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

Ashish Bhargava, Durgesh Kumar Soni, Palash Jain, Joydip Dhar
ABV-IIITM,
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 R_0 is calculated and it is observed that when $R_0 < 1$, then the system will have malicious code free stable steady state. Again, when $R_0 > 1$, 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

Malignant code does not simply influence one PC, it can likewise get into the systems and spread. It can send messages through email and take data or cause much more harm by erasing records. It is a PC program that works for the benefit of a potential interloper to help in assaulting a framework or system. Noxious code can come in different structures. A typical sort of malignant code is the infection, which is a little program appending to different projects or documents and will duplicate itself in a PC and even spread to other arranged PCs. Infections can run from being moderately safe to creating critical harm to a framework. Worms are bits of noxious code making duplicates of itself. Conditions must be a good fit for a worm to multiply. They are made principally utilizing scripting dialects. Trojan steeds are types of vindictive code showing up as protected programming. Be that as it may, that is the way they get into a PC. They might be covering up inside another program and be introduced with a generally safe project. Once in a while they give somebody in a remote area control of the casualty's PC . [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. Just a little division of all known infections have showed up in genuine episodes, mostly in light of the fact that numerous infections are underneath the hypothetical scourge limit. The watched sub exponential rate of viral spread can be clarified by models of confined programming trade. A shockingly little division of machines in all around ensured business situations are tainted. This might be clarified by a model in which, once a machine is observed to be tainted, neighboring machines are checked for infections. This "slaughter signal" thought could be executed in systems to significantly decrease the risk of viral spread.

II. MODEL DEVELOPMENT

We consider two groups of computer nodes, namely, targeted nodes and attacker nodes. In this model attacker targeted

978-1-4673-9802-2/16/$31.00© 2016 IEEE

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; $S1(t)$ 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 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 $N1(t) = S_1(t) + L_1(t) + B_1(t) + R_1(t) + A_1(t)$. 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 $\beta(I) = c1 - c2f(I)$, is incorporated in the transmission term to investigate the effect of firewall security, where $f(I) = I/(m+I)$. In the modeling of malicious code propagation, the incidence function plays a very important role. In many models, the bilinear incidence rate βSI and the standard incidence rate $\beta SI/N$ 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 $\beta(I) = \beta e{-}mI/N$ in the proposed model which is more reasonable than $\beta(I) = \beta e{-}mI$, because $\beta e{-}mI \rightarrow 0$ as $I \rightarrow \infty$, 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, $min\{\beta e{-}m\ I/N\} = \beta e{-}m$ that remains unchanged with respect to the total population size.

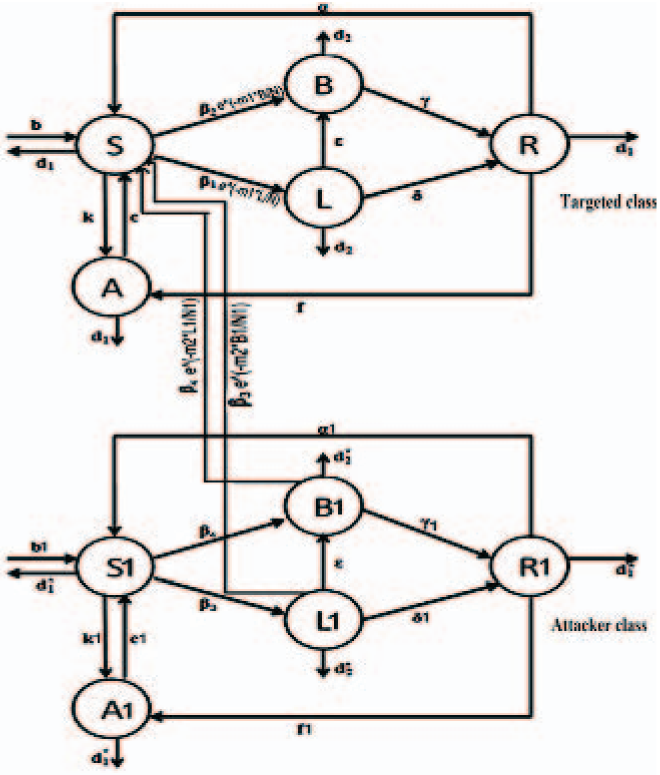

Fig. 1. Schematic Flow of Proposed Model

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:

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

$$\frac{d\widetilde{B}}{d\widetilde{t}} = \widetilde{\beta}_2 e^{-m_1\frac{\widetilde{B}}{\widetilde{N}}}\widetilde{S}\frac{\widetilde{B}}{\widetilde{N}} - \widetilde{d}_2\widetilde{B} + \widetilde{\varepsilon}\widetilde{L} - \widetilde{\gamma}\widetilde{B} + \widetilde{\beta}_2 e^{-m_2\frac{\widetilde{B}_1}{\widetilde{N}_1}}\widetilde{S}\frac{\widetilde{B}_1}{\widetilde{N}_1}, \tag{2}$$

$$\frac{d\widetilde{L}}{d\widetilde{t}} = \widetilde{\beta}_1 e^{-m_1\frac{\widetilde{L}}{\widetilde{N}}}\widetilde{S}\frac{\widetilde{L}}{\widetilde{N}} - \widetilde{d}_2\widetilde{L} - \widetilde{\varepsilon}\widetilde{L} - \widetilde{\delta}\widetilde{L} + \widetilde{\beta}_1 e^{-m_2\frac{\widetilde{L}_1}{\widetilde{N}_1}}\widetilde{S}\frac{\widetilde{L}_1}{\widetilde{N}_1}, \tag{3}$$

$$\frac{d\widetilde{R}}{d\widetilde{t}} = \widetilde{\gamma}\widetilde{B} + \widetilde{\delta}\widetilde{L} - \widetilde{f}\widetilde{R} - \widetilde{\alpha}\widetilde{R} - \widetilde{d}_1\widetilde{R}, \tag{4}$$

$$\frac{d\widetilde{A}}{d\widetilde{t}} = \widetilde{f}\widetilde{R} - \widetilde{d}_1\widetilde{A} + \widetilde{k}\widetilde{S}\widetilde{A} - \widetilde{c}\widetilde{A}, \tag{5}$$

For Attacker nodes:

$$\frac{d\widetilde{S}_1}{d\widetilde{t}} = b_1 - \widetilde{\beta}_4 \widetilde{S}_1 \widetilde{B}_1 - \widetilde{\beta}_3 \widetilde{S}_1 \widetilde{L}_1 - \widetilde{k}_1 \widetilde{S}_1 \widetilde{A}_1 + \widetilde{c}_1 \widetilde{A}_1 - \widetilde{d}_3 S_1 + \widetilde{\alpha}_1 \widetilde{R}_1, \qquad (6)$$

$$\frac{d\widetilde{B}_1}{d\widetilde{t}} = \widetilde{\beta}_4 \widetilde{S}_1 \widetilde{B}_1 - \widetilde{d}_4 \widetilde{B}_1 + \widetilde{\varepsilon}_1 L_1 - \widetilde{\gamma}_1 B_1, \qquad (7)$$

$$\frac{d\widetilde{L}_1}{d\widetilde{t}} = \widetilde{\beta}_3 \widetilde{S}_1 \widetilde{L}_1 - \widetilde{d}_4 \widetilde{L}_1 - \widetilde{\varepsilon}_1 L_1 - \widetilde{\delta}_1 L_1, \qquad (8)$$

$$\frac{d\widetilde{R}_1}{d\widetilde{t}} = \widetilde{\gamma}_1 \widetilde{B}_1 + \widetilde{\delta}_1 \widetilde{L}_1 - \widetilde{f}_1 \widetilde{R}_1 - \widetilde{\alpha}_1 \widetilde{R}_1 - \widetilde{d}_3 \widetilde{R}_1, \qquad (9)$$

$$\frac{d\widetilde{A}_1}{d\widetilde{t}} = \widetilde{f}_1 \widetilde{R}_1 - \widetilde{d}_3 \widetilde{A}_1 + \widetilde{k}_1 \widetilde{S}_1 \widetilde{A}_1 - \widetilde{c}_1 \widetilde{A}_1. \qquad (10)$$

