RATING SYSTEMS FOR ENHANCED CYBER-SECURITY INVESTMENTS

Jie Xu, Yu Zhang and Mihaela van der Schaar
University of California, Los Angeles

ABSTRACT[1]

Networked agents often share security risks but lack the incentive to make (sufficient) security investments if the cost exceeds their own benefit even though doing that would be socially beneficial. In this paper, we develop a systematic and rigorous framework based on rating systems for analyzing and significantly improving the mutual security of a network of agents that interact frequently over a long period of time. When designing the optimal rating systems, we explicitly consider that monitoring the agents' investment actions is imperfect and the heterogeneity of agents in terms of both generated traffic and underlying connectivity. Our analysis shows how the optimal rating system design should adapt to different monitoring and connectivity conditions. Even though this paper considers a simplified model of the networked agents' security, our analysis provides important and useful insights for designing rating systems that can significantly improve the mutual security of real networks in a variety of practical scenarios.

Index Terms— Networked agents, network security, rating systems, imperfect monitoring

1. INTRODUCTION

Establishing a secure network environment requires investments on security technologies (e.g. firewalls, access control etc.) from the agents (e.g. autonomous systems, internet service providers etc.) in the network. Nevertheless, self-interested agents are often tempted to reduce their own security investments in order to reduce their costs [1]. Therefore, a key challenge is how to design efficient incentive schemes to encourage security investments from networked agents. Our approach is exploiting the ongoing nature of the agents' interaction by constructing policies in which the current interactions depend on the past history of interactions within the collection and, in particular, on the extent to which the past behavior of an agent has been in accordance with the recommended behavior (e.g. make security investments and exchange secure traffic). For this, we propose rating systems using the general theory of repeated games [2]. The rating system is implemented by a Rating Agency (RA), which might be operated by a private entity or a governmental agency. In implementing the rating system, the RA collects and aggregates reports from the agents based on which it updates ratings of the agents. Then the RA uses these ratings to recommend security policies for the agents to follow. Particularly, agents reward/punish an agent by employing different security policies (e.g. outbound traffic filtering qualities) for the traffic sent to this agent depending on its rating. Note that the RA has no power to enforce these recommended policies. The agents will actually execute the recommended policies only if they prefer compliance rather than deviation in their self-interest. We say a rating system is *incentive-compatible (IC)* if it has this property. When designing the optimal rating system, we explicitly consider two important practical aspects of the network security problem: monitoring agents' actual security investment action is imperfect and agents are heterogeneous in terms of both generated traffic and underlying connectivity.

Our paper builds on existing research studying the security investment of a network of agents. This literature generally can be classified into two categories. The first category [3][4][5][6] only characterizes the performance loss of the interconnected agents at equilibrium, but does not design incentive schemes to achieve the socially optimal security level. The second category [7][8] designs incentive schemes to encourage security investment. However, these solutions are complex and induce strict social efficiency loss. Moreover, a limitation is that the interaction among agents is modeled as a one-shot game, thereby disregarding the repeated nature of their interaction. Rating or reputation schemes are widely applied to deal with incentive problems in online communities with self-interested users which are interacting repeatedly (i.e. are long-lived) [9][10][11]. Nevertheless, none of these schemes can be directly applied to network security problems because they fail to incorporate many specific features that are critical to characterize the networked agents.

The rest of this paper is organized as follows. Section 2 introduces the repeated security investment game and the incentive design problem. Section 3 describes the proposed rating system. Section 4 determines the optimal rating system parameters under various network scenarios. Section 5 provides illustrative results to highlight the features of the proposed rating system. Section 6 concludes the paper. Omitted proofs can be found in [12].

