Active Nodes Maximization in a Virus Spread Model: An SI2R Malware Propagation Model

Arthur Farel Ngoufo, Arnold Willie Kouam Kounchou, Yezekael Hayel, Charles Kamhoua, Gabriel Deugoué

Active Nodes Maximization in a Virus Spread Model: An SI2R Malware Propagation Model

Arthur NGOUFO[1 [0009−0001−2014−0540]], Willie KOUAM[1,2 [0000−0002−6804−868X]], Yezekael HAYEL[2 [0000−0003−3891−3916]], Gabriel DEUGOUÉ[1 [0000−0003−1015−0902]], and Charles KAMHOUA[3 [0000−0003−2169−5975]]

[1] University of Dschang, Dschang, Cameroon
narthurfarel@gmail.com
willie.kouam@alumni.univ-avignon.fr
agdeugoue@yahoo.fr
[2] CERI/LIA, Avignon Université, France
yezekael.hayel@univ-avignon.fr
[3] DEVCOM Army Research Laboratory, USA
charles.a.kamhoua.civ@army.mil

Abstract. The threat of malware is increasing and poses significant computer security risks to both individuals and organizations. Understanding the tactics employed by these malicious software entities and their dynamics during the epidemic process is crucial for designing robust defense strategies and ensuring the protection of computer systems. In this article, we investigate a population of digital nodes (such as phones, computers, ...) under attack by modeling the network using a susceptible-infected-resistant (SI2R) compartmental model, where hosts can transition between susceptible, infected, or resistant states. Our model considers two types of infected nodes: active nodes, whose resources are exploited, and passive nodes, which spread the virus. Both active and passive nodes can develop resistance with certain probabilities, which are influenced by the resource utilization percentages set by the malware designer. Thus, rather than optimizing resource utilization, the malware's goal is to maximize the number of active hosts at the end of the process. To achieve this objective, we aim to determine the optimal percentage of passive nodes to consider at each period, recognizing that the variation in the number of active nodes depends on the number of passive nodes.

Keywords: Computer networks · Optimal control · Epidemic model · Two timescale method · SPSA method [4]

1 Introduction

Malware, short for malicious software, encompasses a range of threats such as viruses, worms, trojans, and ransomware. These malicious software entities engineered by cyberattackers are designed to disrupt, damage, or gain unauthorized access to computer systems, by exploiting security vulnerabilities. Driven by the prospect of significant financial or political gains, malware creators dedicate considerable efforts towards compromising numerous networked computers to fulfill their nefarious objectives. In recent years, the significance of malware as a pivotal component in security breaches has been underscored by the emergence of zero-day attacks and advanced persistent threats [9,10]. Gaining insight into spreading processes within complex networks is crucial for devising effective control strategies across various domains, including epidemiology and public health [1], as well as the security of cyberphysical networks [8], etc. Given

[4] DISTRIBUTION A. Approved for public release: distribution unlimited.

the high stakes, numerous epidemiological models have been developed to elucidate the dynamics of malware propagation within computer networks. The most basic epidemic model is the SI model, which includes the Susceptible (S) and Infected (I) states. 'Susceptible' describes a vulnerable individual who has not yet been infected, while 'Infected' refers to an individual who is both a carrier and a propagator of the pathogen. Nodes transition from S to I at the rate of infection. The SIR model extends this by adding the recovered (R) state, representing individuals who have recovered and gained immunity. In this model, nodes transition from I to R at the rate of recovery. The SIS model, on the other hand, allows infected nodes to return to the susceptible state, as they do not gain immunity. Finally, the $SEIR$ model introduces the exposed (E) state, indicating individuals who are infected but either asymptomatic or not yet able to transmit the pathogen until they transition to the I state. This model is useful for considering diseases with an incubation period. Basic versions of these epidemic models are generally deterministic but may include probabilistic elements [4,5,7,6]. In our context, we study the behavior of malware that desires to maximize the propagation and then exploit the computational resources for the profit of its creator. Indeed, considering the growing importance of networked or cloud computing, crypto-mining, and other applications, the computing resources available on a network have become a major target for malware. Very often the cyber attacker chooses which of the machines to infect will be used to mine crypto because of the machine's power and which will be used to spread the malware because of their low detection. To simulate how malware spreads and evolves in such a context (to develop effective defense strategies.), we also consider a compartmental model and differentiate between two categories of infected nodes: active nodes, used by the malware designer to exploit resources, and passive nodes, employed solely for propagating the malware within the network. The distinction between these two types of infected nodes is crucial, as it affects the overall impact of the malware on the network. The reduction in the number of passive nodes corresponds to a decrease in the propagation rate, consequently limiting the malware's maximum number of active nodes at the end of the process. Furthermore, using passive nodes' resources to propagate the infection degrades their performance, potentially leading to detection and subsequent cleaning by the device owner. Likewise, high utilization of computational resources in active nodes yields significant immediate gains for the malware designer but slows down the infected targets, increasing the likelihood of detection and removal. Therefore, passive and active nodes can become resistant at any time with certain probabilities that we assume are predetermined. This study thus focuses on a specific aspect of malware propagation: *the maximization of active nodes within a network*. Our main challenge is to determine the optimal percentage of passive nodes to maximize the number of active nodes at the end of the process. By understanding the interplay between active and passive nodes, we can identify strategies that malware designers might use to achieve the goals, thereby informing the development of more robust defense strategies. We employ a susceptible-infected-resistant ($SI2R$) compartmental model to simulate the dynamics of malware propagation. In this model, a susceptible node (at risk of infection) that comes into contact with a passive node can become either active or passive, the transition probabilities from infected state to resistant state are influenced by various factors, including the resource utilization percentages set by the malware designer. The rest of the paper is organized as follows. In the next section, the model and the problem are described. Then, in section 3, we provide the mathematical analysis of the model, by showing the various properties needed to solve the model. Following this, we use the two timescale and $SPSA$ methods to compute the solution of the model in section 4 and make some experiments. We provide a conclusion of our work in section 5.

