2016 Fifth International Conference On Recent Trends In Information Technology

Dynamics of Attack of Malicious Codes on the Targeted Network: Effect of Firewall

Ashish Bhargava, Durgesh Kumar Soni, Palash Jain, Joydip Dhar
ABV-Indian Institute of Information Technology and Management,
Gwalior-474015, Madhya Pradesh

***Abstract*—In this work, a mathematical model has been developed to analyze the spread of a distributed attack on critically targeted resources in a network using firewall security coefficient. The model provides an epidemic framework with two sub-frameworks to consider the difference between the overall behavior of the attacking population and the targeted population. The targeted population and attacking population is divided into five compartments of nodes, viz. Susceptible-Latent-Breaking out-Recovered-Antidotal. With cyber mass action incidence, the boundedness of the system, the feasibility of equilibrium states and their stabilities are analyzed. Basic reproduction number $\mathcal{R}_0$ is calculated and it is observed that when $\mathcal{R}_0 < 1$, then the system will have malicious code free stable steady state. Again, when $\mathcal{R}_0 > 1$, then endemic steady state exists and will be locally asymptotically stable. The impact of firewall security rule base in controlling transmission of malicious objects is analyzed. We are taking firewall security as a media coverage factor in our computer network model of malicious code propagation. Asymptotic local stability method is used as an alternate to find the stability of the system. Finally, a sensitivity analysis of the system parameters for basic reproduction number and endemic equilibrium points has been carried out using normalized forward sensitivity index. Numerical experimentation has been carried out to simulate the system of equations in support of analytical findings.**

I. Introduction

Malicious code does not just affect one computer, it can also get into the networks and spread. It can send messages through email and steal information or cause even more damage by deleting files. It is a computer program that operates on behalf of a potential intruder to aid in attacking a system or network. Malicious code can come in various other forms. A common type of malicious code is the virus, which is a little program attaching to other programs or files and will copy itself in a computer and even spread to other networked computers. Viruses can range from being relatively harmless to causing significant damage to a system. Worms are pieces of malicious code making copies of itself. Conditions have to be right for a worm to proliferate. They are created mainly using scripting languages.

Trojan horses are forms of malicious code appearing as safe software. But that is how they get into a computer. They may be hiding inside another program and be installed with an otherwise safe program. Sometimes they give someone in a remote location control of the victim's computer [1].

These agents acts as a serious threat to the security of the computer networks. An infected computer can have significance performance degradation when attacked by the malicious codes in breaking-out state. Malicious codes have a potential of replicating themselves from one computer to another without you being aware that your machine has become infected [2]. In the era of cloud computing, this threat has become more and more serious as new variants of existing viruses including some new ones are continuously emerging and increasing the vulnerability of the system. This calls for a need to continuously develop new counter-defense mechanisms. The evolution trend of viruses cannot be predicted and thus universal proposal for their avoidance and control cannot be recommended [3].

In a certain sense, malicious codes spread in computer network is epidemic in nature, i.e., the propagation of computer viruses in a system of interacting and integrated computers could be compared with disease transmission in biological world [4]. Keeping the epidemic nature of virus spread certain mathematical models are developed. With the continuous emergence of new type of attacks, there is a need to improve the propagation models. Mathematical modeling has become an important tool in analyzing the spread and control of malicious codes in computer networks. Mathematical models take into account the main factors that govern spread of virus, such as transmission and recovery rates, and predict how the viruses will spread over a period of time. Only a small fraction of all known viruses have appeared in real incidents, partly because many viruses are below the theoretical epidemic threshold. The observed sub-exponential rate of viral spread can be explained by models of localized software exchange. A surprisingly small fraction of machines in well-protected business environments are infected. This may be explained by a model in which, once a machine is found to be infected, neighboring machines are checked for viruses. This "kill signal" idea could be implemented in networks to greatly reduce the threat of viral spread.

