ANALYSIS OF MALICIOUS CODE DYNAMICS WITH TARGET AND ATTACKER NODES USING MATHEMATICAL MODEL

A project report submitted in partial fulfillment of the requirements for B.Tech. Project

B.Tech.

by

Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

विश्वजीवनामृतं ज्ञानम्

ABV INDIAN INSTITUTE OF INFORMATION TECHNOLOGY AND MANAGEMENT
GWALIOR-474 010

2017

CANDIDATES DECLARATION

We hereby certify that the work, which is being presented in the report, entitled **Analysis of Malicious Code Dynamics with Target and Attacker nodes using Mathematical Model**, in partial fulfillment of the requirement for the award of the Degree of **Bachelor of Technology** and submitted to the institution is an authentic record of our own work carried out during the period *May 2017* to *September 2017* under the supervision of **Dr. Joydip Dhar** and **Dr. Anuraj Singh**. We 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 this project, a compartmental model is developed using infection controlling mechanism to figure out the advancement of a appropriated attack on severely targeted groups in a computer network. The model gives an epidemiological design consisting two sub-designs to recognize the disparity between the global nature of the attacker class and the targeted class. The targeted nodes are partitioned into four compartments as Susceptible(S), Infected(I), Quarantine(Q) and Recovered(R) whereas the attacker nodes are partitioned into three compartments as Infected(I), Breaking-out(B) and Recovered(R). The boundedness, the possible feasibility of equilibrium states of the system and their stability are figured out using cyber mass action incidence phenomenon. Basic reproduction number R_0 is observed for various cases and the results proved that R_0 <1 ensures malicious code free stable steady state for the system and R_0>1 ensures the existence of endemic steady state having local asymptotic stability. The impact of controlling transmission through media coverage controlling coefficient of malicious objects is analyzed. The infection controlling factor like firewall coefficient 'm' depends on the types of files under consideration, defined security rules as per firewall rule base and the reliability as well as efficiency of the media coverage factor, e.g., firewall. So, on behalf of media coverage factor, it is taken into consideration. Our objective is to analyze various aspects of malicious code propagation and the effect of media coverage factor, e.g., firewall security within the computer network. To achieve the objective, the effect of media coverage factor 'm' is observed. The stability of the system is retrieved using local asymptotic stability method. Finally, Numerical simulation has been carried out to verify analytic results and most sensitive system parameters for basic reproduction number are observed using normalized forward sensitivity index.

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

ACKNOWLEDGEMENTS

We are highly obliged to our mentors **Dr. Joydip Dhar** and **Dr. Anuraj Singh**, 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 them 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 their valuable guidance, suggestions, astute judgment, constructive criticism and an eye for perfection. Our mentors 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 their 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.

(Alok Singh)   (Neha Singh)   (Saurabh Sharma)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION AND LITERATURE SURVEY

The introduction with literature review, objective of this thesis and platform for the implementation is carried out in this chapter.

1.1 Introduction

The arrival of IT in the previous three or four decades has driven a significant change in the process of data transfer and information exchange. The improvement of network/ IT has put some critical issues like the need of a appropriate cyber security system to shield the important data stored on system and for data in transfer from malevolent objects. Malicious code is any code intentionally integrated, converted or cut out from a software system to damage or debase the system's predetermined function. To predict the behavior of cyber threats and to make the secure cyber system, it is necessary to study and find out the different types of malicious objects (Worm, virus, ransom-ware, etc.) and develop a mathematical model to describe their flow and impact on the system. The stimulating movements of interrelatedness, intricacy and resilience are provoking the grave risk posed by malicious object [2, 10, 16, 17].

1.1.1 Related Definitions

1. **Virus:** The part of malicious code that append to service host and propagate when the infected host program executes is known as a Virus.

2. **Worms:** The piece of malicious code that carry out registered attacks to propagate across the computer network instead of appending themselves to a host program is known a Worm.

3. **Trojan horse:** Malicious code which hides the malicious part inside a useful host program is known as a Trojan Horse.

4. **Ransom-ware:** Ransom-ware is a type of malicious software from crypto-virology that blocks access to the victim's data or threatens to publish it until an amount of release price(ransom) paid.

All the above definitions are explained in [10].

1.1.2 Relation with epidemiology

The above mentioned malicious codes have a severe threat to the security of the networks. A recognizable degradation in the performance can be observed in a computer with malicious objects in the breaking-out (B) state. Malicious codes can replicate themselves from one computer to another without making anyone aware that the machine is affected. This malicious code problem is frequently emerging and increasing the vulnerability of the network. So, there is a necessity to develop a new counter defense techniques to control this threat.

It is seen that the flow of artificial viruses in a system of networked computers could be compared with a disease transmitted by vectors in the case of public health [10]. It is known that spreading of malicious code shows the epidemic nature, i.e., these codes act like infectious diseases in the biological world.

Various epidemic models for malicious codes propagation are based on mathematical modeling [7], which provides an estimate of the evolution of malicious intent over the Computer networks. Mathematical models consider the important parameters responsible for malicious codes propagation, such as rates of transmission and recovery, and identify how the malicious codes (or applications) will spread over a fixed period.

1.2 Numerical Tools Used

MATLAB and Mathematica tools are used to implement the project. At first, the analysis of dynamics of the model is done using the qualitative property of differential equations. Then MATLAB is used for numerical analysis and validation. For the bridging of both analyses, the Mathematica software is used. In this way, the proposed model consisting target and attacker sides with different compartments is analyzed. Runge-Kutta-Fehlberg Method (RKF45)[5] and the concept of Jacobian Matrix and Eigen values are also applied for the solution and analysis purpose.

Key Features:

- Solutions of mathematical equations.

-Graphical representation of node density vs. time for analyzing results.

