Epidemic Response Model for Malware Defense on Computer Networks

Timilehin B. Aderinola, Aderonke F. Thompson, and Boniface K. Alese

Computer Science Department, Federal University of Technology, Akure

ABSTRACT

The Internet came with serious security vulnerabilities. Now, malicious individuals may gain unauthorized access to protected resources and disrupt network services by using malicious software, also known as *malware*. Most malware rapidly self-propagate within a network like an infectious disease. The classical epidemic model has been applied to study malware epidemics in computer networks. This study adapted the *Susceptible-Infected-Susceptible* (SIS) epidemic model to design a defense response model for computer networks and analyse the model obtained using a game theoretic approach of the attacker and defender. The model presented divided a network of fixed population into two compartments modelled with an ordinary differential equation that incorporated the strategies of the attacker and defender. Differential games were formulated and solved based on this model to derive optimal responses to malware epidemics. The SIS epidemic model established could aid optimal decisions for malware defense on computer networks.

Keyword: Epidemic Models, Game Theory, Malware, Differential Games, SIS, Networks, Malware Defenses, Computer Networks

1 INTRODUCTION

A wide variety of activities such as commerce, entertainment, communication, and many more, are now carried out on computer networks. In fact, networked computing is the backbone of many organizations today. In the early seasons of their use, specialized computer systems and networks were operated by professionals. However, once such systems entered the general public, security problems emerged in their numbers. Today, majority of users are not professionals who are familiar with the nature and limitation of these systems. In a *twist in the knife* scenario, there is no shortage of malicious individuals and groups known as attackers, who exploit the weaknesses of networked systems and their users for their own malicious purposes (Tanenbaum, 2003).

Observing that computer networks are getting more complex, and attackers are increasing in ingenuity, (Bloem, Alpcan, & Basar, 2007) predicted that computer networks will remain susceptible to expensive attacks from worms, viruses, Trojans, and other malicious software, which can collectively be referred to as malware. Such attacks are self-spreading and are expensive not only due to the damage they cause but also due to the challenge of preventing and removing them (Alpcan & Basar, 2010).

In 1988, Morris, an Internet worm, rapidly infected 6000 computers, which accounted for about a tenth of all computers on the Internet. In July 2001, the Code Red worm was discovered. It was written to spread until the 20th of the month, attack www.whitehouse.gov until the 28th of the month, and then sleep until the end of the month. The Code Red II worm, though more malicious, was discovered the following month. The losses caused by both worms were estimated to be more than $2.6 billion in damages. The Nimda worm in the year 2001 infected more than 2.2 million servers within a 24 hour period and caused the loss of more than half a billion dollars in damages. The most major worm to hit SQL servers, the Slammer worm, was detected in 2003. It caused Denial of Service (DoS) attack, taking almost the entire Internet offline for several hours (Symantec Security Response, 2006).

The above are only a few of numerous network malware incidences, and the security threat posed by malware keeps increasing. An attribute that marks most malware is the ability to self-propagate rapidly within the network, much like an infectious disease in the case of an epidemic. According to (Zou, Gong, & Towsley, 2003), some malware could spread to infect almost all vulnerable computers on the Internet before man can take effective counteractions, and as the bandwidth of Internet connections keeps

increasing, malware would require even less time to finish the infection task. These kinds of malware require automatic mitigation, since they spread too fast to be contained by human's manual counteractions.

Unsurprisingly, the problems of malware response and removal have caught the interest of the research community. The well-known classical epidemic model has been applied extensively to medical epidemics. Recently, this model has been used to study the propagation and response to malware epidemics in computer networks (Bloem et al., 2007).

The objectives of this research are to:

(i) adapt the Susceptible-Infected-Susceptible (SIS) epidemic model to design a defense response model for computer networks and,
(ii) analyse the model obtained using a game theoretic approach of the attacker and defender.

BACKGROUND

A security attack on a network is any action that compromises the security of information held on the network, and personnel involved in the perpetration of the attack are referred to as attackers. The term malware is a combination of the words **mal**icious and soft**ware**. It refers to malicious software programs developed and deployed by attackers to compromise computer systems by taking advantage of security vulnerabilities (Yu et al., n.d.). There are many forms of malware which include: Viruses, Worms, Trojan Horses, Malicious Mobile Code. Most malware are self-propagating and can spread in a computer network, much like an infectious disease.