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,

$$S = \frac{\widetilde{S}}{\widetilde{N}}, B = \frac{\widetilde{B}}{\widetilde{N}}, \quad L = \frac{\widetilde{L}}{\widetilde{N}}, \quad R = \frac{\widetilde{R}}{\widetilde{N}}, \quad A = \frac{\widetilde{A}}{\widetilde{N}}, \quad S_1 = \frac{\widetilde{S}_1}{\widetilde{N}_1}, \quad B_1 = \frac{\widetilde{B}_1}{\widetilde{N}_1},$$

$$L_1 = \frac{\widetilde{L}_1}{\widetilde{N}_1}, R_1 = \frac{\widetilde{R}_1}{\widetilde{N}_1}, A_1 = \frac{\widetilde{A}_1}{\widetilde{N}_1}, t = \widetilde{d}_1 \widetilde{t}, N = \frac{\widetilde{N}}{\widetilde{N}^0}, N_1 = \frac{\widetilde{N}_1}{\widetilde{N}_1^{\,0}}.$$

Where, $\widetilde{N}^0 = \frac{b}{\widetilde{d}_1}$ and $\widetilde{N}_1^{\,0} = \frac{b}{\widetilde{d}_3}$.

Targeted population and attacker population parameters $\widetilde{d}_1$ and $\widetilde{d}_3$ respectively become $\beta_1 = \frac{\widetilde{\beta}_1}{\widetilde{d}_1}$, $\beta_3 = \frac{\widetilde{\beta}_3}{\widetilde{d}_3}$.

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

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

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

B. Basic Reproduction Number

The definition of basic reproduction number R_0 is as the expected number of secondary cases produced by a single infection in a completely susceptible population. It is considered as the most useful threshold parameter 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,

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

where,

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

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

we get, F(Jacobian of 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 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 rate 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,

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

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,

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

$$\left. \frac{1+\beta_2}{1+d_2+\gamma}, \frac{(1+\beta_4)(1+c_1)}{(k_1)(1+d_3+\gamma_1+\frac{1+c_1}{k_1}} \right\}.$$

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,

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

$$\left. \frac{(1+\beta_2)(1+c)}{(k)(\frac{1+c}{k}+d_2+\gamma)}, \frac{(1+\beta_4)(1+c_1)}{(k_1)(1+d_3+\gamma_1+\frac{1+c_1}{k_1})} \right\}.$$

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

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

$$\left. \frac{(1+\beta_2)(1+c)}{(k)(\frac{1+c}{k}+d_2+\gamma)}, \frac{(1+\beta_4)}{1+d_3+\gamma_1} \right\}.$$

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 $R_{01}<1$, then all the eigenvalues will have negative real parts. Hence, the malicious code free equilibrium *E*1 is locally asymptotically stable, if $R_{01}<1$ and unstable, if $R_{01}>1$.

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.

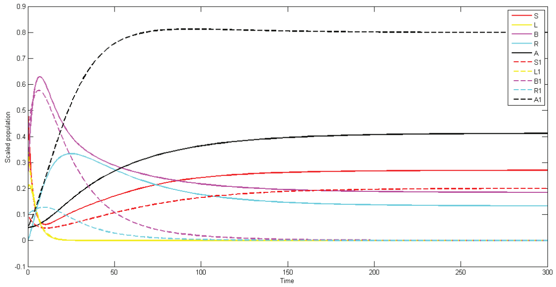

Fig. 2. Node Density vs. Time for different classes with Set 1

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.

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*, E2, E3* 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, and 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.

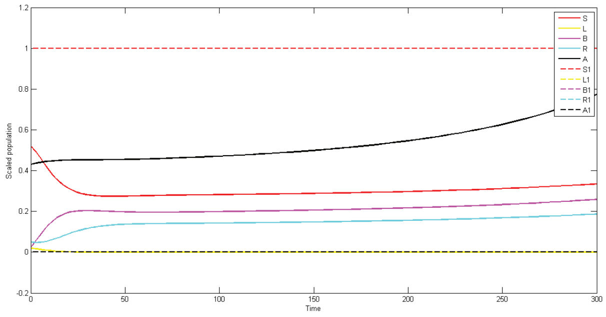

Fig. 3. Node Density vs. Time for different classes with Set 2.

TABLE. II

Feasible steady states and numerical values of basic reproduction number for different parameter set in the model.