Versions:

- MATLAB 8.1 (2013a).

- Wolfram Mathematica(11.1.1).

1.3 Literature Review

It is known that spreading of malicious code is epidemic in nature. Various epidemic models for malicious codes propagation are based on traditional SIR model [7, 10, 16], which gives an estimate of the development of malicious codes in the computer networks.

Many researchers have analyzed the simple epidemic models like Susceptible- Infected model and SIS model with varying population sizes [7, 18]. In SIS and SIR models, they got two thresholds for the models with two types of formulation about the immunity loss and concluded that the number individuals that are affected decreases continuously when there is increment in the value of t and finally, the infection diminishes when the basic reproduction number is found less than 1 [1].

Mishra et al. proposed SEIRS and SEIQRS [11, 17] models and also provided the information and the propagation dynamics of malicious objects(codes) and analyzed the cyber attacking behavior of infected nodes(computer system), while Yang and Yang figured out some of these differences with some faults in the existing models and suggested a common SLBS model [13, 12, 14]. Coates and Thommes suggested an improved SEI (susceptible-exposed- infected) model for the simulation of virus transmission [21] and many other identical models are proposed by various researchers.

Reviewing of article on malicious code dynamics of model consisting two quarantine nodes, it is seen that in the model, both attacker and target sides were taken each with same compartments, which is not reasonable many times [15].

In [8], a SIS model having two-dimensions with vaccination is proposed for paired border towns, which shows a backward branching for some values of parameters. As the results, it was found that a vaccination campaign dedicated to decrease the value of a disease's reproduction number below one may not get success to control the disease. So for the prevention of an epidemic outbreak, a large population of infective persons can cause a high endemicity level to occur rather abruptly even if the reproduction number reduced by vaccine is below some threshold value.

1.3.1 Drawbacks of earlier models

The following drawbacks were found after the review of previous models :

1.3.1.1 Exposed Infected compartment

It is not possible that a computer doesn't have an infection. So, there is no need to consider the exposed state. Since once attacked by malicious code, a computer becomes infected immediately and retains infection, because it can propagate this attack to those computers with some faults in the system. Therefore, an epidemic model shouldn't possess any E compartment [2].

1.3.1.2 I-R Interaction

In a well-defined epidemic model of malicious code propagation, Infected compartment should not interact only to the recovered state. The reasons are :

1. There should have two Infected classified compartments, as I (Infected but not active) compartment for computers with the virus in latent state and B(breaking-out) compartment. The probability with which they recover should be the main issue in the process of modeling. Indeed, recovery of a breaking-out computer is faster because it usually has a recognizable degradation in the performance, which can be identified by the user.

2. In some networks, the phenomenon of quarantine nodes is also taken into consideration as a precaution measure. So, some of the infected nodes will be quarantined once the effect of the virus is known.

1.3.1.3 Not flexible for new types of attacks

In previous models, the possibility of new attacks like ransom-ware was not taken care. In new attacks like ransom-ware, the infected node becomes either a carrier of the virus or bursts and then recovered. So, once the attacker gets control of the personal computer, he can either use it as carrier node, taking it to breaking out state or he can hack it, whenever it is recovered.

1.3.1.4 Both side Q compartment

It is probable that a computer which is infected and the infection is breaking-out, then it can affect the nodes in other networks and quarantine is one of the precautions which anyone can take. But, there is no need for the attacker to consider quarantine as he only wants to corrupt the network with malicious code. So, precautions like isolated nodes may not be taken into account.

1.3.1.5 Permanent Recovery(R) compartment

It is possible that a computer which is recuperated be infected by new types of malicious codes as permanent immunity is impossible. So, an epidemic model should not contain any permanent R(recovered) compartment [2, 21].

In [19], Some anti-malware software is installed in the computer network and continuously updated to minimize the affluence of malicious objects and infected computers. On analyzing the proposed model, two equilibria and a threshold dealing with the malevolent code dynamics were obtained in a network and characterization of stability behavior of equilibria derived for the given model is also explained.

In [6], traditional SIS model is extended to random process from a deterministic process and Stochastic differential equations for infected ones are formulated to prove uniqueness of a positive global solution of these equations and the conditions, for extinction and persistence of disease, are established.

The thesis aims to analyze various malicious code dynamics which can help the anti-malware software in protecting a computer network from malicious attack.

1.4 Objective

The objective of this thesis is to analyze the malicious code dynamics with the target and attacker nodes using a mathematical model. In which, a computer network with the target and attacker nodes for malicious code propagation within the system (Computer network) is considered. The model consists of different compartments (e.g., Susceptible, Infected, antidotal, etc.) and then a mathematical model is developed, and its various analytic behaviors are analyzed.

1.5 Organization of Thesis

The organization of thesis is described as follows: The literature review and discussion of the works done in section 1.3, whereas problem statement and objective are defined in section 1.4. In the next chapter(2), a compartmental model with firewall security coefficient is suggested, and numerical validation and simulation with the analysis of sensitivity are represented in chapter 3. At the end of the report, Conclusion and future scope of the proposed work are devised in chapter 4.