In Biology, there is much interest in the study of infectious diseases. In 1760, David Bernoulli formulated and solved a model for smallpox to evaluate the effectiveness of inoculation of healthy people with the smallpox virus. More deterministic epidemiology most likely started in the 20^{th} century, with mathematical epidemiology growing exponentially starting in the middle of the century. Very numerous types of models have since been formulated, analysed mathematically and applied in managing infectious diseases. Epidemic models are used to describe rapid outbreaks occurring within a year, endemic models help in studying infectious diseases over an extended period of time (Hethcote, 2000).

The Susceptible-Infected-Susceptible (SIS) model is one of the most studied epidemic models. In the SIS model, a network population is divided into

two compartments. The first compartment is termed ‘Susceptible’ (S), representing healthy hosts that are prone to malware infection. The second compartment is termed ‘Infected’ (I), collectively referring to hosts that have been infected with malware and are able to recover. Healthy hosts can move from compartment S to I with an infection rate that depends on interactions with infected hosts. Infected hosts can recover, moving from compartment I to S with some recovery rate (Nowzari, Preciado, Pappas, & May, 2015).

Game theory is used in modelling situations where multiples parties make strategic decisions with outcomes that are interdependent on the decisions of the other parties (Sandholm, 2007). These decision-makers are called players. Each player has an objective function, which is either a utility/benefit function, or a cost/loss function. Each player plays with the aim of maximizing benefit and/or minimizing cost. The cost or loss resulting from the outcome of the game for each player is referred to as the payoff (Alpcan & Basar, 2010).

Network security is essentially a game played between attackers of a network and the administrators of the network who defend the network from such attacks. This game can be well analysed mathematically using game theory. The resulting security games provide a quantitative framework for modelling the actions of the attackers and defenders of a network. Their equilibrium solutions aid in decision making, development of algorithms and in predicting the behaviour of attackers (Alpcan & Basar, 2010).

Differential games are analysed using concepts and techniques of optimal control theory. Equilibrium strategies in open-loop form could be found by solving a two-point boundary value problem for an ordinary differential equation derived from the Pontryagin maximum principle. Equilibrium strategies in feedback form are best found by solving a system of Hamilton-Jacobi-Bellman partial differential equations for the value functions of the players from the principle of dynamic programming (Bressan, 2010).

MODELLING MALWARE EPIDEMICS

2 Related Works

Effective algorithms for early detection of the presence of a worm and the corresponding monitoring system were proposed in (Zou, Gao, & Gong, n.d.). The simple behaviour of a worm was observed based on well-studied epidemic models, which were not detailed enough to reflect the future

dynamics of a worm. Models of network worm propagation and defences were presented in (Liljenstam & Nicol, 2004), used in comparing the effectiveness of passive measures with active measures in malware defense. In (Bloem et al., 2007), the optimization of malicious software removal across multiple networks was studied in order to balance infection and patching costs when multiple connected networks are threatened by malware. An epidemiological model was developed in (Hu, Myers, Colizza, & Vespignani, 2009) that takes into account prevalent security flaws in routers used in wireless channels. Reference (Yu et al., n.d.) investigated the propagation of malware from a global perspective and established a two-layer epidemic model for internetwork malware propagation. The model presented, however, did not consider multiple malware cases.

As observed in (Bensoussan, Kantarcioglu, & Hoe, 2013), the strategies for malware filtering adopted by one host in the network may have impacts on other hosts' strategies, and these interdependent security decisions could be well represented by combining game theoretic modelling with epidemic modelling. Reference (Alese, Iwasokun, & Haruna, 2013) studied deterministic security game frameworks and its adoption to enhance strategic model interactions between attacker and defender in a network environment. However, the spatial location of the defender could always be located by the attacker due to the static nature of the defender. In (Omic & Orda, 2009), a unified framework that combines the SIS epidemic model with a non-cooperative game model was proposed, which failed to account for the strategies of the attacker. In (Bensoussan et al., 2013), a differential game model was developed based on the interactions between botnet herders and defending group, with the state evolving according to a modified SIS epidemic model. The model accounted for the strategies of the botnet herder under a fixed level of defense, and also considered a continuous game between the herder and the defender.

