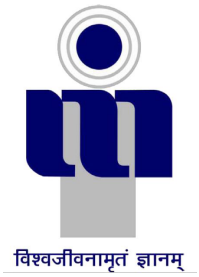
A Compartmental Model for Transmission Dynamics of Distributed Attack of Malicious Codes on the Targeted Network: Effect of Firewall Security

A project report submitted in partial fulfillment of the requirements for the award of the degree of

B.Tech.

by

Durgesh Kumar Soni (2012IPG-032)
Palash Jain (2012IPG-105)
Ashish Bhargava (2012IPG-123)



ABV INDIAN INSTITUTE OF INFORMATION TECHNOLOGY AND MANAGEMENT
GWALIOR-474 015

2015-16

CANDIDATES DECLARATION

We hereby certify that the work, which is being presented in the thesis, entitled **A Compartmental Model for Transmission Dynamics of Distributed Attack of Malicious Codes on the Targeted Network: Effect of Firewall Security**, in partial fulfillment of the requirement for major project of **B.Tech** and submitted to the institution is an authentic record of our own work carried out during the period *May 2015* to *August 2015* under the supervision of **Dr. Joydip Dhar**. We have also cited the reference about the text(s)/ figure(s)/ table(s) from where they have been taken.

Date: Signatures of the Candidates

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Date: Signatures of the Research Supervisors

ABSTRACT

In our work, we have developed a compartmental model using firewall security coefficient for the analysis of the spread of a distributed attack on critically targeted groups in a network. The model gives an epidemic design with two sub-designs to consider the difference between the overall behavior of the attacker class and the targeted class. The targeted nodes and attacker nodes are divided into five compartments as Susceptible - Latent - Breaking out - Recovered- Antidotal. The boundedness of the system, the feasibility of equilibrium states and their stabilities are analyzed using cyber mass action incidence. Basic reproduction number $\mathcal{R}_0$ is observed and it is found that when $\mathcal{R}_0 < 1$, then the system will possess malicious code free stable steady state and, when $\mathcal{R}_0 > 1$, then endemic steady state exists and will have local asymptotic stablity. The impact of firewall security rule base in controlling transmission of malicious objects is analyzed. Some researchers explored the impact of media awareness in biological disease spread using mathematical modeling with transmission coefficient function $\beta(I) = \beta e^{-m\frac{I}{N}}$ and observed that many positive equilibria are possible when the media effect is adequately strong among population [1, 2, 3, 4]. Similarly we are taking firewall security as a media coverage factor in our computer network model of malicious code propagation. The coefficient of firewall security 'm' depends on the types of files under consideration, defined firewall security rules in the firewall rule base and the reliability and efficiency of the firewall. We suggest a way for quantifying the coefficient m of firewall security as :

$$m = -\log_e(a + b - ab),$$

where, 'b' measures the response of the files to the defined security rules. It is considered that the malware propagation rate can be reduced by a proportion 'a' when all received files abide the defined security rules. The stability of the system is observed using local asymptotic stability method. Finally, most sensitive system parameters for basic reproduction number are observed using normalized forward sensitivity index. Numerical simulation has been carried out to verify analytical findings.

Keywords: Computer networks, Compartmental model, Basic reproduction number, Local asymptotic stability, Numerical simulation, Sensitivity analysis, Firewall security rule base.

ACKNOWLEDGEMENTS

We are highly obliged to our mentor **Dr. Joydip Dhar**, and grateful for giving us the autonomy of functioning and experimenting with ideas. We would like to take this opportunity to express our profound gratitude to him not only for their academic guidance, but also for their personal interest in our project and constant support coupled with confidence boosting and motivating sessions which proved very fruitful and were instrumental in infusing self-assurance and trust within us. The nurturing and blossoming of the present work is mainly due to his valuable guidance, suggestions, astute judgment, constructive criticism and an eye for perfection. Our mentor always answered myriad of doubts with smiling graciousness and prodigious patience, never letting us feel that we are novice by always lending an ear to our views, appreciating and improving them and by giving us a free hand in the project. It's only because of his overwhelming interest and helpful attitude, the present work has attained the stage it has.

Finally, 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.

Durgesh Kumar Soni Palash Jain Ashish Bhargava

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

Introduction and Literature Review

1.1 Introduction

In the era of cloud computing, malicious code propagation is critical for any network. Malicious code would not simply have an effect on only one computer, but it can also affect the network. It can also send messages through social networking and steal information or cause severe damage by deleting and corrupting documents. It is a computer program that helps a potential intruder to attack a network. Malicious code are of various types. One type is virus, that is a little program attaching to different packages or documents and will copy itself in a computer or even spread to different networked computer systems. Viruses can variety from being noticeably innocent to causing big damage to a device.
Another type is worm which can replicate itself. Proliferation of worms require certain specific conditions. Scripting languages are used to create worms.
Trojan horses are another type of malicious code which appears as safe program. But it is the way they enter into a computer. They may be a part of another safe program and installed within it. They may give control of the victim's computer to someone in a remote location [5].
These types of malicious code have a severe threat to the security of the networks. A recognizable degradation in the performance could be observed in a computer with malicious codes in breaking-out state. Malicious codes can replicate themselves from one computer

to another without you being aware that your machine is infected. This malicious code problem is growing as a serious threat as new forms of current viruses including some new versions are frequently emerging and increasing the vulnerability of the network. Therefore, there is a necessity to develop a new counter defense techniques to control this threat. The universal proposal for malicious code propagation avoidance and control cannot be recommended because of the difficulty in the analysis of evolution trends of malicious codes [6].

In a proper sense, malicious codes growth (in networks) is epidemic in nature, i.e., it's propagation in a system could be understand using transmission of disease in the biological world. Mathematical models are developed keeping in view the epidemic nature of malicious code propagation. Due to continuous emergence of new types of attacks there is a need to enhance the existing propagation models. Mathematical modeling is growing as an important tool to study and control malicious codes propagation in computer networks. Mathematical models considers the important factors responsible for malicious codes propagation, such as rates of transmission and recovery, and identify how the malicious codes will spread over a fixed time period.

1.2 Organization of Thesis

The thesis is organized as follows: In section 1.3, we carried out literature review and discussed the works done in the context so far. In section 1.4, Problem statement and objective are defined. In chapter 2, a compartmental model using firewall security coefficient is proposed. In chapter 3, numerical simulation and sensitivity analysis are carried out. Conclusion and future scope of the proposed work are portayed in chapter 4.

1.3 Literature Review

Malicious codes propagation in computer networks is epidemic in nature, i.e., the malicious codes propagation could be understand by the transfer of diseases in biological world

[3, 7, 8]. Many epidemic models for malicious codes propagation are based on classical SIR model [9, 10, 11], which provides an estimate of evolution of malicious codes in the computer networks.

Just a little fraction of all recognized malicious codes have showed up in real incidents, because many malicious codes are below the defined threshold epidemic. The models of localized software exchange could be used to explain the identified sub-exponential rate of malicious codes. In a well-secured environments only a little proportion of machines are found to be infected. This may be observed by a model in which, once a machine is contaminated, the majority of its neighboring machines are checked for infections. So, malicious code propagation could be minimized by implementing this idea of 'kill signal'. In all known epidemiological models, an individual's treatment is done autonomously. In any case, consider the following situation, one day Ram finds that one of the program he utilizes on his computer is contaminated with an virus, he removes it. In many models, this would be the story's end. Notwithstanding, for this situation Ram takes it upon himself to give this information to his companions Shyam, Mahesh and Suresh with whom he had shared this program at some point in the most recent couple of weeks. All the while Shyam, Mahesh and Suresh removes infection if discovered and propagate information to their companions. P_{kill} threshold tool is used (above which there is an infinitesimally small probability of an epidemic) e.g. removal of the malicious codes is comulsory if 3 or more out of a typical 10 neighbors receive the kill signal. Kill signal could be used as an epi-epidemic(like an anti-virus epidemic) [7].

An examination of the qualities of computer viruses uncovers the problems in the past models. So, a common generalized epidemic model of viruses is proposed which is called the SLBS model.

1.3.1 Drawbacks of previous models:

1.3.1.1 E(exposed) compartment

It is not possible that a computer doesn't has infectivity. So, no exposed computer exists. Since, once attacked by a malicious code, a computer becomes infected immediately and possesses infectivity, because it can propagate this attack to those computers with certain vulnerabilities in the system. Therefore, an epidemic model shouldn't have any E compartment.

1.3.1.2 Single I compartment

A well defined epidemic model of malicious code propagation should have two classified I compartments, as L(Latent) compartment for computers with virus in latent state and B(breaking-out) compartment. The probability with which they recover, is a main issue in the process of modeling. Indeed, recovery of a breaking-out computer is fast than a computer with virus in latent state because it usually has a recognizable degradation in the performance, which can be identified by the user.

1.3.1.3 Permanent R compartment

It is probable that a computer which is recovered be infected by new types of malicious codes implying that permanent immunity is not possible. So, an epidemic model should not have any permanent R(recovered) compartment [6].

In [12], Some anti-malware softwares are installed and continuously updated in the network to minimize the abundance of malicious objects and infected computers. On analyzing the proposed model, we obtained two equilibria and a threshold governing the dynamics of malicious objects in a computer network. The characterization of stability behavior of obtained equilibria is also discussed in detail. The aim of this study is to assess the potency of anti-malware softwares in protecting a computer network from malicious

attack.

In [13], a novel epidemic SVEIR model with partial immunization is proposed. In the SVEIR model, basic reproduction number, global stabilities of malicious codes free steady state and endemic steady state are proven using Lyapunov function. This epidemic model gives a base for controlling Internet worms. The past models don't cosider hosts with virus in latent state. Actually, an infected host in latent state can spread infection by methods like vulnerability seeking. The previous models do not take this infectivity into consideration. Immunization is one of commonly used method for controlling the propagation process of worms. Some epidemic models with immunization have been proposed. However, these models all assumed that the vaccine hosts obtained the immunization fully. This is not consistent with the reality. In real networks, it is very difficult to obtain the full immunization for the vaccine hosts. Thus, partial immunization should be a fungible and feasible method for eliminating worms, which have been used for predicting and controlling infectious diseases. This paper proposes a new malicious code defending SVEIR epidemic model, with five compartments as Susceptible-Vaccinated-Exposed-Infectious-Recovered.

Standard counsel in regards to control of the vector is to incline toward intercessions that decrease the lifetime of grown-up mosquitoes. The premise for this guidance is a very-old affectability examination of 'vector-limit', for most epidemic models for malaria transmissions and based solely on adult mosquito population dynamics. Recent enhancements in micro-simulation models after a chance to explore the theory of vectorial capacity(including both adult and juvenile mosquito stages in the model). In this study we return to contentions about transmission and it's affectability to mosquito binomic parameters utilizing a versatility of created plans of vectorial limit. We demonstrate that decreasing grown-up survivals have impacts on both grown-up and adolescent population size, which are not represented in conventional plans of vectorial limit and are huge for transmission. Various mosquito population parameters are responsible for versatility of these effects. In general, control is the most touchy to systems that influence grown-up death rate, trailed by blood encouraging recurrence, human blood bolstering propensity,

and in conclusion, to grown-up mosquito populace thickness. These outcomes accentuate more unequivocally on than any other time in recent memory the affectability of transmission to grown-up mosquito mortality, additionally propose the high capability of mixes of mediation including administration of source of larva . This must be finished with alert, however as approach obliges a more cautious thought of expenses, operational challenges and arrangement objectives in connection to gauge transmission [14].

In [15], The effect of anti-virus program on propagation of computer infection is examined by means of building up a scientific model. Considering the anti-virus program may be attacked with a smaller incident rate. The basic reproduction number is calculated. Considering the anti-virus program may not be effective and the virus may be hidden. In this, an epidemic virus model is established. Latent computers and breaking-out computers are sub-divided from infected computers. The effect of anti-virus program on malicious code propagation is considered. By using Lyapunov function, it is found that the malicious-code free equilibrium is globally asymptotically stable if $R_0 \leq 1$. Routh Stabilty criterion is used for the local asymptotic stability derivation. We have essentially focused around the effect of anti-virus program on the propagation of malicious codes by developing an epidemic model. Considering that the anti-virus program may not be excessively successful as it might be an obsolete form or it may not be upgraded, that is, although a computer with anti-virus program, they can even now re-secure the malicious code with a smaller incident rate.

