Cyber-Insurance for Cyber-Security
A Topological Take On Modulating Insurance Premiums

Ranjan Pal
USC, USA
rpal@usc.edu

Pan Hui
T-Labs, Germany
pan.hui@telekom.de

ABSTRACT

A recent conjecture in cyber-insurance research states that for compulsory monopolistic insurance scenarios, charging fines and rebates on fair premiums will incentivize network users to invest in self-defense investments, thereby making cyber-space more robust. Assuming the validity of the conjecture in this paper, we adopt a topological perspective in proposing a mechanism that accounts for (i) the positive externalities posed (through self-defense investments) by network users on their peers, and (ii) network location (based on centrality measures) of users, and provides an appropriate way to proportionally allocate fines/rebates on user premiums. We mathematically justify (via a game-theoretic analysis) that optimal fine/rebates per user should be allocated in proportion to the Bonacich or eigenvector centrality value of the user.

Keywords: cyber-insurance; fines; rebates; self-defense investment; Bonacich centrality; eigenvector centrality

1. INTRODUCTION

The cyberspace[1] has become a fundamental and an integral part of our daily lives. Billions of people nowadays are using the Internet and other computer networks 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 However, all these applications are running on networks, that were built under assumptions, some of which are no longer valid for today's applications, e,g., that all users on a given network can be trusted and that there are no malicious elements propagating in it.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[2] 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 [7]. The impossibility arises primarily due to the following seven 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, and (vii) the problem of a lemons market [1]. In view of the above mentioned inevitable barriers to 100% risk mitigation, the need arises for alternative methods of risk management in cyberspace. Anderson and Moore [2] state that microeconomics, game theory, psychology, social sciences, and law will play as vital a role in effective risk management in the modern and future cyberspace, as did the mathematics of cryptography a quarter century ago. 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*[3], 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[4] liability on the clients, thereby making the cyberspace more robust. The concept of cyber-insurance is also growing in importance for the following three reasons [8]: 1) ideally, cyber-insurance increases network user safety because the insured increases self-defense as a rational response to the increase in insurance premium, 2) 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, and 3) cyber-insurance will lead to a market solution that will

[1]It is the electronic medium of computer networks, via which online communication takes place.

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

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

[4]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.,

be aligned with economic incentives of cyber-insurers, users (individuals/organizations), and security software vendors, i.e., the cyber-insurers will earn profit from appropriately pricing premiums, network users will seek to hedge potential losses, and the software vendors could go ahead with their first-mover and lock-in strategies.

Research Motivation and Contribution: A vital aspect of designing optimal cyber-insurance contracts for heterogenous network users is to set appropriate premiums based on the user risk type[5] [4]. In a recent work [7], Lelarge and Bolot qualitatively state that for compulsory[6] monopolistic cyber-insurance environments, a cyber-insurer could incentivize risk-averse network users into making self-defense investments by charging fines atop fair premiums to high risk users, and providing rebates on fair premiums to low risk users. In this paper we take a quantitative approach to address the problem of appropriate premium modulation based on user risk type.

We adopt a topological perspective in proposing a mechanism that accounts for (i) the positive externalities posed (through self-defense investments) by network users on their peers, and (ii) network location (based on centrality measures) of users, and provides an appropriate way to proportionally allocate fines/rebates on user premiums. We state and mathematically justify (via a game-theoretic analysis) that optimal fine/rebates per user should be allocated in proportion to the Bonacich or eigenvector centrality value of the user.

2. SYSTEM MODEL

We consider a monopolistic cyber-insurer providing full coverage in a compulsory insurance setting. Each client (network user) is risk-averse and invests in self-defense mechanisms to a certain extent. The amount that a user invests contributes to his probability of facing a loss due to cyber-threats. A user's investment amount, in addition to his location in a communication network, determines his risk type. Each user also possess a *Von Neumann-Morgenstern* utility function $u(\cdot)$ that is twice continuously differentiable, and is a function of the self-defense investments of all users in the network. We assume that the cyber-insurer charges fines atop fair premiums to high risk users and provides rebates to low risk users. Each 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 fine/rebate allocation. Node centrality is a standard graph theoretic measure to evaluate the relative importance a node has on the overall graph/network. In this work, node centrality maps to the externality effects a node has on other network nodes. For the purposes of analysis, we adopt the *eigenvector* [3] and *Bonacich* [5] centrality measures 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 score of the node in question than equal connections to low-scoring nodes, which is ideally the case when we consider externality effects due to self-defense investments made by a user in a certain network location.