We present an epidemic model that could aid optimal decisions for malware defense on computer networks. The model present is a Susceptible-Infected-Susceptible (SIS) model, which takes into account re-infection after recovery, taking care of multiple malware cases. The SIS model presented incorporates the strategies of the attacker and defender of the network, and also provides a framework for malware defense under a fixed level of attack.

MODELLING THE STATE OF THE NETWORK

The typical network environment is made of at least a server with various interconnected devices. There are many users on the network, some of

which are malicious users that seek to compromise the security of the network for their personal gain. The System/Network Administrators put up defense mechanisms to protect the Network data and resources.

We obtained a model for the state of the system by adapting and modifying the classical SIS epidemic model to reflect the strategic interactions between the attackers and defenders of the network. The state equation is an ordinary differential equation incorporating variables that denote the level of infection in the network and the controls of the attacker and defender. Based on the state equation, differential games are formulated and solved to give the optimal response to malware epidemics in the network.

Let $x \in \mathbb{R}^N$ describe the state of the system, evolving in time according to the ordinary differential equation

$$\dot{x}(t) = f(t, x, u_1, u_2, \dots u_n), \quad t \in [0, T], \quad x(0) = x_0 \tag{1}$$

where

$u_1 \dots u_n$ are the controls put in place by the two players, which are assumed to satisfy the constraint $u_i(t) \in U_i$, for some given sets U_1, U_2, …, $U_n \subseteq \mathbb{R}^m$.

The goal of the i-th player is to maximize his own payoff, given by the Jacobian:

$$J_i(u_1, \dots u_n) = \phi_i\big(x(T)\big) - \int_0^T L_i\big(t, x(t), u_1(t), u_n(t)\big)dt \tag{2}$$

subject to the constraints of (1)

where

ϕ_i represents terminal payoff, while L_i accounts for running cost and T is the final time.

3 The Epidemic Model

The population *N* of the network is divided into two compartments. The first is called Susceptibles (S), representing healthy hosts that are prone to being infected with malware. The second compartment is called Infectives (I), capturing hosts that are infected with malware and are infectious, but are able to recover. For a fixed population, $I(t) \in \{0, 1, \dots, N\}$ is the number

of infectives, and $S(t) \in \{0, 1, \dots, N\}$, the number of susceptible at time time *t*.

Let $x(t)$ and $y(t)$ represent the fraction of infectives and the fraction of susceptibles respectively, then

$$x(t) = \frac{I(t)}{N}; \text{ and} \tag{3}$$

$$y(t) = \frac{S(t)}{N} \tag{4}$$

The infection rate β is proportional to the product of the number of susceptibles and infectives in the network, and the recovery rate γ depends on the recovery measures put in place for each host. With these parameters, the classical SIS epidemic model is used to describe the evolution of $x(t)$ and $y(t)$ in time by two differential equations:

$$\frac{dx(t)}{dt} = \beta x(t)y(t) - \gamma x(t) \tag{5}$$

$$\frac{dy(t)}{dt} = -\beta x(t)y(t) + \gamma x(t) \tag{6}$$

Since we know that

$$y(t) = 1 - x(t) \tag{7}$$

Equation (7) can be substituted into (5) to obtain a state equation completely in terms of $x(t)$ and the infection and recovery parameters, β and γ.

$$\frac{dx(t)}{dt} = \beta x(t)\big((1 - x(t)\big) - \gamma x(t) \tag{8}$$

Equation (8) is, thus, satisfactory to describe the SIS trends in the network in the event of a malware infection.

4 The State Equation

It is assumed that the network attackers have a set of attack strategies which directly affect the infection rate; and the network administrators (defenders) have a set of defense strategies which directly affect the recovery rate. The effectiveness of defense actions depend on the effectiveness of the defense strategies chosen, and the number of nodes the defense actions are affect,

while the effectiveness of attack depend on the intensity of attack and the amount of effort the attacker puts into the development of malware code. Both attack and defense efforts include effort costs per unit time.

In this scenario, equation (8) is modified to include the control actions of the attacker and defender. Hence,

$$\begin{pmatrix} \dot{x} = ux(1-x) + \beta x(1-x) - vx - \gamma x \\ x(0) = x_{0,} \quad 0 \leq x_0 \leq 1 \end{pmatrix} \tag{9}$$

where

$x(t)$ is written as x;

$u \in [0,1]$ is the attack effort, the attacker's control. It is associated with an effort cost k_A per unit time. Therefore, the total effort cost per unit time of A is given as uk_A.