2. SYSTEM MODEL

We consider a network of agents sending traffic to each other, represented by a set $\mathcal{N} = \{1,2,...N\}$. Let $\lambda_{i,j} \geq 0$ be the traffic rate sent from agent i to agent j and assume $\lambda_{i,i} = 0$, $\forall i \in \mathcal{N}$. The aggregated outbound/inbound traffic of agent i are $\mu_i = \sum_{k=1}^{N} \lambda_{i,k}$ and $\nu_i = \sum_{k=1}^{N} \lambda_{k,i}$,

[1] Financial support was provided by the National Science Foundation under grant 0830556.

respectively. Traffic contains malware (e.g. spam, viruses etc.). In a passive protection system, an agent only deploys security technology that protects itself (e.g. inbound traffic control). In a proactive protection system, the agent can also deploy security technology that protects the agents that connect with it (e.g. outbound traffic control). Proactive protection is more effective because agents have improved control over their own devices and the traffic originating from them. The system designer (i.e. the rating agency) therefore aims to provide agents with incentives to deploy proactive security technology to enhance the overall security of the network.

We assume that without deploying the proactive security technology, each unit of the traffic contains malware with a probability $\overline{p} \in [0,1]$. The proactive technology can reduce this probability to $p \in [\underline{p}, \overline{p}]$ that is determined by the specific security policy, with $\underline{p}$ being the lowest achievable value due to technology constraints. Note that when an agent deploys the proactive technology, it is able to send traffic with different qualities to its receiving agents by choosing the security policies (e.g. by adjusting filtering sampling rates [13]). When the traffic contains malware, the receiving agents has to take recovery measures (e.g. patching), with c_r being the recovery cost per unit infected traffic.

In the security investment game, time is divided into periods of length T. At the beginning of each period, each agent is strategic in choosing to deploy the proactive technology or not by taking an action $a \in \mathcal{A} = \{0,1\}$, where "1" stands for "deploy" and "0" otherwise. The cost of the technology is c_l per unit time (as in [14]). Therefore, the deployment cost per period is $c_l T$. Without loss of generality, we normalize the costs and let $c_r = 1, c_l = c$. Agents are long-lived and discount the utility (the negative of the cost) of the next period by $e^{-\beta T}$ as in [2] where β is the discount ratio. Therefore, the dominant strategy of agents is $a = 0$ for each period since deploying the technology entails only investment expenditures but does not result in immediate benefit.

The objective of the system designer is to design incentive mechanisms to provide agents with incentives to deploy the proactive security technology to enhance the network security. For agent i, denote its security cost by $J(i \mid \pi) = p(i \mid \pi)\nu_i + a_i^{\pi} c$ where $p(i \mid \pi)$ is the average inbound traffic quality and a_i^{π} is the average deployment action under the incentive mechanism π. Let $J(\pi) = \sum_{i \in \mathcal{N}} J(i \mid \pi)$. The design problem is therefore:

$$\underset{\pi}{\text{minimize}} \quad J(\pi); \quad \text{subject to} \quad \pi \text{ is IC} \qquad (1)$$

We make the following assumption on the agent network.

Assumption: $c < (\overline{p} - \underline{p}) \max\{\nu_i, \mu_i\}, \forall i \in \mathcal{N}$.

It indicates that the "first-best" performance (the minimal security cost) of all possible incentive mechanisms, denote by J^{**}, is achieved when all agents deploy the technology. Therefore, $J^{**} = \underline{p} \sum_{i \in \mathcal{N}} \mu_i + Nc$.

3. PROPOSED RATING SYSTEM

In this paper, we design a simple but practical rating system aiming to minimize the overall security cost of the network and show whether the optimal performance can be achieved. We consider a simple binary rating set $\Theta = \{0,1\}$ for illustration purpose. (The analysis can be easily extended to multiple rating sets.) Each agent is assigned with a rating label according to its past security investment actions. The RA recommends different investment strategies (for brevity, we simply call this the recommended strategy) for the agents. The strategy σ_P recommends only agents in the subset $P \in \mathcal{P}$ to deploy the proactive security technology where $\mathcal{P}$ is the space of all subsets of the agent collection. We call $\sigma_{\mathcal{N}}$ the *full deployment strategy* (FDS) and all the other strategy the *partial deployment strategies* (PDSs).