2 Model description

In this section, we outline the problem formulation, providing a comprehensive description of the continuous-time infection model.

Throughout this paper, we denote the population fraction of susceptible nodes at each time t in the network by $m_s(t) \in [0,1]$. The active nodes for the malware are denoted by $m_a(t)$ and belongs to the interval $[0,1]$. The passive nodes that transmit the viruses are represented by $m_p(t) \in [0,1]$, and the population of fully protected nodes at any given time $t \geqslant 0$ is denoted by $m_r(t) \in [0,1]$. Since these variables represent population fractions, we must have $m_s(t)+m_a(t)+m_p(t)+m_r(t) = 1$ at any time $t \geqslant 0$. For simplicity, we will omit the explicit time dependence in the remainder of the paper. The *"susceptible-active, passive-protected"* ($SI2R$) model for the two competing malware is expressed as follows:

$$(\mathcal{S}) : \begin{cases} \dot{m}_s = -\lambda m_s m_p \\ \dot{m}_a = \lambda p m_s m_p - \gamma_0 m_a \\ \dot{m}_p = \lambda(1-p) m_s m_p - \gamma_1 m_p \\ \dot{m}_r = \gamma_0 m_a + \gamma_1 m_p \end{cases}$$

In the preceding system, $\lambda \in [0,1]$ is the infection rate of the malware. A susceptible node that is in contact with a passive infected node also becomes infected with λ rate. This new infected node is either active with probability p or passive with probability $1-p$. If it becomes passive, it is therefore a new contaminator, while if it becomes active, it cannot infect others but contributes rewards to the contamination process. However, this activity may slow down the computer, prompting the computer owner to detect and remove the virus at a rate of γ_0. Passive agents, on the other hand, continue to infect other susceptible machines but can also be discovered with a lower detection rate of $\gamma_1 < \gamma_0$.

As stated before, the malware's objective is to maximize the number of active nodes at the end of the process. That is, to find the optimal probability of making a contaminated agent active, to maximize the peak of the proportion of active agents, as shown by equation (1).

$$\max_{p\in[0,1]} \left(\max_t m_a(t) \right) = \max_{p\in[0,1]} F(p), \tag{1}$$

where $F(p) = \max_t m_a(t)$, represents the malware's objective function, which is the peak of the proportion of active agents for a given p.

A tradeoff arises with p as follows: when p approaches 0, only a small number of new agents become active, while when p approaches 1, only a few passive agents emerge, thereby restricting the infection process.

3 Mathematical analysis of the model

We assume that the rate of susceptible computers who become infected at the initial time is greater than the rate of additional passive computers at the initial time. i.e.:

$$-\lambda m_p(0) + \lambda(1-p) m_s(0) - \gamma_1 < 0. \tag{2}$$

Lemma 1. *The function $f : [0, +\infty[\to \mathbb{R}$ such that $f(t) = m_s(t)m_p(t)$ is decreasing, i.e., $f'(t) < 0$.*

Proof. There are two cases to consider: the case where the m_p function is increasing and the case where it is decreasing.

1. If m_p is decreasing: $f(t) = m_s(t)m_p(t) \iff f'(t) = \dot{m}_s(t)m_p(t) + m_s(t)\dot{m}_p(t) < 0$.
2. If m_p is increasing: $\dot{m}_p > 0$, that is, $m_s(t) > \dfrac{\gamma_1}{\lambda(1-p)}$. Furthermore, $f(t) = m_s(t)m_p(t) \iff f'(t) = m_s(t)m_p(t)(-\lambda m_p(t) + \lambda(1-p)m_s(t) - \gamma_1)$. Let's consider $g(t) = -\lambda m_p(t) + \lambda(1-p)m_s(t) - \gamma_1$, therefore $g'(t) = \lambda m_p(t)(-2\lambda(1-p)ms(t) + \gamma_1)$. Moreover, $m_s(t) > \dfrac{\gamma_1}{\lambda(1-p)} \implies m_s(t) > \dfrac{\gamma_1}{2\lambda(1-p)}$, i.e., $-2\lambda(1-p)ms(t) + \gamma_1 < 0$. Therefore, $g'(t) < 0$, which means that $g(t) < g(0)$ and then $f'(t) = m_s(t)m_p(t)g(t) < m_s(t)m_p(t)g(0)$. According to the hypothesis at equation (2), $(-\lambda m_p(0) + \lambda(1-p)m_s(0) - \gamma_1) < 0$ i.e., $m_s(t)m_p(t)(-\lambda m_p(0) + \lambda(1-p)m_s(0) - \gamma_1) < 0$. Thus, $f'(t) < 0$.

