insurer to contract discriminate its clients. We then provide a theoretical justification of our mechanism being appropriate, via an investment game analysis.

Mechanism: *User cyber-insurance contracts should be differentiated in accordance to the Bonacich/eigenvector centrality of the user in a given communication network.*

Mechanism Justification: We define the following non co-operative investment game played by the users in a network - Each user i invests an amount $x_i \geq 0$ in self-defense investments. He intends to maximize his own utility, which is expressed via the following optimization problem.

$$argmax_{x_i} u_i(x_1, ..., x_n) = x_i - \frac{1}{2}cx_i^2 + \gamma \sum_{j \neq i} l_{ij} x_i x_j.$$

Here $c > 0$ is a marginal cost parameter and γ is an investment spillover parameter. The interpretation of the utility function for each user is a combination of three things. First, we have a linear own-effort effect, which we normalize to have a unity coefficient. Second there is a convex cost in own effort introduced by the quadratic second term and parameterized by c. We assume that each user has the same marginal cost of effort. Finally, there are network complementarities. Each user $j \neq i$ through his self-defense investments presents an externality effect of l_{ij} on user i. The benefit i receives from j is increasing in x_i and x_j, and his total benefit is $\gamma \sum_{j \neq i} l_{ij} x_i x_j$. The marginal benefit to i of investing in self-defense is increasing in the investment level of other users connected to him via the communication network. We have the following theorem characterizing the Nash equilibrium of the game.

Theorem 1. *The investment game has a unique pure-strategy Nash equilibrium if and only if $\frac{\gamma}{c} < 1$, and the equilibrium vector is given as*

$$\overrightarrow{x^{eq}} = \frac{1}{c}\overrightarrow{b}(\boldsymbol{L}, \frac{\gamma}{c}), \tag{1}$$

where $\overrightarrow{b}(\boldsymbol{L}, \frac{\gamma}{c})$ is the vector of Bonacich centralities of $\boldsymbol{L}$ with parameter $\frac{\gamma}{c}$, and is expressed for non-negative $\boldsymbol{L}$ as

$$\overrightarrow{b}(\boldsymbol{L}, \frac{\gamma}{c}) = [\boldsymbol{I} - l\boldsymbol{L}]^{-1}\overrightarrow{1} = \sum_{k=0}^{\infty} (\frac{\gamma}{c})^k \boldsymbol{L}^k \overrightarrow{1}. \tag{2}$$

Proof. Consider the situation when $\frac{\gamma}{c} < 1$. $\frac{\gamma}{c} < 1$ ensures that the solutions to the first-order conditions, which are a system of linear equations, has a solution given by $\overrightarrow{x^{eq}}$ mentioned above. To show uniqueness, note that the payoffs are linear in the actions of other players, so when opponents play mixed strategies, only the expectations of their choices matter. Additionally there is a unique best response to any mixed strategy because the cost of effort is convex. Thus, the Nash equilibrium (NE) of the game is a pure strategy, and is equal to $\overrightarrow{x^{eq}}$. Now consider the case when $\frac{\gamma}{c} \geq 1$. We will prove by the method of contradiction that there exists no pure-strategy NE in this situation. Suppose there exists a NE $\overrightarrow{x^{eq}}$. The first-order conditions imply that

$$\overrightarrow{x^{eq}} = \alpha \mathbf{L} \overrightarrow{x^{eq}} + \frac{1}{c}\overrightarrow{1}. \tag{3}$$

By recursively substituting the entire right-hand side for $\overrightarrow{x^{eq}}$ we get, for every natural number K, the following.

$$\overrightarrow{x^{eq}} = \frac{1}{c}\left\{\sum_{k=0}^{K-1} \alpha^k \mathbf{L}^k\right\}\overrightarrow{1} + \alpha^K \mathbf{L}^K \overrightarrow{x}. \tag{4}$$

Since $\mathbf{L}$ is a column stochastic matrix, so is $\mathbf{L}^k$ for every k. In particular, column i of $\sum_{k=0}^{K} \alpha^k \mathbf{L}^k$ sums to $\sum_{k=0}^{K} \alpha^k \geq K$, and thus some entry of that column exceeds $\frac{K}{n}$. If we choose K such that $\frac{K}{cn}$ exceeds the minimum entry $\overrightarrow{x^{eq}}$, yields a contradiction. Finally, for the case when $\frac{\gamma}{c} \geq 1$, take a mixed-strategy NE $\overrightarrow{F}$, which is a vector of cumulative distribution functions. Create a pure strategy profile $\overrightarrow{x}$ where each j sets x_j to the expectation of his random investment under F_i. Using the linearity of expectations as well as the fact that the payoff of i is linear in each x_j, we find that function $u_i(x_i; \overrightarrow{x_{-i}})$ is the same as $u_i(x_i, \overrightarrow{F_{-i}})$. This gives us a pure strategy NE. Therefore there cannot be a mixed strategy NE when $\frac{\gamma}{c} \geq 1$. **Q.E.D.**

