A non-cooperative resource utilization game between two competing malware

Vineeth Varma, Yezekael Hayel, Irinel-Constantin Morarescu

A non-cooperative resource utilization game between two competing malware

Vineeth S. Varma, Yezekayel Hayel and Irinel-Constantin Morărescu

***Abstract*—In this paper, we consider a population of digital nodes (such as phones, computers, etc.) that are under the attack of two competing malware. These malware infect the nodes in order to exploit their computational resources for specific purposes such as mining crypto-currency, cloud computing, etc. We suppose that each virus spreads following the susceptible-infected-susceptible (SIS) compartmental model. Additionally, we assume that the malware designers can tune the percentage of resource utilization from their host nodes. A higher resource utilization implies a higher instantaneous profit but will also lead to faster detection and elimination (node recovery) of the malware. Once the malware is detected, complete protection of the infected node by means of anti-malware software is also possible at a smaller rate. The proposed setup results in a non-cooperative game between the two players (the malware designers) trying to maximize their profit i.e., the resources utilized from the infected nodes. We characterize and analyze the Nash equilibrium for such a game using a time-scale separation approximation. Finally, we numerically validate the approximation and we compute the price of anarchy.**

***Index Terms*—Computer networks, game theory, compartmental models.**

I. INTRODUCTION

With the ever-growing importance of networked or cloud computing, crypto-mining, and other applications, the computational resources available on a network have become an important target for malicious software, known as malware. Malware is often built by cyber-criminals, and it typically aims to compromise target computers with the ultimate goal of stealing sensitive data or gaining access to private systems. However, in this work, we focus on malware that desires to exploit the computational resources for the profit of their creator, such as by mining crypto-currency. Defense mechanisms such as firewalls and anti-viruses have been developed in order to defend against malicious software but the powerful ones often require investment from the end-users. Moreover, most defense techniques are focused on intrusion detection systems (IDS) [1] and not on supervision systems.

To the best of our knowledge, no work has studied the problem of smart malware that tries to maximize resource utilization without being detected. Specifically, in our setup, a high computational resource utilization will result in large instantaneous profits for the malware designer but will slow the infected targets. Consequently, the owner will be able to easily detect that the device is corrupted. Understanding this trade-off and its impact is essential to design anti-malware strategies from the network point of view. To study this trade-off, we need to analyze the impact of resource utilization in the spread and persistence of the malware on the network. Epidemiological models have been widely and efficiently used to describe the dynamics of malware proliferation over a computer network as seen from [2], [3]. Game theoretical models have also been used to study how the defending nodes may utilize their resources and invest in securing their device or not [4], [5], [6].

Since we consider that the network is under attack by two (competing) malware, classical 1-virus models are insufficient, and we need to look at bi-virus models. In the literature on SIS epidemiological models, a very well known result for the two (competing) virus case is that of the "Winner takes all" [7]. In this case, depending on the initial conditions and the contamination rates of the viruses, one of them becomes extinct and the other propagates all over the network. Note that the term competing here implies that the presence of one virus on a node makes it inaccessible to the other virus. This is the case for some biological viruses. This model has been well studied in the SIS literature and control strategies for reaching the disease-free equilibrium have been proposed in [8].

Unlike the above mentioned works, which study protection strategies with the network agents as the decision makers against an epidemic with fixed parameters, what we study in our paper is the *interaction framework between two malware designers in a game-theoretic setting*. The decision makers (players) in our work are the malware designers, who, before releasing the malware to infect the network, are able to *tune the resource utilization parameter* which impacts their instantaneous profits from an infected node, but also increases the chance for the malware to be detected and removed. Note that similar problem formulations can be encountered in other application domains. For instance, we can consider the opinion dynamics over a social network under the influence of competing marketers. While the SIS model is governed by nonlinear dynamics, in [9] and [10], the authors consider a very basic linear opinion dynamics model ([11]) under the influence of competing entities. They used game-theoretical tools to characterize the Nash equilibrium of the network and the resource allocation in terms of the initial conditions and the node centrality of each individual.

To analyze the game we first emphasize that under a realistic assumption, the overall dynamics evolves on two time scales. Consequently, we first use a rather classical result (see [12] for instance) to decouple the slow and fast dynamics

The work was supported by the ANR under the grant NICETWEET ANR-20-CE48-0009.

V. S. Varma and I-C. Morărescu are with the Université de Lorraine, CNRS, CRAN, F-54000 Nancy, France, constantin.morarescu@univ-lorraine.fr.

Y. Hayel is with the University of Avignon.

leading to good approximations of the original states. With this decoupling the analysis of the game is easier to analyze. The methodology is numerically validated.

The rest of the paper is organized as follows. In Section II, we provide the epidemiological model for the malware spread and the framework for the game between the two competing malware. In Section III, we apply time-scale separation (TSS) on the malware spread to approximate and derive closed-form expressions for the utilities. Next, in Section IV we analyze the resulting non-cooperative game between the two malware and under certain assumptions, provide a characterization of the Nash equilibrium. In Section V numerical examples justify the TSS and demonstrate the feasible utilities, Nash equilibrium, and the price of anarchy for the game. Finally, we provide concluding remarks and perspectives for future research in Section VI.