978-1-4673-9802-2/16/$31.00

II. Model Development

We consider two groups of computer nodes, namely, targeted nodes and attacker nodes. In this model attacker-targeted population is divided into five compartments namely Susceptible, Latent, Breaking-out, Antidotal and Recovered compartment. Here we have divided total computer nodes T into ten classes, namely, $S(t)$ of non- infected targeted computers subjected to possible infection; $S_1(t)$ of non-infected computers of attacker class; $A(t)$, $A_1(t)$ non-infected computers of targeted and attacker class equipped with fully effective antivirus program; $L(t)$, $L_1(t)$ infected computers of targeted and attacker class with virus in latent state; $B(t)$, $B_1(t)$ infected computers of targeted and attacker class with virus in breaking-out state and recovered class population $R(t)$, $R_1(t)$ of recovered ones from the infection in targeted and attacker class respectively. The Schematic diagram of the model shown in the figure1. Here it is assumed that the population has a homogeneous spatial distribution and the mixing of hosts follow the law of mass action, i.e., the local population density is a constant through the total population size [5], [6], [7], [**?**]. Targeted population $N(t) = S(t) + L(t) + B(t) + R(t) + A(t)$ and attacker population $N_1(t) = S_1(t) + L_1(t) + B_1(t) + R_1(t) + A_1(t)$.

The primary goal of this model is to theoretically study the impact of firewall security rule base in controlling transmission of malicious objects [8]. Many researchers investigated the impact of media awareness in biological disease spread using mathematical modeling used transmission coefficient function of the form $\beta(I) = \beta e^{-mI}$ and established that multiple positive equilibria are possible when the media effect is sufficiently strong [9], [10], [11], [12]. Similarly we are taking firewall security as a media coverage factor in our computer network model of malicious code propagation. Non-linear function of the form $\beta(I) = c_1 - c_2 f(I)$, is incorporated in the transmission term to investigate the effect of firewall security, where $f(I) = \frac{I}{m+I}$. In the modeling of malicious code propagation, the incidence function plays a very important role. In many models, the bilinear incidence rate $\beta\tilde{S}\tilde{I}$ and the standard incidence rate $\frac{\beta\tilde{S}\tilde{I}}{N}$ are frequently used, where β measures the effect of both the propagation of the malicious code and the contact transmission rates. However, these incidence functions do not consider the impact of firewall security to the spread and control of malicious code propagation [13].

The use of firewall security and alert has been found beneficial for reducing malicious code propagation. Initially researchers used media induced transmission rate of the form $\beta(I) = \beta e^{-mI}$ which has two major limitations. We consider firewall induced transmission rate as $\beta(I) = \beta e^{-m\frac{I}{N}}$ in the proposed model which is more reasonable than $\beta(I) = \beta e^{-mI}$, because $\beta e^{-mI} \to 0$ as $I \to \infty$, independent of the value of m. Since the firewall security and alertness are not the intrinsic deterministic factor responsible for the transmission, hence it is reasonable to assume that the transmission rate cannot be reduced below a certain level merely through firewall security alert. Moreover, even for a fixed m, the minimum transmission rate differs for different population sizes, which is not very realistic. On the other hand, $min\{\beta e^{-m\frac{I}{N}}\} = \beta e^{-m}$ that remains unchanged with respect to the total population size.

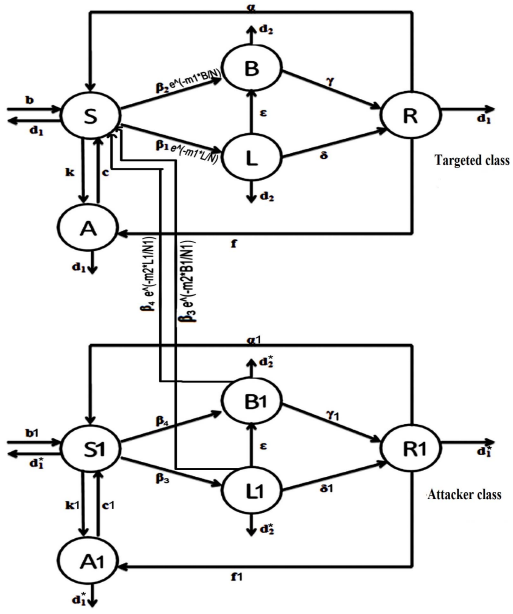

Fig. 1. Schematic Flow of Proposed Model

III. Proposed Mathematical Model

Keeping in view the transmission rates of the schematic flow diagram which is shown in the figure 1. The system is governed by following set of ordinary differential equations and its parameters are discussed in table I:

For Targeted nodes:

$$\frac{d\tilde{S}}{d\tilde{t}} = b - \tilde{\beta}_2 e^{-m_1\frac{\tilde{B}}{\tilde{N}}}\tilde{S}\frac{\tilde{B}}{\tilde{N}} - \tilde{\beta}_1 e^{-m_1\frac{\tilde{L}}{\tilde{N}}}\tilde{S}\frac{\tilde{L}}{\tilde{N}} - \tilde{k}\tilde{S}\tilde{A} + \tilde{c}\tilde{A} - \tilde{d}_1\tilde{S} + \tilde{\alpha}\tilde{R} - \tilde{\beta}_2 e^{-m_2\frac{\tilde{B}_1}{\tilde{N}_1}}\tilde{S}\frac{\tilde{B}_1}{\tilde{N}_1} - \tilde{\beta}_1 e^{-m_2\frac{\tilde{L}_1}{\tilde{N}_1}}\tilde{S}\frac{\tilde{L}_1}{\tilde{N}_1}, \quad (1)$$

$$\frac{d\tilde{B}}{d\tilde{t}} = \tilde{\beta}_2 e^{-m_1\frac{\tilde{B}}{\tilde{N}}}\tilde{S}\frac{\tilde{B}}{\tilde{N}} - \tilde{d}_2\tilde{B} + \tilde{\epsilon}\tilde{L} - \tilde{\gamma}\tilde{B} + \tilde{\beta}_2 e^{-m_2\frac{\tilde{B}_1}{\tilde{N}_1}}\tilde{S}\frac{\tilde{B}_1}{\tilde{N}_1}, \quad (2)$$

$$\frac{d\tilde{L}}{d\tilde{t}} = \tilde{\beta_1} e^{-m_1 \frac{\tilde{L}}{\tilde{N}}} \tilde{S} \frac{\tilde{L}}{\tilde{N}} - \tilde{d_2}\tilde{L} - \tilde{\epsilon}\tilde{L} - \tilde{\delta}\tilde{L} + \tilde{\beta_1} e^{-m_2 \frac{\tilde{L_1}}{\tilde{N_1}}} \tilde{S} \frac{\tilde{L_1}}{\tilde{N_1}}, \quad (3)$$

$$\frac{d\tilde{R}}{d\tilde{t}} = \tilde{\gamma}\tilde{B} + \tilde{\delta}\tilde{L} - \tilde{f}\tilde{R} - \tilde{\alpha}\tilde{R} - \tilde{d_1}\tilde{R}, \quad (4)$$

$$\frac{d\tilde{A}}{d\tilde{t}} = \tilde{f}\tilde{R} - \tilde{d_1}\tilde{A} + \tilde{k}\tilde{S}\tilde{A} - \tilde{c}\tilde{A}, \quad (5)$$

For Attacker nodes:

$$\begin{aligned}\frac{d\tilde{S_1}}{d\tilde{t}} &= b_1 - \tilde{\beta_4}\tilde{S_1}\tilde{B_1} - \tilde{\beta_3}\tilde{S_1}\tilde{L_1} - \tilde{k_1}\tilde{S_1}\tilde{A_1} + \tilde{c_1}\tilde{A_1} \\ &- \tilde{d_3}S_1 + \tilde{\alpha_1}\tilde{R_1}, \end{aligned} \quad (6)$$

$$\frac{d\tilde{B_1}}{d\tilde{t}} = \tilde{\beta_4}\tilde{S_1}\tilde{B_1} - \tilde{d_4}\tilde{B_1} + \tilde{\epsilon_1}L_1 - \tilde{\gamma_1}B_1, \quad (7)$$

$$\frac{d\tilde{L_1}}{d\tilde{t}} = \tilde{\beta_3}\tilde{S_1}\tilde{L_1} - \tilde{d_4}\tilde{L_1} - \tilde{\epsilon_1}L_1 - \tilde{\delta_1}L_1, \quad (8)$$

$$\frac{d\tilde{R_1}}{d\tilde{t}} = \tilde{\gamma_1}\tilde{B_1} + \tilde{\delta_1}\tilde{L_1} - \tilde{f_1}\tilde{R_1} - \tilde{\alpha_1}\tilde{R_1} - \tilde{d_3}\tilde{R_1}, \quad (9)$$

$$\frac{d\tilde{A_1}}{d\tilde{t}} = \tilde{f_1}\tilde{R_1} - \tilde{d_3}\tilde{A_1} + \tilde{k_1}\tilde{S_1}\tilde{A_1} - \tilde{c_1}\tilde{A_1}. \quad (10)$$

where, all the system parameters are positive and described in table I.