CHAPTER 2

DESIGN DETAILS AND IMPLEMENTATION

2.1 Compartment Description

The computer nodes are grouped into two parts: I. targeted nodes and II. attacker nodes. In the proposed model, targeted population is subdivided into four compartments namely Susceptible, Infected, Quarantine and Recovered, while attacker population consists of into three compartments: Infected, Breaking-out and Recovered. Here, total computer nodes fall into seven classes, namely,

1. $S_1(t)$ susceptible nodes of targeted class,

2. $I_1(t)$ infected nodes of targeted class;

3. $I_2(t)$ infected nodes of attacker class;

4. $Q_1(t)$ quarantined nodes of targeted class;

5. $B_2(t)$ infected nodes of attacker class in breaking-out state of malicious code and

6. $R_1(t)$ recovered nodes of targeted class

7. $R_2(t)$ recovered nodes of attacker class

The schematic flow of the model is shown in figure 2.1. Here some assumptions, i.e., the law of mass action and homogeneous spatial distribution in the mixing of hosts is taken into consideration, i.e., through out the total size of population, the density of the local population remains constant. Targeted population:

$$\tilde{N}_1(t) = \tilde{S}_1(t) + \tilde{I}_1(t) + \tilde{Q}_1(t) + \tilde{R}_1(t), \tag{2.1}$$

and attacker population:

$$\tilde{N}_2(t) = \tilde{I}_2(t) + \tilde{B}_2(t) + \tilde{R}_2(t). \tag{2.2}$$

The primary objective of this model is to analyze the effect of parameters used during transmission of information to control the transmission of malicious codes. Some researchers explored the impact of media awareness in biological disease spread using mathematical modeling with transmission coefficient function

$$\beta(I) = \beta e^{-mI/N}, \tag{2.3}$$

and noticed that many positive equilibria are possible when the effect of media is adequately sturdy among the population [4, 9, 19, 20].

Similarly, infection controlling factor on behalf of media coverage '*m*' is taken into consideration. The factor '*m*' depends on the types of files under review, defined firewall security rules in the firewall rule base and the reliability and efficiency of the firewall or any other media coverage factor. The objective of this thesis is to analyze various aspects of malicious code propagation within the computer network.

In the mathematical modeling of propagation of the malicious codes, the incidence function has a significant role. In various mathematical models, $\beta\ SI$ is used as the bilinear incidence rate and $\beta\ SI/N$ is used as the standard occurrence rate, where β quantifies the effect of both the contact transmission rates and the propagation of the malicious object(code). However, the impact of any media coverage factor like firewall security to the spread and control of malicious code propagation is not considered in these occurrence function.

Initially, the expression for transmission rate

$$\beta(I) = \beta e^{-mI},$$

is used by the researchers but it has some faults. So, firewall (media coverage factor) induced contact transmission rate as

$$\beta(I) = \beta e^{-mI/N},$$

is used in the compartmental model which is more rational, because

$$\beta(I) = \beta e^{-mI/N} \rightarrow 0 \qquad \text{as} \qquad I \rightarrow \infty,$$

independent of the nature of m. It is seen that the firewall security and vigilance are only the extrinsic deterministic transmission factor, so it is logical to consider that the rate of transmission cannot be decreased below a threshold level simply through the firewall security alert. Besides further for a fixed value of m, the minimum rate of transmission varies with size of the population, which is impractical.

$$min\{\beta e^{-mI/N} = \beta e^{-m}\}$$

which remains unchanged with the population size[2, 22].

2.2 Mathematical Model and Schematic Flow Diagram

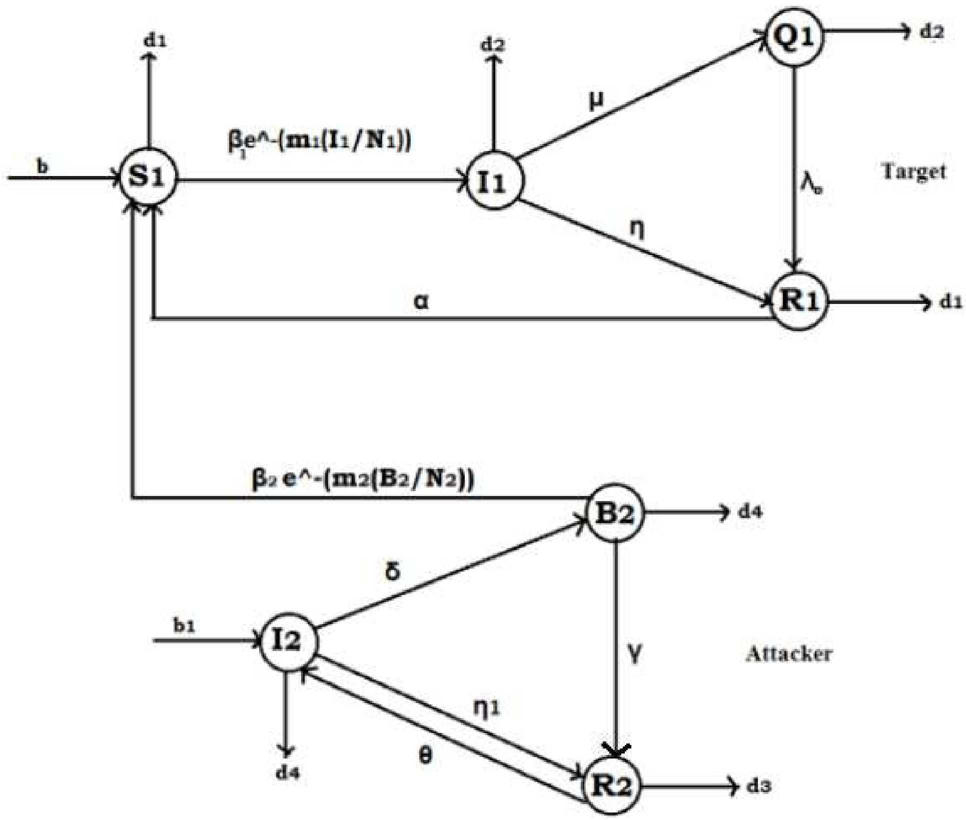

Figure 2.1: Schematic Flow Diagram of the model

Considering the transmission rates shown in the figure 2.1, the following set of ordinary differential equations represents the propagation of malicious codes :

