Inhibition modeling of future malware diffusion with an evolutionary game theory

Hideyoshi Miura*, Tomotaka Kimura†, and Kouji Hirata‡
* Graduate School of Science and Engineering, Kansai University, Osaka, Japan
E-mail: k846996@kansai-u.ac.jp
† Faculty of Science and Engineering, Doshisha University, Kyoto, Japan
E-mail: tomkimur@mail.doshisha.ac.jp
‡ Faculty of Engineering Science, Kansai University, Osaka, Japan
E-mail: hirata@kansai-u.ac.jp

***Abstract*—In this paper, we introduce an inhibition model of future malware diffusion. The literature has predicted that new types of malware that discovers vulnerabilities of normal hosts with the use of the computational resources of infected host will appear in the near future. The infectability of such malware is incomparably high. One of strategies inhibiting the diffusion of the future malware is that we protect the normal hosts by discovering the vulnerabilities before the malware discovers them. The inhibition model in this paper represents the dynamics of the malware diffusion based on an evolutionary game theory under situations where we adopts this strategy. Through numerical calculations, we clarify the behavior of the inhibition model.**

I. Introduction

In recent years, researches on machine learning has been actively conducted and applied to various fields. There exist some researches that discover vulnerabilities in software with the use of machine learning to protect software against malware [6], [8]. Furthermore, to enhance the performance of the machine learning technology, distributed machine learning methods using the computing resources of a large number of inexpensive computers have been developed in the past [5], [7]. These machine learning technologies can be exploited to malicious attacks. Based on these facts, in [3], the authors have introduced a new concept of future malware named self-evolving botnets. They discover vulnerabilities by means of distributed machine learning with the use of the computing resources of infected hosts. By using discovered vulnerabilities, susceptible hosts could get infected and then are embedded into the self-evolving botnets. The authors have provided an epidemic model that represents the infection dynamics as a continuous-time Markov chain. They have shown that the infectability of the self-evolving botnets is too strong and suggested that urgent measures are required.

In [2], an epidemic model that represents the spread of the recently emerged COVID-19 epidemic, taking into account the behavior of people, has been introduced. This model adopts an evolutionary game theory, which can analyze dynamic behavioral changes, to represent the proportion increase/decrease in people with complex behaviors. Furthermore, the authors have examined how the behavior of people suppresses the spread of the virus. The idea of the epidemic model that counters virus spreading by taking into account the behavior of people can be applied to malware spreading on computer networks.

In this paper, we propose an inhibition model with an evolutionary game theory for countering the diffusion of self-evolving botnets. In the proposed model, we assume that there exists a countermeasure group. The group aims to protect normal hosts by discovering vulnerabilities with the use of the computing resources of members in the group before the botnet malware discovers them. The inhibition model represents the dynamics of the malware diffusion based on the evolutionary game theory that considers the selfish behavior of hosts under situations where there exists the countermeasure group. Through numerical calculations, we examine the fraction of hosts that join/leave the countermeasure group and the change in the fraction of infected hosts.

II. Epidemic model of self-evolving botnets

In [4], an epidemic model representing the infection dynamics of self-evolving botnets has been introduced to clarify their infectability. In what follows, we describe the epidemic model briefly.

In the epidemic model, the state of each host in a network is represented by the Susceptible-Infected-Recovered-Susceptible (SIRS) model shown in Fig. 1, where "S" indicates that the host has vulnerabilities, "I" indicates that the host is infected with the botnet malware, and "R" indicates that the host has no known vulnerabilities. The transitions between the states occur according to the following events:

1) Susceptible hosts could get infected with the botnet malware, and then transition to state I.
2) Susceptible hosts and infected hosts transition to state R when they repair their vulnerabilities and eliminate the botnet malware from themselves, respectively.
3) Hosts in state R transition to state S when the botnet malware discovers a new vulnerability.

Let $S(t)$, $I(t)$, and $R(t)$ denote the fraction of the numbers of hosts belonging to states S, I, and R, respectively, at time t, where $S(t)+I(t)+R(t)=1$. The epidemic model represents the infection dynamics with the following ordinary differential

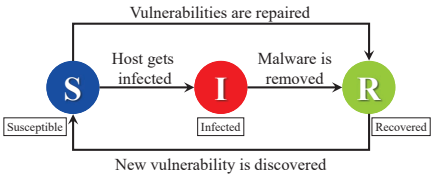

Fig. 1. SIRS model.