In both cases, we obtain the following result $f'(t) < 0$.

■

The previous lemma allows us to prove the following proposition, which states that the malware's objective function is well-defined, which assumes that the maximum of the m_a function exists.

Proposition 1. *The malware's objective function:*

$$F(p) = \begin{cases} m_a(0) \text{ if } \lambda p m_s(0)m_p(0) - \gamma_0 m_a(0) < 0 \\ \dfrac{\lambda p}{\gamma_0} m_s(t_p)m_p(t_p) \text{ otherwise;} \end{cases} \tag{3}$$

where, $t_p \in]0, +\infty[$ is well-defined, and the maximum is unique.

Proof. – If $\lambda p m_s(0)m_p(0) - \gamma_0 m_a(0) < 0$, then $\dot{m}_a$ is decreasing, that is, $m_a(t) \leqslant m_a(0)$, $\forall t \in [0, \infty[$.

– Let's suppose that $\lambda p m_s(0)m_p(0) - \gamma_0 m_a(0) \geqslant 0$, then $\exists t_p \in [0, \infty[$ such that $\dot{m}_a(t_p) = 0$, since $\lim\limits_{t \to +\infty} m_a(t) = 0$. Moreover, $\dot{m}_a(t_p) = 0 \iff \dfrac{\lambda p}{\gamma_0} m_s(t_p)m_p(t_p) = m_a(t_p)$. $F(p)$ is well-defined.

Furthermore, suppose there are $t_1, t_2 \in [0, \infty[$, $t_1 \neq t_2$ such that $F(p) = m_a(t_1) = m_a(t_2)$. In this case, $\dot{m}_a(t_1) = \dot{m}_a(t_2) = 0$. Therefore, $m_a(t_1) = \dfrac{\lambda p f(t_1)}{\gamma_0} = m_a(t_2) = \dfrac{\lambda p f(t_2)}{\gamma_0} \iff f(t_1) = f(t_2)$, with $f(t) = m_s(t)m_p(t)$. However, as shown in the lemma (1), f is a decreasing function, that is, $t_1 < t_2 \implies f(t_1) > f(t_2)$. Thus, $F(p)$ is unique $\forall p \in [0, 1]$.

The proposition (1) above shows that for a fixed $p \in [0, 1]$ there is a unique maximum on $t \in [0, \infty[$. We now need to show that $\max\limits_{p \in [0,1]} F(p)$ exists, since the aim is to determine the probability $p \in [0, 1]$ for which the function $F(p)$ is maximal. To achieve this, we first need to show that the function F is continuous on $[0, 1]$.

Proposition 2. *The function F as previously defined is continuous on the interval* $[0, 1]$.

Proof. Our differential system can be rewritten as $\dot{M}(t) = U(M, p)$, where $M = \begin{bmatrix} m_s \\ m_a \\ m_p \\ m_r \end{bmatrix}$

and $U(M, p) = \begin{bmatrix} -\lambda m_s m_p \\ \lambda p m_s m_s - \gamma_0 m_a \\ \lambda(1-p)m_s m_p - \gamma_1 m_p \\ \gamma_0 m_p + \gamma_1 m_a \end{bmatrix}$

According to the *Cauchy-Lipschitz* theorem, given that the differential system is autonomous (i.e., independent of t) and the function U is continuous with respect to the state variable M and the parameter p, the system, with known initial conditions, admits a unique solution for all $p \in [0,1]$.
Furthermore, as stated in *Pierron Théo's book on Differential Equations*[5], to demonstrate that the solution of the differential system is continuous with respect to p, it suffices to show that U is continuous and globally Lipschitz with respect to the state variable and the parameter p.

Since U is, at least $\mathcal{C}^1$ with respect to p on the compact interval $[0,1]$, U is globally Lipschitz. Thus, the solution is continuous with respect to p, and consequently, the mapping $p \mapsto m_a(t)$ is continuous for all $t \in J$, where J is any segment of $[0, +\infty[$.

■

Lemma 2. *It is certainly not in the malware designer's interest to choose $p = 0$, that is, $F'(0) = 0$.*

Proof. Let's consider $p = 0$, so $\dot{m}_a(t) = \lambda p m_s(t) m_p(t) - \gamma_0 m_a(t)$ becomes $\dot{m}_a(t) = -\gamma_0 m_a(t)$ and then m_a decreases and $F(0) = m_a(0)$. Let now $\epsilon > 0$ very small, such that $\lambda \epsilon m_s(0) m_p(0) - \gamma_0 m_a(0) < 0$, therefore, $F(\epsilon) = m_a(0)$ (according to the definition of $F(p)$).
Moreover, $F'(0) = \lim_{\epsilon \to 0} \dfrac{F(\epsilon) - F(0)}{\epsilon} = \dfrac{m_a(0) - m_a(0)}{\epsilon} = 0$ ■

The proposition (3) below establishes the existence of a solution to the problem:

$$\begin{cases} \dot{M}(t) = U(M,p) \\ p^* \in \arg\max(F(p)),\ F \text{ as defined by}(1) \end{cases} \tag{4}$$

Proposition 3. *1. The problem (4) has at least one solution;*

2. If $\lambda p m_s(0) m_p(0) - \gamma_0 m_a(0) \leqslant 0$ for all $p \in [0,1]$, then the problem has an infinite number of solutions.