For targeted nodes:

$$\frac{d\tilde{S}_1}{d\tilde{t}} = b - d_1\tilde{S}_1 + \tilde{\alpha}\tilde{R}_1 - \tilde{\beta}_1 e^{-m_1\left(\frac{\tilde{I}_1}{\tilde{N}_1}\right)}\left(\frac{\tilde{I}_1}{\tilde{N}_1}\right)\tilde{S}_1 - \tilde{\beta}_2 e^{-m_2\left(\frac{\tilde{B}_2}{\tilde{N}_2}\right)}\left(\frac{\tilde{B}_2}{\tilde{N}_2}\right)\tilde{S}_1, \tag{2.4}$$

$$\frac{d\tilde{I}_1}{d\tilde{t}} = \tilde{\beta}_1 e^{-m_1\left(\frac{\tilde{I}_1}{\tilde{N}_1}\right)}\left(\frac{\tilde{I}_1}{\tilde{N}_1}\right)\tilde{S}_1 + \tilde{\beta}_2 e^{-m_2\left(\frac{\tilde{B}_2}{\tilde{N}_2}\right)}\left(\frac{\tilde{B}_2}{\tilde{N}_2}\right)\tilde{S}_1 - (\tilde{d}_2 + \tilde{\eta} + \tilde{\mu})\tilde{I}_1, \tag{2.5}$$

$$\frac{d\tilde{Q}_1}{d\tilde{t}} = \tilde{\mu}\tilde{I}_1 - \tilde{d}_2\tilde{Q}_1 - \tilde{\lambda}_0\tilde{Q}_1, \tag{2.6}$$

$$\frac{d\tilde{R}_1}{d\tilde{t}} = \tilde{\lambda}_0\tilde{Q}_1 - \tilde{\alpha}\tilde{R}_1 - d_1\tilde{R}_1 + \tilde{\eta}\tilde{I}_1. \tag{2.7}$$

For attacker nodes:

$$\frac{d\tilde{I}_2}{d\tilde{t}} = b_1 - \tilde{d}_4\tilde{I}_2 - \tilde{\delta}\tilde{I}_2 + \tilde{\theta}\tilde{R}_2 - \tilde{\eta}_1\tilde{I}_2, \tag{2.8}$$

$$\frac{d\tilde{B}_2}{d\tilde{t}} = \tilde{\delta}\tilde{I}_2 - \tilde{d}_4\tilde{B}_2 - \tilde{\gamma}\tilde{B}_2, \tag{2.9}$$

$$\frac{d\tilde{R}_2}{d\tilde{t}} = \tilde{\gamma}\tilde{B}_2 - d_3\tilde{R}_2 - \tilde{\theta}\tilde{R}_2 + \tilde{\eta}_1\tilde{I}_2. \tag{2.10}$$

Parameters	**Description**
b, b_1	Recruitment rates of target and attacker classes
d_1, d_3	Natural death rate of targeted and attacker population node
β_1	Contact rate from susceptible class to infected class
β_2	Contact rate from breaking-out to susceptible class
γ	Rate of recovery of computers with malicious codes in breaking-out state
η, η_1	Rate of recovery of computers with malicious codes in infected state
d_2	Death rate in infected target classes(death due to infection and natural death)
λ_0	Rate of recovery of computers with malicious codes in quarantine state
δ	Rate of change of malicious nodes from infected to breaking-out state
θ	Rate of change of recovered nodes into infected nodes(immunity loss)
d_4	Death rate in infected attacker classes(death due to infection and natural death)
α	Rate of change of recovered nodes into susceptible nodes
m_1, m_2	Infection controlling coefficients
μ	Rate of change of malicious nodes from infected to quarantine state

Table 2.1: Description of Parameters

where every system parameter is positive and illustrated in table 2.1.

2.3 Non-dimensionalisation

Due to complicated nature of the equations (2.4)-(2.10), these equations are non-dimensionalized for the above system using:

$$\begin{aligned}
&S_1 = \frac{\tilde{S}_1}{\tilde{N}_1}, \quad I_1 = \frac{\tilde{I}_1}{\tilde{N}_1}, \quad Q_1 = \frac{\tilde{Q}_1}{\tilde{N}_1}, \quad R_1 = \frac{\tilde{R}_1}{\tilde{N}_1},\\
&I_2 = \frac{\tilde{I}_2}{\tilde{N}_2}, \quad B_2 = \frac{\tilde{B}_2}{\tilde{N}_2}, \quad R_2 = \frac{\tilde{R}_2}{\tilde{N}_2}, \quad t = \tilde{d}_1\tilde{t},\\
&N_1 = \frac{\tilde{N}_1}{\tilde{N}_1{}^0}, \quad N_2 = \frac{\tilde{N}_2}{\tilde{N}_2{}^0}, \quad \tilde{N}_1{}^0 = \frac{b}{\tilde{d}_1}, \quad \tilde{N}_2{}^0 = \frac{b_1}{\tilde{d}_3}.
\end{aligned} \tag{2.11}$$

The equivalent non-dimensional system is given by:

For targeted nodes:

$$\begin{aligned}
\frac{dS_1}{dt} &= \frac{(1-S_1)}{N_1} + \alpha R_1 - \beta_1 e^{-m_1 I_1} I_1 S_1 - \beta_2 e^{-m_2 B_2} B_2 S_1 - S_1 + S_1^2\\
&+ d_2 I_1 S_1 + d_2 Q_1 S_1 + R_1 S_1,
\end{aligned} \tag{2.12}$$

$$\begin{aligned}
\frac{dI_1}{dt} &= \beta_1 e^{-m_1 I_1} I_1 S_1 + \beta_2 e^{-m_2 B_2} B_2 S_1 - (d_2 + \eta + \mu) I_1 - \frac{I_1}{N_1} + d_2 I_1^2\\
&+ I_1 S_1 + d_2 Q_1 I_1 + I_1 R_1,
\end{aligned} \tag{2.13}$$

$$\frac{dQ_1}{dt} = \mu I_1 - d_2 Q_1 - \lambda_0 Q_1 - \frac{Q_1}{N_1} + d_2 Q_1^2 + d_2 I_1 Q_1 + Q_1 S_1 + Q_1 R_1, \tag{2.14}$$

$$\frac{dR_1}{dt} = \lambda_0 Q_1 - \alpha R_1 - R_1 + \eta I_1 - \frac{R_1}{N_1} + R_1^2 + d_2 I_1 R_1 + d_2 Q_1 R_1 + R_1 S_1. \tag{2.15}$$