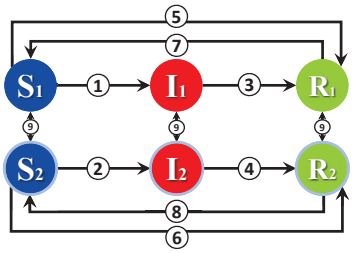

Fig. 2. Infection spread countermeasure model.

equations:

$$\frac{d}{dt}S(t) = -\alpha S(t)I(t) + \eta I(t)R(t) - \delta_s S(t), \quad (1)$$

$$\frac{d}{dt}I(t) = \alpha S(t)I(t) - \delta_i I(t), \quad (2)$$

$$\frac{d}{dt}R(t) = \delta_s S(t) + \delta_i I(t) - \eta I(t)R(t), \quad (3)$$

where α, δ_i, η, and δ_s are parameters denoting the malware infection rate, the malware elimination rate, the new vulnerability discovery rate, and the repair rate, respectively. The self-evolving botnets exploit the computing resources of infected hosts to discover new vulnerabilities. In (1) and (3), the term $\eta I(t)R(t)$ represents this ability, the performance of which is proportional to the number $I(t)$ of infected hosts. As a result, the infectability of the self-evolving botnets becomes too strong, and thus it is difficult for each host to counter against the botnet malware individually.

III. Inhibition Model of Self-Evolving Botnets

A. Inhibition modeling

The inhibition model proposed in this paper assumes that there exists a countermeasure group in a network. The countermeasure group consists of some hosts in the network, which are called member hosts hereafter. It discovers vulnerabilities with the use of computing resources of member hosts in the countermeasure group before the botnet malware discovers them. It then shares the information on the vulnerabilities with other hosts in the network, so that the countermeasure group can protect the hosts and counter the botnet malware. The inhibition model represents the infection dynamics of the botnet malware under the following assumptions:

1) One countermeasure group exists in the network.
2) Any host in the network can participate in the countermeasure group.
3) Member hosts can withdraw from the countermeasure group freely.
4) The vulnerability information discovered by the countermeasure group is shared with all the hosts in the network and repaired immediately.

Fig. 2 shows the state transitions of each host in the inhibition model, which is an extension of the SIRS model shown in Fig. 1. In this model, each host can belong to six states: "S_1", "S_2", "I_1", "I_2", "R_1", and "R_2". States S_n, I_n, and R_n ($n \in \{1, 2\}$) denote susceptible, infected, and recovered states, respectively. If $n = 1$, the host does not belong to the countermeasure group; otherwise, it is a member of the group. Each host transitions according to the following events:

a) Susceptible hosts could get infected by contact with infected hosts (①, ②).
b) Infected hosts transition to the recovered state when the botnet malware is removed from them (③, ④).
c) Susceptible hosts transition to the recovered state by removing their vulnerabilities (⑤, ⑥).
d) When the botnet malware discovers a new vulnerability, recovered hosts transition to the susceptible state (⑦, ⑧)
e) Hosts participate in or withdraw from the countermeasure group (⑨).

Based on these transitions, the inhibition model represents the infection dynamics. Let $S_n(t)$, $I_n(t)$, and $R_n(t)$ ($n \in \{1, 2\}$) denote the fraction of the numbers of susceptible hosts, infected hosts, and recovered hosts, respectively, at time t, where $n = 1$ (resp. $n = 2$) means non-members (resp. members) in the countermeasure group and $S_1(t) + S_2(t) + I_1(t) + I_2(t) + R_1(t) + R_2(t) = 1$. The infection dynamics of the inhibition model is given by the following differential equations:

$$\begin{aligned}\frac{d}{dt}S_1(t) =& -\alpha S_1(t)\{I_1(t) + I_2(t)\} - \delta_s S_1(t) \\ &+ \eta\{I_1(t) + I_2(t)\}R_1(t)C(t) + \tau\Phi_s(t),\end{aligned} \quad (4)$$

$$\begin{aligned}\frac{d}{dt}S_2(t) =& -\alpha S_2(t)\{I_1(t) + I_2(t)\} - \delta_s S_2(t) \\ &+ \eta\{I_1(t) + I_2(t)\}R_2(t)C(t) - \tau\Phi_s(t),\end{aligned} \quad (5)$$

$$\frac{d}{dt}I_1(t) = \alpha S_1(t)\{I_1(t)+I_2(t)\} - \delta_i I_1(t) + \tau\Phi_i(t), \quad (6)$$

$$\frac{d}{dt}I_2(t) = \alpha S_2(t)\{I_1(t)+I_2(t)\} - \delta_i I_2(t) - \tau\Phi_i(t), \quad (7)$$