If an agent deploys the proactive security technology, it can choose different security policies which lead to different traffic qualities ($p \in [\underline{p}, \overline{p}]$) for its receiving agents. The RA recommends a set of qualities $p_\theta, \forall \theta \in \theta$ that depend on only the receiving agents' ratings θ. We assume $p_1 \le p_0$ because the traffic of the receiving agents of high ratings should receive better qualities. Because the deployment cost does not depend on the specific set of traffic qualities, the agents will just (weakly) follow any qualities recommended by the RA and so p_1, p_0 are design parameters of the RA. However, if the agent choose "not deploy", then the quality of its sending traffic is fixed at $\overline{p}$.

A monitoring technology is a measure-valued map $\chi: \mathcal{A} \times \mathcal{A} \to \Delta(\mathcal{S})$, where $\chi(s \mid a, \tilde{a})$ denotes the conditional probability that a signal $s \in \{0,1\}$ was observed given that a was played by an agent when the recommended action is $\tilde{a}$. We assume that $\chi(0 \mid a, \tilde{a}) = \epsilon$ if $a \neq \tilde{a}$ and $\chi(1 \mid a, \tilde{a}) = 1 - \epsilon$ if $a = \tilde{a}$. Monitoring is thus imperfect in that there is an error probability that the observed action is different from the actual deployment action. The rating assessment rule, which is performed at the end of each period, decides how the ratings of the agents should be updated according to the monitored signal $\phi : \Theta \times \mathcal{S} \to \Theta$. Particularly, $\phi(\theta \mid s) = s$. Therefore, an agent that is monitored to be complying with the recommended strategy receives a high rating while an agent that is monitored to be deviating from the recommended strategy receives a low rating. Note that even if an agent

does not deploy the technology, its rating still can be high if the recommended strategy for it is "not deploy".

Under the proposed rating system, the design parameters are summarized by σ, p_1, p_0. In the following of this paper, we design the optimal parameters to minimize the overall security cost under various network environments.

3. OPTIMAL RATING SYSTEM DESIGN

We define the *critical traffic* of a subset P of the agent collection, which will play a critical role for the rating system design problem.

Definition 1: Consider any subset P of the agent collection $\mathcal{N}$. For an agent $i \in P$, let $\nu_i(P)$ be its aggregate inbound traffic originating from all agents in P. The critical traffic of P is $\underline{\nu}(P) = \min_{i \in \mathcal{P}} \nu_i(P)$.

3.1. Optimal security policies

We first fix the recommended strategy to be σ_P and study the optimal security policies (reflected by p_0, p_1). In order to determine whether the rating system described by σ_P and p_0, p_1 is IC, we need to study the agents' IC constraints. The long-term utility of an agent i of rating θ is defined as the discounted sum of its current utility and expected future utility. If all the agents comply to the recommended strategy σ_P, then the long-term utility can be expressed as $\forall \theta \in \Theta$,

$$U_i^{\infty}(\theta \mid \mathbf{a}^{\sigma_P}) = -(p_\theta \nu_i(P) + \overline{p}(\nu_i - \nu_i(P)) + c a_i^{\sigma_P})T - e^{-\beta T}[(1-\epsilon)U_i^{\infty}(\phi(\theta \mid 1) \mid \mathbf{a}^{\sigma_P}) + \epsilon U_i^{\infty}(\phi(\theta \mid 0) \mid \mathbf{a}^{\sigma_P})]$$

The first term is the security cost incurred in the current period and the second term is the discounted utility in the subsequent periods. Alternatively, if agent i unilaterally deviates from σ_P by choosing $\tilde{a}_i \neq a_i^{\sigma_P}$, then its long-term utility becomes

$$U_i^{\infty}(\theta \mid \tilde{a}_i, \mathbf{a}_{-i}^{\sigma_P}) = -(p_\theta \nu_i(P) + \overline{p}(\nu_i - \nu_i(P)) + c\tilde{a}_i)T - e^{-\beta T}[\epsilon U_i^{\infty}(\phi(\theta \mid 1) \mid \mathbf{a}^{\sigma_P}) + (1-\epsilon)U_i^{\infty}(\phi(\theta \mid 0)) \mid \mathbf{a}^{\sigma_P}]$$

The following proposition provides a sufficient and necessary condition for the rating system to be IC.