TABLE I
PARAMETERS DESCRIPTION

Parameters	Description
b,b_1	Recruitment rates
d_1,d_2	Natural death rate of attacker and targeted population nodes
β,β_1	Contact rate from susceptible class to latent class;(in the absence of firewall)
γ,γ_1	Rate of recovery of computers with malicious codes in breaking-out state
δ,δ_1	Rate of recovery of computers with malicious codes in latent state
d_3,d_4	Death rate in infected class(death due to infection and natural death)
ϵ,ϵ_1	Conversion rate of malicious codes from latent to braking-out state
f,f_1	Conversion rate of recovered nodes into antidotal nodes
c,c_1	Conversion rate of antidotal nodes into susceptible nodes
k,k_1	Conversion rate of susceptible nodes into antidotal nodes
α,α_1	Conversion rate of recovered nodes into susceptible nodes
m_1, m_2	Firewall security coefficients

Non-dimensionalise the above system using, $S=\frac{\tilde{S}}{\tilde{N}}$, $B=\frac{\tilde{B}}{\tilde{N}}$, $L=\frac{\tilde{L}}{\tilde{N}}$, $R=\frac{\tilde{R}}{\tilde{N}}$, $A=\frac{\tilde{A}}{\tilde{N}}$, $S_1=\frac{\tilde{S_1}}{\tilde{N_1}}$, $B_1=\frac{\tilde{B_1}}{\tilde{N_1}}$, $L_1=\frac{\tilde{L_1}}{\tilde{N_1}}$, $R_1=\frac{\tilde{R_1}}{\tilde{N_1}}$, $A_1=\frac{\tilde{A_1}}{\tilde{N_1}}$, $t=\tilde{d_1}\tilde{t}$, $N=\frac{\tilde{N}}{\tilde{N^0}}$, $N_1=\frac{\tilde{N_1}}{\tilde{N_1}^0}$. Where, $\tilde{N^0}=\frac{b}{\tilde{d_1}}$ and $\tilde{N_1}^0=\frac{b}{\tilde{d_3}}$. Targeted population and attacker population parameters $\tilde{d_1}$ and $\tilde{d_3}$ respectively become $\beta_1=\frac{\tilde{\beta_1}}{\tilde{d_1}}$, $\beta_3=\frac{\tilde{\beta_3}}{\tilde{d_3}}$.

IV. RESULTS AND DISCUSSION

In this section we will discuss various analyses and results obtained :

A. Boundedness of the System

Our targeted system is bounded, in the simply connected compact set

$$\Omega_\kappa = \left\{(S, L, B, R, A) \in R_+^5 : S + L + B + R + A \leq \frac{b}{\tilde{d}} + \kappa\right\}$$

is positively invariant for the SLBRAS model. Similarly boundedness follows for attacking population.

B. Basic Reproduction Number

The basic reproduction number R_0, is defined as the expected number of secondary cases produced by a single infection in a completely susceptible population. It is considered as one of the most useful threshold parameters to characterize the malicious object propagation. It can be obtained by taking the derivative of infection classes, i.e., 2^{nd} and 3^{rd} equations of attacker system and 2^{nd} and 3^{rd} equations of targeted system.
Let x= (L,B,L_1,B_1) then,

$\frac{dx}{dt}=\mathcal{F}-\mathcal{V}$,

where S, S_1 is the node density of susceptible class and A, A_1 is the node density of antidotal class of targeted and attacker population respectively in malicious codes - free equilibrium state. In this model we have four such states E_1, E_2, E_3 and E_4 and hence we have four basic reproduction number R_{01}, R_{02}, R_{03} and R_{04} respectively. Value of R_{01}, R_{02}, R_{03} and R_{04} are:
For equilibrium state E_1: S=1, A=0, S_1=1, A_1=0 and hence,

R_{01}=$max\{\frac{1+\beta_1}{1+d_2+\delta+\varepsilon}, \frac{1+\beta_3}{1+d_3+\delta_1+\varepsilon_1}, \frac{1+\beta_2}{1+d_2+\gamma}, \frac{1+\beta_4}{1+d_3+\gamma_1}\}$.

C. Local Asymptotic Stability

Now, we explore the local stability of malicious codes-free and endemic equilibrium. Equilibrium state E_1 will be locally asymptotically stable when all eigenvalues of J_{01} variational matrix are negative or having negative real parts. Clearly, if $\mathcal{R}_{01}$<1, then all the eigenvalues will have negative real parts. Hence, the malicious code free equilibrium E_1 is locally asymptotically stable, if $\mathcal{R}_{01}$<1 and unstable, if $\mathcal{R}_{01}$>1.