In partial request E-pestilence model with very irresistible hubs, SIJR model of fragmentary request for the transmission of infection in PC system with regular demise has been introduced. The partial subordinates are portrayed in caputo sense. In this model the hubs have two levels of contamination. Predator-corrector strategy is utilized to acquire the numerical arrangement of exhibited model. A system of fractional order model that is based on the integer model presented, for modeling propagation of viruses in computer network with natural death as follows:-

$D^{\alpha}(S) = b - \mu S - \beta SI,$

$D^{\alpha}(I) = \beta SI + \sigma J - \beta IJ - \gamma I(\mu + \delta),$

$D^{\alpha}(J) = \beta SIJ - (\mu + \delta)J - \sigma J + b,$
$D^{\alpha}(R) = \gamma I - \mu R.$
Where, $0 < \alpha \leq 1$, b is birth rate, μ is natural death rate, δ is crashing rate of nodes due to virus attack, β is the susceptible class (for S to I) and the infectious class (for I to J) transmission rate coefficient, σ is highly infectious class (for J to I) transmission rate coefficient and γ is highly infectious class (for I to R) transmission rate coefficient.
Basic reproduction number $R_0 = \frac{\beta}{\mu+\sigma+\gamma}$. And, it is given as the expected number of secondary infections produced by a single infection host introduced into a totally susceptible population. In most cases if $R_0 > 1$ then, the infection will advance in a population whereas if $R_0 < 1$, then the infection will disappear from the population. It first define the definition of fractional order differentiation and fractional-order integration. For the concept of fractional-order differentiation, it would have considered Caputo's definition. It is beneficial in dealing properly with initial value problems.

In [16], with an expanding worldwide dependence on technology, from managing overseeing national electrical grids to requesting supplies for troops, the security of cyber world turn into an imperative topic around the world. Here, an epidemic $SEI_1I_2R_1R_2$ (Susceptible - Exposed - Infected class 1 - Infected class 2 - Recovered class 1 - Recovered class 2) model for propagation of malicious codes in a network is developed to go through the nature of removed class on cyber war. An examination of fundamental reproduction number has been carried out and worldwide strength of an assault free state is built up. Besides, starting recreation results demonstrate the framework conduct, dependability investigation for assault free state, effect of removed class in the system for minimizing the contamination and the positive effect of expanding efforts to establish safety on malicious codes propagation in computer network.
In this paper, it examines assaulting conduct of malevolent articles that debilitate the IT security framework inside of associations. The significant assaults are the Denial of Service (DoS) assault and the appropriated form (DDoS). This paper gives the thought regarding how these assaults function actually, and examine approaches to anticipate them in the system. A DoS assault misuses this circumstance by tweaking TCP bundles to make server react to pernicious, manufactured system demands.

It accept that the system being partitioned into two distinctive sub-systems or compartments and the aggregate hubs (N) in system are helpless towards the the attack by cyber criminals. The attacker attacks the n (n<N) number of hubs in the sub-system making them very irresistible and the clients are not able to open a particular sites. These n number of hubs are set in a class I_1. We additionally accept that when the infectious nodes are flooding the most and the impact of antivirus is negligible in that same hub, they are for all time expelled from the system say k (<n) as their recuperation is weak. The remaining n-k irresistible hubs are sufficiently competent to transmit the infection to the hubs of another sub-system making the extent of hubs irresistible and we say it I_2 class. Antivirus programming is keep running at particular time interim to recuperate hubs in I_2 class. It accept the slamming of hubs because of equipment/programming termed as common passing and assault of malevolent item is termed as death because of assault. Numerical Tools Used: Jacobian Matrix and eigen values, Runga-Kutta Fahlberg Method of request 4 and 5 and MATLAB. The rate of recuperation is high when upgraded adaptation antivirus is keep running into the hubs. In this way, it prescribes the product association to keep up these parameters for against infection programming [16].

In [17], a dynamic model was developed which was a prototype for defining vertical transmission of viruses into the networks. Then, in [18] interplay capturing was defined between viruses and anti-viruses. Bimal kumar Mishra and Dinesh Saini jointly developed some mathematical models on propagation of malicious codes in the computer networks in 2007 [19, 20]. In [4], a SEQIRS model was proposed which was taken into consideration the effect of media coverage, quarantine and isolation with some already existing immunity. Ren, Jianguo and Xu, Yonghong and Zhang, Chunming ,used the idea of delay in propagation of malicious codes in computer networks and then they defined some techniques for controlling it optimally [21].

1.4 Problem Statement and Objective

The main objective of our work is to propose an epidemic model for propagation of malicious codes in computer networks. This model is developed to enhance the previous work done in this area.

To achieve this goal, we have developed a model which considers two classes of nodes namely, targeted and attacker classes, and these classes aresub-divided into five compartments each(viz., Susceptible-Latent-Breaking out-Recovered-Antidotal). We have also taken into consideration the effect of firewall security coefficient 'm', to analyze its effect on malicious code propagation.

CHAPTER 2

Proposed Mathematical Model

2.1 Compartment Description

We consider two groups of computer nodes, namely, targeted nodes and attacker nodes. In this model attacker-targeted nodes are sub-divided into 5 compartments namely Susceptible, Latent, Breaking-out, Antidotal and Recovered. Here, total computer nodes are divided into ten classes, namely, $S(t)$ susceptible targeted computers; $S_1(t)$ susceptible 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 malicious code in breaking-out state and recovered class population and $R(t), R_1(t)$ are recovered class population in targeted and attacker class respectively. The schematic flow of the model is shown in the figure2.1. Here certain assumptions are made like homogeneous spatial distribution and the law of mass action is followed in the mixing of hosts, i.e., through out the total population size, the local population density is a constant. 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 main objective of this model is to analyze the impact of firewall security rule base in controlling transmission of malicious objects. Some researchers explored the impact of media awareness in biological disease spread using mathematical modeling with transmis-

sion coefficient function, $\beta(I) = \beta e^{-m\frac{I}{N}}$ and observed that many positive equilibria are possible when the media effect is adequately strong among population [1, 2, 3, 4]. Similarly, we are taking firewall security as a media coverage factor in our computer network model of malicious code propagation. Non-linear function given by $\beta(I) = b_1 - b_2 f(I)$, is used in the transmission term to observe the effect of firewall security, where $f(I) = \frac{I}{m+I}$. In the mathematical modeling of malicious code propagation, the incidence function has a significant role. In various mathematical models, $\beta\tilde{S}\tilde{I}$ is used as the bilinear incidence rate and $\frac{\beta\tilde{S}\tilde{I}}{N}$ is used as the standard incidence rate, where β quantifies the effect of both the contact transmission rates and the propagation of the malicious code. However, the impact of firewall security coefficient to the spread and control of malicious code propagation is not considered in these incidence function.

Firewall security coefficient utilization and alert has been found beneficial for reducing malicious code propagation. Initially, the expression for transmission rate $\beta(I) = \beta e^{-mI}$ is used by the researchers but it has some flaws. We used firewall induced contact transmission rate as $\beta(I) = \beta e^{-m\frac{I}{N}}$ in our compartmental model which is more rational, because $\beta e^{-mI} \to 0$ as $I \to \infty$, independent of the nature of m. Since the firewall security and alertness are only the extrinsic deterministic factor for the transmission, so it is rational to consider that the rate of transmission cannot be decreased below a fixed level simply through firewall security alert. Besides, further for a fixed value of m, the minimum rate of transmission varies with population size, which is unrealistic. Secondly, $min\{\beta e^{-m\frac{I}{N}}\} = \beta e^{-m}$ which remains unaltered with the population size.

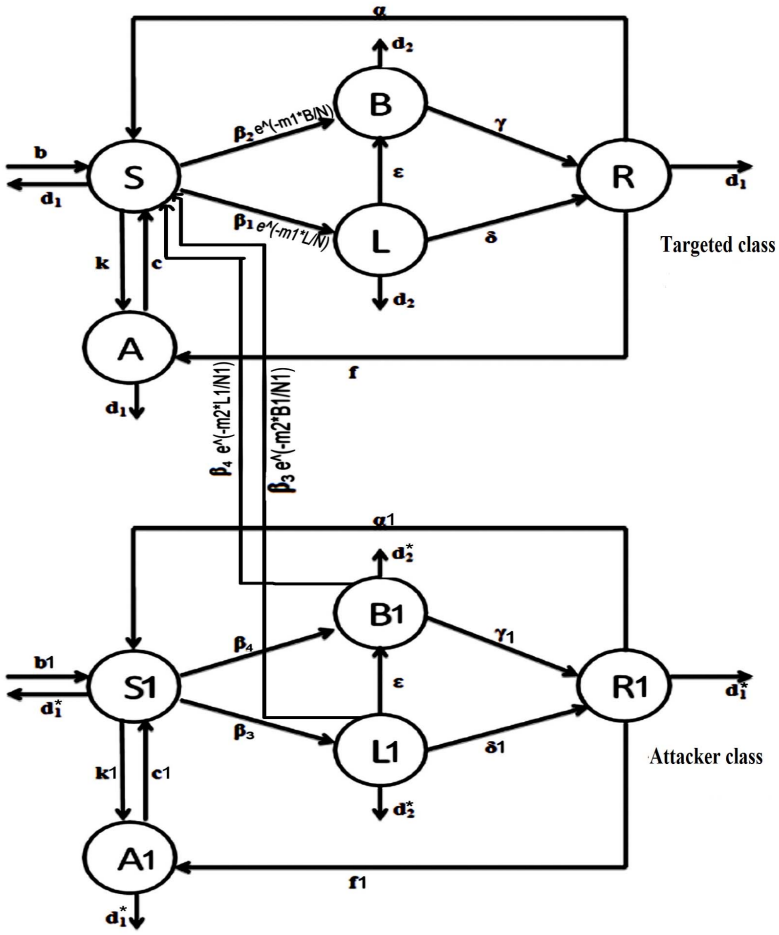


Figure 2.1: Schematic Flow of Proposed Model

2.2 Mathematical Model

Keeping in view the transmission rates of the schematic flow diagram which is shown in the figure 2.1. The system is defined by following set of ordinary differential equations:

For targeted nodes:

$$\begin{aligned}\frac{d\tilde{S}}{d\tilde{t}} &= b - \tilde{\beta}_2 e^{-m_1\frac{\tilde{B}}{\tilde{N}}}\tilde{S}\frac{\tilde{B}}{\tilde{N}} - \tilde{\beta}_1 e^{-m_1\frac{\tilde{L}}{\tilde{N}}}\tilde{S}\frac{\tilde{L}}{\tilde{N}} - \tilde{k}\tilde{S}\tilde{A} + \tilde{c}\tilde{A} - \tilde{d}_1\tilde{S} \\ &+ \tilde{\alpha}\tilde{R} - \tilde{\beta}_2 e^{-m_2\frac{\tilde{B}_1}{\tilde{N}_1}}\tilde{S}\frac{\tilde{B}_1}{\tilde{N}_1} - \tilde{\beta}_1 e^{-m_2\frac{\tilde{L}_1}{\tilde{N}_1}}\tilde{S}\frac{\tilde{L}_1}{\tilde{N}_1}, \qquad (2.1)\end{aligned}$$

$$\frac{d\tilde{B}}{d\tilde{t}} = \tilde{\beta}_2 e^{-m_1\frac{\tilde{B}}{\tilde{N}}}\tilde{S}\frac{\tilde{B}}{\tilde{N}} - \tilde{d}_2\tilde{B} + \tilde{\epsilon}\tilde{L} - \tilde{\gamma}\tilde{B} + \tilde{\beta}_2 e^{-m_2\frac{\tilde{B}_1}{\tilde{N}_1}}\tilde{S}\frac{\tilde{B}_1}{\tilde{N}_1}, \qquad (2.2)$$

$$\frac{d\tilde{L}}{d\tilde{t}} = \tilde{\beta}_1 e^{-m_1\frac{\tilde{L}}{\tilde{N}}}\tilde{S}\frac{\tilde{L}}{\tilde{N}} - \tilde{d}_2\tilde{L} - \tilde{\epsilon}\tilde{L} - \tilde{\delta}\tilde{L} + \tilde{\beta}_1 e^{-m_2\frac{\tilde{L}_1}{\tilde{N}_1}}\tilde{S}\frac{\tilde{L}_1}{\tilde{N}_1}, \qquad (2.3)$$

$$\frac{d\tilde{R}}{d\tilde{t}} = \tilde{\gamma}\tilde{B} + \tilde{\delta}\tilde{L} - \tilde{f}\tilde{R} - \tilde{\alpha}\tilde{R} - \tilde{d}_1\tilde{R}, \qquad (2.4)$$

$$\frac{d\tilde{A}}{d\tilde{t}} = \tilde{f}\tilde{R} - \tilde{d}_1\tilde{A} + \tilde{k}\tilde{S}\tilde{A} - \tilde{c}\tilde{A}. \qquad (2.5)$$