Theorem Intuition: The intuition for the theorem is that user self-defense investments are proportional to his network position as measured by the Bonacich centrality. The users who invest the most are ones who benefit the most from feedback loops of network complementarities. *Thus, it makes perfect sense for a cyber-insurer to contract discriminate a user based on his location in a communication network, in turn justifying our mechanism.* When $\frac{\gamma}{c} \geq 1$, the network spillovers are so big that there exists no Nash equilibrium because users would always want to invest more. One way to see this is that the investment game is a supermodular game so the best response mapping converges to the lowest Nash equilibrium when the mapping starts from the lowest action. When $\frac{\gamma}{c} \geq 1$, this dynamic is explosive enough for no equilibrium to exist.

The Bonacich centrality is closely related to the eigenvector centrality. We now formally define eigenvector centrality and show (as an extension to a theorem in [4]) via Theorem 2 that that Bonacich centrality converges to the eigenvector centrality when network feedback loops become large.

Definition. For a given non-negative path-connected matrix $\mathbf{L}$, the eigenvector centrality $\overrightarrow{e}(\mathbf{L})$ is the unique right column eigenvector of $\mathbf{L}$ with non-negative entries, and summing to 1. Uniqueness of the eigenvector follows from the *Perron-Frobenius* theory of non-negative matrices [9]. The individual centrality of each node is $e_i(\mathbf{L})$.

Theorem 2. *Given a non-negative, path-connected*[4]*, and aperiodic matrix $\boldsymbol{L}$ having largest eigenvalue of magnitude m, we have*

$$lim_{\frac{\gamma}{c} \to m^{-1}} \frac{\overrightarrow{b}(\boldsymbol{L}, \frac{\gamma}{c})}{B(\boldsymbol{L}, \frac{\gamma}{c})} = \overrightarrow{e}(\boldsymbol{L}), \tag{5}$$

where $B(\boldsymbol{L}, \frac{\gamma}{c})$ is the sum of the entries in $\overrightarrow{b}(\boldsymbol{L}, \frac{\gamma}{c})$.

[4] A path is a walk whose nodes are distinct.

Proof. Let $\mathbf{T} = \mu^{-1}\mathbf{L}$. Aperiodicity of $\mathbf{L}$ implies that $\mathbf{T}^k$ has a positive diagonal entry for large enough k [5]. This implies that all eigenvalues of $\mathbf{L}$ are smaller that μ [9]. This implies that $\mathbf{G}$ = $lim_{k\to\infty}\mathbf{T}^k$, where $\mathbf{G}$ is defined as

$$\mathbf{G} = \frac{\overrightarrow{e}(\mathbf{L})\overrightarrow{e}(\mathbf{L}')'}{\overrightarrow{e}(\mathbf{L}')'\overrightarrow{e}(\mathbf{L})}, \tag{6}$$

where $\mathbf{L}$' is the transpose of $\mathbf{L}$. Our first step is to show that $lim_{a\to 1}(1-a)(\mathbf{I}-a\mathbf{T})^{-1}$ exists and equals $\mathbf{G}$. We then use this result to prove the theorem result. To achieve our first step, let $\delta > 0$. Choose a K large enough such that for all $k > K$, we have $||\mathbf{T}^k - \mathbf{G}|| < \frac{\delta}{2}$, and choose $a < 1$ such that $|\sum_{k=0}^{K}(1-a)a^k| < \frac{\delta}{4}$. Here $||\cdot||$ is the supremum norm on the n-th dimensional real space. According to the Neumann series and its convergence [9], the following holds.

$$(1-a)(1-a\mathbf{T})^{-1} = \sum_{k=0}^{\infty}(1-a)a^k\mathbf{T}^k. \tag{7}$$

Thus, we have from the triangle inequality that

$$||\sum_{k=0}^{K}(1-a)a^k\mathbf{T}^k - \mathbf{G}|| \le A, \tag{8}$$

where

$$A = \sum_{k=0}^{K}(1-a)a^k||\mathbf{T}-\mathbf{G}|| + \sum_{k=K+1}^{\infty}(1-a)a^k||\mathbf{T}-\mathbf{G}||.$$