3. Otherwise ($\exists\ p \in [0,1], \lambda p m_s(0) m_p(0) - \gamma_0 m_a(0) > 0$), the solution is non-trivial for certain conditions on initial values and parameters that we will determine, i.e., $p^* \in (0,1)$. In other words i.e. it is in the cyber attacker's interest to invest in passive and active nodes simultaneously.

Proof. 1. Since F is a continuous function on a compact set, it admits a maximum.

2. Let us suppose that $\lambda p m_s(0) m_p(0) - \gamma_0 m_a(0) \leqslant 0$ for all $p \in [0,1]$. According to the definition of F, we have $F(p) = m_a(0)$ for all $p \in [0,1]$.
3. Let's consider the following system:

$$(S) : \begin{cases} \dot{m}_s(t) = -\lambda m_p(t) m_s(t) \\ \dot{m}_p(t) = \lambda(1-p) m_p(t) m_s(t) - \gamma_1 m_p(t) \end{cases}$$

We aim to determine the solutions very close to m_s and m_p; dividing the second equation of (S) by the first one, we obtain: $\dfrac{dm_p}{dm_s} = -(1-p) + \dfrac{\gamma_1}{\lambda m_s}$, i.e.,

$$m_p(t) = -(1-p) m_s(t) + \frac{\gamma_1}{\lambda} \ln(m_s(t)) + m_p(0) + (1-p) m_s(0) - \frac{\gamma_1}{\lambda} \ln(m_s(0)).$$

[5] https://perso.eleves.ens-rennes.fr/ tpier758/cours/edo.pdf

We substitute this back to obtain a new differential equation depending only on m_s:

$$\dot{m}_s(t) = \lambda(1-p)m_s^2(t) - \gamma_1 m_s(t)\ln(m_s(t)) - \lambda\left(m_p(0) + (1-p)m_s(0) - \frac{\gamma_1}{\lambda}\ln(m_s(0))\right). \quad (5)$$

Using a first-order approximation of the function $t \mapsto \ln(m_s(t))$: $\ln(m_s(t)) \approx \ln(m_s(0)) - \lambda m_p(0)t$. Substituting this into (5), we get a new differential equation for $\tilde{m}_s$, which is an approximation of m_s:

$$x'(t) = Ax^2(t) - (B - Ct)x(t) \quad (6)$$

where $x(t) = \tilde{m}_s(t)$, $A = \lambda(1-p)$, $C = \gamma_1\lambda m_p(0)$, and $B = \lambda m_p(0) + Am_s(0)$. The solution (6) is given by:

$$\tilde{m}_s(t) = \frac{\exp(-Bt + Ct^2/2)}{\frac{1}{m_s(0)} + K(t)}, \quad \text{with} \quad K(t) = \int_0^t -A\exp(-Bu + Cu^2/2)du \quad (7)$$

Now substituting $\tilde{m}_s(t)$ back into the second equation of (S), we get an approximate value $\tilde{m}_p$ of m_p:

$$\tilde{m}_p(t) = \frac{pm_p(0)}{m_s(0)}\frac{\exp(-\gamma_1 t)}{\frac{1}{m_s(0)} + K(t)}. \quad (8)$$

The expression for $\tilde{m}_a$ is therefore given by:

$$\tilde{m}_a(t) = \exp(-\gamma_0 t)\left(m_a(0) + \lambda\int_0^t p\frac{m_s(0)m_p(0)\exp(\gamma_0 u - \gamma_1 u)\exp(-Bu + C\frac{u^2}{2})}{(1 + m_s(0)K(u))^2}\,du\right) \quad (9)$$

We want to show that $F'(1) < 0$. We know that for all $p \in [0,1]$, there exists $t_p \in [0, +\infty[$ such that $F(p) = m_a(t_p, p)$. Therefore, it is sufficient to show that $\tilde{m}_a(t_{1-\epsilon}, 1-\epsilon) > \tilde{m}_a(t_1, 1)$. We will first fix the time in the expression of $\tilde{m}_a$ and compare $\tilde{m}_a$ as a function of the probability p. We will gradually eliminate the terms that do not influence our comparison and study the remaining function. At a result, we need to show that the function

$$p \longmapsto \int_0^t p\frac{m_s(0)m_p(0)\exp(-Bu + Cu^2/2)}{(1 + m_s(0)K(u))^2}\,du \quad \text{is decreasing at 1.}$$

Note that, if we consider three positive functions f, g, and h

$$\int_0^t f(u)du < \int_0^t g(u)\,du \implies \int_0^t f(u)h(u)du < \int_0^t g(u)h(u)\,du$$

.

$$\text{Let} \quad g(t,p) = \int_0^t \exp(-Bu + Cu^2/2) \quad \text{and} \quad G(t,p) = \int_0^t p\frac{m_s(0)m_p(0)\exp(-Bu + Cu^2/2)}{(1 + m_s(0)K(u))}du.$$

After integration, $G(t,p) = \dfrac{pg(t,p)}{1 - \lambda(1-p)m_s(0)g(t,p)}$, and then, $\dfrac{\partial G}{\partial p}(t,1) = g(t,1) + \dfrac{\partial g}{\partial p}(t,1) - \lambda m_s(0)g^2(t,1)$; since $\dfrac{\partial G}{\partial p}(t,p) = \dfrac{g(t,p)(1 - \lambda(1-p)m_s(0)g(t,p)) + p\dfrac{\partial g}{\partial p}(t,p) - \lambda p m_s(0)g^2(t,p)}{(1 - \lambda(1-p)m_s(0)g(t,p))^2}$.