The basic reproduction number can be obtained by taking the derivative of infection classes, i.e., 2^{nd} and 3^{rd} equations of attacker system and 2^{nd} and 3^{rd} equations of targeted system. Let x= (L,B,L_1,B_1) then,

$\frac{dx}{dt}=\mathcal{F}-\mathcal{V}$,

where, $\mathcal{F} = \begin{pmatrix} \beta_2 e^{-m_1 B} SB + \beta_2 e^{-m_2 B_1} SB_1 + BS \\ \beta_1 e^{-m_1 L} SL + \beta_1 e^{-m_2 L_1} SL_1 + LS \\ \beta_4 S_1 N_1 B_1 + B_1 S_1 \\ \beta_3 S_1 N_1 L_1 + S_1 L_1 \end{pmatrix}$,

$\mathcal{V} = \begin{pmatrix} d_2 B - \varepsilon L + \gamma B + \frac{B}{N} - d_2 B^2 - BR - BA - d_2 BL \\ d_2 L + \varepsilon L + \delta B + \frac{L}{N} - d_2 L^2 - RL - AL - d_2 BL \\ d_3 B_1 - \varepsilon L_1 + \gamma B_1 + \frac{B_1}{N_1} - d_3 L_1 B_1 - d_3 {B_1}^2 - B_1 R_1 - B_1 A_1 \\ d_3 L_1 + \varepsilon L_1 + \delta L_1 + \frac{L_1}{N_1} - d_3 L_1 B_1 - d_3 {L_1}^2 - L_1 R_1 - L_1 A_1 \end{pmatrix}$,

we get, F(Jacobian of $\mathcal{F}$ at malicious codes-free equilibrium)=

$$\begin{pmatrix} (\beta_2+1)S & 0 & \beta_2 S & 0 \\ 0 & (\beta_1+1)S & 0 & \beta_1 S \\ 0 & 0 & (\beta_4+1)S_1 & 0 \\ 0 & 0 & 0 & (\beta_3+1)S_1 \end{pmatrix},$$

and, V(Jacobian of $\mathcal{V}$ at malicious codes-free equilibrium)=

$$\begin{pmatrix} \gamma-A+d_2+1 & -\varepsilon & 0 & 0 \\ 0 & \varepsilon-A+\delta+d_2+1 & 0 & 0 \\ 0 & 0 & \gamma_1-A_1+d_3+1 & -\varepsilon_1 \\ 0 & 0 & 0 & d_3-A_1+\varepsilon_1+\delta_1+1 \end{pmatrix}.$$

where, F is the matrix of rates of secondary infection and V is the matrix of rates of transmission. Then, the basic reproductive number R_0 is defined as the dominant eigenvalue of FV^{-1}.

$$R_0=max\left\{\frac{S(1+\beta_1)}{1+d_2+\delta+\varepsilon-A}, \frac{S_1(1+\beta_3)}{1+d_3+\delta_1+\varepsilon_1-A_1}, \frac{S(1+\beta_2)}{1+d_2+\gamma-A}, \frac{S_1(1+\beta_4)}{1+d_3+\gamma_1-A_1}\right\},$$

where S, S_1 is the node density of susceptible class and A, A_1 is the node density of antidotal class of targeted and attacker population respectively in malicious codes - free equilibrium state. In this model we have four such states E_1, E_2, E_3 and E_4 and hence we have four basic reproduction number R_{01}, R_{02}, R_{03} and R_{04} respectively. Value of R_{01}, R_{02}, R_{03} and R_{04} are:

For equilibrium state E_1: S=1, A=0, S_1=1, A_1=0 and hence,

$$R_{01}=max\{\frac{1+\beta_1}{1+d_2+\delta+\varepsilon}, \frac{1+\beta_3}{1+d_3+\delta_1+\varepsilon_1}, \frac{1+\beta_2}{1+d_2+\gamma}, \frac{1+\beta_4}{1+d_3+\gamma_1}\}.$$

Similarly for E_2: S=1, A=0, $S1=\frac{1+c_1}{k_1}$, $A_1=1-\frac{1+c_1}{k_1}$ and hence,

$$R_{02}=max\{\frac{1+\beta_1}{1+d_2+\delta+\varepsilon}, \frac{(1+c_1)(1+\beta_3)}{(k_1)(1+d_3+\delta_1+\varepsilon_1\frac{1+c_1}{k_1})}, \frac{1+\beta_2}{1+d_2+\gamma}, \frac{(1+\beta_4)(1+c_1)}{(k_1)(1+d_3+\gamma_1+\frac{1+c_1}{k_1}}\}.$$