For attacker nodes:

$$\frac{d\tilde{S}_1}{d\tilde{t}} = b_1 - \tilde{\beta}_4\tilde{S}_1\tilde{B}_1 - \tilde{\beta}_3\tilde{S}_1\tilde{L}_1 - \tilde{k}_1\tilde{S}_1\tilde{A}_1 + \tilde{c}_1\tilde{A}_1 - \tilde{d}_3 S_1 + \tilde{\alpha}_1\tilde{R}_1, \qquad (2.6)$$

$$\frac{d\tilde{B}_1}{d\tilde{t}} = \tilde{\beta}_4\tilde{S}_1\tilde{B}_1 - \tilde{d}_4\tilde{B}_1 + \tilde{\epsilon}_1 L_1 - \tilde{\gamma}_1 B_1, \qquad (2.7)$$

$$\frac{d\tilde{L}_1}{d\tilde{t}} = \tilde{\beta}_3\tilde{S}_1\tilde{L}_1 - \tilde{d}_4\tilde{L}_1 - \tilde{\epsilon}_1 L_1 - \tilde{\delta}_1 L_1, \qquad (2.8)$$

$$\frac{d\tilde{R}_1}{d\tilde{t}} = \tilde{\gamma}_1\tilde{B}_1 + \tilde{\delta}_1\tilde{L}_1 - \tilde{f}_1\tilde{R}_1 - \tilde{\alpha}_1\tilde{R}_1 - \tilde{d}_3\tilde{R}_1, \qquad (2.9)$$

$$\frac{d\tilde{A}_1}{d\tilde{t}} = \tilde{f}_1\tilde{R}_1 - \tilde{d}_3\tilde{A}_1 + \tilde{k}_1\tilde{S}_1\tilde{A}_1 - \tilde{c}_1\tilde{A}_1. \qquad (2.10)$$

where all the system parameters are positive and described in table 2.1.

Parameters	Description
b, b_1	Recruitment rates
d_1, d_2	Natural death rate of attacker and targeted population nodes
β_1, β_3	Contact rate from susceptible class to latent class;(in the absence of firewall security)
β_2, β_4	Contact rate from susceptible class to breaking-out class;(in the absence of firewall security)
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

Table 2.1: Parameters Description

Non-dimensionalise the above system using,

$S = \frac{\tilde{S}}{\tilde{N}}$, $B = \frac{\tilde{B}}{\tilde{N}}$, $L = \frac{\tilde{L}}{\tilde{N}}$, $R = \frac{\tilde{R}}{\tilde{N}}$, $A = \frac{\tilde{A}}{\tilde{N}}$, $S_1 = \frac{\tilde{S_1}}{\tilde{N_1}}$, $B_1 = \frac{\tilde{B_1}}{\tilde{N_1}}$, $L_1 = \frac{\tilde{L_1}}{\tilde{N_1}}$, $R_1 = \frac{\tilde{R_1}}{\tilde{N_1}}$, $A_1 = \frac{\tilde{A_1}}{\tilde{N_1}}$, $t = \tilde{d_1}\tilde{t}$, $N = \frac{\tilde{N}}{\tilde{N^0}}$, $N_1 = \frac{\tilde{N_1}}{\tilde{N_1}^0}$,$\tilde{N^0} = \frac{b}{\tilde{d_1}}$ and $\tilde{N_1}^0 = \frac{b}{\tilde{d_3}}$.

The equivalent non-dimensional system is given by:

For targeted nodes:

$$\begin{aligned}\frac{dS}{dt} &= \frac{(1-S)}{N} - \beta_2 e^{-m_1 B} SB - \beta_1 e^{-m_1 L} SL - kSAN + cA - S + \alpha R \\ &- \beta_2 e^{-m_2 B_1} SB_1 - \beta_1 e^{-m_2 L_1} SL_1 + S^2 + d_2 SL + d_2 SB + RS + AS, \end{aligned} \tag{2.11}$$

$$\begin{aligned}\frac{dB}{dt} &= \beta_2 e^{-m_1 B} SB - d_2 B + \epsilon L - \gamma B + \beta_2 e^{-m_2 B_1} SB_1 - \frac{B}{N} + BS + d_2 B^2 \\ &+ d_2 BL + BR + BA, \end{aligned} \tag{2.12}$$

$$\begin{aligned}\frac{dL}{dt} &= \beta_1 e^{-m_1 L} SL - d_2 L - \epsilon L - \delta L + \beta_1 e^{-m_2 L_1} SL_1 - \frac{L}{N} + SL \\ &+ d_2 L^2 + d_2 BL + RL + AL, \end{aligned} \tag{2.13}$$

$$\frac{dR}{dt} = \gamma B + \delta L - fR - \alpha R - R - \frac{R}{N} + RS + d_2 RB + d_2 RL + R^2 + RA, \tag{2.14}$$

$$\frac{dA}{dt} = fR - A - cA + kASN - \frac{A}{N} + AS + d_2AB + d_2AL + AR + A^2. \quad (2.15)$$

For attacker nodes:

$$\frac{dS_1}{dt} = \frac{(1-S_1)}{N_1} - \beta_4 S_1 B_1 N_1 - \beta_3 S_1 L_1 N_1 + c_1 A_1 - k_1 S_1 A_1 N_1 - S_1 + \alpha_1 R_1 + S_1^2 + d_3 S_1 B_1 + d_3 S_1 L_1 + S_1 R_1 + S_1 A_1, \quad (2.16)$$

$$\frac{dB_1}{dt} = \beta_4 S_1 B_1 N_1 - d_3 B_1 + \epsilon_1 L_1 - \gamma_1 B_1 - \frac{B_1}{N_1} + B_1 S_1 + d_3 {B_1}^2 + d_3 B_1 L_1 + B_1 R_1 + B_1 A_1, \quad (2.17)$$

$$\frac{dL_1}{dt} = \beta_3 S_1 L_1 N_1 - d_3 L_1 - \epsilon_1 L_1 - \delta_1 L_1 - \frac{L_1}{N_1} + S_1 L_1 + d_3 {L_1}^2 + d_3 B_1 L_1 + R_1 L_1 + A_1 L_1, \quad (2.18)$$

$$\frac{dR_1}{dt} = \gamma_1 B_1 + \delta_1 L_1 - f_1 R_1 - \alpha_1 R_1 - R_1 - \frac{R_1}{N_1} + R_1 S_1 + d_3 R_1 B_1 + d_3 R_1 L_1 + {R_1}^2 + R_1 A_1, \quad (2.19)$$

$$\frac{dA_1}{dt} = f_1 R_1 - A_1 - c_1 A_1 + k_1 A_1 S_1 N_1 - \frac{A_1}{N_1} + A_1 S_1 + d_3 A_1 B_1 + d_3 A_1 L_1 + A_1 R_1 + {A_1}^2. \quad (2.20)$$

Where targeted nodes and attacker nodes parameters are dimensionalised by $\tilde{d_1}$ and $\tilde{d_3}$ respectively.

2.3 Boundedness of the System

To verify our system is bounded, we classify the boundedness of the system into two parts , i.e., one for targeted and other for attacker nodes. For targeted population we define,

$$\tilde{N}(\tilde{t}) = \tilde{S}(\tilde{t}) + \tilde{L}(\tilde{t}) + \tilde{B}(\tilde{t}) + \tilde{R}(\tilde{t}) + \tilde{A}(\tilde{t}),$$

then,

$$\frac{d\tilde{N}}{d\tilde{t}} = \frac{d\tilde{S}}{d\tilde{t}} + \frac{d\tilde{L}}{d\tilde{t}} + \frac{d\tilde{B}}{d\tilde{t}} + \frac{d\tilde{R}}{d\tilde{t}} + \frac{d\tilde{A}}{d\tilde{t}},$$

$$\frac{d\tilde{N}}{d\tilde{t}} = b - \tilde{d}_1\tilde{S} - \tilde{d}_2\tilde{B} - \tilde{d}_2\tilde{L} - \tilde{d}_1\tilde{R} - \tilde{d}_1\tilde{A}.$$

Again, let

$$d = \min\left\{\tilde{d}_1,\ \tilde{d}_2\right\},$$

then,

$$\frac{d\tilde{N}}{d\tilde{t}} \leq b - d[\tilde{S} + \tilde{L} + \tilde{B} + \tilde{R} + \tilde{A}] = b - d\tilde{N}.$$

If $\tilde{N}(\tilde{t}) > (b/d)$, then $\frac{d\tilde{N}}{d\tilde{t}} < 0$, implying $limsup_{t\to\infty}\tilde{N}(\tilde{t}) \leq \frac{b}{d}$. After a moment of reflection, it can be seen that, for arbitrarily small $k > 0$, simply connected compact set

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

is positively invariant for this model. Hence, our proposed system is well posed.
Similarly we can define boundedness for the Attacker population.

$$\frac{d\tilde{N}_1}{d\tilde{t}} = b_1 - \tilde{d}_3\tilde{S}_1 - \tilde{d}_4\tilde{B}_1 - \tilde{d}_4\tilde{L}_1 - \tilde{d}_3\tilde{R}_1 - \tilde{d}_3\tilde{A}_1.$$

Again, let

$$d_1 = \min\left\{\tilde{d}_3,\ \tilde{d}_4\right\},$$

then,

$$\frac{d\tilde{N}_1}{d\tilde{t}} \leq b_1 - d_1[\tilde{S}_1 + \tilde{L}_1 + \tilde{B}_1 + \tilde{R}_1 + \tilde{A}_1] = b_1 - d_1\tilde{N}_1.$$

If $\tilde{N}_1(\tilde{t}) > \frac{b_1}{d_1}$, then $\frac{d\tilde{N}_1}{d\tilde{t}} < 0$, implying $limsup_{t\to\infty}\tilde{N}_1(\tilde{t}) \leq \frac{b_1}{d_1}$. After a moment of reflection, it can be seen that, for arbitrarily small $k_1 > 0$, simply connected compact set

$$\Omega_{k_1} = \{(\tilde{S}_1, \tilde{L}_1, \tilde{B}_1, \tilde{R}_1, \tilde{A}_1) \in {R_+}^5 : \tilde{S}_1 + \tilde{L}_1 + \tilde{B}_1 + \tilde{R}_1 + \tilde{A}_1 \leq \frac{b_1}{d_1} + k_1\}.$$

CHAPTER 3

Dynamic Behavior of the System

3.1 Steady States and their Stability

Equilibrium Points: The equilibrium points are generated using following set of equations and dynamics of the model is analysed using these set of points:

$$\frac{dS}{dt} = 0 = \frac{dL}{dt} = \frac{dB}{dt} = \frac{dR}{dt} = \frac{dA}{dt} = \frac{dS_1}{dt} = \frac{dL_1}{dt} = \frac{dB_1}{dt} = \frac{dR_1}{dt} = \frac{dA_1}{dt}$$

from the system of targeted and attacker class equations.