$v \in [0,1]$ denotes the defense effort, the defender's control, with effort cost k_D per unit time. The total effort cost per unit time of D is given as vk_D.

The term $ux(1-x)$ accounts for the increase in infection due to continuous attack, while $\beta x(1-x)$ accounts for increase in infection due to contagion.

EPIDEMIC RESPONSE

Two-player differential security games are formulated to model the strategic interactions between the network attackers. The first game is considered under a fixed level of attack, in which there is no ongoing attack effort. The second game is a zero-sum differential game between the attacker and the defender, and the framework from which an equilibrium solution could be obtained is given.

5 Defense Response under a Fixed Level of Attack

In this game, it is assumed that there is no actively ongoing attack effort, and the defenders of the network are simply trying to manage the contagion in the network after the network has been compromised. Here, the focus is on the optimal strategy of the defender. Therefore, the control of the attacker is not considered. The game, then, becomes an optimal control problem for the defender. From (9), state equation becomes:

$$\dot{x} = \beta x(1-x) - vx - \gamma x, \quad x(0) = x_{0,} \; 0 \leq x_0 \leq 1 \tag{10}$$

The objective of the defender is to keep the number of infected nodes in the network at the barest minimum possible. At that same time, the defenders also want to minimize costs, since the deployment of defense strategies would involve certain personnel and equipment costs, added to the fixed operating costs they may be running.

Let C represent the operating cost of the defender. The cost function $f(x)$, which the defender seeks to minimize, should satisfy the conditions $f'(x) > 0$ and $f''(x) > 0$. This is based on the feasible assumption that the defender's running costs increases at an increasing rate as the percentage of infected nodes in the network increases. In other words, the more the percentage of the infected nodes in the network, the more running costs the defenders incur. It is also logical to assume that the running costs of the attacker decreases at a decreasing rate as the percentage of infected nodes in the network increases, that is, the attacker's cost function satisfies the conditions $f'(x) < 0$ and $f''(x) > 0$.

Let the defenders cost function be:

$$f(x) = \mathrm{C} + x^2 v k_D \tag{11}$$

The defender's objective is to minimize the discounted total cost (running costs plus effort cost) with a constant discount rate σ over an infinite time horizon, subject to the dynamics of (10).

$$J\big(v(x)\big) = \int_0^{\infty} e^{-\sigma t}(\mathrm{C} + x^2 v k_D)dt, \;\; 0 \leq v(x) \leq 1 \tag{12}$$

The optimal control is found by applying Pontryagin's minimum principle. From (10) and (11), the current value Hamiltonian is

$$H(x, v, p) = \mathrm{C} + x^2 v k_D + \lambda\big(\beta x(1 - x) - vx - \gamma x\big) \tag{13}$$

$$H_v = \frac{\partial H}{\partial v} = x(kx - \lambda) \tag{14}$$

$$\dot{\lambda} = -H_x = -2v k_D x + \lambda(\beta(2x - 1) + v + \gamma) \tag{15}$$

The optimal control takes a bang-bang form and a possible singular form at the steady state $\dot{x} = 0$. Solving (10) for v at $\dot{x} = 0$,

$$v = \beta(1 - x) - \gamma \tag{16}$$

So that

$$v^*(x) = \begin{cases} 1 & \text{if } H_v < 0 \\ v = \beta(1-x) - \gamma & \text{if } H_v = 0 \\ 0 & \text{if } H_v > 0 \end{cases} \quad (17)$$

where $v^*(x)$ denotes the optimal defense effort.

Equation (17) implies that when H_v is negative, the defender should apply the full defense effort such that $v(x) = 1$, and when H_v is positive, they should apply no defense effort, that is, $v(x) = 0$. The region in which $H_v = 0$ is referred to as singular, which shows a steady-state property such that the control and state variables are constant in the region. Here, an intermediate defense effort $v(x) = \beta(1-x) - \gamma$ should be applied.