Notation. Let $\mathbb{R}_{\geq 0} = [0, \infty)$ denote the set of non-negative real numbers. For the ease of exposition, when $k \in \{1, 2\}$ is a player index, to refer to the index of the other player as $-k$, i.e. $-k := 3-k$. We say that a function $f : \mathbb{R} \mapsto \mathbb{R}$ is of order ϵ and denote this by $O(\epsilon)$ if there exist a constant $M \in \mathbb{R}_{\geq 0}$ such that $|f(x)| < M\epsilon, \forall x$.

II. PROPOSED PROBLEM FORMULATION

A. Malware infection model

Our model is inspired by the well-known compartmental epidemic modeling in [13]. In particular two types of infection are considered, which are not often studied in such models and for this feature, we refer to the model in [7]. We use $S(t) \in [0, 1]$ to denote the population fraction of susceptible nodes in the network, $I_1(t), I_2(t) \in [0, 1]$ to denote nodes infected with the first and second malware respectively and finally we use $P(t) \in [0, 1]$ to denote the population of fully protected nodes at any given $t \in \mathbb{R}_{\geq 0}$. As all these variables denote the population fractions, we must have $S(t) + I_1(t) + I_2(t) + P(t) = 1$ at any time $t \geq 0$. For ease of exposition, we will skip explicitly denoting the time dependence for the rest of the paper. The two (competing) malware "susceptible-infected-susceptible-protected" (SISP) model is written as follows.

$$\begin{array}{rcl} \dot{S} & = & -\gamma_1 S I_1 - \gamma_2 S I_2 + \delta_1(u_1) I_1 + \delta_2(u_2) I_2 \\ \dot{I}_1 & = & +\gamma_1 S I_1 - \delta_1(u_1) I_1 - \mu_1(u_1) I_1 \\ \dot{I}_2 & = & +\gamma_2 S I_2 - \delta_2(u_2) I_2 - \mu_2(u_2) I_2 \\ \dot{P} & = & \mu_1(u_1) I_1 + \mu_2(u_2) I_2. \end{array} \tag{1}$$

Here, $\gamma_1, \gamma_2 \in \mathbb{R}_{\geq 0}$ are the infection rates of malware one and two respectively. The resource utilization by malware $k \in \{1, 2\}$ is given by $u_k \in \mathcal{U}$, which is the decision variable for malware k. We consider $|\mathcal{U}| < \infty$ and $\mathcal{U} \subset \mathbb{R}_{>0}$ (a finite discrete set with positive real elements), with $u_{\min} = \min(\mathcal{U}) > 0$ the minimum amount of resources that must be utilized for a malware to be useful. The functions $\delta_k : \mathcal{U} \to \mathbb{R}_{\geq 0}$ and $\mu_k : \mathcal{U} \to \mathbb{R}_{\geq 0}$ denote the recovery rate and protection rates, respectively. A higher resource utilization implies a higher chance of the malware being detected and therefore being purged from the host or for the host to install powerful anti-malware software, making it permanently free of infection from all malware. Thus, δ_k and μ_k are strictly increasing functions.

B. The non-cooperative game model

The revenue (or profit/utility) accumulated by each malware k after it's deployment at time $t = 0$ is given by

$$R_k(u_1, u_2) = \int_0^\infty u_k I_k(t) dt. \tag{2}$$

This expression corresponds to the total amount of computational resources exploited by malware k from the population of nodes over an infinite horizon of time. Clearly, malware interact through the number of infected devices. We define the non-cooperative game $\mathcal{G} := (\{1, 2\}, \{\mathcal{U}, \mathcal{U}\}, \{R_1, R_2\})$ where

1) The set of players (malware designers) is given by $\{1, 2\}$,
2) the action set for each player is $\mathcal{U}$ and
3) the utility function for each player k is $R_k(u_1, u_2)$.

Our objective is to characterize the Nash equilibrium (NE) of this game and to numerically study the price of anarchy, i.e., the loss of total revenue at the social optimum when compared to the NE. To recall, a strategy (u_1^*, u_2^*) is said to be a pure NE if and only if

$$R_k(u_k, u_{-k}^*) \leq R_k(u_1^*, u_2^*) \tag{3}$$

for all $u_k \in \mathcal{U}$ and for all $k \in \{1, 2\}$. That is, no player can increase its revenue by unilaterally deviating from the NE strategy.

III. REVENUE APPROXIMATION UNDER TIME-SCALE SEPARATION

Evaluating $R_k(u_1, u_2)$ analytically is challenging due to the non-linear dynamics (1). Thus, we apply TSS in order to approximate the revenue under the following assumption.

Assumption 1. *There exists a small $\epsilon \in \mathbb{R}_{\geq 0}$ (we write $\epsilon << 1$) such that for all $k \in \{1, 2\}$ and $u_k \in \mathcal{U}$ one has*

$$\mu_k(u_k) \leq \epsilon \delta_k(u_k) \tag{4}$$

The practical meaning of Assumption 1 is that deleting a detected malware is free of cost as the host can uninstall or delete the associated program (at rate δ_k) as soon as it is detected. On the other hand, installing a powerful anti-malware software (at rate μ_k) as soon as a malware is detected is rare since it is not free. Thus, we typically have that $\mu_k(u_k)$ is much smaller than $\delta_k(u_k)$.