$$\begin{aligned}\frac{d}{dt}R_1(t) =& \delta_i I_1(t) + \delta_s S_1(t) \\ &- \eta\{I_1(t) + I_2(t)\}R_1(t)C(t) + \tau\Phi_r(t),\end{aligned} \quad (8)$$

$$\begin{aligned}\frac{d}{dt}R_2(t) =& \delta_i I_2(t) + \delta_s S_2(t) \\ &- \eta\{I_1(t) + I_2(t)\}R_2(t)C(t) - \tau\Phi_r(t),\end{aligned} \quad (9)$$

where α, δ_i, η, and δ_s are the same parameters as those in (1)-(3). In addition, τ is a parameter representing the increase rate

in the number of hosts that participate in the countermeasure group. $\Phi_s(t)$, $\Phi_i(t)$, and $\Phi_r(t)$ are variables that determine the behavior of hosts participating in or withdrawing from the countermeasure group, which are derived based on the evolutionary game theory discussed in Section III-B. $C(t)$ is a function that represents the efficiency of the countermeasure group, which is defined later.

In (4)-(7), $\alpha S_n(t)\{I_1(t) + I_2(t)\}$ indicates the average fraction of susceptible hosts getting infected per unit time at time t because $\alpha\{I_1(t) + I_2(t)\}$ is the infectivity of infected hosts. In (6)-(9), $\delta_i I_n(t)$ indicates the average fraction of infected hosts whose the botnet malware is eliminated per unit time at time t. Also, in (4), (5), (8), and (9), $\delta_s S_n(t)$ means the average fraction of susceptible hosts whose vulnerabilities are repaired per unit time at time t. In (4), (5), (8), and (9), $\eta\{I_1(t) + I_2(t)\}R_n(t)C(t)$ indicates the average fraction of recovered hosts whose new vulnerability is found by the botnet malware per unit time at time t. Note that $\eta\{I_1(t) + I_2(t)\}$ means the vulnerability discovery capability of the botnet malware, which implies that the botnet malware exploits the computing resources of infected hosts to discover new vulnerabilities. On the other hand, $C(t)$ $(0 \leq C(t) \leq 1)$ indicates the efficiency of the countermeasure group, which is used to weaken the vulnerability discovery capability of the botnet malware. In this paper, we define $C(t)$ as

$$C(t) = 1 - \{S_2(t) + I_2(t) + R_2(t)\}. \tag{10}$$

(10) supposes that the countermeasure group discovers new vulnerabilities with the use of the computing resources of member hosts (i.e., $S_2(t) + I_2(t) + R_2(t)$) before the botnet malware discovers them, so that it weakens the discovery capability of the botnet malware in proportion to the number of the member hosts.

B. Behavior of hosts based on the evolutionary game theory

We here determine variables $\Phi_s(t)$, $\Phi_i(t)$, and $\Phi_r(t)$ which represents the selfish behavior of hosts based on the evolutionary game theory. Let us assume that there exist two strategies that hosts can take. The strategy 1 is that the hosts do not participate in the countermeasure group (i.e., states S_1, I_1, and R_1). On the other hand, the strategy 2 is that the hosts participate in the countermeasure group (i.e., states S_2, I_2, and R_2). Furthermore, we assume the following:

- Each host reviews its strategy randomly.
- In case of the review, the host compares the cost of the current strategy with the other strategy.
- Based on the comparison, the host determines whether it changes the strategy or not.

Therefore, $\Phi_s(t)$, $\Phi_i(t)$, and $\Phi_r(t)$ are given by

$$\begin{aligned}\Phi_s(t) =& S_2(t)\{S_1(t) + I_1(t) + R_1(t)\}\Theta(\pi_2, \pi_1) \\ &- S_1(t)\{S_2(t) + I_2(t) + R_2(t)\}\Theta(\pi_1, \pi_2),\end{aligned} \tag{11}$$

$$\begin{aligned}\Phi_i(t) =& I_2(t)\{S_1(t) + I_1(t) + R_1(t)\}\Theta(\pi_2, \pi_1) \\ &- I_1(t)\{S_2(t) + I_2(t) + R_2(t)\}\Theta(\pi_1, \pi_2),\end{aligned} \tag{12}$$

$$\begin{aligned}\Phi_r(t) =& R_2(t)\{S_1(t) + I_1(t) + R_1(t)\}\Theta(\pi_2, \pi_1) \\ &- R_1(t)\{S_2(t) + I_2(t) + R_2(t)\}\Theta(\pi_1, \pi_2),\end{aligned} \tag{13}$$