6 Defense Response When under Attack

In this game, the objective function is taken to be

$$J(u,v) = \int_0^\infty e^{-\sigma t}(C + u^2x - v^2x)\,dt, \quad (18)$$

which the attacker wants to maximize and the defender wants to minimize. The gain of the attacker represents a loss to the defender. The goal is to find the optimal control pair (u^*, v^*) such that

$$J(u^*, v) \geq J(u^*, v^*) \geq J(u, v^*) \quad (19)$$

This implies that the attacker cannot increase his gain by choosing a strategy other than $u^*(t)$, neither can the defender reduce his losses by choosing a strategy other than $v^*(t)$. The necessary conditions for u^* and v^* to satisfy the condition given above are given by an application of Pontryagin's maximum principle. Obtaining these conditions, the Hamiltonian is formed from (9) and (18) as follows:

$$H = C + x(u^2 - v^2) + p\left((ux + \beta x)(1-x) - x(v-\gamma)\right) \quad (20)$$

$$H_u = 2ux + px(1-x) \quad (21)$$

$$H_v = -2vx - px \quad (22)$$

The adjoint variable $p(t)$ satisfies $\dot{p} = -H_x$,

$$\dot{p} = v^2 - u^2 + p(u(2x-1) + \beta(2x-1) + v + \gamma) \quad (23)$$

Let $a = (u(2x-1) + \beta(2x-1) + v + \gamma)$ (24)

$$\dot{p} = v^2 - u^2 + pa \quad (25)$$

Solving (25),

$$p = \frac{1}{a}(u^2 - v^2) + ae^{a(t-K)} \tag{26}$$

where K is a constant.

Solving for u^* in (9) at the steady-state, where $v = 1$ and $\dot{x} = 0$,

$$u^* = \frac{1-\gamma}{1-x} - \beta \tag{27}$$

Solving for v^* in this same region, where $\dot{x} = 0$, assuming the defender can estimate the effort of the attackers within an error margin $\pm\varepsilon$,

$$v^* = (u + \varepsilon + \beta)(1 - x) - \gamma \tag{28}$$

The optimal strategies for the attacker and defender are given by

$$u^*(x) = \begin{cases} 1 & \text{if } H_v < 0 \\ u = \frac{1-\gamma}{1-x} - \beta & \text{if } H_v = 0 \\ 0 & \text{if } H_v > 0 \end{cases} \tag{29}$$

$$v^*(x) = \begin{cases} 1 & \text{if } H_v < 0 \\ v = (u + \varepsilon + \beta)(1 - x) - \gamma & \text{if } H_v = 0 \\ 0 & \text{if } H_v > 0 \end{cases} \tag{30}$$

Equation (29) implies that when H_u is negative, the attacker will apply the full attack effort such that $u(x) = 1$, and when H_v is positive, there will be no attack, that is, $u(x) = 0$. The region in which $H_u = 0$ is referred to as singular, which shows a steady-state property such that the control and state variables are constant in the region. Here, an intermediate attack effort $u = \frac{1-\gamma}{1-x} - \beta$ is applied.

The response of the defender given in (30) is similar to that given in (17). However, if the defender is able to estimate the effort of the attacker with a high level of precision, the effectiveness of the defense effort applied would increase.

7 NUMERICAL SIMULATION

All parameters used for simulations and their descriptions are summarized in Table 1.

TABLE I
SUMMARY OF NUMERICAL SIMULATION PARAMETERS

Parameter	Description
N	Total number of nodes in the network
$[t_0, t_f]$	Time range for the simulation
I_0	Number of infected nodes at time t_0
β	Infection rate
γ	Recovery rate
v^*	Optimal epidemic response

The first simulation was carried out on the SIS epidemic model presented in (8) for 1000 nodes over a timeframe of 15 days, with an infection rate much less than the recovery rate. The results of this simulation are shown in Fig. 1. A second simulation was run using (8) with parameters identical to those of the first, but with the infection rate greater than the recovery rate, shown in Fig. 2.

From Fig. 1, it is clear that in the event of an epidemic in a network of N nodes, if there are no effective countermeasures, the number of susceptibles tends towards zero, and the number of infectives would tend towards N. However, if the rate of recovery is sufficiently greater than the rate of infection, the whole population can never get infected. The trends reach a state where *S* and *I* remain relatively constant.