Now, we denote the winning malware by

$$k^*(u_1, u_2) = \left\{ k \in \{1, 2\} \,\middle|\, \frac{\delta_k(u_k)}{\gamma_k} < \min\left\{ \frac{\delta_{-k}(u_{-k})}{\gamma_{-k}}, 1 \right\} \right\} \tag{5}$$

For convenience, we will drop the dependence of k^* on (u_1, u_2) and we will simply call it k^*. Note that k^* becomes an empty set (no winner or loser) if $\frac{\delta_1(u_1)}{\gamma_1} = \frac{\delta_2(u_2)}{\gamma_2}$. We use $\phi_k(u_1, u_2)$ to denote the success of malware k given by

$$\phi_k(u_1, u_2) = \begin{cases} 1 & \text{if } k^* = k \\ 0.5 & \text{if } k^* = \emptyset \text{ and } \frac{\delta_k(u_k)}{\gamma_k} < 1 \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

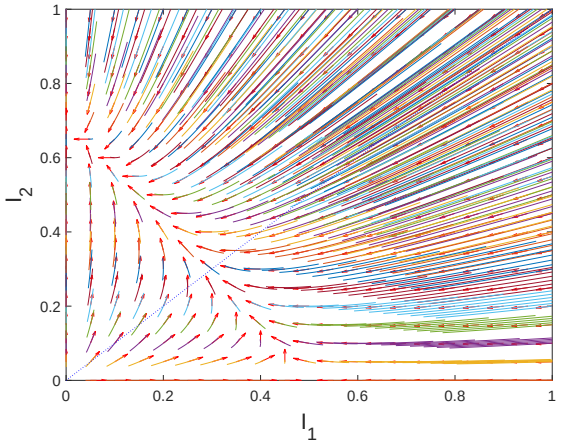

Fig. 1. Phase portrait, i.e., the vector field associated to $(\dot{I}_1, \dot{I}_2)$ for each value of (I_1, I_2), of (1) with $\gamma_1 = \gamma_2 = 0.1$, $\delta_1 = 0.05$, $\delta_2 = 0.03$ and $\mu_1 = \mu_2 = 0$.

Theorem 1. *Under Assumption 1, we have*

$$R_k(u_1, u_2) = \phi_k(u_1, u_2)\left(1 - \frac{\delta_k(u_k)}{\gamma_k}\right)\frac{u_k}{\mu_k(u_k)} + O(\epsilon) \quad (7)$$

for any $I_1(0) > 0, I_2(0) > 0$.

Proof. First, note that we consider $\delta_k(u_k) < \gamma_k$ for at least one $k \in \{1, 2\}$ as otherwise both the malware will die out quickly, making it a trivial case resulting in almost zero revenue for both. This implies that for any u_1, u_2, we can write $\gamma_k := \epsilon^{-1}\mu_k g_k$ and $\delta_k := \epsilon^{-1}\mu_k d_k$ where g_k, d_k are functions of $O(1)$ under assumption 1. We omit the dependence on actions (u_1, u_2) for ease of exposition for the rest of the proof as they do not change during the course of the dynamics.

We apply time-scale separation according to methodology described in the chapter on singular perturbations in [12]. Since $O(\gamma) = 1$, we say that $t_f = t$ is the fast time scale and $t_s = \epsilon t$ is the slow time scale. This allows us to rewrite (1) in the slow time scale as follows.

$$\begin{array}{rcl} \epsilon\frac{dS}{dt_s} & = & -\mu_1 g_1 SI_1 - g_2\mu_2 SI_2 + d_1\mu_1 I_1 + d_2\mu_2 I_2 \\ \epsilon\frac{dI_1}{dt_s} & = & \mu_1 I_1(g_1 S - d_1) - \epsilon\mu_1 I_1 \\ \epsilon\frac{dI_2}{dt_s} & = & \mu_2(g_2 SI_2 - d_2 I_2) - \epsilon\mu_2 I_2 \\ \frac{dP}{dt_s} & = & \mu_1 I_1 + \mu_2 I_2. \end{array} \quad (8)$$

We can similarly rewrite (1) in the fast time scale as

$$\begin{array}{rcl} \frac{dS}{dt_f} & = & -\gamma_1 SI_1 - \gamma_2 SI_2 + \delta_1\mu_1 I_1 + \delta_2\mu_2 I_2 \\ \frac{dI_1}{dt_f} & = & I_1(\gamma_1 S - \delta_1) - \epsilon\frac{\gamma_1}{g_1} I_1 \\ \frac{dI_2}{dt_f} & = & \mu_2(g_2 SI_2 - d_2 I_2) - \epsilon\frac{\gamma_2}{g_2} I_2 \\ \frac{dP}{dt_f} & = & \epsilon\frac{\gamma_1}{g_1} I_1 + \epsilon\frac{\gamma_2}{g_2} I_2. \end{array} \quad (9)$$

It is noteworthy that the dynamics of the fast states S, I_1, I_2 do not depend on the slow state P. This simplifies the expression of the slow and fast approximations. In the sequel we use S^f, I_1^f, I_2^f and P^s to denote the approximations of S, I_1, I_2 and P after the decoupling of the slow and fast dynamics.

