Modeling the Impact of User Awareness on Immunization Strategies

Baharan Mirzasoleiman[1], Hamid R. Rabiee[1], Mostafa Salehi[2]
[1]Sharif University of Technology, [2]University of Tehran

***Abstract*—Despite the efforts to design better antivirus software, malware continue to spread and cause enormous damages. Effect of immunizing computer systems as the most effective control policy for preventing such infections is two-fold. On one hand, it increases the global immunity of the network by providing indirect protection for unimmunized systems. On the other hand, raising the awareness of users from the possibility of infection can trigger behavioral changes by which users take measures to reduce their systems' susceptibility using the antivirus software. Here, we propose the Behavior-Immunity model that allows measurement of vaccination effect based on the indirect protective effect of immunization strategies. It also provides a mean to utilize human behavioral changes to enhance the effectiveness of immunization strategies. In this work, we focus on the word of mouth as the source of user awareness and show that immunization schema can appropriately utilized the behavioral changes to practice better results. We also present a methodology for network immunization which is provably close to the optimal solution. Extensive computational experiments on some synthetic and real-world networks revealed that this strategy offers a significant improvement over well-studied targeted immunization method based on degree centrality.**

***Index Terms*—infection, antivirus, immunization, behavioral response, economic optimization**

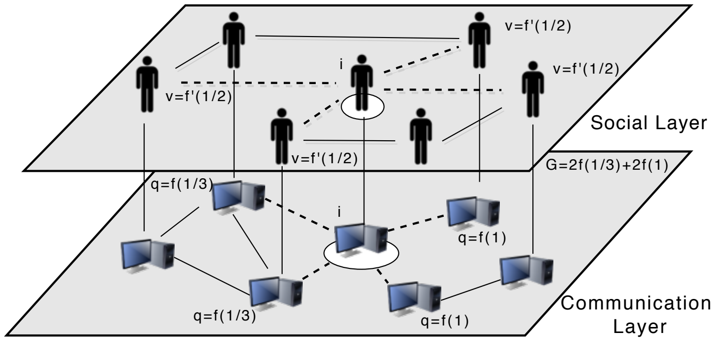

Fig. 1: The two layer network structure. Immunization of computer i provides indirect immuity for their neighbors in the bottom communication layer (q). At the same time, user i increases the awareness of her/his social neighbors about the malware and raises their willingenss to buy the anti-virus (v) and immunize their systems. Such behavioral reactions can directly affect the infection dynamics. The Values of q and v are calculated assuming constant link weights.

I. Introduction

The fast growth of Internet and other communication networks makes them a suitable target for malicious activities. An infection spreads through the links of such networks constructed by computers and their communication channels and caused millions or even billions of dollars in damage by preventing the network from doing its proper functionality [1]. The process by which malicious objects such as worms, trojan horses and computer viruses travel through computer networks is analogous to the process of spreading epidemics through a population. Concerning these similarities, classical epidemic models like SIR and SIS has been widely adopted and used to study the action of malicious objects throughout a network.

Vaccination (running anti-malicious software) is still known to be the most effective and long lasting method for preventing diffusion of infections. The protective effect of vaccination strategies extends beyond vaccinated to unvaccinated members of a network. Immunized nodes provide a measure of protection for those who have not developed immunity by disrupting the chain of infection between infected and susceptible nodes.

Consider a malware that is being spread through a computer network. In this settings, we are dealing with a two layer network as shown in Fig (1). The top layer is a social network of individuals and their social contacts. The bottom layer is a network of computers interconnected by communication channels that allow sharing of resources and information. While infection is begin spread through the bottom communication layer, awareness about presence of the malware arises in the top social layer and triggers behavioral changes of people trying to protect their computers by proactively installing antivirus patches to prevent infection by malware. Such reactions in the corresponding social layer can directly affect the infection dynamics and alter the progression of the infectious agent in the bottom layer.

Recently, substantial effort has been devoted to understand the effect of human behavior on infection dynamics [2]–[6]. However, such efforts have not always made its way into mathematical models. Economic incentives affect the people's decision and reaction in case of an outbreak. Surprisingly, there has been relatively little systematic investigation into understanding economic principles of human behavior and its effect on the way individuals respond to the risk of infection. Understanding the interplay between human behavior and economic incentives can significantly enhance the design of optimal prevention and treatment programs that takes account of the costs of disease and control.

In this paper, we provide a detailed presentation of a Behavior-Immunity Model that allows measurement of vaccination effect based on the indirect protective effect of immunization strategies. Based on our model, we would be able to obtain an estimation from the efficiency of different immunization methods without assuming a set of initial infected agents and relying on an specific epidemiological model for spread of epidemics. It also provides a mean to link human behavior to infection dynamics by having informed individuals try to buy the anti-malware software and reduce the susceptibility of their systems. Incorporating behavior into immunity model enhance its utility in evaluating control measures and help us design formal economic optimizations which allocate the minimum possible resources to achieve the best possible effect [7].