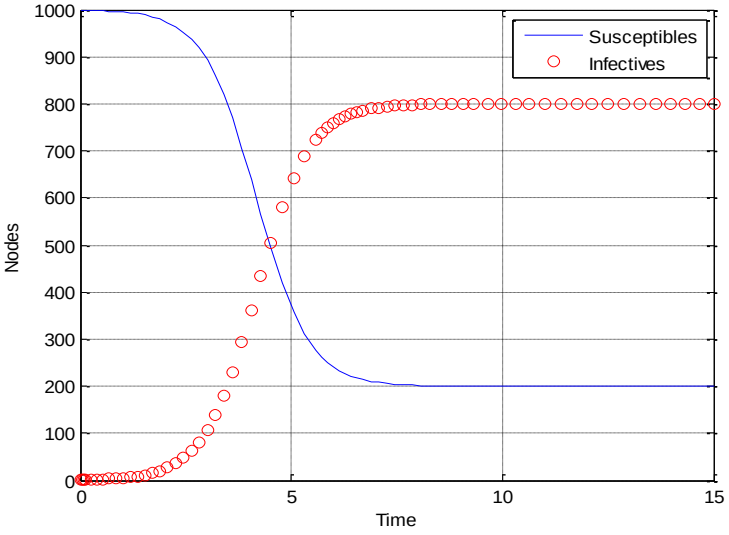

Figure 1: Simulation of SIS Trends With $\beta \ll \gamma$.

$N = 1000; [t_0, t_f] = [0, 15]; I_0 = 1; \beta = 0.002; \gamma = 0.4$

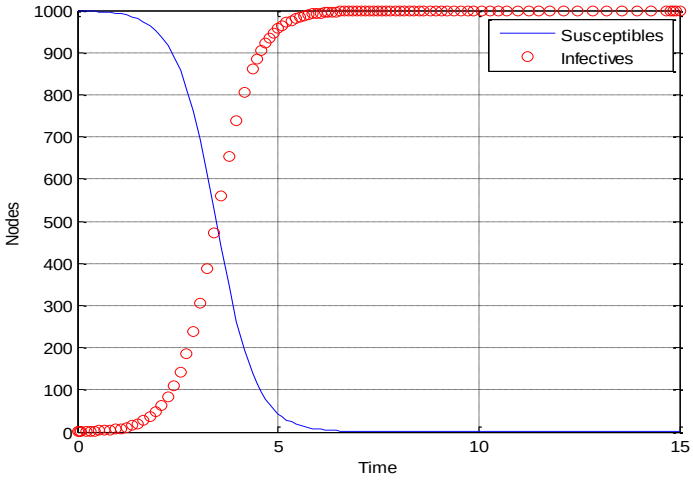

Figure 2: Simulation of SIS Trends With $\beta > \gamma$
$N = 1000; [\boldsymbol{t_0}, \boldsymbol{t_f}] = [0, 15]; \boldsymbol{I_0} = 1; \boldsymbol{\beta} = 0.002; \boldsymbol{\gamma} = 0.001$

The third simulation was run incorporating the defense response in (17). The results are shown in Fig. 3.

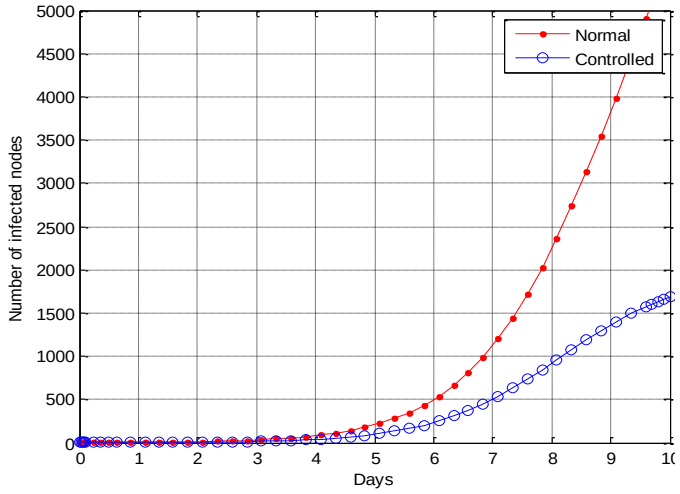

Figure 3: Simulation of Proposed Epidemic Response
$N = 5000; [t_0, t_f] = [0, 10]; I_0 = 1; \beta = 0.000466; \gamma = 0.4; v = v^*$

8 FUTURE RESEARCH DIRECTIONS

The security game is modelled as a zero-sum differential game, leaning on the assumption that the losses of the defender count as gain for the attacker, and vice versa. This assumption may not always be true in the real life attack and defense scenario. Future work in this area could consider a non-zero sum differential game in order to better capture the real life network attack and defense scenario.