where $\Theta(\pi_a, \pi_b)$ is the probability that a host taking strategy $a \in \{1, 2\}$ changes its strategy to $b \in \{1, 2\} \setminus a$, and π_n is the cost of strategy $n \in \{1, 2\}$. They are given by

$$\Theta(\pi_a, \pi_b) = \frac{1}{1 + \exp\left[\dfrac{\pi_a - \pi_b}{\kappa}\right]}, \tag{14}$$

$$\pi_1 = -\alpha\delta_w\{I_1(t) + I_2(t)\}, \tag{15}$$

$$\pi_2 = -\Omega, \tag{16}$$

where κ is a temperature coefficient that determines how sensitive the host is to the change in its strategy. δ_w and Ω denote weight parameters for the costs of the strategy 1 and the strategy 2, respectively.

In (11)-(13), $X\{S_n(t) + I_n(t) + R_n(t)\}$ $(X \in \{S_k(t), I_k(t), R_k(t)\}, (k, n) \in \{(1, 2), (2, 1)\})$ indicates the average fraction of hosts taking strategy k that contact with hosts taking strategy n. The hosts change their strategies with the probability $\Theta(\pi_a, \pi_b)$. Therefore, (11)-(13) means the average fractions of hosts that change their strategies. Note that the probability $\Theta(\pi_a, \pi_b)$ is determined according to the difference between the costs of the strategies. The cost π_1 of the strategy 1 is proportional to the number of infected hosts, which implies that non-member hosts tend to participate in the countermeasure group as the number of infected hosts increases. This behavior is based on a psychological factor (e.g., many people receive vaccination when infectious disease such as COVID-19 spreads). On the other hand, the cost π_2 of the strategy 2 is constant, which means that each member host provides a certain amount of its computing resource.

IV. Evaluation

A. Model

We examine the behavior of our inhibition model through numerical calculations. We use MATLAB [1] to calculate the differential equations (4)-(9). The initial state of the fraction of hosts in each state is set to $(S_1(0), S_2(0), I_1(0), I_2(0), R_1(0), R_2(0)) = (0.9998, 0.0001, 0.0001, 0, 0, 0)$. This assumes that in the initial state, there are a few infected hosts and the other hosts are susceptible. Furthermore, a few susceptible hosts are members of the countermeasure group. We set the parameters as follows: $\alpha = 10$, $\eta = 10$, $\delta_s = 1$, $\delta_i = 1$, $\tau = 1$, $\delta_w = 1$, and $\kappa = 0.1$.

B. Results

Fig. 3 shows the fraction of the number of hosts in each state against the time elapsed where the weight parameter of the strategy 1 is $\Omega = 1$. In the figure, "Countermeasure" represents the fraction of the number of member hosts in the countermeasure group. As we can see from the figure, in the early stage of infection, about 80% of hosts get infected. As the time elapses, the number of member hosts in

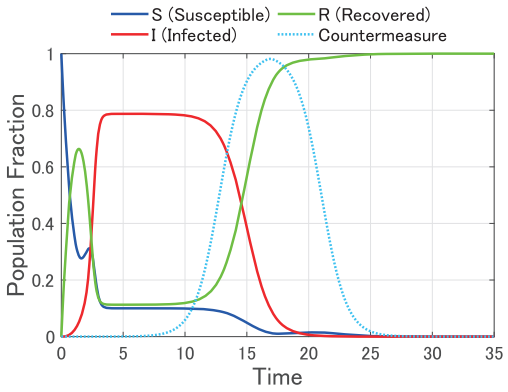

Fig. 3. Fraction of the number of hosts in each state ($\Omega = 1$).

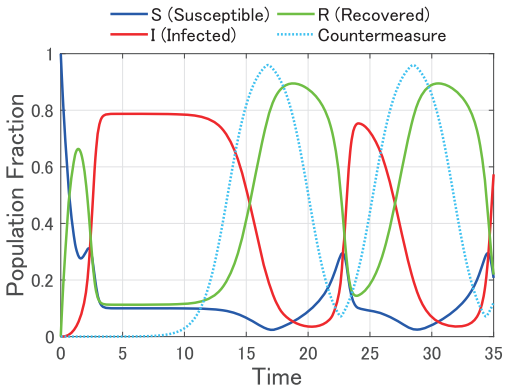

Fig. 4. Fraction of the number of hosts in each state ($\Omega = 2$).

the countermeasure group increases, followed by the number of recovered hosts. As a result, the malware spreading can be suppressed. This result implies that the countermeasure group works well. After the malware spreading is suppressed, the member hosts withdraw from the countermeasure group because the cost π_2 is not negligible.

