A Game Theoretic Model for Network Virus Protection

Iyed Khammassi, Rachid Elazouzi, Majed Haddad, Issam Mabrouki

A Game Theoretic Model for Network Virus Protection

Iyed Khammassi*†, Rachid Elazouzi*, Majed Haddad* and Issam Mabrouki†
*University of Avignon, 84000 Avignon, FRANCE
Email: firstname.lastname@univ-avignon.fr
†University of Manouba, Manouba, Tunisia
issam.mabrouki@hanalab.org

***Abstract*—Security is crucial for information systems. In a company, security management is traditionally controlled via a centralized single-point. However, when we deal with multiple computer systems interconnected in a wide area networks (WAN), the use of a central authority for security management is completely meaningless. In this paper, we propose a distributed decision-making designed to thwart viruses in a WAN. A key aspect is whether owners of devices are willing to update their anti-virus in order to protect their computers or not to pay for an anti-virus update and take the risk to be contaminated. Given the fact that computers are interconnected via networks and the Internet, the risk of being infected does not only depend on each computer's strategy, but also on the strategies chosen by other computers in the network. This makes the virus protection problem much more challenging. To do so, we model the interaction between nodes as a non-cooperative game in which each node decides *individually* whether to update the anti-virus or not. The virus spread is assumed to follow a biologically inspired epidemic model in which the dynamic of sources that disseminate the virus evolves as function of the popularity of virus using the influence linear threshold model. We first provide a full characterization of the equilibria of the game and then we investigate the impact of the update cost. In particular, we study the performance of the strategies at the equilibrium in terms of the update cost and the network size on both the security management system and the anti-virus producers. These results give some helpful insights on how secure is decentralizing anti-virus update decisions.**

I. Introduction

The Internet continues to grow exponentially and many applications continue to appear on the Internet, with immediate benefits to end users. However, these network-based applications and services can pose security risks to devices. Recently, many attacks have been launched against business, users and governments that are attributed to some decentralized online communities acting anonymously in a coordinated manner. Despite the important efforts spent by many security companies, researchers, and government institutes, information system security is still of great concern [1], [2]. One of the important security risks is the propagation of some sophisticated virus throughout the internet, in which each infected node becomes a new source of infection. The problem of virus propagation has been studied through huge number of papers focusing mainly on epidemic thresholds and immunization policies [3]–[5]. Recently, many papers proposed biological models to characterize the behavior of virus spread and study how to immune the computer system [6].

To manage the network security, a lot of efforts have been devoted to study virus propagation and its characteristics [7]. Nodes (which could be either smartphones, machines or tablets) can use some anti-virus software with curing tools to ensure protection from the spread of virus throughout the network [8]. A key issue for protecting nodes from new viruses and other threats is the frequency of the anti-virus update. Many of the anti-virus products are client/server, in which the system may have a plan for how often nodes should update their anti-virus.

A fundamental source of difficulty in developing efficient protection is to fully observe and control the network. As a consequence, full control and observability is impossible, leading to systems that are vulnerable to local as well as remote attacks. On the other hand, distributing the anti-virus update decision throughout the network has to meet several constraints when evaluating the security risk. Indeed, a major source of complication in network security is the typically autonomous nature of decision making in the network. The performance of such a security solution is usually made under the assumption that nodes are willing to use an anti-virus for protection. In this setting, a crucial aspect is whether owners of devices are willing to update their anti-virus in order to be protected, or to avoid the payment for an anti-virus update and take the risk to be contaminated. Any successful security solution should consider those factors. Given the fact that computers are interconnected via networks and the Internet, the risk of being infected not only depends on each computer's strategy, but also on the strategies chosen by other computers in the network. This makes the virus protection problem much more challenging.

In this paper, we study the influence of the system parameters on the equilibrium performance to provide better strategies to the security management system and the anti-virus producer. To address these issues, we model the problem as a non-cooperative game. We consider a source S which propagates the virus through the network. The virus spread is assumed to follow a biologically inspired epidemic model in which the dynamic of sources that disseminate the virus evolves as function of the popularity of virus using the Homogeneous Influence Linear Threshold (HILT) model

[9]. The HILT model focuses on the threshold behavior in influence propagation. One key example is when enough of our friends bought a product, we may be influenced and converted to follow the same action. In our context, when a virus reaches some level of popularity, other sources may participate in the dissemination of the virus. We first study the dynamic of both the infection process and the activation process. Then, we conduct a thorough analysis on the existence and the uniqueness of different types of Nash equilibria where both the security management system and the anti-virus producer strategies are addressed.