Fast dynamics: Setting $\epsilon \to 0$ in (9), we have the following dynamics.

$$\begin{array}{rcl} \frac{dS^f}{dt_f} & = & -\gamma_1 SI_1 - \gamma_2 SI_2 + \delta_1 I_1 + \delta_2 I_2 \\ \frac{dI_1^f}{dt_f} & = & +\gamma_1 SI_1 - \delta_1 I_1 \\ \frac{dI_2^f}{dt_f} & = & +\gamma_2 SI_2 - \delta_2 I_2 \\ \frac{dP^s}{dt_f} & = & 0 \end{array} \quad (10)$$

This dynamics corresponds to the classical two competing-virus SIS model studied in Section 4.2 of [7], which has exactly one stable equilibrium at $S^f = \frac{\delta_{k^*}}{\gamma_{k^*}}$, $I_{k^*}^f = 1 - S^f - P^s$ and $I_{-k^*}^f = 0$ when $k^* \neq \emptyset$ (there is a clear winner). We illustrate this result with a phase portrait of the fast dynamics in Figure 1. On the other hand, if there is no clear winner, i.e., $k^* = \emptyset$, co-existence of the two malware becomes possible. In this case, we will assume symmetric initial conditions which results in an equilibrium of the fast dynamics at $I_k^f(T) = 0.5 - 0.5\frac{\delta_1}{\gamma_1}$ for both players and $S^s = \frac{\delta_1}{\gamma_1}$.

Slow dynamics: Without any loss of generality, let's consider that $k^* = 1$. Setting $\epsilon \to 0$ in (8), we obtain $S^f = \frac{\delta_1}{\gamma_1} = g_1/d_1$ and $I_2^f = 0$ to satisfy the first three lines. All that remains is the slow dynamics

$$\frac{dI_1^f}{dt_s} = -\mu_k I_1^f = -\frac{dP^s}{dt_s} \quad (11)$$

Since $P(0) = 0$, applying the results in [12], we obtain

$$I_{k^*}(t) = I_{k^*}^f(t) + O(\epsilon) = \left(1 - \frac{\delta_{k^*}(u_{k^*})}{\gamma_{k^*}}\right)\exp(-\mu_{k^*} t) + O(\epsilon)$$

for all $t > 0$. Additionally as $I_k(t)$ is exponentially converging to 0, even the integral of the approximation term should be bounded and of the order of ϵ. Thus, we have

$$\tilde{R}_{k^*}(u_1, u_2) = \int_0^\infty u_{k^*}\left(1 - \frac{\delta_{k^*}(u_{k^*})}{\gamma_{k^*}}\right)\exp(-\mu_{k^*} t)dt \quad (12)$$

with $\tilde{R}_{k^*}(u_1, u_2) - R_{k^*}(u_1, u_2) = O(\epsilon)$. Thus results in (7) for all cases with a clear winner and half of this expression in case of a tie. □

Indeed, it is clear that when the two malware do not co-exist on the same host, the analysis is much simpler as the only stable equilibrium is that of the one with the smaller recovery rate for the reduced-order dynamics. On the other hand, when both malware may co-exist, there are two (locally) stable equilibria for the reduced-order dynamics and thus the equilibrium reached depends a lot on the initial conditions as will be demonstrated in Section V.D. Since $I_1(0), I_2(0)$ are assumed to be non-controllable, we consider that $I_1(0) = I_2(0)$ when we evaluate the revenue during a "tie" (both malware have the same ratio between their recovery and spreading rates). Next, we study the game $\mathcal{G}$ when the revenue function is given by the results in Theorem 1.

IV. Non-cooperative game analysis

In this section, we characterize the NE of the non-cooperative game $\mathcal{G}$ defined in Section II. The results from

Theorem 1 provide a closed-form expression for the utility functions, and this allows us to write the best response of player k to an action u_{-k} by the other player as

$$BR_k(u_{-k}) = \arg\max_{\mathcal{U}} \left\{ \left(1 - \frac{\delta_k(u_k)}{\gamma_k}\right) \frac{u_k}{\mu_k(u_k)} \phi_k(u_1, u_2) \right\}$$

Next, we characterize the NE of the game $\mathcal{G}$ as stated in the following.

A. Existence of pure NE

The existence of pure NE is usually not guaranteed in non-cooperative games, whereas in our setting we have the proof of its existence. Additionally, for some cases, the non-cooperative game may have several pure NE.

Proposition 1. *The game $\mathcal{G}$ admits at least one pure NE given by*

1) $(u_{\min}, u_{\min})$ *if* $\frac{\delta_1(u_{\min})}{\gamma_1} = \frac{\delta_2(u_{\min})}{\gamma_2}$,
2) *All* $(BR_1(u_{\min}), u_2)$ *with* $u_2 \in \mathcal{U}$ *such that* $k^*(BR_1(u_{\min}), u_2) = 1$, *when* $\frac{\delta_1(u_{\min})}{\gamma_1} < \frac{\delta_2(u_{\min})}{\gamma_2}$,
3) *All* $(u_1, BR_2(u_{\min}))$ *with* $u_1 \in \mathcal{U}$ *such that* $k^*(u_{\min}, BR_2(u_{\min})) = 2$ *otherwise.*

Furthermore, any additional NE (u_1, u_2) if they exist, must satisfy $\frac{\delta_1(u_1)}{\gamma_1(u_1)} = \frac{\delta_2(u_2)}{\gamma_2(u_2)}$.