Two data layers composing the Behavior-Immunity model. The communication layer models the indirect immunity provided by the nodes equipped with antivirus for their neighbors and offer a measure to determine the population-level or global immunity of the network. The social layer models the willingness of individuals to pay a price to buy and install the antivirus software on their computers. The source of the information which leads to behavioral changes can be of global or local nature. In the first case, all people are effected from the same sources, often mass media or companies providing protection against cyber threats. However, in the latter case, people base their decisions and consequent reactions on their awareness from the local prevalence of an infection, such as hearing from someone who witnessed the infection first hand. Studies have revealed that awareness of the local prevalence of an infection not covered by media or companies acting against cyber threats has a more impact on people's decision, and can trigger larger cascades of behavioral changes in response to epidemic [8].

Based on the proposed model, we present a general methodology for network immunization which uses the minimum budget required for globally immunizing the network against infection. Those who installed the antivirus patches increase the awareness of their friends about the infection and presence of an appropriate antivirus software. The positive feedbacks people receive from their friends about the software increase their willingness to buy and use the antivirus. When local awareness triggers behavioral responses, people will have different *valuations* for the antivirus. In such settings, the cost of immunizing nodes are not constant. Even in the unit-cost case, finding an immunization strategy which maximized the global immunity in a network is NP-hard [9]. However, we show that based on our Behavior-Immunity model, the global immunity function of the network is non-negative, monotone and submodular, i.e., it satisfies the intuitive "*diminishing returns*" property: The marginal improvement in the global immunity while vaccinating a nodes decreases as the set of immunized nodes increases.

We also provide computational experiments on artificially constructed model networks as well as several social and technological networks, showing that change in the behavior of people trying to protect themselves against the infection has significant impact on reducing the infectivity of the network. The interesting observation is that, immunization strategies that gives the same priority to all nodes. i.e., selects the nodes with the same probability to be vaccinated could hardly exploit behavioral changes in the population to improve its result. On the other hand, immunization schemas which take account of the heterogeneity of scale-free networks could appropriately utilized the behavioral changes to practice better results. Our proposed strategy can effectively utilize the effect of locally spreading awareness to prevent an infection from breaking out in the network.

II. Behavior-Immunity Model Definition

Consider a collection of computers interconnected by communication channels $\mathcal{G}_1 = (A, E_1)$ and a set B of computer users with their possible social contacts $\mathcal{G}_2 = (B, E_2)$. Without loss of generality, we can make the simplified but justifiable assumption that each user only uses his/her own computer. The total set of users with their computers can be considered as a two layer network $\mathcal{G} = (\mathcal{V}, E)$ in which $\mathcal{V} = A \cup B$ and $E = E_1 \cup E_2 \cup E_3$ where $E_3 = \{(A_1, B_1), (A_2, B_2), ..., (A_n, B_n)\}$ and $n = |A| = |B|$. A piece of malware such as a computer virus or a self propagating worm can spread through the bottom communication layer with or without user interaction. Such process is often accompanied by a rise in awareness of users in the top social layer and a subsequent change in their behaviour. Users aware of the malware can take measures to reduce their susceptibility by installing anti-virus patches on their computers. At the same time, they can provide their social neighbors by information about the presence of the malware. The Behavior-Immunity model is composed of two layers. The communication layer models the effect of installing anti-virus on the dynamic of malware propagation. The social layer models the valuation of users for buying the anti-virus to protect their computers. In the following we provide a detailed presentation of each data layer and of the basic equations that defines the computational model.

A. Communication Layer and the Global Immunity Model

The computers equipped with anti-virus do not become infected with the malware and do not transmit the infection while exchanging data. Hence, they reduce the risk of infectivity for their susceptible neighbors and protects them from being exposed to the risk of infection.

Consider a network of computers interconnected by communication channels along which information can be shared and exchanged $\mathcal{G}_1 = (A, E_1)$. Infection can spread along the edges between susceptible and infected computers. In case of an outbreak, each node $i \in A$ can become infected through a contact by any of its infected neighbors in the network. On the other hand, i benefits from the protection provided by its neighbors equipped with anti-malware software. When the network is modeled by a graph, the indirect immunity that node i acquires, can be modeled as a function, $q_i : 2^A \to R^+$ of its immunized neighbors in the graph, i.e. $q_i(S) = f_i(\sum_{j \in S \cup \{i\}} w_{ij} / \sum_{k \in A} w_{ik})$ where $S \subseteq A \setminus \{i\}$ is the set of all computer that have been already immunized in the network and w_{ij} is the weight of link e_{ij}.

If n nodes have already acquired immunity against the infection, the global immunity of the network, $G(.)$, is equal to the sum of the immunity of all nodes, i.e. $G = \sum_{i=1}^{n} q_i(.)$. In general, $G(.)$ is the expected fraction of nodes that wont become infected in case of an outbreak. In this work we assume that functions f_i are non-negative, monotone and concave. Such concavity results a concave global immunity function which has also been demonstrated by empirical studies (see figure 1 in [10]). Such concave immunity functions have another implication: once sufficiently many nodes have become vaccinated, it is easy to see that additional vaccination have little impact on the global immunity of the network.