We notice that $\dfrac{\partial G}{\partial p}(0,1) = 0$, therefore, we need to show that the function $t \longmapsto h(t) = g(t,1) + \dfrac{\partial g}{\partial p}(t,1) - \lambda m_s(0)g^2(t,1)$ is decreasing for slightly larger values of t.

$h'(t) = g'(t)[1 - 2\lambda m_s(0)g(t,1) + \lambda m_s(0)t]$, and the function $q(t) = 1 - 2\lambda m_s(0)g(t,1) + \lambda m_s(0)t$ is decreasing if its derivative is negative.

$$q'(t) = -2\lambda g'(t,1) + \lambda m_s(0) = -2\lambda m_s(0)\exp(-Bt + C\frac{t^2}{2}) + \lambda m_s(0) < 0$$
$$\iff \exp(-Bt + C\frac{t^2}{2}) > \frac{1}{2} \iff \lambda m_p(0) - 2\gamma_1 \ln(2) < 0$$

The function h' is decreasing, but $h'(0) > 0$ and $\lim_{t\to+\infty} h'(t) = -\infty$. By the intermediate value theorem, $\exists! t_0 \in \mathbb{R}_+^*$ such that $h'(t_0) = 0$. We have to show that there exists $t_1 \in \mathbb{R}_+^*$ such that $t_0 \leqslant t_1 < t_{max}$, the point that maximizes m_a (note that, $t_1 < t_{max} \iff \dot{\tilde{m}}_a(t_1) > 0$, since $\dot{\tilde{m}}_a(t_{max}) = 0$ and $\dot{\tilde{m}}_a$ is an increasing function). This implies that at the moment when m_a reaches its maximum, the function h' is negative, hence the function h is decreasing. Consequently, the function G decreases towards 1, and thus $F'(1) < 0$.

$$\dot{\tilde{m}}_a(t) = \lambda\tilde{m}_s(t)\tilde{m}_p(t) - \gamma_0\tilde{m}_a(t) = \lambda m_p(0)m_s(0)\exp(-\gamma_1 t)\exp(-Bt + C\frac{t^2}{2}) - \gamma_0\exp(-\gamma_0 t)(m_a(0)$$
$$+ \lambda\int_0^t m_s(0)m_p(0)\exp(\gamma_0 u - \gamma_1 u)\exp(-Bu + C\frac{u^2}{2})\,du)$$

By using the above condition $\exp(-Bt + C\frac{t^2}{2}) > \frac{1}{2}$ and the inequality,

$$\int_0^t m_s(0)m_p(0)\exp(\gamma_0 u - \gamma_1 u)\exp(-Bu + C\frac{u^2}{2})\,du \leq \exp(\gamma_0 t - \gamma_1 t)\int_0^t \exp(-Bu + C\frac{u^2}{2})\,du$$

we obtain,

$$\dot{\tilde{m}}_a(t) > m_p(0)m_s(0)\left[\lambda\exp\left(-\frac{\gamma_1 t}{2}\right) - \gamma_0\exp(-\gamma_0 t)m_a(0) - \gamma_0\exp(-\gamma_1 t)\int_0^t \exp\left(-Bu + \frac{Cu^2}{2}\right)du\right]$$

We observe from the expressions of h' and $\dot{\tilde{m}}_a$ that it is sufficient to find t_1 that satisfies the following inequalities:

$$\lambda\int_0^{t_1}\exp(-Bu + C\frac{u^2}{2})\,du < \frac{\lambda}{2\gamma_0} - m_a(0) \tag{10}$$
$$1 - 2\lambda m_s(0)\int_0^{t_1}\exp(-Bu + C\frac{u^2}{2})du + \lambda m_s(0)t \leqslant 0 \tag{11}$$

From (10), such a t_1 is then such that : $\frac{1 + \lambda m_s(0)t_1}{2\lambda m_s(0)} \leqslant \frac{1}{2\gamma_0} - \frac{m_a(0)}{\lambda} \iff t_1 \leqslant \frac{-1}{\lambda m_s(0)} + \frac{1}{\gamma_0} - \frac{2m_s(0)}{\lambda}$

since from (11), $\frac{1 + \lambda m_s(0)t_1}{2\lambda m_s(0)} \leqslant \int_0^{t_1}\exp(-Bu + C\frac{u^2}{2})\,du$.