For attacker nodes:

$$\frac{dI_2}{dt} = \frac{(1-I_2)}{N_2} - d_4 I_2 - \delta I_2 + \theta R_2 - \eta_1 I_2 + d_4 I_2^2 + d_4 I_2 B_2 + I_2 R_2, \tag{2.16}$$

$$\frac{dB_2}{dt} = \delta I_2 - d_4 B_2 - \gamma B_2 - \frac{B_2}{N_2} + d_4 B_2^2 + d_4 I_2 B_2 + B_2 R_2, \tag{2.17}$$

$$\frac{dR_2}{dt} = \gamma B_2 - R_2 - \theta R_2 + \eta_1 I_2 - \frac{R_2}{N_2} + R_2^2 + d_4 I_2 R_2 + d_4 B_2 R_2. \tag{2.18}$$

Where population parameters of both classes are dimensionalised by d_1 and d_3 respectively.

2.4 Boundedness of the System

For the verification of boundedness of the defined system, the systems is classified into two parts, i.e., targeted and the Attacker Population. For targeted population, the equations are:

$$\tilde{N}_1(t) = \tilde{S}_1(t) + \tilde{I}_1(t) + \tilde{Q}_1(t) + \tilde{R}_1(t),$$

then,

$$\frac{d\tilde{N}_1}{d\tilde{t}} = \frac{d\tilde{S}_1}{d\tilde{t}} + \frac{d\tilde{I}_1}{d\tilde{t}} + \frac{d\tilde{Q}_1}{d\tilde{t}} + \frac{d\tilde{R}_1}{d\tilde{t}},$$

$$\frac{d\tilde{N}_1}{d\tilde{t}} = b - \tilde{d}_1\tilde{S}_1 - \tilde{d}_2\tilde{I}_1 - \tilde{d}_2\tilde{Q}_1 - \tilde{d}_1\tilde{R}_1 \tag{2.19}$$

Again, let

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

then,

$$\frac{d\tilde{N}_1}{dt} \leq b - d[\tilde{S}_1 + \tilde{I}_1 + \tilde{Q}_1 + \tilde{R}_1] = b - d\tilde{N}_1.$$

If

$$\tilde{N}_1(t) > (b/d), \text{ then } \frac{d\tilde{N}_1}{dt} < 0,$$

implying

$$lim_{t\to\infty}\tilde{N}_1(t) \leq b/d.$$

It can be seen after a moment of observation, that, simply connected compressed set

$$\Omega_k = \{(\tilde{S}_1, \tilde{I}_1, \tilde{Q}_1, \tilde{R}_1) \in R_+{}^4 : \tilde{S}_1 + \tilde{I}_1 + \tilde{Q}_1 + \tilde{R}_1 \leq b/d\}, \tag{2.20}$$

is positively invariant for the model. Hence, the suggested system is well mannered. Similarly, boundedness of the Attacker nodes can also be defined.

$$\tilde{N}_2(t) = \tilde{I}_2(t) + \tilde{B}_2(t) + \tilde{R}_2(t),$$

then,

$$\frac{d\tilde{N}_2}{d\tilde{t}} = +\frac{d\tilde{I}_2}{d\tilde{t}} + \frac{d\tilde{B}_2}{d\tilde{t}} + \frac{d\tilde{R}_2}{d\tilde{t}},$$

$$\frac{d\tilde{N}_2}{d\tilde{t}} = b_1 - \tilde{d}_4\tilde{I}_2 - \tilde{d}_4\tilde{B}_2 - \tilde{d}_3\tilde{R}_2 \tag{2.21}$$

Again, let

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

then,

$$\frac{d\tilde{N}_2}{dt} \leq b_1 - d_1[\tilde{I}_2 + \tilde{B}_2 + \tilde{R}_2] = b_1 - d_1\tilde{N}_2.$$

If

$$\tilde{N}_2(t) > (b_1/d_1), \text{ then } \frac{d\tilde{N}_2}{dt} < 0,$$

entailing

$$lim_{t\to\infty}\tilde{N}_2(t) \le b_1/d_1.$$

It can be seen after a moment of observation, that, simply connected compressed set

$$\Omega_{k1} = \{(\tilde{I}_2, \tilde{B}_2, \tilde{R}_2) \in {R_+}^3 : \tilde{I}_2 + \tilde{B}_2 + \tilde{R}_2 \le b_1/d_1\}, \tag{2.22}$$

is also positively invariant for the model.

In the next chapter, the dynamic behavior of all possible steady states of the system will be analyzed.