Similarly for E_3: $S=\frac{1+c}{k}$, $A_1=1-\frac{1+c}{k}$, $S1=\frac{1+c_1}{k_1}$, $A_1=1-\frac{1+c_1}{k_1}$ and hence,

$$R_{03}=max\{\frac{(1+\beta_1)(1+c)}{(k)(\frac{1+c}{k}+d_2+\delta+\varepsilon)}, \frac{(1+c_1)(1+\beta_3)}{(k_1)(1+d_3+\delta_1+\varepsilon_1\frac{1+c_1}{k_1})}, \frac{(1+\beta_2)(1+c)}{(k)(\frac{1+c}{k}+d_2+\gamma)}, \frac{(1+\beta_4)(1+c_1)}{(k_1)(1+d_3+\gamma_1+\frac{1+c_1}{k_1})}\}.$$

Similarly for E_4: $S=\frac{1+c}{k}$, $A_1=1-\frac{1+c}{k}$, $S1$=1, A_1=0 and hence,

$$R_{04}=max\{\frac{(1+\beta_1)(1+c)}{(k)(\frac{1+c}{k}+d_2+\delta+\varepsilon)}, \frac{(1+\beta_3)}{1+d_3+\delta_1+\varepsilon_1}, \frac{(1+\beta_2)(1+c)}{(k)(\frac{1+c}{k}+d_2+\gamma)}, \frac{(1+\beta_4)}{1+d_3+\gamma_1}\}.$$

D. Numerical Experimentation

The targeted and attacker system has been solved and simulated using numerical methods and the behavior of the nodes in different classes are observed with respect to the time.

E. Feasible Steady States

For the model, feasible steady states for different parameter sets are calculated. A steady state is feasible if all the classes have non-negative values at this point. The feasibility of steady states for different parameter sets along with basic reproduction number for all malicious codes - free equilibrium states are shown in Table II.

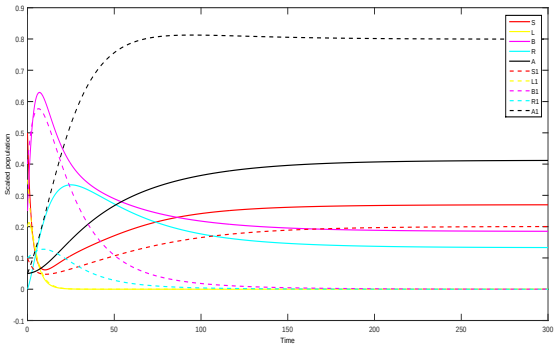

Fig. 2. Node Density vs. Time for different classes with Set 1

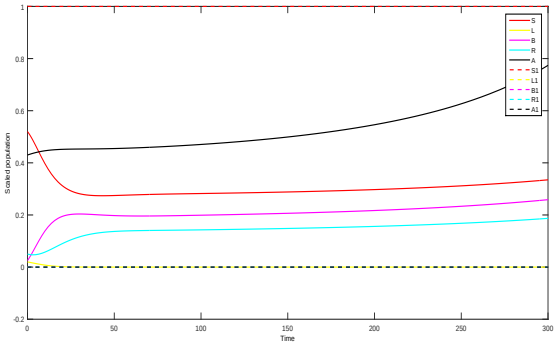

Fig. 3. Node Density vs. Time for different classes with Set 2

We plot a curve to understand the behavior of the classes with time. Figures show the node density of susceptible, latent, Breaking out, recovered and antidotal nodes of attacker and targeted class for different parameter sets with respect to time. Since E_1,E_2,E_3 and E_4 are the disease free states so they would be present in every set of equilibrium states if their reproduction number R_0<1, otherwise equilibrium will tend to some other state if their R_0>1.

Figure 2 is plotted with parameter Set 1 and initial points (0.5, 0.2, 0.25, 0, 0.05, 0.1, 0.35, 0.4, 0.1, 0.05). In this figure at steady state node density of S, B, R, A and S_1 classes are greater than zero and possible feasible states are E_1, E_2, E_3, E_4, E_9 and E_{10}. Since all the reproduction number is greater than 1. Hence, we can conclude from the figure 2 that, E_9 is the stable steady state.

Figure 3 is plotted with parameter Set 2 and initial points (0.5, 0.2, 0.25, 0, 0.05, 0.1, 0.35, 0.4, 0.1, and 0.05). Similarly, from the figure we can conclude that E_1, E_2, E_3 and E_4 are the feasible steady states.