As stated before, we know that h' is first positive before becoming negative, so it suffices to find that t_1 that satisfies (10) and makes h' negative. Then, by the intermediate value theorem, we will know that $t_0 \mid h'(t_0) = 0$ is located before $t_{max} \mid \dot{\tilde{m}}_a(t_{max}) = 0$.
Note that, $\int_0^t \exp(-Bt + C\frac{u^2}{2})\,du \geqslant \exp(\frac{-B^2}{2C})t$, therefore,

$$1 - 2\lambda m_s(0)\int_0^t \exp(-Bu + C\frac{u^2}{2})du + \lambda m_s(0)t \leqslant 1 - 2\lambda m_s(0)\exp(\frac{-B^2}{2C})t + \lambda m_s(0)t \leqslant 0 \quad \text{for}$$

$t \geqslant \dfrac{1}{1-2\exp(\dfrac{-B^2}{2C})\lambda m_s(0)}$. A sufficient condition to find $t_1 \in \mathbb{R}_+^*$ such that $\mathrm{t}_0 \leqslant \mathrm{t}_1 < \mathrm{t}_{\max}$ is : $\dfrac{1}{1-2\exp(\dfrac{-B^2}{2C})\lambda m_s(0)} \leqslant \dfrac{-1}{\lambda m_s(0)} + \dfrac{1}{\gamma_0} - \frac{2m_s(0)}{\lambda}$. Therefore, with the above sufficient, but not necessary conditions satisfied, the solution to the control problem is non-trivial, i.e.,

$$\frac{1}{1-2\exp(\frac{-B^2}{2C})\lambda m_s(0)} \leq \frac{-1}{\lambda m_s(0)} + \frac{1}{\gamma_0} - \frac{2m_s(0)}{\lambda} \text{ and } \lambda m_p(0) - 2\gamma_1 \ln(2) < 0 \implies F'(1) < 0. \quad (12)$$

■

4 Numerical resolution of the control problem by two timescale convergence and the *SPSA* method

4.1 Overview

We introduce the function N defined by the following differential equation: $\dot{N}(t) = max(0, \dot{m}_a(t))$. Since m_a has a maximum for all p, then N reaches this same maximum and becomes constant, i.e., $\lim\limits_{t\to+\infty} N(t) = \max\limits_{t>0} m_a(t)$. The idea here is to build an algorithm where we use two-speed scales. We use the *two timescale method,* consisting of a fast dynamic to calculate the epidemic peak and a slow dynamic to compute the probability that maximizes the epidemic peak [3]. The optimal control problem thus becomes:

$$\begin{cases} \dot{M}(t) = f(t,p) \\ \dot{p} = \nabla F(p);\ F\ defined\ by\ (1) \end{cases}$$

4.2 Algorithm

We use the variable-step gradient descent method for the dynamics of the differential system and the $SPSA$ (simultaneous perturbation stochastic approximation) method [2] for updating the probability p. We then have the following numerical scheme:

$$\begin{cases} M(n+1) = M(n) + a_n \dot{M}(n) \\ N(n+1) = N(n) + a_n max(0, \dot{m}_a(n)) \\ p(n+1) = p(n) + b_n g(p(n)) \end{cases}$$

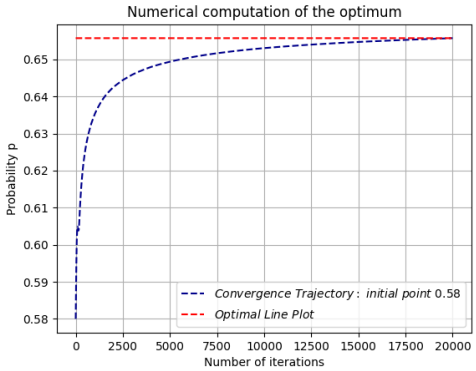
Where g is an approximation of the objective function F. We thus have:

$$g(p(n)) = \frac{F(p(n) + c_n \Delta_n) - F(p(n) - c_n \Delta_n)}{2c_n \Delta_n}$$

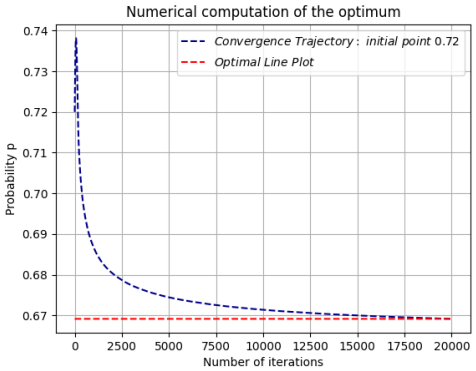
The sequences $a_n,\ b_n\ et\ c_n$ are chosen so that, $\sum\limits_n a_n = \sum\limits_n b_n = \infty$, $\sum\limits_n (a_n^2 + b_n^2) < \infty$, $\dfrac{b_n}{a_n} \to 0$. The last condition characterizes the faster convergence of the system's dynamics compared to that of p, Δ_n is a random sequence.

4.3 Numerical evaluation

For numerical evaluation, we consider $a_n = a/n$, $b_n = b/(1 + n\log(n))$, $c_n = c/n^7$ and Δ_n a sequence of random variables of the normal distribution. We make simulations with initial values $m_a(0) = 0.1$, $m_p(0) = 0.05$ and $m_s(0) = 0.85$. Another parameters set are $\lambda = 0.1$, $\gamma_0 = 0.01$, $\gamma_1 = 0.005$.