CHAPTER 3

RESULTS AND DISCUSSION

3.1 Steady States and their Stability

3.1.1 Equilibrium Points

The points of equilibrium are achieved using the following set of equations and dynamics of the model is analyzed using these set of points:

$$\frac{dS_1}{dt} = 0 = \frac{dI_1}{dt} = \frac{dQ_1}{dt} = \frac{dR_1}{dt} = \frac{dI_2}{dt} = \frac{dB_2}{dt} = \frac{dR_2}{dt} \tag{3.1}$$

from the system of targeted and attacker class equations. If infection is not present in the system, then it has following malicious codes-free equilibrium state:

$$E_1 = (1, 0, 0, 0, \hat{I}_2, \hat{B}_2, \hat{R}_2),$$

and one endemic equilibrium state:

$$E_2 = (\check{S}_1, \check{I}_1, \check{Q}_1, \check{R}_1, \check{I}_2, \check{B}_2, \check{R}_2).$$

Here it is retrieved that the equilibrium point E_1 is on the S_1 - I_2 - B_2 - R_2 plane and is always possible since all the other parameters are greater than 0. For the calculation of the feasibility of the endemic steady state E_2 for different parameter sets, the numerical values of parameters are adopted. The expressions for the equilibrium points are used to retrieve the conditions for stability of malicious-code free solutions. To avoid infection propagation, it will be advantageous to get the minimum recovery rate.

3.2 Basic Reproduction Number

The anticipated number of secondary infection cases originated by a single infection in an entirely susceptible population is called Basic reproduction number, R_0. To characterize the malicious object propagation, it is considered as one of the most useful barrier (threshold parameter) [1]. Let

$$x = (I_1, Q_1, I_2, B_2).$$

Then, the derivative of infection classes, i.e., equations (2.13) and (2.14) of targeted system and equations (2.16) and (2.17) equations of attacker system is given by,

$$\frac{dx}{dt} = \mathcal{F} - \mathcal{V}, \tag{3.2}$$

Where,

$$\mathcal{F} = \begin{bmatrix} \beta_1 e^{-m_1 I_1} I_1 S_1 - \beta_2 e^{-m_2 B_2} B_2 N_2 S_1 \\ Q_1 S_1 \\ 0 \\ 0 \end{bmatrix},$$

$$\mathcal{V} = \begin{bmatrix} (d_2 + \eta + \mu) I_1 + \frac{I_1}{N_1} - d_2 I_1^2 - I_1 S_1 - d_2 Q_1 I_1 - I_1 R_1 \\ -\mu I_1 + d_2 Q_1 + \lambda_0 Q_1 + \frac{Q_1}{N_1} - d_2 Q_1^2 - d_2 I_1 Q_1 - Q_1 R_1 \\ -\frac{(1-I_2)}{N_2} + d_4 I_2 + \delta I_2 - \theta R_2 + \eta_1 I_2 - d_4 I_2^2 - d_4 I_2 B_2 - I_2 R_2 \\ -\delta I_2 + d_4 B_2 + \gamma B_2 + \frac{B_2}{N_2} - d_4 B_2^2 - d_4 I_2 B_2 - B_2 R_2 \end{bmatrix},$$

Therefore,
F(Jacobian of F at malicious codes-free equilibrium)=

$$\begin{bmatrix} (\beta_1 + 1) S_1 & 0 & 0 & \beta_2 S_1 \\ 0 & S_1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

and,
V(Jacobian of V at malicious codes-free equilibrium)=

$$\begin{bmatrix} (d_2 + \eta + \mu + 1) & 0 & 0 & 0 \\ -\mu & (d_2 + \lambda_0 + 1) & 0 & 0 \\ 0 & 0 & (1 + d_4 + \delta + \eta_1) & 0 \\ 0 & 0 & -\delta & (d_4 + \gamma + 1) \end{bmatrix}.$$

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

$$R_0 = max\left\{ \frac{(\beta_1 + 1) S_1}{(d_2 + \mu + \eta + 1)}, \frac{S_1}{(d_2 + \lambda_0 + 1)} \right\}, \tag{3.3}$$

Where S_1 shows the node density of susceptible nodes of targeted population in non endemic equilibrium state. This model has one such state E_1 and hence there is only one basic reproduction number R_0. Value of R_0 is: For equilibrium state E_1, S_1=1 and hence,

$$R_0 = max\left\{\frac{(\beta_1 + 1)}{(d_2 + \mu + \eta + 1)}, \frac{1}{(d_2 + \lambda_0 + 1)}\right\}. \tag{3.4}$$

Applying the same procedure for the proposed system (2.4)-(2.10), we get basic reproduction number,

$$\tilde{R}_0 = \frac{\tilde{\beta}_1}{(\tilde{d}_2 + \tilde{\mu} + \tilde{\eta})}. \tag{3.5}$$

3.3 Local Asymptotic Stability

The local asymptotic stability of both, malicious codes-free and endemic equilibrium, is specified. The generalized Jacobian matrix is given as follows:

$$J = \begin{bmatrix} -2 + 2S_1 & d_2S_1 - \beta_1S_1 & d_2S_1 & \alpha + S_1 & 0 & -\beta_2S_1 & 0 \\ 0 & a_{22} & 0 & 0 & 0 & \beta_2S_1 & 0 \\ 0 & \mu & a_{33} & 0 & 0 & 0 & 0 \\ 0 & \eta & \lambda_0 & a_{44} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a_{55} & 0 & \theta \\ 0 & 0 & 0 & 0 & \delta & -1 - d_4 - \gamma & 0 \\ 0 & 0 & 0 & 0 & \eta_1 & \gamma & -2 - \theta \end{bmatrix},$$

Where,

$$\begin{aligned} a_{22} &= -1 - d_2 - \eta - \mu + \beta_1S_1 + S_1, \\ a_{33} &= -1 - d_2 - \lambda_0 + S_1, \\ a_{44} &= -2 + \alpha + S_1, \\ a_{55} &= -1 - d_4 - \eta_1 - \delta. \end{aligned}$$