Parameters	**Set 1**	**Set 2**
$\boldsymbol{\beta_1}$	0.6	0.6
$\boldsymbol{\beta_2}$	0.5	0.5
k	0.06	0.06
c	0.03	0.03 3
$\boldsymbol{\alpha}$	0.05	0.05
$\mathbf{d_2}$	0.04	0.08
$\boldsymbol{\epsilon}$	0.3	0.3
$\boldsymbol{\gamma}$	0.045	0.45
$\boldsymbol{\delta}$	0.025	0.25
f	0.02	0.02
$\boldsymbol{\beta_3}$	0.4	0.4
$\boldsymbol{\beta_4}$	0.3	0.3
$\mathbf{f_1}$	0.15	0.15
$\mathbf{k_1}$	0.05	0.05
$\mathbf{c_1}$	0.01	0.01
$\boldsymbol{\alpha_1}$	0.04	0.04
$\mathbf{d_3}$	0.05	0.05
$\boldsymbol{\gamma_1}$	0.035	0.35
$\boldsymbol{\delta_1}$	0.02	0.2
$\boldsymbol{\epsilon_1}$	0.25	0.25
feasible SS	$E_1.E_2.E_3.$	$E_1.E_2.E_3.E_4$
R_{01}	0.58803	0.9523
R_{02}	5.88034	0.9523
R_{03}	3.52822	0.8000
R_{04}	2.94421	0.4767

V. Estimation of firewall security coefficient

The firewall is the central part of a well-defined network security policy. The aim of the Check Point Firewall Rule Base is to create rules that only allow the pre-defined connections.

A. Order of Rule Enforcement

The Firewall assesses associations and authorizes the Rule Base in a successive way. The Firewall examines every association that goes to the system and analyzes the information (source, destination, administration, and so on.) to the principal standard. In the event that the association coordinates the standard, the Firewall applies the activity of that run the show. On the off chance that the association does not coordinate the principle, the Firewall proceeds with the following guideline in the Rule Base.

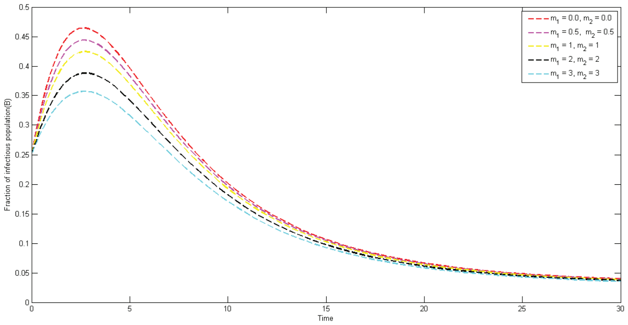

Fig. 4. Effect of *m* on *B* when *R*0<1.

B. Firewall rule priority

Since you can make firewall decides that have obvious clashes, it is vital to comprehend the request in which the principles are prepared.

C. Authenticated bypass

These are guidelines in which the override piece rules choice is chosen. These tenets permit coordinating system movement that would some way or another be blocked. The system activity must be verified by utilizing a different association security guideline. You can utilize these principles to allow access to the PC to approved system executives and approved system investigating gadgets.

D. Block connection

These standards obstruct all coordinating inbound system activity.

E. Allow connection

These standards permit coordinating inbound system activity. Since the default conduct is to piece spontaneous inbound system activity, you should make a permit tenet to bolster any system program or administration that must have the capacity to acknowledge inbound associations. The coefficient of firewall security, m ought to rely on upon the kind of files(data) under thought, characterized firewall security rules in the firewall standard base and the unwavering quality and proficiency of the firewall. We propose a strategy for evaluating the coefficient m of firewall security as,

$$m = -\log(p+q-pq),$$

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}	$\beta_2,\beta_3,\beta_4,k,c$
R_{04}	β_1,β_2,k,c

VII. Future Scope

This work can be stretched out by including more control techniques, for example, time delay for flare-up and time fluctuating enlistment rate. Consider the accompanying situation, one day, Alice finds that one of the projects she utilizes on her PC is tainted with an infection. She kills it, in many models, this would be the end of the story. Be that as it may, for this situation Alice takes it upon herself to illuminate her companions Bob, Carol, and Dave, with whom she had traded programming at some point amid the most recent couple of weeks. All the while Bob, Carol and Dave annihilates infection if found and illuminate to their companions. This might be clarified by a model in which, once a machine is observed to be contaminated, neighboring machines are checked for infections. This "execute signal" thought could be actualized in systems to enormously lessen the risk of viral spread [14].