TABLE II
FEASIBLE STEADY STATES AND NUMERICAL VALUES OF BASIC REPRODUCTION NUMBER FOR DIFFERENT PARAMETER SET IN THE MODEL

Parameters	**Set 1**	**Set 2**
β_1	0.6	0.6
β_2	0.5	0.5
k	0.06	0.06
c	0.03	0.03 3
α	0.05	0.05
d_2	0.04	0.08
ϵ	0.3	0.3
γ	0.045	0.45
δ	0.025	0.25
f	0.02	0.02
β_3	0.4	0.4
β_4	0.3	0.3
f_1	0.15	0.15
k_1	0.05	0.05
c_1	0.01	0.01
α_1	0.04	0.04
d_3	0.05	0.05
γ_1	0.035	0.35
δ_1	0.02	0.2
ϵ_1	0.25	0.25
feasible SS	$E_1, E_2, E_3,$	E_1, E_2, E_3, E_4
$\mathcal{R}_{01}$	0.58803	0.9523
$\mathcal{R}_{02}$	5.88034	0.9523
$\mathcal{R}_{03}$	3.52822	0.8000
$\mathcal{R}_{04}$	2.94421	0.4767

V. ESTIMATION OF FIREWALL SECURITY COEFFICIENT

The firewall is the core of a well-defined network security policy. The goal of the Check Point Firewall Rule Base is to create rules that only allow the specified connections.

A. Order of Rule Enforcement

The Firewall inspects connections and enforces the Rule Base in a sequential manner. The Firewall inspects each connection that comes to the network and compares the data (source, destination, service, etc.) to the first rule. If the connection matches the rule, the Firewall applies the action of that rule. If the connection does not match the rule, the Firewall continues with the next rule in the Rule Base.

B. Firewall rule priority

Because you can make firewall rules that have apparent conflicts, it is important to understand the order in which the rules are processed.

C. Authenticated bypass

These are rules in which the override block rules option is selected. These rules allow matching network traffic that would otherwise be blocked. The network traffic must be authenticated by using a separate connection security rule. You can use these rules to permit access to the computer to authorized network administrators and authorized network troubleshooting devices.

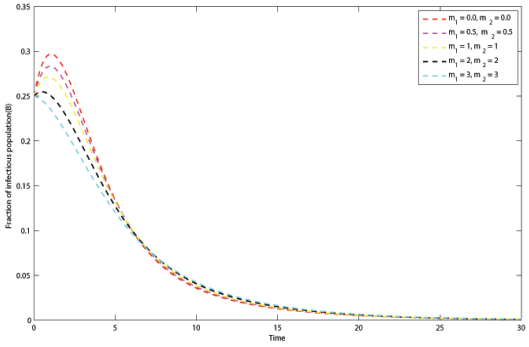

Fig. 4. Effect of m on B when $R_0<1$

D. Block connection

These rules block all matching inbound network traffic.

E. Allow connection

These rules allow matching inbound network traffic. Because the default behavior is to block unsolicited inbound network traffic, you must create an allow rule to support any network program or service that must be able to accept inbound connections.

The coefficient of firewall security, m should depend on the types of files(data) under consideration, defined firewall security rules in the firewall rule base and the reliability and efficiency of the firewall. We propose a method for quantifying the coefficient m of firewall security as, $m=-\log_e(p+q-pq)$, where, q quantifies the response of the files to the defined security rules. For our work we can add certain rules by monitoring the behavior of attacker class. When the files will be received in targeted class, they will be checked according to the rules defined in the firewall rule base. If they response correctly to all these rules then $q=0$ and if they don't match any of the rules then $q=1$ and it is assumed that the malware propagation rate can be reduced by p fraction, when all received files follow the defined security rules.

VI. CONCLUSION

In this work, an SLBRA epidemic model with distributed attack on targeted resources is proposed and analyzed using stability theory of ordinary differential equations incorporating firewall security rule base. The important observations of this work are as follows:

- For the proposed model sixteen equilibrium states are calculated out of which four are malicious codes free equilibrium and rest are endemic in nature. Basic reproduction number for the disease free equilibrium states has been calculated and it has been found that if $R_0<1$, then malicious code free

equilibrium is stable and, if $R_0>1$, then the endemic equilibrium is stable. These conditions are verified by local asymptotic stability of the system.