Proof. We prove this case by case. First, if $\frac{\delta_1(u_{\min})}{\gamma_1} = \frac{\delta_2(u_{\min})}{\gamma_2}$ we have that $\frac{\delta_k(u_k)}{\gamma_k} > \frac{\delta_{-k}(u_{\min})}{\gamma_{-k}}$ for any $u_k > u_{\min}$ as δ_k is a strictly increasing function. This implies that $R_k(u_k; u_{-k} = u_{\min}) = 0$ for all $u_k > u_{\min}$, proving that $(u_{\min}, u_{\min})$ is a NE for this case.

In the second case, player 1 is playing its best response to player 2 and so by definition can not improve his utility by deviating. On the other hand, player 2 is losing and has 0 revenue for all $u_2 \in \mathcal{U}$ as $u_{\min}$ is already the smallest action playable. Thus, it can not improve its utility either. Thus, $(BR_1(u_{\min}), u_{\min})$ is a NE if $k^*(BR_1(u_{\min}), u_{\min}) = 1$. Similar arguments hold for case 3.

Next, consider that there exists some NE (u_1, u_2) such that $\frac{\delta_1(u_1)}{\gamma_1(u_1)} \neq \frac{\delta_2(u_2)}{\gamma_2(u_2)}$. This excludes the additional NE case mentioned in the proposition statement. Without loss of generality let's say $\frac{\delta_1(u_1)}{\gamma_1(u_1)} > \frac{\delta_2(u_2)}{\gamma_2(u_2)}$. This means that player 2 is the winner of the epidemic and thus $R_1(u_1, u_2) = 0$. If, $u_1 = u_{\min}$, then $BR_2(u_{\min})$ is by definition the best choice for player 2 and so all the NE are fully captured by case 3).

Otherwise, if $u_1 > u_{\min}$ and $u_2 \notin BR_2(u_{\min})$, and (u_1, u_2) is an NE, then $u_2 \in BR(u_1)$ by definition of the NE and the best response. This implies that $\frac{\delta_1(u_{\min})}{\gamma_1} < \frac{\delta_2(u_2)}{\gamma_2}$ as the best responses must match otherwise. Then player 1 can deviate to $u_{\min}$ and improve his utility as $u_2 \neq BR_2(u_{\min})$, and (u_1, u_2) is therefore not an NE by contradiction. □

The previous proposition shows the existence of at least one pure NE, but non-cooperative games generally allow for multiple Nash equilibria [14]. In next section, we are able to determine them explicitly by assuming linear recovery and protection rates.

B. Special cases for the recovery and protection rates

Consider two adjacent elements of $\mathcal{U}$ (recall that $\mathcal{U}$ is a finite discrete set), i.e., any $U_1, U_2 \in \mathcal{U}$ with $U_1 < U_2$ such that there exists no other $U \in \mathcal{U}$ such that $U_1 < U < U_2$. Now, we say that the action set is dense with order $\alpha > 1$ if $U_2 \leq \alpha U_1$ for all U_1, U_2 adjacent.

Assumption 2.

$$\delta_k(u_k) := a_k + b_k u_k \tag{13}$$

and $\mu_k(u_k) = \epsilon \delta_k(u_k)$ *with* $a_k, b_k \in \mathbb{R}_{\geq 0}$, $\epsilon \in (0, 1)$ *and small.*

Since ϵ is taken to be small, Assumption 2 automatically implies that Assumption 1 is satisfied. Now, we have the following result for the uniqueness of the NE.

Proposition 2. *Under Assumption 2, the only pure NE for game $\mathcal{G}$ are the ones stated in Proposition 1 items (1)-(3) if $\mathcal{U}$ is of order $\alpha \leq 2$.*

Proof. Consider that there exists some NE (u_1, u_2) other than the ones described in Proposition 1 items 1)-3). That is consider that (u_1, u_2) is an NE with $\frac{\delta_1(u_1)}{\gamma_1(u_1)} = \frac{\delta_2(u_2)}{\gamma_2(u_2)}$. Due to there being no winner, the utility for player 1 is given by

$$R_1(u_1, u_2) = (1 - \frac{a_1 + b_1 u_1}{\gamma_1}) \frac{u_1}{2\epsilon(a_1 + b_1 u_1)} \tag{14}$$

Now, consider that player 1 deviates his strategy to $u_1' = u_1 - \Delta$. His new utility is given by

$$R_1(u_1 - \Delta, u_2) = (1 - \frac{a_1 + b_1 u_1 - \Delta}{\gamma_1}) \frac{u_1 - \Delta}{\epsilon(a_1 + b_1 u_1 - b_1 \Delta)} \tag{15}$$

as he wins. We have

$$\begin{aligned} &R_1(u_1 - \Delta, u_2) - R_1(u_1, u_2) > \\ &C \left(\tfrac{u_1 - \Delta}{(a_1 + b_1 u_1 - b_1 \Delta)} - 0.5 \tfrac{u_1}{(a_1 + b_1 u_1)} \right) > \\ &C \left(\tfrac{u_1 - \Delta}{(a_1 + b_1 u_1)} - 0.5 \tfrac{u_1}{(a_1 + b_1 u_1)} \right) \end{aligned} \tag{16}$$

where $C = \epsilon^{-1} \left(1 - \frac{a_1 + b_1 u_1 - \Delta}{\gamma_1}\right)$ which is positive if $\Delta \leq u_1/2$. Since $u_1 \leq 2u_1'$ for any u_1, u_1' adjacent, (u_1, u_2) can not be an NE, resulting in a contradiction. □