9 CONCLUSION

This study has established a Susceptible-Infected-Susceptible (SIS) epidemic response model that could help system/network administrators to make optimal decisions for malware defense on computer networks by combining epidemic modelling with game theoretic principles. The model presented captures the strategies of the attacker and defender in a network security game scenario. From this model, the SIS trends in the network can be seen, that is, given the network population and the infection parameters, the expected levels of infection in the network at any point in time can be forecasted. By applying the defense response models presented, the fraction of infected hosts at a given time can be kept at a minimum, thereby minimizing the running costs for the organization network. The defense response could also be improved by estimating the intensity of attack on the network with a greater level of precision.

6 REFERENCES

Alese, B. K., Iwasokun, G. B., & Haruna, D. (2013). DSGM-Based analysis of Computer Networks Security. *International Journal for Information Security Research*, *3*(1 and 2).

Alpcan, T., & Basar, T. (2010). *Network Security: A Decision and Game Theoretic Approach* (Pre-Print). Cambridge University Press.

Bensoussan, A., Kantarcioglu, M., & Hoe, C. (2013). A Game-Theoretical Approach for Finding Optimal Strategies in a Botnet Defense Model.

Bloem, M., Alpcan, T., & Basar, T. (2007). An Optimal Control Approach to Malware Filtering. In *2007 46th IEEE Conference on Decision and Control* (pp. 6059–6064).

Bressan, A. (2010). Noncooperative Differential Games . A Tutorial, 1–80.

Hethcote, H. W. (2000). The Mathematics of Infectious Diseases. *Society for Industrial and Applied Mathematics*, *42*(4), 599–653.

Hu, H., Myers, S., Colizza, V., & Vespignani, A. (2009). WiFi networks and malware epidemiology. *Proceedings of the National Academy of Sciences of the United States of America*, *106*(5), 1318–1323. https://doi.org/10.1073/pnas.0811973106

Liljenstam, M., & Nicol, D. M. (2004). Comparing passive and active worm defenses. *Proceedings - First International Conference on the Quantitative Evaluation of*

Systems, QEST 2004, 18–27. https://doi.org/10.1109/QEST.2004.1348012
Nowzari, C., Preciado, V. M., Pappas, G. J., & May, O. C. (2015). Analysis and Control of Epidemics A survey of spreading processes on complex networks.
Omic, J., & Orda, A. (2009). Protecting Against Network Infections : A Game Theoretic Perspective, 1485–1493.
Sandholm, W. H. (2007). Evolutionary Game Theory ∗.
Symantec Security Response. (2006). Timeline of Major Events in Internet Security, (February), 1–15.
Tanenbaum, A. S. (2003). Computer Networks. *World Wide Web Internet And Web Information Systems*, *52*(169), 349–351. https://doi.org/10.1016/j.comnet.2008.04.002
Yu, S., Member, S., Gu, G., Barnawi, A., Guo, S., & Stojmenovic, I. (n.d.). Malware Propagation in Large-Scale Networks, 1–14.
Zou, C. C., Gao, L., & Gong, W. (n.d.). Monitoring and Early Warning for Internet Worms.
Zou, C. C., Gong, W., & Towsley, D. (2003). Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense. In *Proceedings of the 2003 ACM Workshop on Rapid Malcode (WORM'03)*.

KEY TERMS:

Epidemic models: differential equations that show the trends of a disease in a population over time with a set of well-defined parameters.

Game theory: the study of models that describe the strategic interactions between individuals, taking into consideration the costs and benefits.

Differential games: games that deal with conflict problems in systems whose states are described by differential equations.

BIOGRAPHICAL NOTES

T. B. Aderinola is with the Computer Science Department, the Federal University of Technology, Akure, Nigeria.

A. F. Thompson is with the Computer Science Department, Federal University of Technology, Akure, Nigeria.

B. K. Alese is with the Computer Science Department, Federal University of Technology, Akure, Nigeria.

REFERENCE

Reference to this paper should be made as follows: Aderinola, T. B., Thompson, A. F. and Alese, B. K. (2017). Epidemic Response Model for Malware Defense on Computer Networks. *International Journal on Cyber Situational Awareness*, Vol. 2, No. 1, pp69-84.