System has sixteen equilibrium states. It has following four malicious codes-free equilibrium states:

$E_1 = (1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$,

$E_2 = (1, 0, 0, 0, 0, \frac{1+c_1}{k_1}, 0, 0, 0, 1 - \frac{1+c_1}{k_1})$,

$E_3 = (\frac{1+c}{k}, 0, 0, 0, 1 - \frac{1+c}{k}, 1, 0, 0, 0, 0)$,

$E_4 = (\frac{1+c}{k}, 0, 0, 0, 1 - \frac{1+c}{k}, \frac{1+c_1}{k_1}, 0, 0, 0, 1 - \frac{1+c_1}{k_1})$,

and twelve endemic equilibrium states:

$E_5 = (1, 0, 0, 0, 0, \hat{S}_1, 0, \hat{B}_1, \hat{R}_1, \hat{A}_1)$,

$E_6 = (1, 0, 0, 0, 0, \hat{S}_1, \hat{L}_1, \hat{B}_1, \hat{R}_1, \hat{A}_1)$,

$$E_7 = (\tfrac{1+c}{k}, 0, 0, 0, 1 - \tfrac{1+c}{k}, \hat{S}_1, 0, \hat{B}_1, \hat{R}_1, \hat{A}_1),$$

$$E_8 = (\tfrac{1+c}{k}, 0, 0, 0, 1 - \tfrac{1+c}{k}, \hat{S}_1, \hat{L}_1, \hat{B}_1, \hat{R}_1, \hat{A}_1),$$

$$E_9 = (\hat{S}, 0, \hat{B}, \hat{R}, \hat{A}, 1, 0, 0, 0, 0),$$

$$E_{10} = (\hat{S}, 0, \hat{B}, \hat{R}, \hat{A}, \tfrac{1+c_1}{k_1}, 0, 0, 0, 1 - \tfrac{1+c_1}{k_1}),$$

$$E_{11} = (\hat{S}, 0, \hat{B}, \hat{R}, \hat{A}, \hat{S}_1, 0, \hat{B}_1, \hat{R}_1, \hat{A}_1),$$

$$E_{12} = (\hat{S}, 0, \hat{B}, \hat{R}, \hat{A}, \hat{S}_1, \hat{L}_1, \hat{B}_1, \hat{R}_1, \hat{A}_1),$$

$$E_{13} = (\hat{S}, \hat{L}, \hat{B}, \hat{R}, \hat{A}, 1, 0, 0, 0, 0),$$

$$E_{14} = (\hat{S}, \hat{L}, \hat{B}, \hat{R}, \hat{A}, \tfrac{1+c_1}{k_1}, 0, 0, 0, 1 - \tfrac{1+c_1}{k_1}),$$

$$E_{15} = (\hat{S}, \hat{L}, \hat{B}, \hat{R}, \hat{A}, \hat{S}_1, 0, \hat{B}_1, \hat{R}_1, \hat{A}_1),$$

$$E_{16} = (\hat{S}, \hat{L}, \hat{B}, \hat{R}, \hat{A}, \hat{S}_1, \hat{L}_1, \hat{B}_1, \hat{R}_1, \hat{A}_1).$$

Here we observed that the equilibrium point E_1 is on the $S - S_1$ plane and the equilibrium point E_2 is on the $S - S_1 - A_1$ plane. Also the equilibrium point E_3 is on the $S - A - S_1$ plane and the equilibrium point E_4 is on the $S - A - S_1 - A_1$ plane in the space and all other equilibrium states are interior points on the space. Steady state E_1 is always feasible since all the other parameters are positive. State E_2, E_3 and E_4 are feasible when $\frac{1+c}{k} \leq 1$ and $\frac{1+c_1}{k_1} \leq 1$. Numerical values of parameters are used to calculate the feasibility of other non-malicious code free steady states for different parameter sets.

The expressions for the equilibrium points are used to obtain the conditions for stability of malicious-code free solutions. To avoid infection propagation, it will be useful for obtaining the minimum recovery rate.

3.2 Basic Reproduction Number

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

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

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)=

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

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

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

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. This model has 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,

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

3.3 Local Asymptotical Stability

We define the local asymptotic stability of malicious codes-free and endemic equilibrium. Jacobian matrix which is applicable for all the equilibrium points is given below:

$$\begin{pmatrix}
a_1 & a_2 & a_3 & & a_5 & 0 & -S\beta_1 & -S\beta_2 & 0 & 0 \\
0 & & 0 & 0 & 0 & 0 & S\beta_1 & 0 & 0 & 0 \\
0 & \epsilon & a_7 & 0 & 0 & 0 & 0 & 0 & 0 & S\beta_2 \\
0 & \delta & \gamma & a_8 & 0 & 0 & 0 & 0 & 0 & 0 \\
2A + Ak(1+S) & a_9 & a_{10} & a_{11} & a_{12} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & a_{13} & a_{14} & a_{15} & a_{16} & a_{17} \\
0 & 0 & 0 & 0 & 0 & 0 & a_{18} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \epsilon_1 & a_{19} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \delta_1 & \gamma_1 & a_{20} & 0 \\
0 & 0 & 0 & 0 & 0 & a_{21} & a_{22} & a_{23} & a_{24} & a_{25}
\end{pmatrix}$$

where,

$a_1 = 3 + A + 3S - kA(1+S)$,

$a_2 = -1 + S + d_2S - kAS - \beta_1S$,

$a_3 = -1 + S + d_2S - kAS - \beta_2S$,

$a_4 = -1 + 2S - kAS + \alpha$,

$a_5 = -1 + c + 2S - k(1+A)S$,

$a_6 = -1 + A - d_2 + S + \beta_1S - \delta - \epsilon$,

$a_7 = -d_2 + \beta_2S - \gamma - 1 + A + S$,

$a_8 = -2 + A - f + S - \alpha$,

$a_9 = A + d_2A + kAS$; $a_{10} = A + d_2A + kAS$,

$a_{11} = 2A + f + kAS$; $a_{12} = -2 + 3A - c + S + k(1+A)S$,

$a_{13} = -3 + A_1 - k_1A_1 + 3S_1 - k_1A_1S_1$,

$a_{14} = -1 + S_1 + d_3S_1 - k_1A_1S_1 - \beta_3S_1$,

$a_{15} = -1 + S_1 + d_3S_1 - k_1A_1S_1 - \beta_4S_1$,

$a_{16} = -1 + 2S_1 - k_1A_1S_1 + \alpha_1$,

$a_{17} = -1 + c_1 + 2S_1 - k_1(1+A_1)S_1$,

$a_{18} = -1 + A_1 + S_1 + \beta_3S_1 - d_3 - \delta 1 - \epsilon_1$,

$a_{19} = -1 + A_1 - d_3 + S_1 + \beta_3S_1 - \delta_1 - \epsilon_1$,

$a_{20} = -2 + A_1 - f_1 + S_1 - \alpha_1$,

$a_{21} = 2A_1 + k_1A_1 + k_1A_1S_1,$

$a_{22} = A_1 + d_3A_1 + k_1A_1S_1,$

$a_{23} = A_1 + d_3A_1 + k_1A_1S_1,$

$a_{24} = 2A_1 + f_1 + k_1A_1S_1,$

$a_{25} = -2 + 3A_1 - c_1 + S_1 + k_1S_1 + k_1A_1S_1.$

At malicious codes - free equilibrium, the variational matrix E_1 is as follows:

$$\begin{pmatrix} 0 & a_1 & d_2-\beta_2 & 1+\alpha & a_3 & 0 & -\beta_1 & -\beta_2 & 0 & 0 \\ 0 & a_2 & 0 & 0 & 0 & 0 & \beta_1 & 0 & 0 & 0 \\ 0 & \epsilon & a_5 & 0 & 0 & 0 & 0 & \beta_2 & 0 & 0 \\ 0 & \delta & \gamma & -1-f-\alpha & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & f & a_4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & d_3-\beta_3 & d_3-\beta_4 & 1+\alpha_1 & a_6 \\ 0 & 0 & 0 & 0 & 0 & 0 & a_7 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \epsilon_1 & -d_3+\beta_4-\gamma_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \delta_1 & \gamma_1 & -1-f1-\alpha_1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & f1 & a_8 \end{pmatrix}.$$

Where,

$a_1 = d_2 - \beta_1$, $a_2 = -d_2 + \beta_1 - \delta - \epsilon$, $a_3 = 1 + c - k$,$a_4 = -1 - c - k_0$, $a_5 = -d_2 + \beta_2 - \gamma$, $a_6 = 1 + c_1 - k_1$, $a_7 = -d_3 + \beta_3 - \delta 1 - \epsilon_1$, $a_8 = -1 - c_1 - k_1S_1$.

The eigenvalues of this matrix are:

$$\{0, 0, 0, -1 - c + k, -1 - f - \alpha, -1 - f_1 - \alpha_1, -d_2 + \beta_2 - \gamma, -d_3 + \beta_4 - \gamma_1,$$

$$-d_2 + \beta_1 - \delta - \epsilon, -d_3 + \beta_3 - \delta_1 - \epsilon_1\}.$$

Equilibrium state E_1 is said to be locally asymptotically stable when all eigenvalues of J_{01} are having negative real parts or negative in nature. So, if $\mathcal{R}_{01} < 1$, then all the eigenvalues will have negative real parts. Hence, we can say the malicious code free equilibrium E_1 is locally asymptotically unstable, if $\mathcal{R}_{01} > 1$ and stable, if $\mathcal{R}_{01} < 1$.

Similarly, the eigenvalues of Jacobian matrix J_{02} for malicious codes free equilibrium state E_2, are given by:

$$\left\{0, -1 - c + k, 0, 0, -(1 - \frac{1 + c_1}{k_1}k_1), -1 - f - \alpha, -1 - f_1 - \alpha_1, -d_2 + \beta_2 - \gamma,\right.$$

$$-d_3+\frac{(1+c_1)(\beta_4)}{k_1}-\gamma_1,\ -d_2+\beta_1-\delta-\epsilon,-d_3+\frac{(\beta_3)(1+c_1)}{k_1}-\delta_1-\epsilon_1\Bigg\},$$

which shows that if $\mathcal{R}_{02}<1$, then J_{02} will have negative real parts for all the eigenvalues. Hence, E_2 is locally asymptotically stable.

Similarly, the eigenvalues of Jacobian matrix J_{03} for malicious codes free equilibrium state E_3, are given by,

$$\Bigg\{0,-1-\frac{1+c}{k}k,0,-(1-\frac{1+c_1}{k_1})k_1,-1-f-\alpha,-1-f_1-\alpha_1,-d_2+\frac{(\beta_2)(1+c)}{k}-\gamma,$$

$$-d_3+\frac{(1+c_1)(\beta_4)}{k_1}-\gamma_1,\ -d_2+\frac{\beta_1(1+c)}{k}-\delta-\epsilon,-d_3+\frac{\beta_3(1+c_1)}{k_1}-\delta_1-\epsilon_1\Bigg\},$$

which shows that if $\mathcal{R}_{03}<1$, then J_{03} will have negative real parts for all the eigenvalues. Hence, E_3 is locally asymptotically stable.

Similarly, the eigenvalues of Jacobian matrix J_{04} for malicious codes free equilibrium state E_4, are given by,

$$\Bigg\{0,-1-\frac{1+c}{k}k,0,-1-c_1+k_1,-1-f-\alpha,-1-f_1-\alpha_1,-d_2+\frac{\beta_2(1+c)}{k}-\gamma,$$

$$-d_3+\beta_4-\gamma_1,-d_2+\frac{\beta_1(1+c)}{k}-\delta-\epsilon,-d_3+\beta_3-\delta_1-\epsilon_1\Bigg\},$$

which shows that if $\mathcal{R}_{04}<1$, then J_{04} will have negative real parts for all the eigenvalues. Hence, E_4 is locally asymptotically stable.

3.4 Numerical Simulation

Numerical methods are used to solve the system of equations for the targeted and attacker system. For the different classes the behavior of the nodes is observed with respect to the time. The targeted and attacker system has been solved and simulated and the behavior of the nodes in different classes are observed with respect to the time.