Since $\mathbf{T}$ and $\mathbf{G}$ are stochastic, and that the matrix norm is at most 1, from the previous equation we have

$$||\sum_{k=0}^{K}(1-a)a^k\mathbf{T}^k - \mathbf{G}|| \le \delta. \tag{9}$$

Thus, we prove the first step in our goal to prove the theorem. Now we know that

$$(1-a)\overrightarrow{b}(\mathbf{T},a) = (1-a)(\mathbf{I}-a\mathbf{T})^{-1}\overrightarrow{1}. \tag{10}$$

Therefore for any $\epsilon > 0$, there exists a $\delta > 0$ so that the following inequation holds: $||(1-a)(\mathbf{I}-a\mathbf{T})^{-1} - \mathbf{G}|| < \delta$, which implies for all i that

$$|\frac{b_i(\mathbf{T},a)}{B(\mathbf{T},a)} - \frac{\sum_j G_{ij}}{\sum_{j,k} G_{jk}}| < \epsilon. \tag{11}$$

Recalling that $\frac{\sum_j G_{jk}}{\sum_{j,k} G_{jk}} = e_i(\mathbf{T})$, we have using the proof of the first step that

$$|\frac{b_i(\mathbf{T},a)}{B(\mathbf{T},a)} - \overrightarrow{e}(\mathbf{T})| < \delta. \tag{12}$$

This completes the proof. **Q.E.D.**

Theorem Intuition. Bonacich centrality of user i is computed by starting with a baseline centrality of 1 (corresponds to the linear own-effort term in our investment game), and sums all walks[5] starting at i, with walks of length k getting weight $(\frac{\gamma}{c})^k$. The eigenvector centrality measures relative node importance by giving equal weights to all walks starting at i. The higher the value of $\frac{\gamma}{c}$, greater is the importance of long walks for Bonacich centrality. In the limit, the baseline effect and the short-distance walks are completely insignificant. Thus, when the network feedback becomes large, the ratio of the Bonacich centralities converge to the ratio of eigenvector centralities.

In view of the result in Theorem 2, we infer that the connotations of the Nash equilibrium in Theorem 1 in regard to contract discriminating network users, exactly hold (in the limiting cases) when we consider the eigenvector centrality measure instead of the Bonacich centrality measure.

IV. Conclusion

In this paper we devised a technique that accounts for the topological location of a network user and enables a cyber-insurer to contract discriminate its clients. We showed that it is appropriate to discriminate user cyber-insurance contracts based on their Bonacich/Eigenvector centralities. The rationale behind our result arises from the fact that users tend to optimally invest in security mechanisms proportion to their Bonacich/Eigenvector centralities, in turn generating proportional amounts of network externalities. Thus, it is fair to contract discriminate users based on these network centrality measures.

References

[1] G. A. Akerlof. The market for lemons - quality uncertainty and the market mechanism. *Quarterly Journal of Economics*, 84(3), 1970.

[2] R. Anderson and T. Moore. Information security economics and beyond. In *Information Security Summit*, 2008.

[3] R. Bohme and G. Schwartz. Modeling cyber-insurance: Towards a unifying framework. In *WEIS*, 2010.

[4] P. B. Bonacich. Power and centrality: A family of measures. *American Journal of Sociology*, 92, 1987.

[5] R. Durett. *Probability Theory and Examples*. Thomson, 2005.

[6] A. Hoffman. Internalizing externalities of loss prevention through insurance monopoly. *Geneva Risk and Insurance Review*, 32, 2007.

[7] M. O. Jackson. *Social and Economic Networks*. Princeton University Press, 2008.

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

[9] C. D. Meyer. *Matrix Analysis and Linear Algebra*. SIAM Press, 2000.

[10] N.Shetty, G.Schwarz, M.Feleghyazi, and J.Walrand. Competitive cyber-insurance and internet security. In *WEIS*, 2009.

[5] A walk in $\mathbf{L}$ [7] is a sequence of nodes $i_1, ...i_K$ not necessarily distinct such that $l_{i_k i_{k+1}} > 0$ for each $k \,\epsilon\, \{1, ..., K-1\}$. The length of a walk is K and its weight is $\Pi_{k=1}^{K} l_{i_k i_{k+1}}$.