In a communication network, several factors should be considered in determining the link weights. Among them are the number of messages interchanging between i and j and the security vulnerabilities of i. Since in real networks exact information about these parameters cannot be obtained, we assume that we know the distribution from which the link weights are drawn. With this assumption, each w_{ij} is drawn independently from a distribution F_{ij} for all $j \in S$. The distribution $F_{i,S}$ can be derived from the distribution F_{ij} for all $j \in S$ and each $q_i(.)$ can be treated as random variables from distribution $F_{i,S}$ for all $S \subseteq A \setminus \{i\}$ and for all $i \in A$.

B. Social Layer and the Behavioral Model

As contagions spread through the communication network, it will be accompanied by behavioural responses of users trying to protect their computers against the infection. The actions taken by individuals can have strong effects on the epidemic dynamics of the infection.

In social networks, people are affected by decisions of their friends. The feedbacks people receive from their neighbors have significant impact on their decision to adopt the same behavior. In case of an outbreak, those who immunized their computers against the infection increases the awareness of their peers and raise their willingness to become vaccinated. The information people receive from their neighbors will lead to self-initiated, voluntary behavior by which people try to protect their devices from being infected. The more the number of people who are aware about the contagion, the more valuation individuals have for buying the software patches and protect their devices.

Based on the above discussion the valuation of individual i to immunized her/his device can be modeled as a function $v_i : 2^B \rightarrow R^+$ of people who have already vaccinated their computers against infection, i.e. $v_i(S) = f'_i(\sum_{j \in S \cup \{i\}} w_{ij} / \sum_{k \in B} w_{ik})$. The validity of this approach has been demonstrated by empirical studies: [11], [12] studied the probability of joining a community given that some of your friends were already members. [13] studies the effect of social influence on increasing the buyers valuation for an item.

The link weights represent the influences that individuals have on each others. Studies like [11] used the link structure of online social networks to estimate w_{ij}. However, without having exact information about the influences, we assume that we have distributional information about them. With this assumption, the link weights are derived independently from distribution function F'_{ij}. Note that $\sum_{k \in B} w_{ij}$ in the denominator is just a scaling factor for normalizing the influences and does not change the validity of the model. The distribution $F'_{i,S}$ can be derived from the distribution F'_{ij} for all $j \in S$.

C. Properties of the Global immunity model

Naturally, the global immunity function $G(S)$ is *non-negative* and monotone, i.e. for all $A \subseteq B \subseteq V, G(A) \leq G(B)$. Monotonicity of G implies that vaccinating a device can only increase the global immunity in the network. However, the most interesting property of G is its submodularity.

Theorem 1. *Let $I_i(S)$ be the immunity function for node i given that set S have already become vaccinated. If all the immunity functions I_i for $i \in V$ are non-negative, monotone and submodular, then the expected global immunity function $g(S) = \sum_{i \in V \setminus S} I_i(S)$ is a non-negative submodular set function.*

Proof. We use the following facts about submodular functions to prove the sumbodularity of G.

Fact 1. Submodularity is closed under nonnegative linear combinations, i.e. for any submodular functions $f_1, f_2, ..., f_k$ and real numbers $\alpha_1, \alpha_2, ..., \alpha_k$. Then, the set function $g : 2^V \rightarrow R$ where $g(S) = \sum_{i=1}^{k} \alpha_i f_i(S)$ is a submodular function. Consider any submodular function f, the set function g where $g(S) = f(V \setminus S)$ is also submodular. Moreover, for a fixed subset $T \subset V$, function g where $g(S) = f(S \cup T)$ is also submodular.

Using the above facts, in the following we show that assuming monotone concave immunity function I_i for $i \in V$, the global immunity function $G(S)$ is a nonnegative submodular function.

Since the immunity function of the individuals, I_i are non-negative for all $i \in V$, the global immunity of the network $G = \sum_{i=1}^{n} I_i$ is also a non-negative function. In order to prove the submodularity of G, we need to prove that for any set $A \subseteq V$ and $B \subseteq V$:

$$G(A) + G(B) \geq G(A \cup B) + g(A \cap B),$$

Monotonicity of I_i for $i \in V$ follows from the non-negativity of the weights and the non-negativity and monotonicity of f_i. Using this fact, for each $i \in (A \setminus B) \cup (B \setminus A)$ we have:

$$\sum_{i \in A \setminus B} I_i(B) + \sum_{i \in B \setminus A} I_i(A) \geq \sum_{i \in A \setminus B} I_i(A \cap B) + \sum_{i \in B \setminus A} I_i(A \cup B) \tag{1}$$

Now, using submodularity of I_i, for each $i \in V \setminus (A \cup B)$,

$$I_i(A) + I_i(B) \geq I_i(A \cup B) + I_i(A \cap B)$$

Therefore, summing the above inequality for all $i \in V \setminus (A \cup B)$, we get:

$$\sum_{i \in V \setminus (A \cup B)} I_i(A) + \sum_{i \in V \setminus (A \cup B)} I_i(B) \geq \sum_{i \in V \setminus (A \cup B)} I_i(A \cup B) + \sum_{i \in V \setminus (A \cup B)} I_i(A \cap B) \tag{2}$$