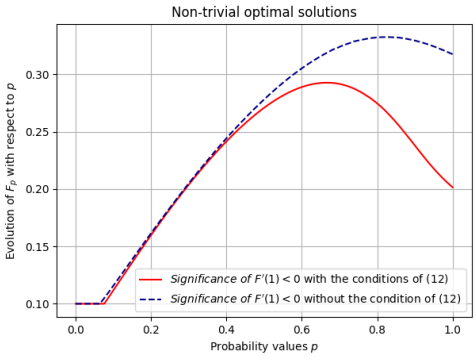


(a) **Optimal value approximation starting from a lower initial value** $p_0 = 0.58$**.** Employing a two-scale convergence algorithm combined with the SPSA method, *we achieve convergence to an approximate optimum probability value* $p = 0.6557$.

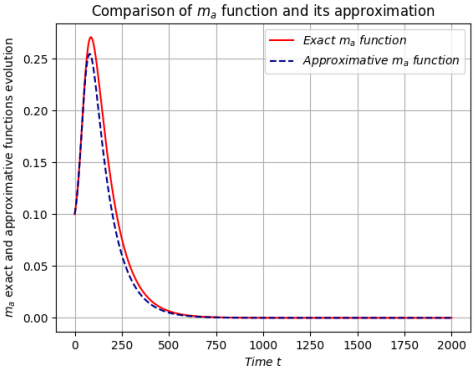


(b) **Optimal value approximation starting from an upper initial value** $p_0 = 0.72$**.** Applying a two-scale convergence algorithm combined with the SPSA method, *we achieve convergence to an approximate optimum probability value* $p = 0.6691$.

Fig. 1: Optimal probability computation for two initial distinct values of p_0.



(a) **Representation of the function** F**.** From the preliminary results, under certain sufficient but not necessary conditions, the optimal probability p is non-trivial ($p \notin \{0, 1\}$). *For instance, in this case, the optimal probability is* $p \approx 0.666$ *for* $m_p(0) = 0.05$. *Moreover, when* $m_p(0) = 0.12$, *the conditions of* (12) *are not satisfied but,* $p \approx 0.824$.



(b) **Comparison of** m_a **functions.** Simulations over 2000 periods for $p = 0.5$ indicate that *the approximate value* $\tilde{m}_a$ *of the function* m_a *we propose is close to the exact value of* m_a *obtained by solving the system* $\mathcal{S}$.

Fig. 2: Non-trivial optimum computation (2a) & m_a functions' comparison (2b).

The objectives of these experiments are threefold: (1a) and (1b) to establish the convergence of the applied method towards the optimal solution within our model (the optimal line is obtained by plotting the straight line passing through the last point of convergence of the algorithm), (2a) to demonstrate the existence of a non-trivial optimal solution under the conditions specified in (12), and (2b) to assess the approximation error of the function m_a graphically.

5 Conclusion

In this study, we explored the dynamics of malware propagation within a network of digital nodes using the susceptible-infected-resistant ($SI2R$) compartmental model, focusing on maximizing the number of active nodes—those whose resources are exploited by the malware—by strategically determining the optimal percentage of passive nodes of the infection process. Our analysis revealed that the variation in the number of active nodes is intrinsically linked to the number of passive nodes, demonstrating how malware designers can maximize resource exploitation. Indeed, as illustrated in Figure (2a), when the initial number of passive nodes is low, the malware designer tends to invest heavily to increase the number of passive nodes, favoring lower values of p. Our findings contribute to the field by offering new perspectives on malware strategies and informing the development of more effective countermeasures. However, our work has certain limitations, particularly that the value of p is fixed throughout the process and that the number of new active nodes during the process does not depend on the number of previous ones. Future research should apply the $SI2R$ model to real-world data for validation, expand the model to include additional factors such as varying infection rates and network topologies and develop automated systems for dynamic defense strategies based on real-time data and predicted malware behavior. Ultimately, our study highlights the importance of strategic analysis in understanding and combating malware, advancing theoretical knowledge, and practical cybersecurity strategies to protect digital networks.

Acknowledgments

The research was sponsored by the U.S. Army Research Office and was accomplished under Cooperative Agreement Numbers W911NF-19-2-0150, W911NF-22-2-0175, and Grant Number W911NF-21-1-0326. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

6 Appendix

Lemma 3. *1. Let us consider the following differential equation:*

$$x'(t) = Ax^2(t) - (B - Ct)x(t) \tag{13}$$

With the initial condition

$$x(0) = m_s(0)$$

So the solution of (13) is given by (14)

$$x = \frac{\exp(-Bt + Ct^2/2)}{\dfrac{1}{m_s(0)} + K(t)}, \quad \text{with} \quad K(t) = \int_0^t -A\exp(-Bu + Cu^2/2)du \tag{14}$$

2. *Let us suppose that:*

$$\dot{\tilde{m}}_p(t) = \lambda(1-p)\tilde{m}_p(t)x(t) - \gamma_1\tilde{m}_p(t)$$

with the initial condition $\tilde{m}(0) = m_p(0)$ *Then*

$$\tilde{m}_p(t) = \frac{pm_p(0)}{m_s(0)} \frac{\exp(-\gamma_1 t)}{\frac{1}{m_s(0)} + K(t)}.$$