Proposition 1: The rating system with σ_P and p_0, p_1 is IC if and only if, $\forall i \in \mathcal{N}, \forall \theta \in \Theta$,

$$(1-2\epsilon)e^{-\beta T}[U_i^{\infty}(\phi(\theta \mid 1) \mid \mathbf{a}^{\sigma_P}) - U_i^{\infty}(\phi(\theta \mid 0) \mid \mathbf{a}^{\sigma_P})] \geq (2a_i^{\sigma_P} - 1)cT \quad (2)\square$$

Proposition 1 is based on the "one-shot" deviation principle [2] and shows that if an agent cannot gain by unilaterally deviating from σ_P only in the current period and following σ_P afterwards, it cannot gain by switching to any other strategies (possibly multiple-shot deviations) either, and vice versa. The condition (2) states that an agent has no incentive to deviate if and only if its future loss outweighs its current gain upon deviation. Using this result, we are able to determine the existence of the IC rating system and the optimal traffic qualities.

Theorem 1: If $\epsilon \leq \frac{1}{2}\left(1 - \frac{e^{\beta T} c}{(\overline{p} - \underline{p})\underline{\nu}(P)}\right)$, then the optimal traffic qualities are $p_1^* = \underline{p}$, $p_0^* = e^{\beta T} \frac{c}{(1-2\epsilon)\underline{\nu}(P)} + \underline{p}$; Otherwise, the rating system cannot be IC. $\square$

Theorem 1 states that if the monitoring technology is accurate enough, then at least one IC rating system exists and moreover, the optimal traffic qualities p_0, p_1 can be analytically determined. However, if the monitoring error is too large, then any rating system is not IC in which some agents will want to deviate from the recommended strategy σ_P. When the IC rating system exists, the optimal traffic quality indicates the tradeoff of the punishment between incentive-compatibility and the efficiency loss. To make the rating system IC, the punishment (i.e. p_0) should be strong enough such that the agents in P do not have incentives to deviate. However, the punishment should not be too strong that it induces additional efficiency loss. Using these optimal traffic qualities we can obtain the overall security cost as:

$$J^*(\sigma_P) = \left[\underline{p} + \frac{\epsilon}{1-2\epsilon}\frac{e^{\beta T} c}{\underline{\nu}(P)}\right]\sum_{i \in P} \mu_i + \overline{p}\sum_{i \notin P} \mu_i + \mid P \mid c \quad (3)$$

3.2. Optimal recommended strategy

In the previous subsection, we determined the optimal traffic qualities given a recommended strategy σ_P. However, we did not specify which recommended strategy will lead to the minimal overall security cost among all possible strategies. In this subsection, we determine the optimal recommended strategy.

The recommended strategy space is very large. For an agent collection with N agents, the cardinality of this space is 2^N. Searching in this space is thus a demanding task for the RA. Intuitively, the optimal strategy seems to be $\sigma_{\mathcal{N}}$ (i.e. the FDS). If this intuition would be correct, then the RA can simply choose $\sigma_{\mathcal{N}}$ to be the recommended strategy. Therefore, it is important to understand when $\sigma_{\mathcal{N}}$ is indeed the optimal strategy. The following theorems provide two sufficient conditions for $\sigma_{\mathcal{N}}$ to be optimal.