We then examine the impact of the cost $\pi_2 = -\Omega$ for the countermeasure group. Fig. 4 shows the fraction of the number of hosts in each state against the time elapsed where $\Omega = 2$. From this figure, we observe that member hosts are more likely to withdraw from the countermeasure group, compared with the result in Fig. 3. Therefore, the number of member hosts rapidly decreases before the botnet malware is completely eliminated. As a result, the infection of the botnet malware spreads again. These results indicate that the cost for the countermeasure should be low in order to suppress the spreading of the botnet malware.

Finally, we examine the impact of the infectivity of the botnet malware. Fig. 5 shows the fraction of the number of infected hosts against the time elapsed where $\Omega = 1$. We plot the results of different values of the malware infection rate α. Note that the high malware infection rate means the high infectivity of the botnet malware. As we can see from the figure, the increasing speed of the number of infected host becomes high as the infection rate α increases. Meanwhile, when α is large, the botnet malware is eliminated fast. This is because hosts are more likely to participating in the countermeasure group when the infectivity of the botnet malware is strong, so that the countermeasure group works efficiently.

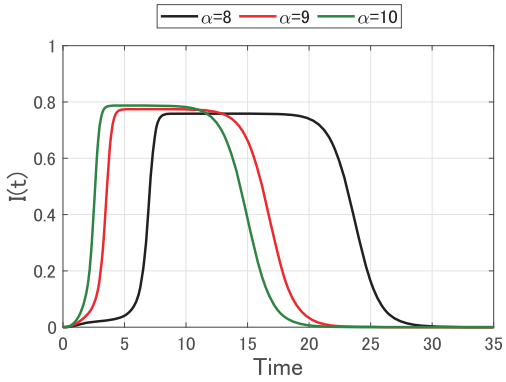

Fig. 5. Impact of the infectivity of the botnet malware ($\Omega = 1$).

V. Conclusions

In this paper, we proposed an inhibition model for countering the diffusion of future malware. The inhibition model represents the dynamics of the malware diffusion based on the evolutionary game theory that considers the selfish behavior of hosts under situations where there exists a countermeasure group. Through numerical calculations, we examined the behavior of the inhibition model. As a future work, we will evaluate the effect of various parameters, such as the repair rate, because the parameters are different for hosts in the real world. In addition, we will consider the spreading behavior of the self-evolving botnets in more realistic scenarios.

Acknowledgement This research was partially supported by JSPS KAKENHI Grant No. 20H04184.

References

[1] MATLAB, https://jp.mathworks.com/products/matlab.html, accessed Jun. 15, 2021.
[2] M. A. Amaral, M. M. de Oliveira, and M. A. Javarone, "An epidemiological model with voluntary quarantine strategies governed by evolutionary game dynamics," *Chaos, Solitons & Fractals*, Volume 143, 2020 (DOI: 10.1016/j.chaos.2020.110616).
[3] T. Kudo, T. Kimura, Y. Inoue, H. Aman, and K. Hirata, "Stochastic modeling of self-evolving botnets with vulnerability discovery," *Computer Communications*, vol. 124, pp. 101–110, 2018.
[4] Y. Kumai, K. Hongyo, T. Kimura, and K. Hirata, "Infection dynamics of self-evolving botnets with deterministic modeling," *in Proc. the 33rd International Conference on Information Networking (ICOIN 2019)*, Kuala Lumpur, Malaysia, Jan. 2019.
[5] E. Meeds, R. Hendriks, S. Faraby, M. Bruntink, and M. Welling, "MLitB: machine learning in the browser," *PeerJ Computer Science*, 2015.
[6] R. Scandariato, J. Walden, A. Hovsepyan, and W. Joosen, "Predicting vulnerable software components via text mining," *IEEE Transactions on Software Engineering*, vol. 40, no. 10, pp. 993–1006, 2014.
[7] M. Wang, H. Zhou, M. Guo, and Z. Zhang, "A scalable and topology configurable protocol for distributed parameter synchronization," *in Proc. Asia-Pacific Workshop on Systems*, Beijing, China, Jun. 2014.
[8] F. Yamaguchi, F. Lindner, and K. Rieck, "Vulnerability extrapolation: assisted discovery of vulnerabilities using machine learning," *in Proc. USENIX on Offensive Technologies*, San Francisco, CA, Aug. 2011.