Proof. 1. This is a Bernoulli equation, and we will solve it by a change of variable.
Let $Z = 1/X$

$$x'(t) = Ax^2(t) - (B - Ct)x(t) \quad \Longleftrightarrow \quad -\frac{Z'(t)}{Z^2(t)} = \frac{A}{Z^2(t)} - (B - Ct)\frac{1}{Z}$$

The equation in Z is then written as:

$$Z'(t) = -A + (B - Ct)Z$$

The solution of the homogeneous equation is given by:

$$Z(t) = K\exp(Bt - \frac{Ct^2}{2}) \quad K \in \mathbb{R}$$

To determine a particular solution of the equation in Z, we vary the constant K and look for the particular solution in the form $Z(t) = K(t)\exp(Bt - \frac{Ct^2}{2})$ and we have:

$$Z'(t) + K'(t)\exp(-Bt + \frac{Ct^2}{2}) = -A + (B - Ct)Z$$

Thus,

$$K'(t) = -A\exp(Bt - \frac{Ct^2}{2})) \quad \Longleftrightarrow \quad K(t) = \int_0^t -A\exp(-Bu + \frac{Cu^2}{2})du + C_1$$

A particular solution of the equation in Z is:

$$Z(t) = \exp(Bt - \frac{Ct^2}{2})\int_0^t -A\exp(-Bu + \frac{Cu^2}{2})du$$

The general solution for Z is then given by:

$$Z(t) = \exp(Bt - \frac{Ct^2}{2})(K + \int_0^t -A\exp(-Bu + \frac{Cu^2}{2})du)$$

The solution of (13) is given by:

$$x(t) = \frac{\exp(-Bt + \frac{Ct^2}{2})}{K + \int_0^t -A\exp(-Bu + \frac{Cu^2}{2})du}$$

Using the initial conditions, we obtain:

$$x = \frac{\exp(-Bt + Ct^2/2)}{\frac{1}{m_s(0)} + K(t)}, \quad \text{with} \quad K(t) = \int_0^t -A\exp(-Bu + \frac{Cu^2}{2})du$$

2. We have

$$\begin{aligned}
& \dot{\tilde{m}}_p(t) = A\tilde{m}_p(t)x(t) - \gamma_1\tilde{m}_p \\
\iff \quad & \frac{\dot{\tilde{m}}_p(t)}{\tilde{m}_p} = Ax - \gamma_1 \\
\iff \quad & \frac{\dot{\tilde{m}}_p(t)}{\tilde{m}_p} = \frac{\exp(-Bt + Ct^2/2)}{\frac{1}{m_s(0)} + K(t)} - \gamma_1 \\
\implies \quad & \ln(\tilde{m}_p(t)) = -\ln(\frac{1}{m_s(0)} + K(t)) - \gamma_1 t \implies \qquad \tilde{m}_p(t) = k_2 \frac{\exp(-\gamma_1 t)}{\frac{1}{m_s(0)} + K(t)} \quad k_2 \in \mathbb{R}
\end{aligned}$$

By using the initial condition, we then obtain:

$$\tilde{m}_p(t) = \frac{m_p(0)}{m_s(0)} \frac{\exp(-\gamma_1 t)}{\frac{1}{m_s(0)} + K(t)}.$$

References

1. Bailey, N.T.: The mathematical theory of infectious diseases and its applications. No. 2nd ediition (1975)
2. Bhatnagar, S., Prasad, H., Prashanth, L., Bhatnagar, S., Prasad, H., Prashanth, L.: Stochastic approximation algorithms. Stochastic Recursive Algorithms for Optimization: Simultaneous Perturbation Methods pp. 17–28 (2013)
3. Borkar, V.: Multiple Timescales, pp. 117–138 (02 2024). https://doi.org/10.1007/978-981-99-8277-6_8
4. Brauer, F., Van den Driessche, P., Wu, J., Allen, L.J.: Mathematical epidemiology, vol. 1945. Springer (2008)
5. Kermack, W.O., McKendrick, A.G.: A contribution to the mathematical theory of epidemics. Proceedings of the royal society of london. Series A, Containing papers of a mathematical and physical character **115**(772), 700–721 (1927)
6. Li, M.Y., Muldowney, J.S.: Global stability for the seir model in epidemiology. Mathematical biosciences **125**(2), 155–164 (1995)
7. Pastor-Satorras, R., Vespignani, A.: Epidemic spreading in scale-free networks. Physical review letters **86**(14), 3200 (2001)
8. Roy, S., Xue, M., Das, S.K.: Security and discoverability of spread dynamics in cyber-physical networks. IEEE Transactions on Parallel and Distributed Systems **23**(9), 1694–1707 (2012)
9. Singh, S., Sharma, P.K., Moon, S.Y., Moon, D., Park, J.H.: A comprehensive study on apt attacks and countermeasures for future networks and communications: challenges and solutions. The Journal of Supercomputing **75**, 4543–4574 (2019)
10. Winkler, I., Gomes, A.T.: Advanced persistent security: a cyberwarfare approach to implementing adaptive enterprise protection, detection, and reaction strategies. Syngress (2016)