Theorem 2: If $\epsilon \leq \frac{A}{1+2A}$ where $A = \min_{i \in \mathcal{N}}\left\{\frac{(\overline{p} - \underline{p})\mu_i - c}{\sum_{i \in \mathcal{N}} \mu_i} \frac{\underline{\nu}(\mathcal{N})}{e^{\beta T} c}\right\}$, then $\sigma_{\mathcal{N}}$ is the optimal recommended strategy. $\square$

Theorem 2 unravels the impact of the imperfect monitoring on the performance of the FDS. In fact, according to (3), the optimal performance of a rating system with the FDS can actually asymptotically achieve the "first-

best" performance J^{**} as ϵ goes to 0. However, monitoring is never perfect in practice. In some scenarios, it could even be relatively large if the monitoring technology is not good enough. In the following, we determine a structural result of the agent network such that the FDS is optimal.

Theorem 3: For $\epsilon \le \frac{B}{1+2B}$ where $B = \min_{i \in \mathcal{N}} \left\{ \frac{(\overline{p}-\underline{p})u_i - c}{u_i} \frac{\underline{\nu}(\mathcal{N})}{e^{\beta T} c} \right\}$, If $\forall$ subset P such that $\underline{\nu}(P) \le \underline{\nu}(\mathcal{N})$, then $\sigma_{\mathcal{N}}$ is optimal. □

We first note that B is much larger than A, especially when the collection size is large. Therefore, the restriction on the monitoring technology is much milder than that in Theorem 2. The intuition behind Theorem 3 is that if for any P we must use a stronger punishment (since $\underline{\nu}(P) \le \underline{\nu}(\mathcal{N})$) to make the associated PDS IC, then this PDS must induces a higher security cost than the FDS. Theorem 3 provides a theoretical characterization on the sufficient condition for the FDS to be optimal when the monitoring error is large. However, determining all $\underline{\nu}(P)$ is still computationally complex and hence, we propose an *Iterative Deletion (ID)* algorithm that requires at most N iterations to find the optimal recommended strategy.

Iterative Deletion (ID) Algorithm

Input: Agent collection $\mathcal{N}$, traffic matrix Λ
Output: Optimal recommended strategy σ_P^*

Compute $J^*(\sigma_{\mathcal{N}})$ using (3);
Set $P = \mathcal{N}$, iteration index
while $P \neq \varnothing$, do:
  if $\underline{v}(P) > \underline{v}(\mathcal{N})$
    Compute $J^*(\sigma_P)$ using (3);
  end if
  Set $P = P - \{i : v_i(P) = \underline{v}(P)\}$; (**Iterative deletion**)
end while
Choose P that minimizes $J^*(\sigma_P)$ on the iteration path.

4. ILLUSTRATIVE RESULTS

In this section, we provide numerical results to illustrate the features of our proposed rating system. We fix $c = 0.3$, $\overline{p} = 0.3$, $\underline{p} = 0.05$, $T = 2$ and $\beta = 1$.

We first consider an agent collection with identical connectivity degrees with each agent and identical traffic rate $\lambda_0 = 1$ on each edge. We vary the degree d to investigate the impact of the connectivity on the optimal design parameters. Fig. 1 shows the optimal traffic qualities for the low rating agents and the optimal overall security costs under various monitoring errors. When the agent collection becomes denser (i.e. d is larger), agents obtain more benefits from the proactive security technology deployed by their connected agents and therefore, their IC constraints are easier to be satisfied. Hence, a lower p_0 can be used. This further leads to a lower overall security cost. It also shows that a lower security cost is achieved when the monitoring error is smaller. Moreover, simply choosing $p_0 = \overline{p}$ will result in enormous efficiency loss.

Next, we show how the ID algorithm works for a specific deployment scenario in Fig. 2 (traffic rates are shown on the edge in the connection graph). For simplicity, we assume symmetric traffic arrival rate between any two connected agents. In each iteration, the agent with the lowest aggregate inbound traffic is deleted (marked by "x" in the table). The minimal security cost is achieved when agents 3,4,5,6 are recommended to deploy the security technology.