[5]A user is generally either of a high risk type or a low risk type, depending on the amount of risk he faces from cyber-threats.

[6]Compulsory cyber-insurance is necessary for an insurance market to exist. This fact has been stated in [7] and proven in [10].

3. MECHANISM AND ITS JUSTIFICATION

In this section, we propose a mechanism that helps a monopolistic cyber-insurer to proportionally allocate fines or rebates on user premiums based on the users' location in a communication network. First, we define our mechanism statement. We then provide a theoretical justification of our mechanism being appropriate, via an investment game analysis.

Mechanism: *Charge fines atop high risk user premiums and provide rebates on low risk user premiums, in proportion to the Bonacich/eigenvector centrality of the users 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 a 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. The latter statement makes perfect sense under compulsory insurance environments as they incentivize user self-defense investments. We have the following theorem characterizing the Nash equilibrium of the game. We omit the proof of the theorem due to lack of space.

Theorem 1. *The investment game has a unique 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*

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

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 allocate fines/rebates on fair premiums based on user 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 [5]) via Theorem 2 that that Bonacich centrality converges to the eigenvector centrality when network feedback loops become large. We omit the proof of the theorem due to lack of space.

Definition 2. 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 $e_i(L)$.

Theorem 2. *Given a non-negative, path-connected*[7]*, and aperiodic matrix $\boldsymbol{L}$ having largest eigenvalue of magnitude m, we have*

$$lim_{\frac{\gamma}{c} \to m^{-1}} \frac{\overrightarrow{b}(\boldsymbol{L}, \frac{\gamma}{c})}{B(\boldsymbol{L}, \frac{\gamma}{c})} = \overrightarrow{e}(\boldsymbol{L}), \tag{3}$$

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

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[8] 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 appropriately allocating fines/rebates to network users, exactly hold (in the limiting cases) when we consider the eigenvector centrality measure instead of the Bonacich centrality measure.

An interesting corollary of Theorem 2 is related to the investment share of a subset S of users in a communication network, when there are high investment spillovers. We define the investment share of a subset S of network users as

$$IS_S(\mathbf{L}, \frac{\gamma}{c}) = \frac{\sum_{i \,\epsilon\, S} x_i^{eq}}{\sum_{i \,\epsilon\, N} x_i^{eq}}, \tag{4}$$

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

[8]A walk in $\mathbf{L}$ [6] 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 $\Pi_{k=1}^{K} l_{i_k i_{k+1}}$.

where $\overrightarrow{x^{eq}}$ is the Nash equilibrium investment vector of users according to Theorem 1. We now state the corollary.

Corollary 1. *Given $\boldsymbol{L}$ as being path-connected and aperiodic, the investment share of a subset S of network users approaches the eigenvector centrality of S with respect to $\boldsymbol{L}$, as $\frac{\gamma}{c}$ approaches 1 in the limit, i.e.,*

$$lim_{\frac{\gamma}{c} \to 1} IS_S(\boldsymbol{L}, \frac{\gamma}{c}) = \overrightarrow{e}(\boldsymbol{L}). \tag{5}$$

4. CONCLUSION

In this paper, we proposed a mechanism that accounts for (i) the positive network externalities due to user self-defense investments, and (ii) user location in a communication network, in guiding a cyber-insurer to allocate appropriate fines/rebates on insurance premiums to its clients. We showed (via a game-theoretic analysis) that optimal fine (rebates) per user should be allocated in proportion to the Bonacich or eigenvector centrality value of the user.

The methodology in this paper is also applicable in the case when a cyber-insurer needs to provide proportional benefits to their clients for taking certain security related actions that generates positive effects in a network. For example, several phone companies nowadays are coming up with secure mobile OSs. These companies can tie up in a business venture with ISP insurance agencies like Deutsch Telekom or AT&T, who have complete topological information of their network. The ISP might proportionally reward a client (based on his centrality measure) adopting a secure OS by a certain phone company (by modulating their premiums), and in return get business commissions from the phone company for enabling its OS to become more popular.

5. 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: Where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society*, 367, 2009.

[3] C. Ballester, A. Calvo-Armengol, and Y. Zenou. Who's who in networks. wanted: The key player. *Econometrica*, 74, 2006.

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

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

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

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

[8] R. P. Majuca, W. Yurcik, and J. P. Kesan. The evolution of cyberinsurance. *Information Systems Frontier*, 2005.

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

[10] R. Pal, L. Golubchik, and K. Psounis. Aegis: A novel cyber-insurance model. In *IEEE/ACM GameSec*, 2011.