3.4.1 Feasible Steady States

For the model, for different parameter sets feasible steady states are simulated and analysed. At any point if all the classes have non-negative values, then a steady state is said to be feasible at this point. Following table 3.1 shows the feasibility of steady states with basic reproduction number and for different parameter set.

We plot a curve to understand the behavior of the classes with time. Figures show the node density of S, L, B, R and A nodes of attacker and targeted class. Since E_1, E_2, E_3 and E_4 are the malicious code 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 states if their $R_0 > 1$. All observations are done with respect to the time and by using different parameter sets.

Figure 3.1 is plotted with parameter set 1 and initial point (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 , S_1 and A_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 that E_{10} is the stable steady state.

Figure 3.2 is plotted with parameter set 1 and initial point (0.52, 0.02, 0.025, 0.05, 0.43, 1, 0, 0, 0, and 0). Similarly, we can conclude that E_1, E_2, E_3, E_4, E_9 and E_{10} are the feasible steady states and E_9 is the stable steady state.

Figure 3.3 is plotted with parameter set 2 and initial point (0.5, 0.2, 0.25, 0, 0.05, 0.1, 0.35, 0.4, 0.1, and 0.05). Similarly, we can conclude that E_1, E_2, E_3 and E_4 are the feasible steady states and E_4 is the stable steady state.

Figure 3.4 is plotted with parameter set 3 and initial point (0.5, 0.2, 0.25, 0, 0.05, 0.1, 0.35, 0.4, 0.1 and 0.05). In this possible feasible states are E_3 and E_4. Since one of the reproduction number is greater than 1, hence we can conclude that E_4 is the stable steady state.

Parameters	**Set 1**	**Set 2**	**Set 3**	**Set 4**	**Set 5**	**Set 6**
$\boldsymbol{\beta_1}$	0.6	0.6	0.7	1	0.87	0.73
$\boldsymbol{\beta_2}$	0.5	0.5	0.4	0.8	0.43	0.50
$\mathbf{k}$	0.06	0.06	0.06	0.16	0.036	0.06
$\mathbf{c}$	0.03	0.03	0.03	0.08	0.06	0.03
$\boldsymbol{\alpha}$	0.05	0.05	0.05	0.15	0.10	0.058
$\mathbf{d_2}$	0.04	0.08	0.1	0.1	0.121	0.25
$\boldsymbol{\epsilon}$	0.3	0.3	0.4	0.4	0.46	0.4
$\boldsymbol{\gamma}$	0.045	0.45	0.1	0.1	0.15	0.1
$\boldsymbol{\delta}$	0.025	0.25	0.03	0.03	0.15	0.03
$\mathbf{f}$	0.02	0.02	0.08	0.1	0.208	0.08
$\boldsymbol{\beta_3}$	0.4	0.4	0.7	0.8	0.87	0.47
$\boldsymbol{\beta_4}$	0.3	0.3	0.6	0.8	0.6	0.46
$\mathbf{f_1}$	0.15	0.15	0.05	0.1	0.605	0.05
$\mathbf{k_1}$	0.05	0.05	0.08	0.1	0.040	0.08
$\mathbf{c_1}$	0.01	0.01	0.03	0.06	0.03	0.03
$\boldsymbol{\alpha_1}$	0.04	0.04	0.07	0.27	0.07	0.07
$\mathbf{d_3}$	0.05	0.05	0.15	0.15	0.15	0.35
$\boldsymbol{\gamma_1}$	0.035	0.35	0.15	0.15	0.51	0.15
$\boldsymbol{\delta_1}$	0.02	0.2	0.03	0.03	0.30	0.03
$\boldsymbol{\epsilon_1}$	0.25	0.25	0.35	0.35	0.35	0.35
feasible SS	$E_1, E_2, E_3,$ $E_4, E_9, E_{10}.$	E_1, E_2, E_3, E_4	E_3, E_4	E_3, E_4, E_9, E_{10}	E_9, E_{10}	E_3, E_4
$\mathcal{R}_{01}$	0.58803	0.9523	1.99987	3.99948	1.58644	1.42853
$\mathcal{R}_{02}$	5.88034	0.9523	1.99983	3.99948	1.58664	1.42853
$\mathcal{R}_{03}$	3.52822	0.8000	1.99987	2.66644	2.64571	0.92006
$\mathcal{R}_{04}$	2.94421	0.4767	1.00117	2.00079	2.64571	0.71513

Table 3.1: Feasible steady states and basic reproduction number for different parameter set in the model

Figure 3.5 is plotted with set 4 and initial point (0.2, 0, 0.25, 0.09, 0.46, 0.6, 0, 0, 0, and 0.4). Similarly, we can conclude that E_3, E_4, E_9 and E_{10} are the feasible steady states and E_{10} is the stable steady state.

Figure 3.6 is plotted with parameter set 5 and initial point (0.5, 0.2, 0.25, 0, 0.05, 0.1, 0.35, 0.4, 0.1 and 0.05). In this observed feasible states are E_9 and E_{10}. From the figure it is clear that E_{10} is the stable steady state.

Figures 3.7 and 3.8 are plotted with different initial points for parameter set 6 and the observed feasible states are E_3 and E_4. For the initial point (0.5 0.02 0.03 0 0.45 1 0 0 0 0), E_3 is the observed stable steady state and E_4 is the observed stable steady state for the initial point (0.5 0.2 0.25 0 0.05 0.1 0.35 0.4 0.1 0.05).

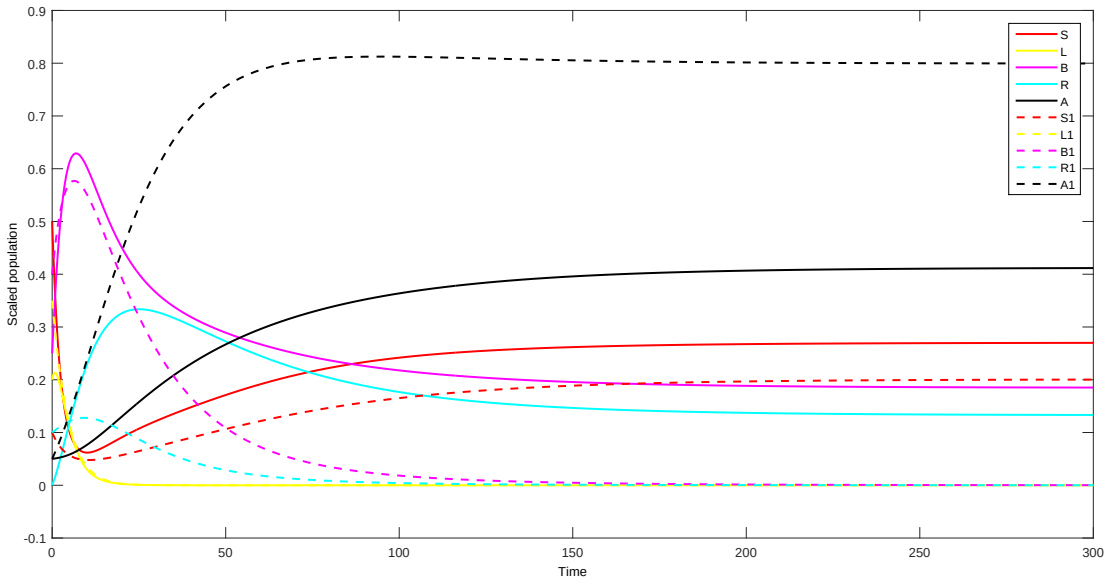


Figure 3.1: Node Density vs. Time for set 1 initial point(0.5 0.2 0.25 0 0.05 0.1 0.35 0.4 0.1 0.05)

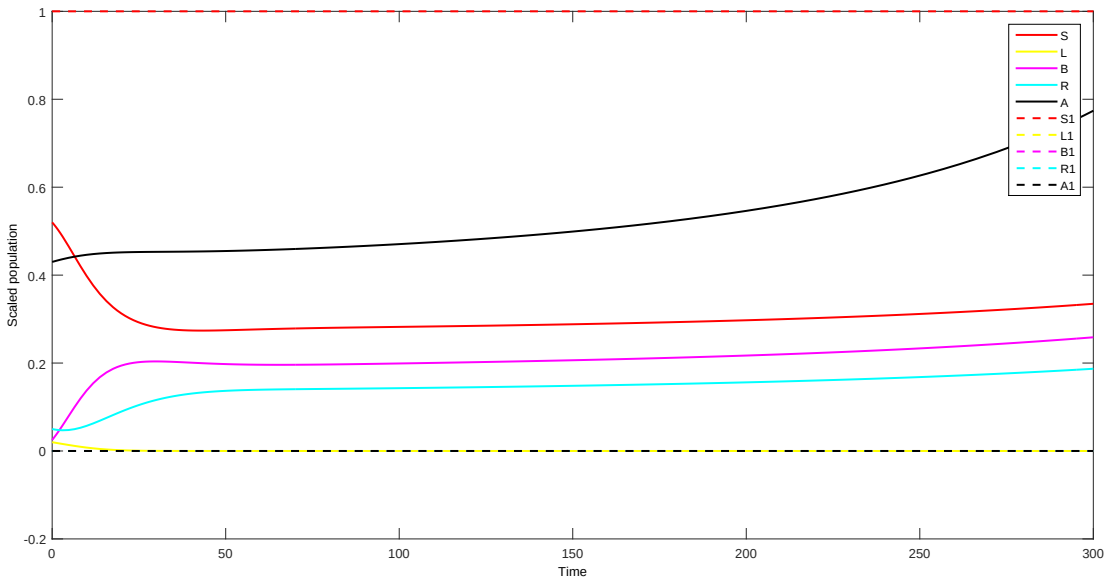


Figure 3.2: Node Density vs. Time for set 1 initial point(0.52 0.02 0.025 0.05 0.43 1 0 0 0 0)

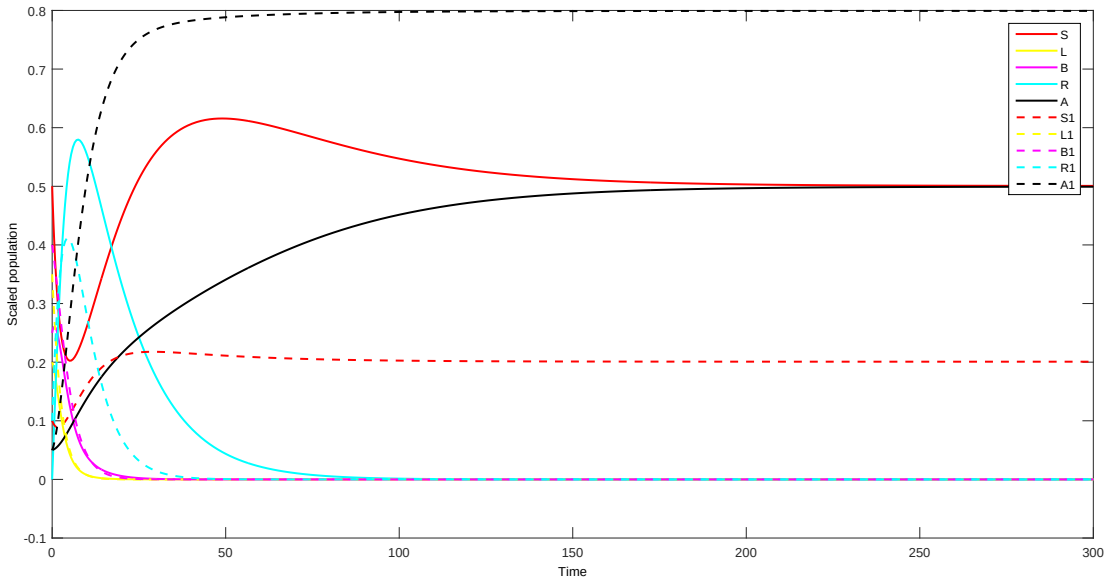


Figure 3.3: Node Density vs. Time for set 2 initial point(0.5 0.2 0.25 0 0.05 0.1 0.35 0.4 0.1 0.05)