At non endemic equilibrium, the variation matrix E is given below:

$$J = \begin{bmatrix} 0 & d_2-\beta_1 & d_2 & 1+\alpha & 0 & -\beta_2 & 0 \\ 0 & \beta_1-d_2-\eta-\mu & 0 & 0 & 0 & \beta_2 & 0 \\ 0 & \mu & -d_2-\lambda_0 & 0 & 0 & 0 & 0 \\ 0 & \eta & \lambda_0 & -1-\alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1-d_4-\eta_1-\delta & 0 & \theta \\ 0 & 0 & 0 & 0 & \delta & -1-d_4-\gamma & 0 \\ 0 & 0 & 0 & 0 & \eta_1 & \gamma & -2-\theta \end{bmatrix}$$

The eigenvalues of this matrix are:$\{0, \quad \beta_1-d_2-\eta-\mu, \quad -d_2-\lambda_0, \quad -1-\alpha,$
$\frac{-(-2a^3+3^{3/2}(-4a^3d-a^2c^2+18acd+4c^3+27d^2)^{1/2}+9ac+27d)^{1/3}}{(3*2^{1/3})}+$
$\frac{(2^{1/3}(3c-a^2))}{(3(-2a^3+3^{3/2}(-4a^3d-a^2c^2+18acd+4c^3+27d^2)^{1/2}+9ac+27d)^{1/3})}+\frac{a}{3},$
$\frac{((1-3^{1/2}i)(-2a^3+3^{3/2}(-4a^3d-a^2c^2+18acd+4c^3+27d^2)^{1/2}+9ac+27d)^{1/3})}{(6*2^{1/3})}$
$-\frac{((1+3^{1/2}i)(3c-a^2))}{(3*2^{2/3}(-2a^3+3^{3/2}(-4a^3d-a^2c^2+18acd+4c^3+27{d^2}^{1/2}+9ac+27d^{1/3}}+\frac{a}{3},$
$\frac{((1+3^{1/2}i)(-2a^3+3^{3/2}(-4a^3d-a^2c^2+18acd+4c^3+27d^2)^{1/2}+9ac+27d)^{1/3})}{(6*2^{1/3})}$
$-\frac{((1-3^{1/2}i)(3c-a^2))}{(3*2^{2/3}(-2a^3+3^{3/2}(-4a^3d-a^2c^2+18acd+4c^3+27{d^2}^{1/2}+9ac+27d^{1/3}}+\frac{a}{3}\}$. Where,

$$\begin{aligned} a &= -4-2d_4-\eta_1-\delta-\gamma-\theta, \\ b &= -1-b_4, \\ c &= b^2-\gamma b-2\theta b-4b-\eta_1 b+\eta_1\gamma+2\eta_1\theta+2\eta_1-\delta b+\delta\gamma+\delta\theta+2\delta+2\gamma+\theta\gamma, \\ d &= \theta\eta_1 b+2b^2-2\gamma b-2\eta_1 b+2\gamma\eta_1-2\delta b+2\delta\gamma+\theta b^2+\gamma\theta b-\delta\theta b. \end{aligned}$$

Equilibrium state E_1 is said to be locally asymptotically stable when all eigenvalues of J_{01} variation matrix will be having negative real parts or when it is negative in nature. So, if R_0<1, then all the eigenvalues will possess negative real parts. Hence, it can be said the malicious code free equilibrium E_1 is locally asymptotically unstable if R_0>1 and stable, if R_0<1.

3.4 Numerical Experimentation

Numerical methods are used to determine and analyze the system of equations for the targeted and attacker system. The behaviors of the nodes are examined for the different classes. The targeted and attacker system has been determined and simulated and the nature of the nodes in both of the classes are observed. All of these analyses are done concerning the time.

3.4.1 Feasible Steady States

In this step, possible steady states are simulated and analyzed for different parameter sets for the proposed model. If all the classes possess non-negative values at any point, then a steady state is said to be feasible at that point. Table 3.1 shows the feasibility of steady states related to the particular basic reproduction number and for different parameter set.

Various curves are plotted to observe the nature of the classes with respect to time. These Graphical plots show the density S_1, I_1, Q_1 and R_1 nodes of attacker class and I_2, B_2 and R_2 targeted class. Since E_1 is the malicious code free state so it would be present in all of the set of equilibrium states if their reproduction number R_0 <1, otherwise equilibrium will tend to E_2 state if their R_0>1. All observations are done with respect to the time and with different parameter sets.

Parameters (Non-Dimensional)	**Set A**	**Set B**	**Parameters (With Dimensions)**	**Set C**	**Set D**
b	7.5	7.5	b	1	75
d_1	0.003	0.003	d_1	0.3	0.3
β_1	0.001	0.01	$\tilde{\beta}_1$	0.5	2.5
β_2	0.006	0.30	$\tilde{\beta}_2$	0.6	0.6
μ	0.003	0.003	$\tilde{\mu}$	0.3	0.3
λ_0	0.008	0.0008	$\tilde{\lambda}_0$	0.8	0.8
d_4	0.075	0.0075	$\tilde{d}_4$	10	2.5
b_1	7.5	7.5	$\tilde{b}_1$	75	75
d_3	0.02	0.02	$\tilde{d}_3$	2.0	2.0
η	0.004	0.0004	$\tilde{\eta}$	0.4	0.4
η_1	0.175	0.0175	$\tilde{\eta}_1$	17.5	7.5
α	0.010	0.0005	$\tilde{\alpha}$	1.0	1.0
d_2	0.4	0.004	$\tilde{d}_2$	0.4	0.4
γ	0.0005	0.01	$\tilde{\gamma}$	0.75	0.75
δ	0.009	0.027	$\tilde{\delta}$	1.9	0.9
θ	0.10	0.20	$\tilde{\theta}$	10	10
m_1	2	2	m_1	6	2
m_2	3	2	m_2	6	2
Feasible SS	E_1	E_2	Feasible SS	E_1	E_2
R_{01}	0.0098	1.2500			
R_{02}	0.0073	0.3846	$\tilde{R}_0$	0.4545	2.2727

Table 3.1: Possible steady states with respect to the reproduction number for different parameter set(Dimensional and non-dimensional) in the model

The graph shown in figure 3.1 is plotted according to parameter set A with initial population (0.4, 0.02, 0.1, 0.1, 0.25, 0.25 and 0.25). It can be seen that node density of S_1, I_2, B_2 and R_2 classes at steady state are greater than zero, and E_1 is the possible steady state. It can be seen from the table that R_{01} <1 and R_{02} <1, hence it can be concluded from the figure3.1 that E_1 is the stable steady state, i.e., malicious code free equilibrium is stable.