II. Network model

Consider a WAN that consists of a large population of N computer systems (CS) or nodes. We represent the users network by a connected graph $G = (N, N_s, E)$ where N is the number of nodes in the network, N_s is the number of sources (hackers) in the network and E is the set of edges. The sources S generate a virus and nodes in the network become susceptible to be infected by this virus.The distance $d_{i,j}$ between two nodes i and j in a graph is the number of edges in a shortest path. Each node i decides individually to protect himself from the virus by installing an anti-virus. Obviously, all nodes have an incentive to protect themselves until the virus extinction. However, every anti-virus update costs a price U_c. Hence, the strategy adopted by a node corresponds to a certain utility it receives and this utility depends on actions performed by N nodes. Nodes with outdated anti-virus are vulnerable to the virus spread process, and lose an infection cost I_c if they were infected. An infected node can recover after a curing time using various tools (e.g., through a clean-up software). Under this setting, nodes shall immunize themselves during the period of the virus spread while minimizing the anti-virus update cost. We denote the users strategies by $\mu = (\mu_1, \mu_2, \ldots, \mu_N)$. Let $N(\mu)$ the set of users who choose not to update their anti-virus and thus are susceptible to the infection.

A. Modeling active sources evolution

A source S can infect a target user i regardless of the distance $d_{S,i}$. A source is said to be active if it disseminates the virus in the network, otherwise it is said inactive. We associate the dynamic of active sources A_s with the popularity of the virus which is measured by the number of nodes infected by this virus. We model this influence process using HILT model. The evolution of the number of active sources is modeled following a given evolving in continuous time process. Each source j chooses a threshold $\theta_j \in [0, 1]$ from an arbitrary threshold distribution with a cumulative density function (c.d.f) F. Hence, a source becomes active if the popularity, which is measured by the number of infected nodes, exceeds θ_j. Sources' decisions are based on a function of the set of nodes that are infected. Let T be a monotone threshold function. The diffusion process follows a general structure of the Linear Threshold Model.
From [9], we have :

$$T(x) = h_f(x) = \frac{f(x)}{1 - F(x)}$$

where h_f is the hazard function [10] for the c.d.f and f is the survival distribution (Uniform, Exponential,Weibull...).
A source j becomes active in step t if

$$T\left(\sum_{i \in N(\mu)} v_i(t-1)\right) \geq \theta_j, \tag{1}$$

where $v_i(t)$ is the probability to be infected.
Under the HILT model, the following proposition describes the dynamic of the number of actives sources at time t.

Proposition 1. *The dynamic of the number of active sources that disseminate the virus, is given by*

$$\dot{S}(t) = -\delta_S S(t) + \lambda \frac{f(\bar{X}(t))}{1 - F(\bar{X}(t))}(N_s - S(t)), \tag{2}$$

where $\bar{X}(t)$ is the number of infected nodes till time t, and $\delta_S S(t)$ is the set of the sources which are no longer interested to the virus and move from the active state to the susceptible state. A source is influenced by the cumulative infection process with a rate λ.

Due to the lack of space, all the proofs and complementary analysis can be found in the technical report [11].

B. The Security Game

We consider a security game [12], in which nodes choose individually whether to invest in the anti-virus protection by updating their anti-virus versions. Each node has two strategies: either to invest in the anti-virus protection, i.e., pure strategy *update* (U), or not to invest, i.e., pure strategy *not update* (NU). Mixed strategies, i.e., probability distribution over the two actions, are also possible. Each strategy corresponds to certain payoff for the node. We denote the users strategies by μ. Notice that nodes may prefer not to invest in an anti-virus update when the network is protected enough, i.e., there is enough nodes in the network that have the anti-virus update. Indeed, a node may also be protected by other nodes' update. This means that the risk to be infected decreases with the number of anti-virus activated throughout the network. Accordingly, the payoff of a node depends on the actions performed by the $N - 1$ nodes.
We denote by $V_j(\xi, k_U)$ the long term fitness of a node j, given that it plays the strategy $\xi \in \{U, NU\}$, and that k_U is the number of updated anti-virus. The fitness is given by

$$V_j(\xi, k_U) = \begin{cases} -U_c & j \notin N(\mu) \\ -v_{j\infty} I_c & j \in N(\mu) \end{cases} \tag{3}$$

where $v_{j\infty}$ is the probability to be infected until the virus extinction.