V. Numerical performance analysis

A. Validity of TSS approximation

First, we demonstrate that (1) is well approximated by the TSS done in Theorem 1. For this purpose, we take $\gamma_1 = \gamma_2 = 0.1$, $\delta_1(u_1) = 0.01 + 0.05u_1$, $\delta_2(u_2) = 0.01 + 0.03u_2$ with $u_1 = u_2 = 1$. We then take $\mu_k(u_k) = 0.1\delta_k(u_k)$ in the first figure and $\mu_k(u_k) = 0.02\delta_k(u_k)$ in the second figure, i.e., the TSS factor $\epsilon = 0.1$ and 0.02 respectively to represent relatively higher and lower protection rates.

In the simulation for Figure 2, we compute that $R_1(u_1, u_2) = 10.5$ and $R_2(u_1, u_2) = 134$ versus $\hat{R}_2(u_1, u_2) = 150$, where $\hat{R}$ denotes the TSS approximation from Theorem 1. This indicates a relative error, i.e. $\frac{\hat{R}_2(u_1,u2) - R_2(u_1,u2)}{\hat{R}_2(u_1,u2)}$ of 11%. On the other hand, in Figure 3, we observe $R_1(u_1, u_2) = 13$ and $R_2(u_1, u_2) = 727$ with the TSS approximation $\hat{R}_2(u_1, u_2) = 750$ indicating a

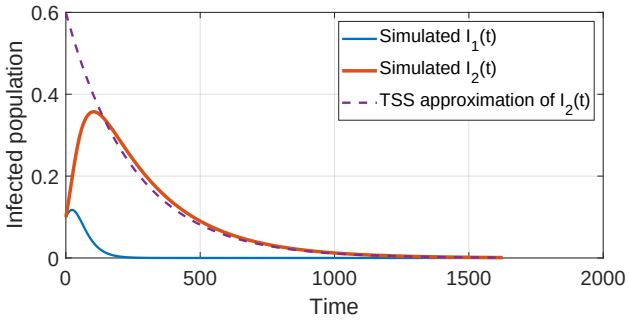

Fig. 2. The first malware is seen to die out faster than the second but still gains some revenue due to ϵ being not so small.

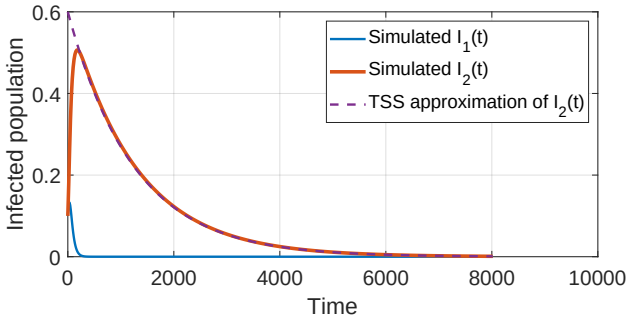

Fig. 3. The first malware dies out rapidly and gains very little revenue and the TSS approximation is quite good for the infected population of the second malware.

relative error of around 3%. Simulations with other values of $\epsilon \in \{0.005, 0.01, 0.05, 0.2\}$ suggest that the relative error is of the order of ϵ.

B. NE analysis of the game $\mathcal{G}$

Next, we will take $\gamma_1 = \gamma_2 = 0.1$, $\delta_1 = \delta_2 = 0.01 + 0.03u_1$, $\mu_k = 0.02\delta_k(u_k)$, $\mathcal{U} = \{0.1, 0.2, .., 1\}$ and plot all the feasible utilities in Figure 4, with the NE marked in red. Note that these rate functions satisfy Assumption 2. Indeed, as proven in Proposition 1, $(u_{\min}, u_{\min})$ is a NE and is in fact the only NE as proven in 2 for this case as $\mathcal{U}$ is of order 2.

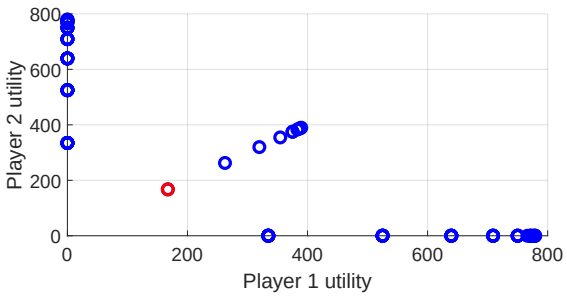

Fig. 4. All the feasible utilities with the NE marked in red.

Next, we remove some of the elements of the action set and demonstrate that when the order of the set is higher than two, multiple NE may exist. First, we look at all the resulting utilities with $\mathcal{U} = \{0.1, 0.2, 0.7\}$ in Table I, which allows exactly one pure NE at $(0.1, 0.1)$. However, removing the element 0.2 from the action set results in multiple NE as can be seen from Table II with $(0.7, 0.7)$ being an additional NE. The two tables above highlight an effect similar to the famous Braess' Paradox, allowing additional options results in a poor NE for both players. In the second case, if both malware play $u_k = 1$ they don't gain anything by deviating. On the other hand, allowing the action 0.2 as in Table I allows either player to deviate and improve their utility.