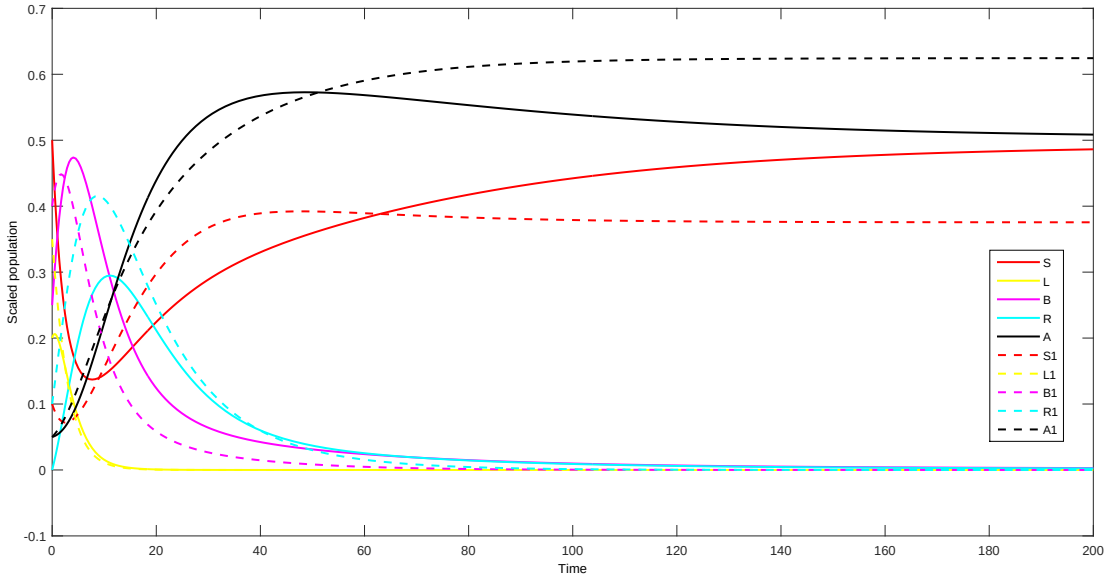


Figure 3.4: Node Density vs. Time for set 3 initial point(0.5 0.2 0.25 0 0.05 0.1 0.35 0.4 0.1 0.05)

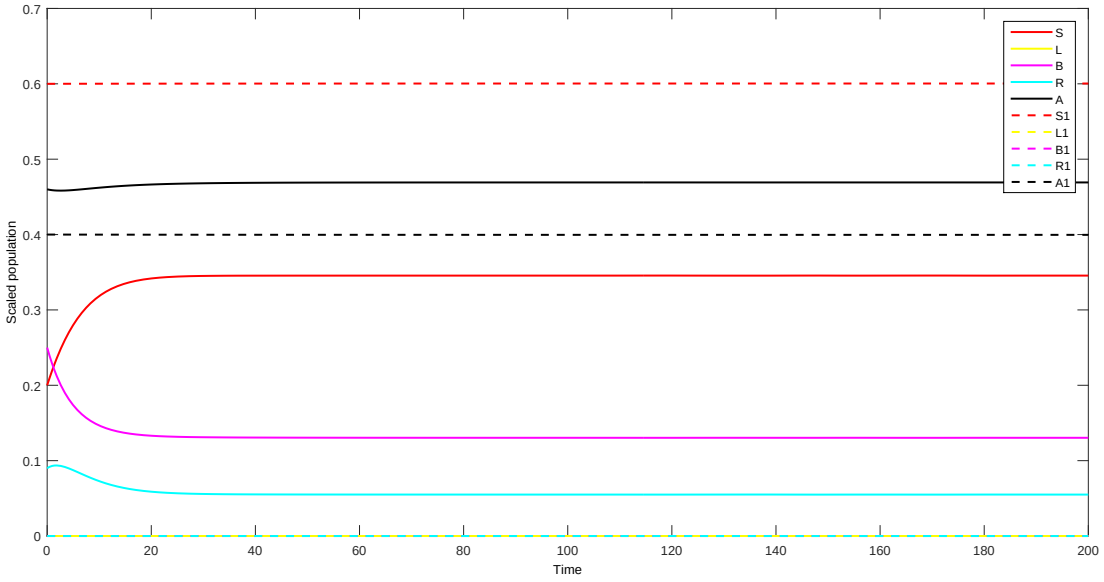


Figure 3.5: Node Density vs. Time for set 4 initial point(0.2 0 0.25 0.09 0.46 0.6 0 0 0 0.4)

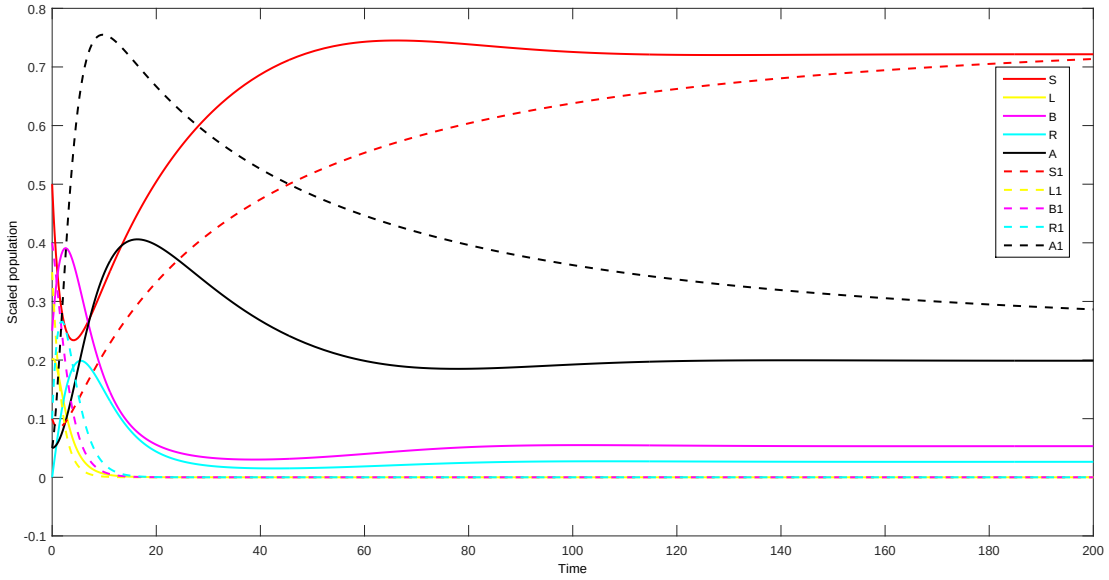


Figure 3.6: Node Density vs. Time for set 5 initial point(0.5 0.2 0.25 0 0.05 0.1 0.35 0.4 0.1 0.05)

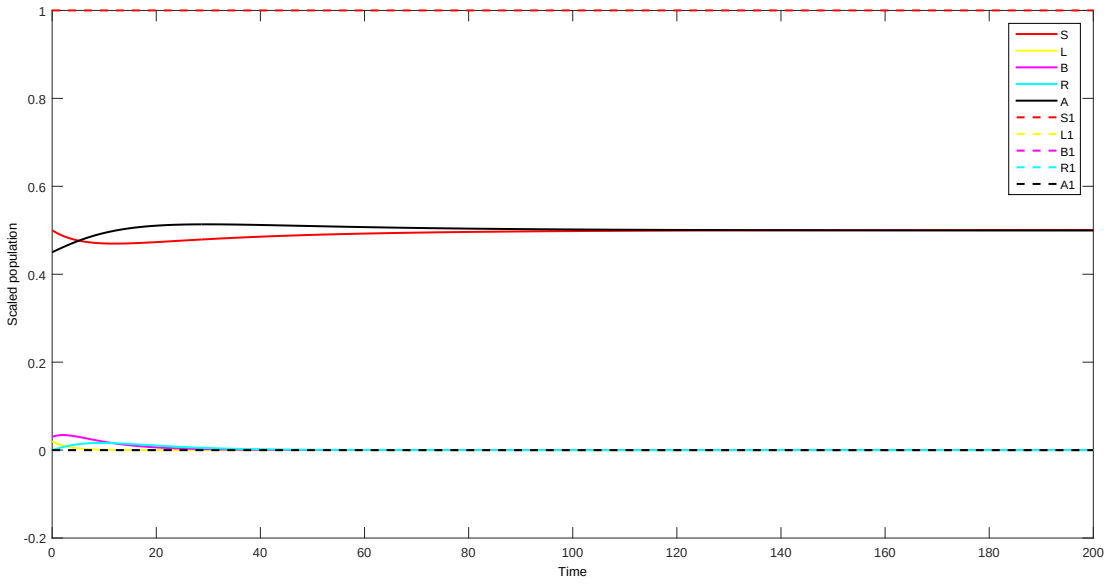


Figure 3.7: Node Density vs. Time for set 6 initial point(0.5 0.02 0.03 0 0.45 1 0 0 0 0)

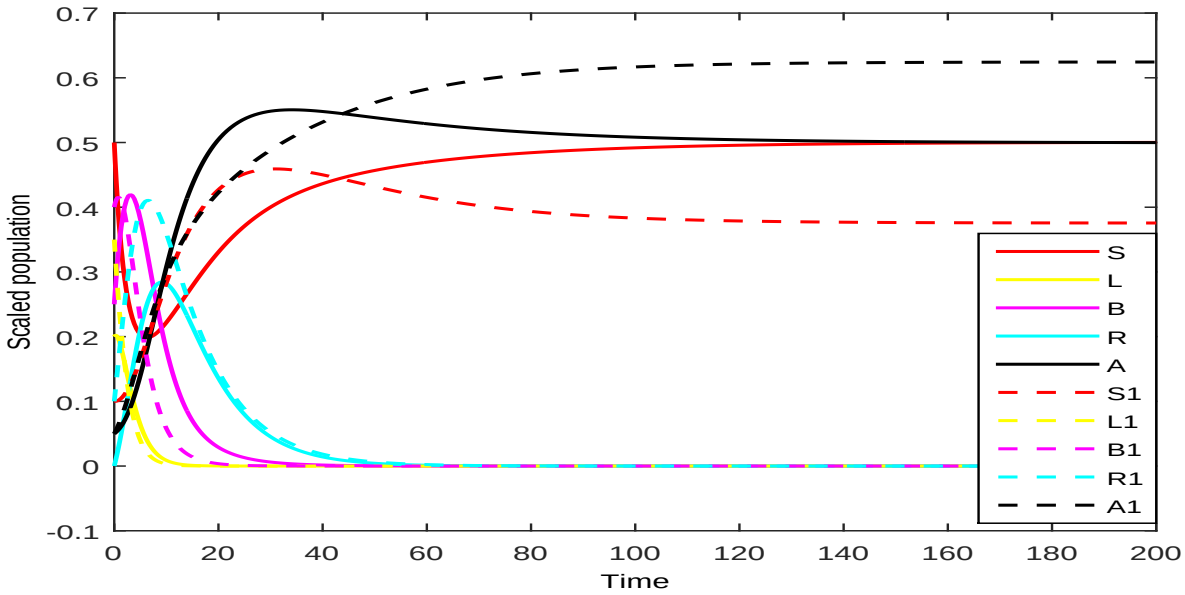


Figure 3.8: Node Density vs. Time for set 6 initial point(0.5 0.2 0.25 0 0.05 0.1 0.35 0.4 0.1 0.05)

3.5 Estimation of Firewall Security Coefficient

The firewall is the central security of a network. The objective of the firewall is to create rules and policies which allows only particular connections.

3.5.1 Order of rule enforcement

The firewall keeps track of every connection and enforces the rule base sequentially. The firewall monitors every connection and compares that connection for the consistency with service, data and destination. If the connection is valid then firewall applies that rule otherwise, it checks for the next matching rule in the Rule base.

3.5.2 Firewall rule priority

Since we can define firewall rules that have apparent conflicts, it is important to understand the sequence in which the rules are executed.

3.5.3 Authenticated bypass

These rules allow matched network traffic otherwise it would be blocked. A separate connection security rule would be used to authenticate the network traffic. These rules are used to allow access to any computer to an authorized troubleshooting device and network administrator.