C. Modeling infection dynamic

To model the spreading process under the influence of a curing process, we choose the Susceptible Infected Susceptible (SIS) model, which is one of the most studied epidemic models [13], [14]. Each node in the network is either infected or healthy. A node i can be infected by a neighbor with an infection rate β_i or by a source with an infection rate γ_i, and is cured with a curing rate δ. Once cured and healthy, the node is again prone to the virus. Denote by A the adjacency matrix of the graph. The state of a node at time t is represented by the vector $x(t)$ which is equal to 1 when node i is infected (with probability $v_i(t)$), and 0 when node i is healthy (with probability $1 - v_i(t)$). When a node updates its anti-virus, it is assumed to be directly immune to the virus and not part of the epidemic process anymore. In this case, we consider that a source S is influenced by the cumulative number of infected nodes $\bar{X}$ and it will be active when

$$\bar{X}(t) \geq \theta \tag{4}$$

We consider the symmetric case for sources and nodes . We assume that a node contacts an active source with a rate γ and other nodes with a rate β. Before evaluating the dynamics of the the infected nodes $X(t)$, we study the dynamic of sources $S(t)$ under the activation process.

A source S is active when the number of infected nodes $\bar{X}(t)$ reaches the target value θ. Let $\bar{X}(t)$ be the dynamic of infected nodes disregarding the curing process. The sources contact $(N - k_U - X(t))$ susceptible nodes with a rate γ. Therefore, we can write the dynamics of $\bar{X}(t)$ as follows

$$\dot{\bar{X}}(t) = (\beta X(t) + \gamma S(t))(N - k_U - X(t)) \tag{5}$$

Recall that $S(t)$ is the set of active sources which participate in the infection process by time t. By applying Condition (4), we can write the sources dynamics as follows

$$\dot{S}(t) = -\delta_S S(t) + \lambda h_F(\bar{X}(t))(N_s - S(t)) \tag{6}$$

The dynamics of $X(t)$ is given by:

$$\dot{X}(t) = -\delta X(t) + (\beta X(t) + \gamma S(t))(N - k_U - X(t)) \tag{7}$$

The above equation gives the dynamics of infected nodes under the sources activation process. All nodes aim to be enough protected during the lifetime of the virus. In the steady-state the infection probability $v_{i\infty}$ can be expressed as [15]:

$$v_{i\infty} = \frac{\beta \mid N(\mu) \mid v_\infty + \gamma N_s \frac{f(\bar{v})}{f(\bar{v})+\delta_s}}{\beta \mid N(\mu) \mid v_\infty + \gamma N_s \frac{f(\bar{v})}{f(\bar{v})+\delta_s} + \delta} \tag{8}$$

where $\bar{v} = \sum_{k \in N(\mu)} v_{k\infty}$ and $\mid N(\mu) \mid$ stands for the number of elements that choose not to update their anti-virus.

III. Characterization of the Equilibrium

In this section, we will study and characterize the different Nash equilibrium types for our security game.

1) Pure Nash Equilibrium:

Definition 1. *At a Nash equilibrium (NE), no player can improve its fitness by unilaterally deviating from the equilibrium.*

For the proposed game a NE in pure strategies exists if and only if the following two conditions are satisfied

$$\forall 1 \leq j \leq N; \begin{cases} V_j(NU, k_U - 1) \leq V_j(U, k_U) \\ V_j(NU, k_U) \geq V_j(U, k_U + 1) \end{cases} \tag{9}$$

We are interested in the existence and uniqueness of the pure NE which is characterized by the number ψ of players investing in the anti-virus.

A unique pure NE exists for the proposed security game when $V_j(NU, \psi) = V_j(U, \psi)$.