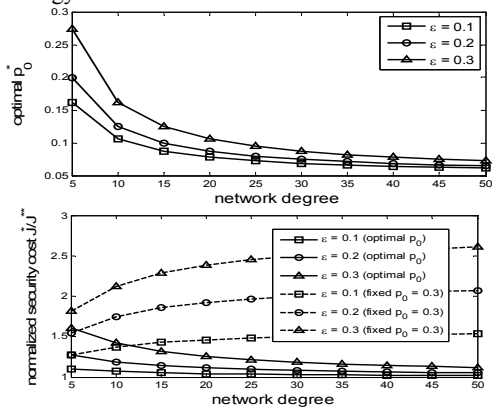
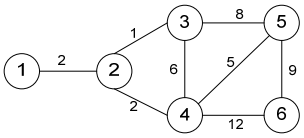


Fig. 1 Impact of the monitoring errors and the network connectivity



agent	**1**	**2**	**3**	**4**	**5**	**6**	**J**
t=1	**2**	5	15	25	22	21	7.58
t=2	x	**3**	15	25	22	21	6.98
t=3	x	x	**14**	23	22	21	6.74
t=4	x	x	x	17	**14**	21	>6.74
t=5	x	x	x	12	x	12	>6.74

Fig. 2 Illustration of the ID algorithm.

5. CONCLUSION

In this paper, we studied the design problem of rating systems aimed at encouraging security investment within a network of agents that interact regularly and over a long period of time. We showed that it is possible to exploit the ongoing nature of the interaction to design rating systems to improve the mutual security. Our analysis showed that the monitoring technology and the traffic and the connectivity structure of the network can strongly influence the agents' self-interested investment decisions. Surprisingly, a lower security cost may be achieved by recommending partial deployment of the security technology than by recommending full deployment. The proposed rating systems can be used to design security policies that can deal with a variety of other security problems besides the one considered in this paper.

12. REFERENCES

[1] R. Anderson, "The economics of information security," Science, 317, 610 (2006).

[2] G. Mailath and L. Samuelson, Repeated games and reputations: long-run relationships, Oxford University Press, 2006.

[3] H.Kunreuther and G. Heal, "Interdependent security," Journal of Risk and Uncertainty, vol. 26, no. 2-3, 2003.

[4] M. LeLarge, "Economics of malware: epidemic risks model, network externalities and incentives," Allerton 2009.

[5] J. Omic, A. Orda, P. van Mieghem, "Protecting against network infections: a game theoretic perspective," IEEE INFOCOM 2009.

[6] V. S. A. Kumar, R. Rajaraman, Z. Sun, R. Sundaram, "Existence theorems and approximation algorithms for generalized network security games," IEEE ICDCS, 2010

[7] J. Bolot, M. Lelarge, "A new perspective on Internet security using Insurance," IEEE INFOCOM, 2008.

[8] M. Parameswarn, X. Zhao, A. Whinston, and F. Fang, "Reengineering the Internet for better security," Computer, 40(1), pp. 40-44, Jan. 2007

[9] F. Millan, J. Jaramillo, R. Srikant, "Achieving cooperation in multihop wireless networks of selfish nodes," Gamenets 2006.

[10] C. Dellarocas, "Reputation mechanisms design in online trading environments with pure moral hazard," Information Systems Research, Vol. 16, No. 2, pp. 209-230, June 2005.

[11] Y. Zhang and M. van der Schaar, "Reputation-based incentive protocols in crowdsourcing applications," IEEE INFOCOM 2012.

[12] J. Xu, Y. Zhang and M. van der Schaar, "Designing rating systems to promote mutual security for interconnected networks," UCLA technical report, online: http://arxiv.org/abs/1211.2287, 2012.

[13] J. Wang, Z. Ge, T.F. Znati and A. Greenberg, "Traffic-aware firewall optimization strategies," IEEE ICC 2006

[14] M. Bloem, T. Aplean, S. Schmidt, "Malware filtering for network security using weighted optimality measures," IEEE International Conference on Control Applications (CCA), 2007.