- It is observed from the analysis that the coefficient of media coverage m does not affect R_0 and hence the qualitative features of the model remains unaltered.
- We conclude that use of firewall security rule base helps to mitigate the problem of malicious code propagation in the network by lowering the level of infectious nodes at steady state.
- Finally, Normalized forward sensitivity indices are calculated for effective reproduction number and state variables at endemic equilibrium with respect to various parameters and respective sensitive parameters are identified and shown in Table III:

TABLE III
SENSITIVE PARAMETERS

R_0	Sensitive Parameters
R_{01}	β_1,β_2,β_4
R_{02}	β_1,β_2
R_{03}	β_2,β_3,β_4,k,c
R_{04}	β_1,β_2,k,c

VII. FUTURE SCOPE

This work can be extended by adding more control strategies such as time delay for outbreak and time varying recruitment rate. Consider the following scenario, one day, Alice discovers that one of the programs she uses on her PC is infected with a virus. She eradicates it, in most models, this would be the end of the story. However, in this case Alice takes it upon herself to inform her friends Bob, Carol, and Dave, with whom she remembers having exchanged software sometime during the last few weeks. Simultaneously Bob, Carol and Dave eradicates virus if found and inform to their friends.This may be explained by a model in which, once a machine is found to be infected, neighboring machines are checked for viruses. This "kill signal" idea could be implemented in networks to greatly reduce the threat of viral spread[14].

ACKNOWLEDGMENT

We are grateful to our Institution and colleagues whose constant encouragement served to renew spirit, refocus attention and energy and helped us in carrying out this work.

REFERENCES

[1] R. T. Goswami and B. K. Mishra, "Information and the dynamics of seir e-epidemic model for the spreading behavior of malicious objects in computer network," *International Journal of Engineering Science and Technology*, vol. 4, no. 10, pp. 4275–4282, 2012.

[2] F. Wang, Y. Yang, D. Zhao, and Y. Zhang, "A worm defending model with partial immunization and its stability analysis," *Journal of Communications*, vol. 10, no. 4, 2015.

[3] X. Yang and L.-X. Yang, "Towards the epidemiological modeling of computer viruses," *Discrete Dynamics in Nature and Society*, vol. 2012, 2012.

[4] O. J. Brady, H. C. J. Godfray, A. J. Tatem, P. W. Gething, J. M. Cohen, F. E. McKenzie, T. A. Perkins, R. C. Reiner Jr, L. S. Tusting, T. W. Scott *et al.*, "Editor's choice: Adult vector control, mosquito ecology and malaria transmission," *International health*, vol. 7, no. 2, p. 121, 2015.

[5] J. R. Piqueira, B. F. Navarro, and L. H. Monteiro, "Epidemiological models applied to viruses in computer networks," *Journal of Computer Science*, vol. 1, no. 1, pp. 31–34, 2005.

[6] J. R. Piqueira, A. A. de Vasconcelos, C. E. Gabriel, and V. O. Araujo, "Dynamic models for computer viruses," *Computers & Security*, vol. 27, no. 7, pp. 355–359, 2008.

[7] B. K. Mishra and D. K. Saini, "Seirs epidemic model with delay for transmission of malicious objects in computer network," *Applied Mathematics and Computation*, vol. 188, no. 2, pp. 1476–1482, 2007.

[8] A. Misra, M. Verma, and A. Sharma, "Capturing the interplay between malware and anti-malware in a computer network," *Applied Mathematics and Computation*, vol. 229, pp. 340–349, 2014.

[9] J. Cui, Y. Sun, and H. Zhu, "The impact of media on the control of infectious diseases," *Journal of Dynamics and Differential Equations*, vol. 20, no. 1, pp. 31–53, 2008.

[10] Y. Liu and J.-a. Cui, "The impact of media coverage on the dynamics of infectious disease," *International Journal of Biomathematics*, vol. 1, no. 01, pp. 65–74, 2008.

[11] G. P. Sahu and J. Dhar, "Analysis of an sveis epidemic model with partial temporary immunity and saturation incidence rate," *Applied Mathematical Modelling*, vol. 36, no. 3, pp. 908–923, 2012.

[12] ——, "Dynamics of an seqihrs epidemic model with media coverage, quarantine and isolation in a community with pre-existing immunity," *Journal of Mathematical Analysis and Applications*, vol. 421, no. 2, pp. 1651–1672, 2015.

[13] M. Sun, D. Li, D. Han, and C. Jia, "Impact of anti-virus software on computer virus dynamical behavior," *International Journal of Modern Physics C*, vol. 25, no. 05, p. 1440010, 2014.

[14] J. O. Kephart, S. R. White, and D. M. Chess, "Computers and epidemiology," *Spectrum, IEEE*, vol. 30, no. 5, pp. 20–26, 1993.