2) Mixed Nash Equilibrium: Let us now discuss the case when every node maintain a probability distribution over the two actions (U, NU). The advantage of this mixed equilibrium compared to the pure one is that a node can invest in protection only for a fraction of the time and stay susceptible the rest of the time. This kind of equilibrium is more efficient for our case because we study a homogeneous population with fixed update and infection cost. In a mixed strategy game, a node i can decide to invest in protection (playing U) with probability p_i or keep protected only by his neighbors (playing NU) with probability $(1 - p_i)$.

$\mathbf{p} = (p_1, p_2, \ldots, p_N), \forall i p_i \geq 0$, is the mixed strategy profile. For $p_i \notin \{0, 1\}$ we have a fully mixed strategy profile. We note (p_i, p_{-i}) if node i uses strategy p_i and other use $p_{-i} = (p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_N)$.

We denote by $V_i(p, p_{-i})$ the playoff of a node i which invest in anti-virus with probability p.

Definition 2. *A mixed strategy $p_i^* \in [0, 1]$ is a NE if for each player i (where $i = 1, \ldots, N$) we have*

$$U_i(p_1^*, \ldots, p_{i-1}^*, p_i^*, p_{i+1}^*, ., p_N^*) \geq U_i(p_1^*, \ldots, p_{i-1}^*, p_i, p_{i+1}^*, \ldots, p_N^*) \tag{10}$$

for every mixed strategy $p_i \in [0, 1]$.

If $\forall i, {p^*}_i \notin \{0, 1\}$ then we call p^* fully mixed NE.

Every finite strategic game has a mixed strategy NE [16]. There exists a unique fully mixed NE p^* for the proposed game and it is solution of

$$\sum_{k=1}^{N} C_{k-1}^{N-1} (p^*)^{k-1} (1 - p^*)^{N-k} V(U, k) = 0 \tag{11}$$

3) Equilibrium with Mixers and Non-Mixers: The mixers are the players that choose a mixed strategy. We suppose that a part of the population chooses to play a pure strategy U or NU and the rest of the players are mixers. We will study the existence of the equilibrium in this case. Let $N_U \in \{0, 1, \ldots, N\}$ be the number of players choosing the pure strategy U, and $N_{NU} \in \{0, 1, \ldots, N\}$ be the number of players choosing the pure strategy NU.

The $N - N_U - N_{NU}$ players use the mixed strategy. Let $p^* \in (0,1)$ be the probability with which the mixers choose the strategy U. Moreover, we denote by $V_U(N_U, N_{NU}, p)$ the fitness of the node who updates its anti-virus and $V_{NU}(N_U, N_{NU}, p)$ the fitness for the node who does not update its anti-virus. A necessary condition for the strategy (N_U, N_{NU}, p^*) to be a NE (with at list one mixer) is that the mixer is indifferent whether it chooses a pure strategy U or NU. This translates mathematically as follows

$$V_U(N_U + 1, N_{NU}, p^*) = V_U(N_U, N_{NU} + 1, p^*) \qquad (12)$$

A unique NE of type (N_U, N_{NU}, p^*) exists for this case, and is solution of

$$\sum_{k=0}^{N-N_U-N_{NU}} C_{k-1}^{N-N_U-N_{NU}} (p^*)^{k-1} \cdot (1-p^*)^{N-N_U-N_{NU}-k} V(U, N_U + k) = 0. \qquad (13)$$

We prove that this NE of type (N_U, N_{NU}, p^*) exists only for $N_U < \psi$ and $N_U + N_{NU} \leq N - 2$. In this section, we have studied different NE types under the activation process $S(t)$. We summarize the different NE types as following:

- **Pure Nash Equilibrium**: There exists a unique NE when the utility of U is equal to the utility of NU and we must update exactly ψ nodes to get this equilibrium,
- **Mixed Nash Equilibrium**: A unique fully mixed NE p^* exists and it is solution of Equation (11),
- **Mixer and Non-Mixer Nash Equilibrium**: We characterize this equilibrium by the necessary condition (12). A unique NE exists and it is solution of Equation (13).

IV. Numerical Evaluation

In this section, we provide a numerical analysis of the performances of the proposed security game. We first evaluate the infection probability at the equilibrium. To do so, we solve Equation (11) to get the activation probability at the equilibrium. We show how the activation and the infection process depend on the system parameters, such as the number of nodes N and the update cost Uc.