TABLE I
(REVENUE 1, REVENUE 2) WITH SEVERAL CHOICES OF ACTIONS. THE ONLY PURE NE STRATEGY IS $(0.1, 0.1)$.

Actions	$u_1 = 0.1$	$u_1 = 0.2$	$u_1 = 0.7$
$u_2 = 0.1$	(167,167)	(0,334)	(0,334)
$u_2 = 0.2$	(334,0)	(262,262)	(0,525)
$u_2 = 0.7$	(334,0)	(525,0)	(390,390)

TABLE II
(REVENUE 1, REVENUE 2) FOR A SMALLER SET OF ACTIONS.

Actions	$u_1 = 0.1$	$u_1 = 0.7$
$u_2 = 0.1$	(167,167)	(0,334)
$u_2 = 0.7$	(334,0)	(390,390)

C. Interpretation and discussion

Typically in game theory, the "social optimum" is defined as the strategy profile maximizing the sum of the individual utilities. Then, the price of anarchy compares the sum of the utilities at the NE to that at the social optimum. However, in this context, where the players are malicious entities, the objective of the network and of the public, in general, is to minimize the profits earned by the malware. In this sense, anarchy is something desired.

In the example studied in Table I, $(0.7, 0.7)$ is the strategy maximizing the sum utility of the two players which results in $R_1 = R_2 = 390$. However, due to the competition between the malware, the only NE is one with $R_1 = R_2 = 167$. In a broader sense, the implication here is that when multiple malware or viruses compete on a common network, the one utilizing the least resources "wins" as it is harder to detect or is not worth it for the users to be protected against. If the software or hardware allows for a much smaller $u_{\min}$ and the malware can be tuned well ($\mathcal{U}$ is of sufficiently small order), the NE will be correspondingly worse. For example, if $\mathcal{U} = \{0.05, 0.1, 0.2, 0.7\}$ the NE utility becomes 96 for both players. Therefore, allowing malware more freedom in their choice of creating codes that utilize a smaller value of resources may result in intensifying the competition between the malware, resulting in them earning smaller profits, consequently improving the end-user welfare.

D. Alternate virus model

The model (1) assumes that the two malware can not co-exist on the same computer. This kind of epidemiological model is perfectly suited for certain virus strains but may not always be suitable for computer viruses and malware. Thus,

we will also provide a brief analysis of the two non-interacting virus SISP model written as follows.

$$\begin{aligned}
\dot{S} &= -\gamma_1 S I_1 - \gamma_2 S I_2 + \delta_1(u_1) I_1 + \delta_2(u_2) I_2 \\
&\quad + \delta_M(u_1, u_2) I_M \\
\dot{I}_1 &= +\gamma_1 S I_1 - \gamma_2 I_1 I_2 - \delta_1(u_1) I_1 - \mu_1(u_1) I_1 \\
\dot{I}_2 &= +\gamma_2 S I_2 - \gamma_1 I_1 I_2 - \delta_2(u_2) I_2 - \mu_2(u_2) I_2 \\
\dot{I}_M &= (\gamma_1 + \gamma_2) I_1 I_2 - (\delta_1(u_1) + \delta_2(u_2)) I_M \\
&\quad - (\mu_1(u_1) + \mu_2(u_2)) I_M \\
\dot{P} &= \mu_1(u_1) I_1 + \mu_2(u_2) I_2 + \mu_M(u_1, u_2) I_M
\end{aligned} \tag{17}$$

This model allows for both malware to co-exist on the same computer, however, the presence of the two malware will imply a higher recovery and protection rate as the user will easily detect the presence of malware. The TSS approximation for (17) can be done in a similar fashion as in Theorem 1 to obtain the fast dynamics

$$\begin{aligned}
\dot{S} &= -\gamma_1 S I_1 - \gamma_2 S I_2 + \delta_1(u_1) I_1 + \delta_2(u_2) I_2 + \delta_M I_M \\
\dot{I}_1 &= +\gamma_1 S I_1 - \delta_1(u_1) I_1 - \gamma_2 I_1 I_2 \\
\dot{I}_2 &= +\gamma_2 S I_2 - \delta_2(u_2) I_2 - \gamma_1 I_1 I_2 \\
\dot{I}_M &= (\gamma_1 + \gamma_2) I_1 I_2 - (\delta_1 + \delta_2) I_M \\
\dot{P} &= 0
\end{aligned} \tag{18}$$

First, note that $S = \frac{\delta_k}{\gamma_k}$, $I_k = 1 - S$, $I_{-k} = 0$, $I_M = 0$ are two equilibria for this dynamics. However, unlike the previous system, when $\frac{\delta_k}{\gamma_k} < 1$ for both the malware, the two endemic equilibria are locally stable as seen from the phase portrait in Figure 5 obtained by setting $I_M \to 0$. While this is not the main focus of the paper, it is interesting to note that even in the case where both malware may co-exist in the same computer, there is still a clear "winner takes all" behavior, with the winner being decided by both the epidemiological parameters as well as the initial conditions.