3.5.4 Block connection

These rules restrict all matched incoming network traffic.

3.5.5 Allow connection

These defined rules allow matched incoming network traffic. Because the general criteria is to restrict distrustful incoming network traffic, we must define an allow rule to help any network program or service that must be able to accept incoming 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 define a way for measuring the value m of firewall security as:

$$m = -\log_e(a + b - ab),$$

where, 'b' measures 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 'b'=0 and if they don't match any of the rules then 'b'=1 and it is supposed that the malware propagation rate can be reduced by proportion 'a', when each received files abide the defined security rules.

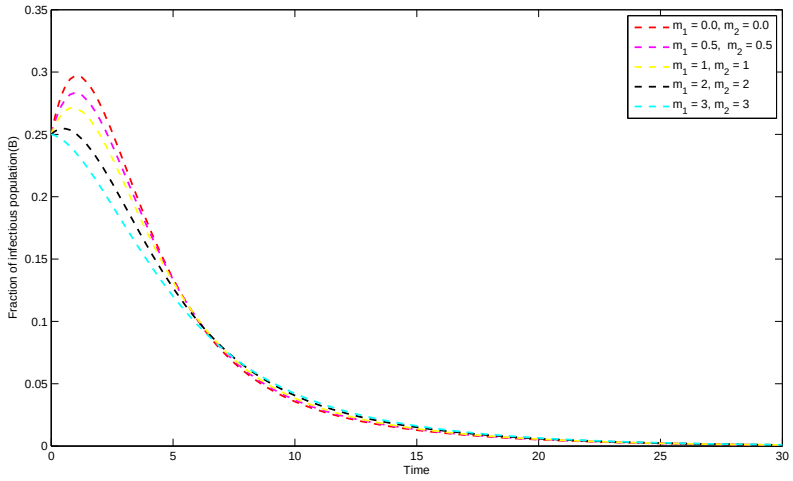


Figure 3.9: Effect of m on B when $R_0 < 1$

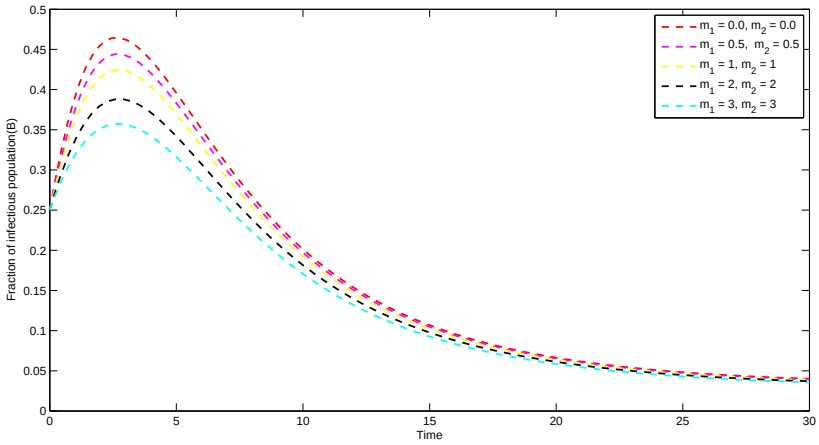


Figure 3.10: Effect of m on B when $R_0 > 1$

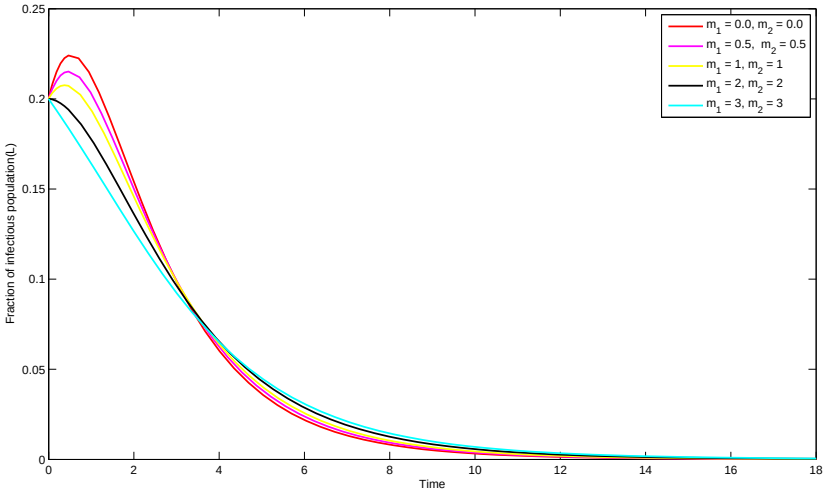


Figure 3.11: Effect of m on L when $R_0 < 1$

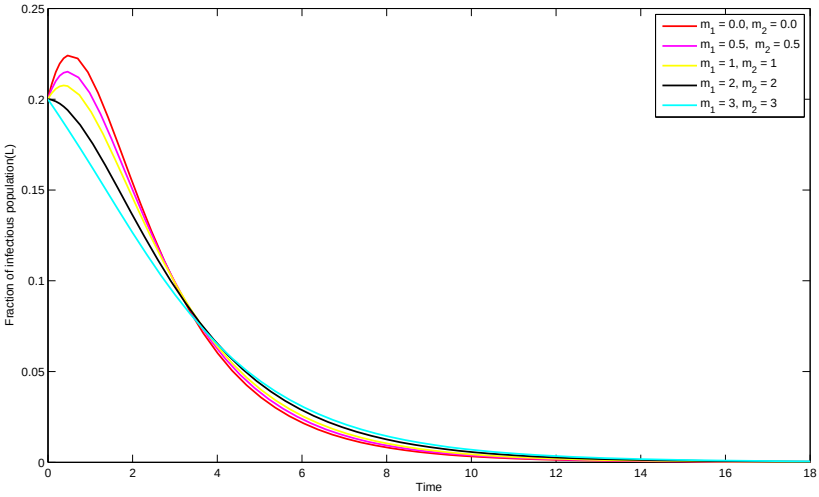


Figure 3.12: Effect of m on L when $R_0 > 1$

3.6 Sensitivity Analysis:

Normalized forward sensitivity index is used for the sensitivity analysis of basic reproduction number. Sensitivity indices enable us to quantify the relative change in a state variable with respect to a slight change in the system parameter. The ratio of the relative change in the variable to the relative change in the particular system parameter is known as the normalized forward sensitivity index of the variable to that parameter. The sensitivity index may also be expressed using partial derivatives [22]. Let p is a parameter and u is the function of p, a small perturbation δ_p to the parameter p and the corresponding change in u as δ_u:

$$\delta_u = u(p+\delta_p) - u(p) = \frac{u(p+\delta_p) - u(p)}{\delta_p}.\delta_p \approx \delta_p \frac{\partial u}{\partial p}.$$

The normalized forward sensitivity index of a variable, u, that depends on a parameter, p, is defined as:

$$\Upsilon_p^u = \frac{\partial u}{\partial p} \times \frac{p}{u}.$$

Estimation and measurement of most sensitive parameter has to be done carefully, because a small change in the parameter will tend to relatively huge quantitative change. However, estimation of less sensitive parameter does not require as much effort, since a small change in the parameter will not lead to huge change in the quantity. With respect to each parameter, we derived analytical expressions for sensitivity index of R_0. The normalized sensitivity indices for parameters are obtained as given in the following table. The sensitivity indices of the basic reproduction numbers R_{01}, R_{02}, R_{03} and R_{04} for all the parameter sets are listed below:

Parameters	$\Upsilon_{y_j}^{\mathcal{R}_{01}}$ **Set 1**	$\Upsilon_{y_j}^{\mathcal{R}_{01}}$ **Set 2**	$\Upsilon_{y_j}^{\mathcal{R}_{01}}$ **Set 3**	$\Upsilon_{y_j}^{\mathcal{R}_{01}}$ **Set 4**	$\Upsilon_{y_j}^{\mathcal{R}_{01}}$ **Set 5**	$\Upsilon_{y_j}^{\mathcal{R}_{01}}$ **Set 6**
$\boldsymbol{\beta_1}$	0	0.999	0	0	0	0
$\boldsymbol{\beta_2}$	0.999	0	0	0.999	0.999	0.9999
$\mathbf{k}$	0	0	0	0	0	0
$\mathbf{c}$	0	0	0	0	0	0
$\boldsymbol{\alpha}$	0	0	0	0	0	0
$\mathbf{d_2}$	-0.47	-0126	0	-0.499	-0.446	-0.72
$\boldsymbol{\epsilon}$	0	-0.476	0	0	0	0
$\boldsymbol{\gamma}$	-0.529	0	0	-0.499	-0.553	-0.285
$\boldsymbol{\delta}$	0	-0.396	0	0	0	0
$\mathbf{f}$	0	0	0	0	0	0
$\boldsymbol{\beta_3}$	0	0	0	0	0	0
$\boldsymbol{\beta_4}$	0	0	0.99	0	0	0
$\mathbf{f_1}$	0	0	0	0	0	0
$\mathbf{k_1}$	0	0	0	0	0	0
$\mathbf{c_1}$	0	0	0	0	0	0
$\boldsymbol{\alpha_1}$	0	0	0	0	0	0
$\mathbf{d_3}$	0	0	-0.499	0	0	0
$\boldsymbol{\gamma_1}$	0	0	-0.499	0	0	0
$\boldsymbol{\delta_1}$	0	0	0	0	0	0
$\boldsymbol{\epsilon_1}$	0	0	0	0	0	0

Table 3.2: Normalized sensitivity indices for different parameter sets with respect to R_{01}

1. Normalized sensitivity indices for different parameter sets with respect to R_{01} are shown in the table: 3.2.

We observed that β_1, β_2 and β_4 are highly sensitive. $d_2, \epsilon, \delta, \gamma, d_3$, and γ_1 are moderately sensitive and $k, c, \alpha, f, \beta_3, f_1, k_1, c_1, \alpha_1, \delta_1$ and ϵ_1 are independent of R_{01}. For example $\Upsilon_{d_2}^{\mathcal{R}_{01}}$ for set 1 = -0.47, hence, increasing (decreasing) d_2 by 1% will decrease (increase) R_{01} by 0.47%.

Parameters	$\Upsilon_{y_j}^{\mathcal{R}_{02}}$ **Set 1**	$\Upsilon_{y_j}^{\mathcal{R}_{02}}$ **Set 2**	$\Upsilon_{y_j}^{\mathcal{R}_{02}}$ **Set 3**	$\Upsilon_{y_j}^{\mathcal{R}_{02}}$ **Set 4**	$\Upsilon_{y_j}^{\mathcal{R}_{02}}$ **Set 5**	$\Upsilon_{y_j}^{\mathcal{R}_{02}}$ **Set 6**
$\boldsymbol{\beta_1}$	0	0.999	0	0	0	0
$\boldsymbol{\beta_2}$	0.999	0	0	0.999	0.999	0.9999
$\boldsymbol{\alpha}$	0	0	0	0	0	0
$\mathbf{d_2}$	-0.47	-0.126	-0.49	-0.49	-0.44	-0.71
$\boldsymbol{\epsilon}$	0	-0.476	0	0	0	0
$\boldsymbol{\gamma}$	-0.529	0	-0.499	-0.499	-0.533	-0.285
$\boldsymbol{\delta}$	0	-0.396	0	0	0	0
$\mathbf{f}$	0	0	0	0	0	0
$\boldsymbol{\beta_3}$	0	0	0	0	0	0
$\boldsymbol{\beta_4}$	0	0	0	0	0	0
$\mathbf{f_1}$	0	0	0	0	0	0
$\mathbf{k_1}$	0	0	0	0	0	0
$\mathbf{c_1}$	0	0	0	0	0	0
$\boldsymbol{\alpha_1}$	0	0	0	0	0	0
$\mathbf{d_3}$	0	0	0	0	0	0
$\boldsymbol{\gamma_1}$	0	0	0	0	0	0
$\boldsymbol{\delta_1}$	0	0	0	0	0	0
$\boldsymbol{\epsilon_1}$	0	0	0	0	0	0

Table 3.3: Normalized sensitivity indices for different parameter sets with respect to R_{02}

2. Normalized sensitivity indices for different parameter sets with respect to R_{02} are shown in the table: 3.3.

We observed that β_1 and β_2 are highly sensitive. d_2, ϵ, δ, and γ, are moderately sensitive and $k, c, \alpha, f, \beta_3, f_1, k_1, c_1, \alpha_1, \delta_1, \beta_4$ and ϵ_1 are independent of R_{02} . For example $\Upsilon_{\beta_2}^{\mathcal{R}_{02}}$ for set $1 = 0.99$, hence, increasing (decreasing) d_2 by 1% will increase (decrease) R_{02} by 0.99% .