A. System characteristics

Fig. 1 and Fig. 2 illustrate the behavior of the infected nodes $X(t)$ and the sources $S(t)$ as function of the time for different activation probabilities $(0.01, 0.1, 0.5)$ and a contact rate $\beta = 10^{-3}$. We further take $X(0) = 0$ and $S(0) = 5$. As expected, we remark a cause-effect phenomenon between the nodes and sources. The number of infected nodes increases as a result of the virus spread till reaching a given infection rate. Then, when the virus popularity reaches a certain level, the participating in the virus spread increases yielding an increase in the number of sources.

In the proposed game model, activation probability is a fundamental parameter and is related to how many nodes install the new anti-virus software. To analyze effects of the activation probability, p is set to three different values

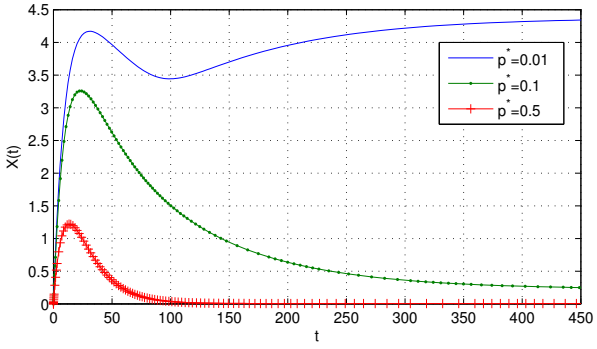

Fig. 1. The infection process for different activation probabilities p, where $N = 100$, $N_s = 50$, $\beta = 1 \times 10^{-3}$, $\gamma = 1 \times 10^{-3}$, $\delta = 1 \times 10^{-1}$, $\delta_S = 1 \times 10^{-1}$, $\lambda = 5 \times 10^{-6}$, $X(0) = 0$, $S(0) = 5$, $Ic = 1$ and $Uc = 0.1$.

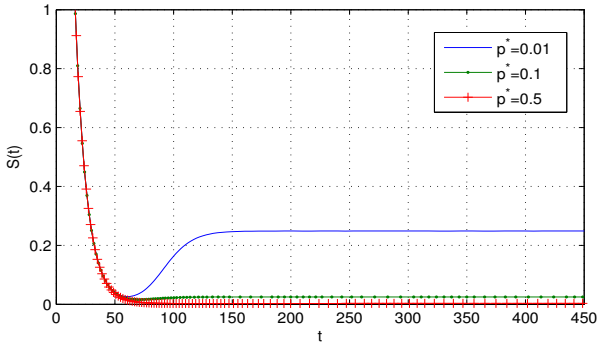

Fig. 2. Sources behaviour for different activation probabilities.

$(0.01, 0.1, 0.5)$. Fig. 1 shows that the number of infected nodes $X(t)$ slightly fluctuates before reaching a stable (absorbing) state. In general, the higher the activation probability is, the faster $X(t)$ decreases. This is due to the fact that increasing the activation probability implies a decrease in the risk of being infected for susceptible nodes. Notice that, depending on the activation probability, the virus may disappear completely or become scars. We will discuss this point later in the paper.

Fig. 2 depicts the dynamics of the interested sources in the virus spread for different p. We clearly notice that, for low activation probability values, e.g., $p = 0.01$, $S(t)$ decreases until the virus popularity reaches a target value. When the activation probability increases to $p = 0.5$, we can see that the number of sources are decreasing gradually to vanish eventually.

Fig. 3 illustrates the time evolution of the infection probability for different activation probabilities p. We remark that, from $p = 0.495$, the infection probability monotonically decreases till completely vanishing at $t = 230$. This suggests that using an activation probability higher that 0.495 is worthless as, from $p = 0.495$, the virus is going to disappear in any case. Unless otherwise stated, we will use the following parameters: $N = 500$, $N_s = 50$, $\beta = 1 \times 10^{-4}$, $\gamma = 1 \times 10^{-3}$, $\delta = 0.1$, $\delta_S = 0.1$, $\lambda = 1 \times 10^{-4}$, $X(0) = 0$, $S(0) = 10$, $Ic = 1$ and $Uc = 0.1$. We notice by t_f the time of epidemic extinction