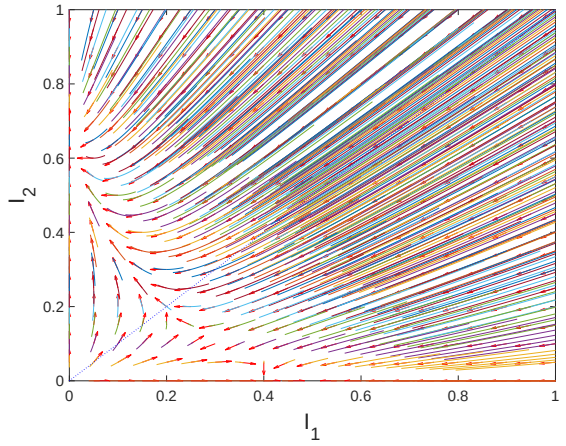

Fig. 5. Phase portrait of (17) with $\gamma_1 = \gamma_2 = 0.1$, $\delta_1 = 0.05$, $\delta_2 = 0.03$ and $\mu_1 = \mu_2 = 0$.

Thus, to simplify, we assume that $I_1(0) = I_2(0)$. Now, if $\frac{\delta_1}{\gamma_1} < \frac{\delta_2}{\gamma_2}$, for any $I_1 \geq I_2$, $I_1 < 1 - \frac{\delta_1}{\gamma_1}$, we have

$$\dot{I}_1 - \dot{I}_2 = +\gamma_1 S I_1 - \delta_1(u_1) I_1 - (\gamma_2 S I_2 - \delta_2(u_2) I_2) \tag{19}$$

which is positive as $I_1(t) \geq I_2(t)$ inductively and $\frac{\delta_1}{\gamma_1} < \frac{\delta_2}{\gamma_2}$. Therefore, the equilibrium with $I_1 = 0$ is never reached and since the only other stable equilibrium is the one with $S = \frac{\delta_1}{\gamma_1}$, $I_1 = 1 - S$, $I_2 = 0$, this equilibrium is reached. Similar arguments hold for the winner being player 2 when $\frac{\delta_1}{\gamma_1} > \frac{\delta_2}{\gamma_2}$. Thus, the results of this case correspond with that of Theorem 1 when the initial conditions are symmetric and maybe obtained in a similar fashion following the proof of Theorem 1.

VI. Conclusion

In this paper, we study a game model which characterizes the competition between two malware trying to take over a network. We use an epidemiological model to characterize the spread of each malware as a function of their resource utilization rate and then provide a closed-form expression for the malware revenue using time-scale separation. We are then able to characterize the Nash equilibrium for the resulting game under the assumption that both malware starts with the same number of infected nodes. Numerical simulations demonstrate the validity of the time-scale approximation and the features of the game such as the price of anarchy. In future works, we would like to consider several regions or clusters in the network with a given interaction graph between these regions to have a more realistic model of the network as studied in [8].

References

[1] R. Kemmerer and G. Vigna, "Intrusion detection: a brief history and overview," *Computer*, vol. 35, no. 4, pp. supl27–supl30, 2002.

[2] S. Peng, S. Yu, and A. Yang, "Smartphone malware and its propagation modeling: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 925–941, 2013.

[3] S. Yu, G. Gu, A. Barnawi, S. Guo, and I. Stojmenovic, "Malware propagation in large-scale networks," *IEEE Transactions on Knowledge and data engineering*, vol. 27, no. 1, pp. 170–179, 2014.

[4] T. Spyridopoulos, G. Oikonomou, T. Tryfonas, and M. Ge, "Game theoretic approach for cost-benefit analysis of malware proliferation prevention," in *IFIP International Information Security Conference*. Springer, 2013, pp. 28–41.

[5] Y. Hayel, S. Trajanovski, E. Altman, H. Wang, and V. M.P., "Complete game-theoretic characterization of sis epidemics protection strategies," in *53rd IEEE Conference on Decision and Control*. IEEE, 2014, pp. 1179–1184.

[6] A. R. Hota and S. Sundaram, "Game-theoretic vaccination against networked sis epidemics and impacts of human decision-making," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 4, pp. 1461–1472, 2019.

[7] B. A. Prakash, A. Beutel, R. Rosenfeld, and C. Faloutsos, "Winner takes all: competing viruses or ideas on fair-play networks," in *Proceedings of the 21st International Conference on World Wide Web*, 2012, pp. 1037–1046.

[8] J. Liu, P. E. Paré, A. Nedić, C. Y. Tang, C. L. Beck, and T. Başar, "Analysis and control of a continuous-time bi-virus model," *IEEE Transactions on Automatic Control*, vol. 64, no. 12, pp. 4891–4906, 2019.

[9] A. M. Masucci and A. Silva, "Strategic resource allocation for competitive influence in social networks," in *Communication, Control, and Computing (Allerton), 2014 52nd Annual Allerton Conference on*. IEEE, 2014, pp. 951–958.

[10] V. S. Varma, I.-C. Morărescu, S. Lasaulce, and S. Martin, "Marketing resource allocation in duopolies over social networks," *IEEE Control systems letters*, vol. 2, no. 4, pp. 593–598, 2018.

[11] M. H. DeGroot, "Reaching a consensus," *Journal of the American Statistical Association*, vol. 69, no. 345, pp. 118–121, 1974.

[12] H. K. Khalil, *Nonlinear Systems (2nd ed.)*. Society for Industrial and Applied Mathematics, 1996.

[13] N. Bailey, *The mathematical theory of infectious diseases and its applications*. New York: Hafner Press, 1975.

[14] J. T. D. Fudenberg, *Game Theory*. The MIT Press, 1991.