Parameters	$\Upsilon_{y_j}^{\mathcal{R}_{03}}$ **Set 1**	$\Upsilon_{y_j}^{\mathcal{R}_{03}}$ **Set 2**	$\Upsilon_{y_j}^{\mathcal{R}_{03}}$ **Set 3**	$\Upsilon_{y_j}^{\mathcal{R}_{03}}$ **Set 4**	$\Upsilon_{y_j}^{\mathcal{R}_{03}}$ **Set 5**	$\Upsilon_{y_j}^{\mathcal{R}_{03}}$ **Set 6**
$\boldsymbol{\beta_1}$	0	0	0	0	0	0
$\boldsymbol{\beta_2}$	0	0	0	0	0.99	0.99
$\mathbf{k}$	0	0	0	0	-0.99	-0.99
$\mathbf{c}$	0	0	0	0	0.99	0.99
$\boldsymbol{\alpha}$	0	0	0	0	0	0
$\mathbf{d_2}$	0	0	0	0	-0.44	-0.71
$\boldsymbol{\epsilon}$	0	0	0	0	0	0
$\boldsymbol{\gamma}$	0	0	0	0	-0.55	-0.28
$\boldsymbol{\delta}$	0	0	0	0	0	0
$\mathbf{f}$	0	0	0	0	0	0
$\boldsymbol{\beta_3}$	0	0.99	0	0	0	0
$\boldsymbol{\beta_4}$	0.99	0	0.99	0.99	0	0
$\mathbf{f_1}$	0	0	0	0	0	0
$\mathbf{k_1}$	0	0	0	0	0	0
$\mathbf{c_1}$	0	0	0	0	0	0
$\boldsymbol{\alpha_1}$	0	0	0	0	0	0
$\mathbf{d_3}$	-0.58	-0.09	-0.499	-0.499	0	0
$\boldsymbol{\gamma_1}$	-0.411	0	-0.499	-0.499	0	0
$\boldsymbol{\delta_1}$	0	-0.399	0	0	0	0
$\boldsymbol{\epsilon_1}$	0	-0.499	0	0	0	0

Table 3.4: Normalized sensitivity indices for different parameter sets with respect to R_{03}

3. Normalized sensitivity indices for different parameter sets with respect to R_{03} are shown in the table: 3.4.

We observed that β_2, β_3, β_4, k and c are highly sensitive, $d_2, \epsilon_1, \gamma, \gamma_1$ and δ_1, and , are moderately sensitive and $\alpha, f, \delta, \beta_1, f_1, k_1, c_1$ and α_1 are independent of R_{03} . For example $\Upsilon_{\gamma}^{\mathcal{R}_{03}}$ for set 5 = -0.55, hence, increasing (decreasing) d_2 by 1% will decrease(increase) R_{03} by 0.55% .

Parameters	$\Upsilon_{y_j}^{\mathcal{R}_{04}}$ **Set 1**	$\Upsilon_{y_j}^{\mathcal{R}_{04}}$ **Set 2**	$\Upsilon_{y_j}^{\mathcal{R}_{04}}$ **Set 3**	$\Upsilon_{y_j}^{\mathcal{R}_{04}}$ **Set 4**	$\Upsilon_{y_j}^{\mathcal{R}_{04}}$ **Set 5**	$\Upsilon_{y_j}^{\mathcal{R}_{04}}$ **Set 6**
$\boldsymbol{\beta_1}$	0	0.99	0	0	0	0
$\boldsymbol{\beta_2}$	0.99	0	0.99	0.99	0.99	0.99
$\mathbf{k}$	-0.99	-0.99	-0.99	-0.99	-0.99	-0.99
$\mathbf{c}$	-0.99	-0.99	-0.99	-0.99	-0.99	-0.99
$\boldsymbol{\alpha}$	0	0	0	0	0	0
$\mathbf{d_2}$	-0.47	-0.12	-0.49	-0.49	-0.44	-0.71
$\boldsymbol{\epsilon}$	0	-0.47	0	0	0	0
$\boldsymbol{\gamma}$	-0.52	0	-0.49	-0.49	-0.55	-0.28
$\boldsymbol{\delta}$	0	-0.39	0	0	0	0
$\mathbf{f}$	0	0	0	0	0	0
$\boldsymbol{\beta_3}$	0	0	0	0	0	0
$\boldsymbol{\beta_4}$	0	0	0	0	0	0
$\mathbf{f_1}$	0	0	0	0	0	0
$\mathbf{k_1}$	0	0	0	0	0	0
$\mathbf{c_1}$	0	0	0	0	0	0
$\boldsymbol{\alpha_1}$	0	0	0	0	0	0
$\mathbf{d_3}$	0	0	0	0	0	0
$\boldsymbol{\gamma_1}$	0	0	0	0	0	0
$\boldsymbol{\delta_1}$	0	0	0	0	0	0
$\boldsymbol{\epsilon_1}$	0	0	0	0	0	0

Table 3.5: Normalized sensitivity indices for parameters set with respect to R_{04}

4. Normalized sensitivity indices for different parameter sets with respect to R_{04} are shown in the table: 3.5.

We observed that β_1, β_2, k and c are highly sensitive. d_2, ϵ, γ and δ are moderately sensitive and $\alpha, \alpha_1, f, \beta_3, \beta_4, \delta_1, \gamma_1, \beta_1, d_3, f_1, k_1, c_1$ and ϵ_1 are independent of R_{04}. For example $\Upsilon_k^{\mathcal{R}_{04}}$ for set 1 = -0.99, therefore, increasing (decreasing) d_2 by 1% will decrease(increase) R_{04} by 0.99%.

CHAPTER 4

Conclusion and Future Scope

4.1 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:

- The proposed model has sixteen equilibrium states out of which four are malicious codes free equilibrium and rest are endemic in nature. Basic reproduction number for the malicious codes free equilibrium states has been observed and it has been found that the malicious code free equilibrium is stable, if $R_0 < 1$ and, the endemic equilibrium is stable, if $R_0 > 1$. Local asymptotic stability is used as a mathematical tool to verify the system.

- The coefficient of firewall security m is defined as

  $$m = -\log_e(a + b - ab),$$

  where, 'b' measures the response of the files to the defined security rules. It is considered that the malware propagation rate can be reduced by a proportion 'a', when all received files abide the defined security rules.

- We have observed that the basic reproduction number R_0 is not affected by the

coefficient of firewall security and hence the qualitative features of the model don't change.

- We conclude that the use of firewall security rule base helps to mitigate the problem of malicious code propagation in the network by minimizing the level of infected nodes at steady state.

- The stability of the system is observed using local asymptotic stability method and numerical simulation has been carried out to verify analytical findings. Finally, the most sensitive system parameters for basic reproduction number are observed using normalized forward sensitivity index. We observed the most sensitive parameters for Basic Reproduction Number which are shown in the table below, estimation of these parameters should be done very carefully.

Basic Reproduction Number	Most Sensitive Parameters
R_{01}	$\beta_1, \beta_2, \beta_4$
R_{02}	β_1, β_2
R_{03}	$\beta_2, \beta_3, \beta_4, k, c$
R_{04}	β_1, β_2, k, c

4.2 Future Scope

This work can be extended by considering a time delay for outbreak and time variant birth rate. In addition, classification of susceptible nodes could be done for a more generalized model. In all known epidemiological models, an individual's treatment is done autonomously. In any case, consider the following situation, one day Ram finds that one of the program he utilizes on his computer is contaminated with an virus, he removes it. In many models, this would be the story's end. Notwithstanding, for this situation Ram takes it upon himself to give this information to his companions Shyam, Mahesh and Suresh with whom he had shared this program at some point in the most recent couple of weeks. All the while Shyam, Mahesh and Suresh removes infection if discovered and propagate information to their companions. This may be observed by a model in which, once a machine is contaminated, the majority of its neighboring machines are checked for

infections. So, we can extend our model to further minimize malicious code propagation by implementing this 'kill signal' idea.

REFERENCES

[1] J. Cui, Y. Sun, H. Zhu, The impact of media on the control of infectious diseases, Journal of Dynamics and Differential Equations 20 (1) (2008) 31–53.

[2] Y. Liu, J.-a. Cui, The impact of media coverage on the dynamics of infectious disease, International Journal of Biomathematics 1 (01) (2008) 65–74.

[3] G. P. Sahu, J. Dhar, Analysis of an sveis epidemic model with partial temporary immunity and saturation incidence rate, Applied Mathematical Modelling 36 (3) (2012) 908–923.

[4] G. P. Sahu, J. Dhar, 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 421 (2) (2015) 1651–1672.

[5] R. T. Goswami, 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 4 (10) (2012) 4275–4282.

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

[7] J. O. Kephart, S. R. White, D. M. Chess, Computers and epidemiology, Spectrum, IEEE 30 (5) (1993) 20–26.

[8] H. Molen, Math on malware, Inform Syst Audit Control Assoc J 3 (2011) 41–46.

[9] W. O. Kermack, A. G. McKendrick, A contribution to the mathematical theory of epidemics, in: Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, Vol. 115, The Royal Society, 1927, pp. 700–721.

[10] W. O. Kermack, A. G. McKendrick, Contributions to the mathematical theory of epidemics. ii. the problem of endemicity, in: Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, Vol. 138, The Royal Society, 1932, pp. 55–83.

[11] W. O. Kermack, A. G. McKendrick, Contributions to the mathematical theory of epidemics. iii. further studies of the problem of endemicity, Proceedings of the Royal Society of London. Series A 141 (843) (1933) 94–122.

[12] A. Misra, M. Verma, A. Sharma, Capturing the interplay between malware and anti-malware in a computer network, Applied Mathematics and Computation 229 (2014) 340–349.

[13] F. Wang, Y. Yang, D. Zhao, Y. Zhang, A worm defending model with partial immunization and its stability analysis, Journal of Communications 10 (4).

[14] 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 7 (2) (2015) 121.

[15] M. Sun, D. Li, D. Han, C. Jia, Impact of anti-virus software on computer virus dynamical behavior, International Journal of Modern Physics C 25 (05) (2014) 1440010.

[16] B. K. Mishra, A. Prajapati, Mathematical model on attack by malicious objects leading to cyber war, International Journal of Nonlinear Science 17 (2) (2014) 145–153.

[17] B. K. Mishra, S. K. Pandey, Dynamic model of worms with vertical transmission in computer network, Applied Mathematics and Computation 217 (21) (2011) 8438–8446.

[18] A. K. Misra, M. Verma, A. Sharma, Capturing the interplay between malware and anti-malware in a computer network, Applied Mathematics and Computation 229 (2014) 340–349.

[19] B. K. Mishra, G. M. Ansari, Mathematical models on interaction between computer virus and antivirus software inside a computer system, International Journal of Computer and Network Security 2 (8) (2010) 84–89.

[20] B. K. Mishra, D. Saini, Mathematical models on computer viruses, Applied Mathematics and Computation 187 (2) (2007) 929–936.

[21] J. Ren, Y. Xu, C. Zhang, Optimal control of a delay-varying computer virus propagation model, Discrete Dynamics in Nature and Society 2013 (2013) 1–7.

[22] N. Chitnis, J. M. Hyman, J. M. Cushing, Determining important parameters in the spread of malaria through the sensitivity analysis of a mathematical model, Bulletin of mathematical biology 70 (5) (2008) 1272–1296.