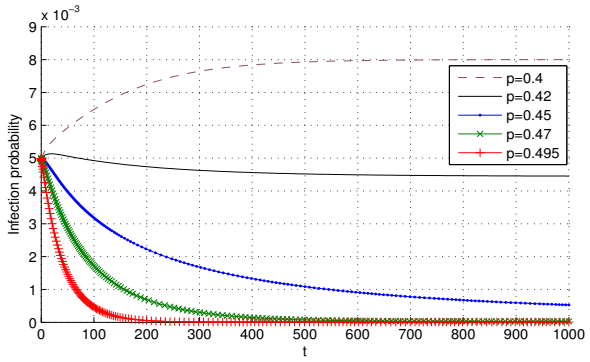

Fig. 3. The infection probability for different activation probabilities, where $N = 100$, $\beta = 1 \times 10^{-3}$, $\gamma = 1 \times 10^{-3}$, $\delta = 1 \times 10^{-1}$, $\delta_S = 1 \times 10^{-1}$, $\lambda = 1 \times 10^{-4}$, $X(0) = 0$, $S(0) = 5$, $Ic = 1$ and $Uc = 0.1$.

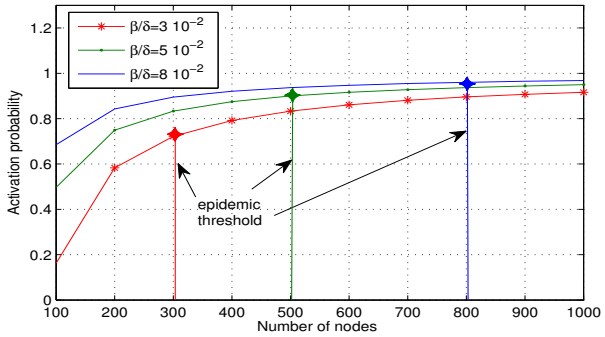

Fig. 4. The activation probability for increasing number of nodes.

corresponding to the time for which we have $X(t) = 0$. For this parameters, a virus extinction time t_f exists and we can compute the infection probability in $[0, \ldots, t_f]$.

B. System performances at the equilibrium

1) Fully mixed equilibrium : Let us now evaluate the performances of the proposed security game. We characterize the equilibrium in Section III by solving the polynomial Equation in (11). We solve (11) to get a unique solution $p^* = 0.29$ at the equilibrium.

2) Mixer and non-mixer equilibrium: Here, we have N_U nodes that always update their anti-virus (pure strategy update) and N_{NU} that never update their anti-virus (pure strategy not update). The $N - N_{NU} - N_U$ mixers update the anti-virus with an activation probability p. Verifying Condition (12), we vary the N_U and the N_{NU} to find the activation probability for the mixers at the equilibrium. For $N = 500$ and $Uc = 0.1$, we get $p^* = 0.19$ for all the mixers when $N_U = 50$ and $N_{NU} = 70$.

C. Effects of the network size

To proceed further with the analysis, we resort to evaluate the impact of the network size on the system behavior at the equilibrium.

In Fig. 4, we plot the activation probability as function of the network size. It is clearly shown that the activation probability increases when the network is larger which is somehow obvious as a larger network tends to provide greater risk of infection among nodes. On the other hand, we know from [17] that the relation between the epidemic threshold τ_c and the transmission to disease-induced mortality ratio $\frac{\beta}{\delta}$ translates to the following conditions

- if $\frac{\beta}{\delta} < \tau_c$, the virus dies out over time,
- if $\frac{\beta}{\delta} > \tau_c$, the virus survives and the infection becomes an epidemic.

In the particular case of a complete graph, the epidemic threshold is given by $\tau_c = \frac{1}{N-1}$. Thus, in the proposed network, the infection dies when $N < \frac{\delta}{\beta} + 1$. Increasing $\frac{\beta}{\delta}$, the number of nodes satisfying the epidemic threshold is larger. This result gives incentive to manage their network parameters (β ,δ, N) so that the infection dies out over time.

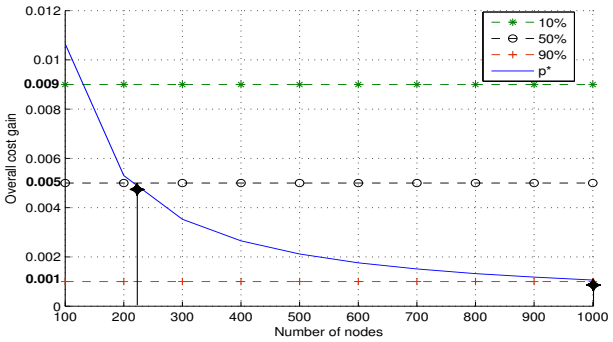

Fig. 5. The overall cost gain as function of the number of nodes.

To evaluate the performance of the equilibrium, we compare, in Fig. 5, the overall cost gain, defined as $G = \frac{U_c N - p^* U_c N}{U_c N}$ to simpler policies where one may activate a given percentage of the nodes in the system depending on the general policy of the company. For instance, a conservative policy is more likely to update 90% of the nodes, whereas a lax policy is more likely to update 10% of the entire nodes in the system.

So far, we have been interested in the influence of network parameters (β, δ, N) on the the security management system. Now, we will study how the network parameters influence the anti-virus producers decision.

D. Effects of the update cost

Let us now study the impact of the update cost on the system behavior at the equilibrium.

Fig. 6 gives the time evolution of the activation probability considering different values of β/δ. We find the update cost U_c^* for which the probability of activation is equal to 0. This specific value U_c^* is very important for the anti-virus producers to manage the U_c, as approaching U_c the this limit value U_c^*. The U_c^* increases with β/δ, as the risk of infection increases with β/δ.

Fig. 7 illustrates the infection probability in $[0, \ldots, t_f]$ as function of the update cost. At the equilibrium, the infection probability increases with the update cost. This is justified by the fact that the number of nodes participating in the

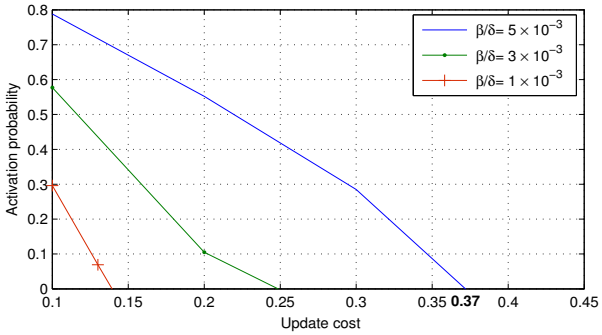

Fig. 6. The activation probability as function of the update cost.

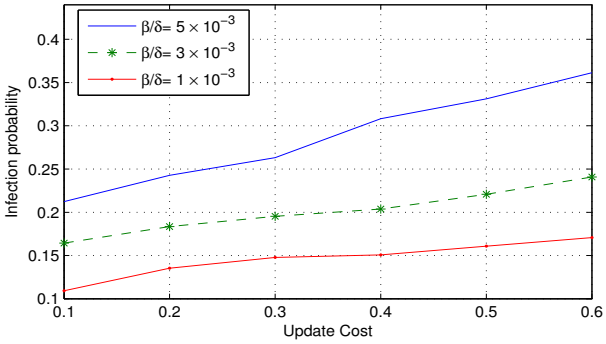

Fig. 7. The infection probability as function of the update cost.

anti-virus activation decreases as the update cost increases, yielding a higher infection risk. In Fig. 8, we plot the infected node evolution in time at the equilibrium considering different update costs U_c. We observe that $X(t)$ increases until a certain t^* and then it decreases till the epidemic extinction, i.e., when $X(t) = 0$. It is shown that the more the update cost is lower, the more the t^* and the epidemic extinction are lower. This result helps the anti-virus producers to manage the update cost. Increasing the U_c, we have more infected nodes in the network. Reaching ${U_c}^*$, no node is interested in the update. The anti-virus producers are interested to reach a target performance of update cost to maximize the gain.

V. CONCLUSION

We have studied a game theoretic model for network virus protection under an activation process. The virus spread dynamics is modeled as an epidemic process. We have first studied the dynamic of both the infection process and the activation process. Then, we have established the existence and the uniqueness of different types of Nash equilibrium. Both the the security management system and the anti-virus producer strategies have been addressed. Notably, it has been shown that, depending on the network topology, one has incentive to manage the network parameters in such a way we ensure that the infection dies out at finite-time horizons. The proposed approach goes toward the vision of a computer immune system, whereby the decision to update the anti-virus or not is taken in a distributed way across the nodes.

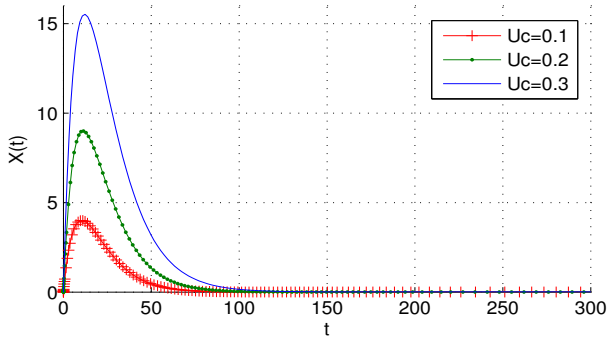

Fig. 8. Infected nodes for different update costs with $N = 100$, $N_s = 50$, $\beta = 1 \times 10^{-4}$, $\gamma = 1 \times 10^{-3}$, $\delta = 0.1$, $\delta_S = 0.1$, $\lambda = 1 \times 10^{-4}$, $X(0) = 0$, $S(0) = 10$ and $Ic = 1$.

REFERENCES

[1] J. Sen, "A survey on security and privacy protocols for cognitive wireless sensor networks," *CoRR*, vol. abs/1308.0682, 2013.

[2] S. Sharma, G. Gupta, and P. R. Laxmi, "A survey on cloud security issues and techniques," *CoRR*, vol. abs/1403.5627, 2014.

[3] C. Castillo-Chávez, W. Huang, and J. Li, *Competitive exclusion in Gonorrhea models and other sexually-transmitted diseases*. Mathematical Sciences Institute, Cornell University, 1993.

[4] N. Masuda, "Immunization of networks with community structure," *New Journal of Physics*, vol. 11, no. 12, pp. 1–8, 2009.

[5] J. Omic, J. M. Herndez, and P. V. Mieghem, "Network protection against worms and cascading failures using modularity partitioning." in *International Teletraffic Congress*. IEEE, 2010, pp. 1–8.

[6] S. M. Abdulla and O. Zakaria, "Devising a biological model to detect polymorphic computer viruses artificial immune system (aim): Review," in *ICCTD*, Washington, DC, USA, 2009.

[7] C. Jin, J. Liu, and Q. Deng, "Network virus propagation model based on effects of removing time and user vigilance." *I. J. Network Security*, vol. 9, no. 2, pp. 156–163, 2009.

[8] J. Omic, A. Orda, and P. V. Mieghem, "Protecting against network infections: A game theoretic perspective." in *INFOCOM*. IEEE, 2009, pp. 1485–1493.

[9] D. Kempe, J. Kleinberg, and E. Tardos, "Maximizing the spread of influence through a social network," in *KDD '03*, 2003.

[10] D. Cox, *Renewal Theory*. Methuen & Co., 1970.

[11] I. Khammassi, R. Elazouzi, M. Haddad, and I. Mabrouki, "A game theoretic model for network virus protection," Technical Research Report, Octobre 2014. [Online]. Available: http://arxiv.org/abs/1410.3688

[12] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, pp. 25:1–25:39, Jul. 2013. [Online]. Available: http://doi.acm.org/10.1145/2480741.2480742

[13] P. V. Mieghem, J. Omic, and R. Kooij, "Virus spread in networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 1–14, 2009.

[14] P. V. Mieghem, "The viral conductance of a network," *Computer Communications*, vol. 35, no. 12, pp. 1494–1506, 2012.

[15] ——, "The n-intertwined SIS epidemic network model," *Computing*, vol. 93, no. 2-4, pp. 147–169, 2011. [Online]. Available: http://dx.doi.org/10.1007/s00607-011-0155-y

[16] K.-K. Tan, J. Yu, and X.-Z. Yuan, "Existence theorems of nash equilibria for non-cooperative n-person games," *International Journal of Game Theory*, vol. 24, no. 3, pp. 217–22, 1995.

[17] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos, "Epidemic thresholds in real networks," *ACM Trans. Inf. Syst. Secur.*, vol. 10, no. 4, pp. 1:1–1:26, Jan. 2008.