The graph shown in figure 3.2 is plotted according to parameter set A with initial population (0.30, 0.30, 0.11, 0.25, 0.50, 0.20 and 0.25). Similarly, it can be observed

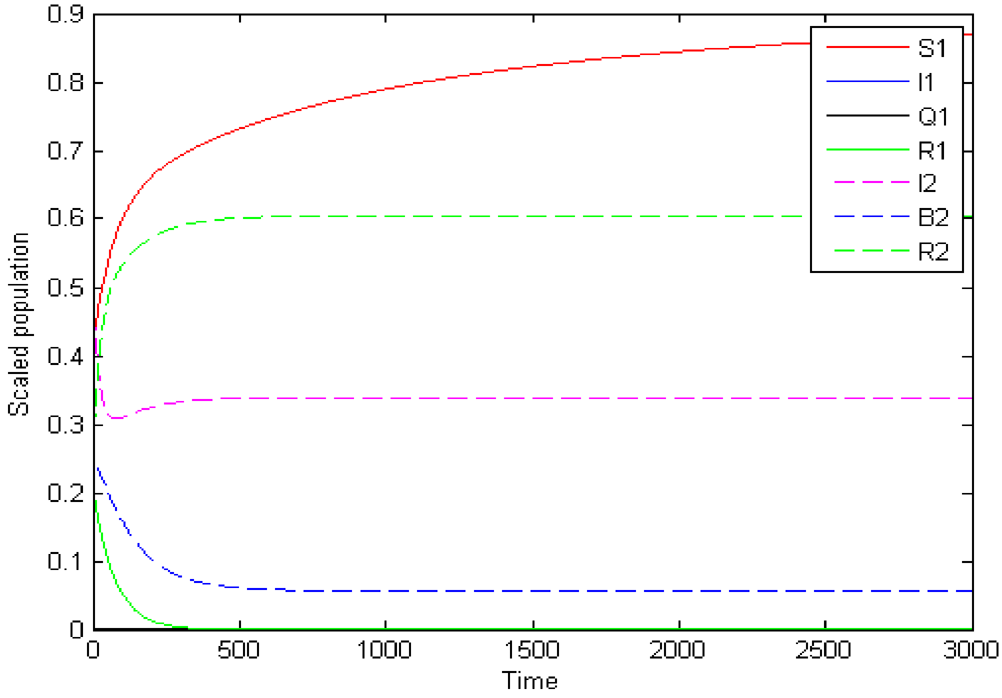

Figure 3.1: Graph between node density and time for set A with initial population (0.4, 0.02, 0.02, 0.2, 0.50, 0.25, 0.25)

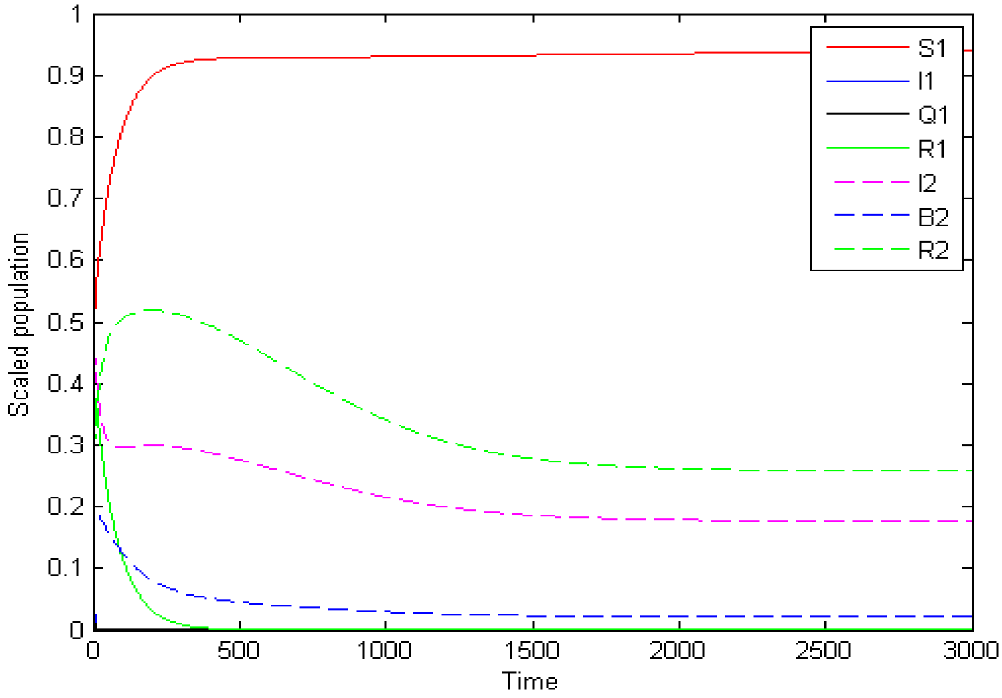

Figure 3.2: Graph between node density and time for set A with initial population (0.30, 0.30, 0.11, 0.25, 0.50, 0.20, 0.25)

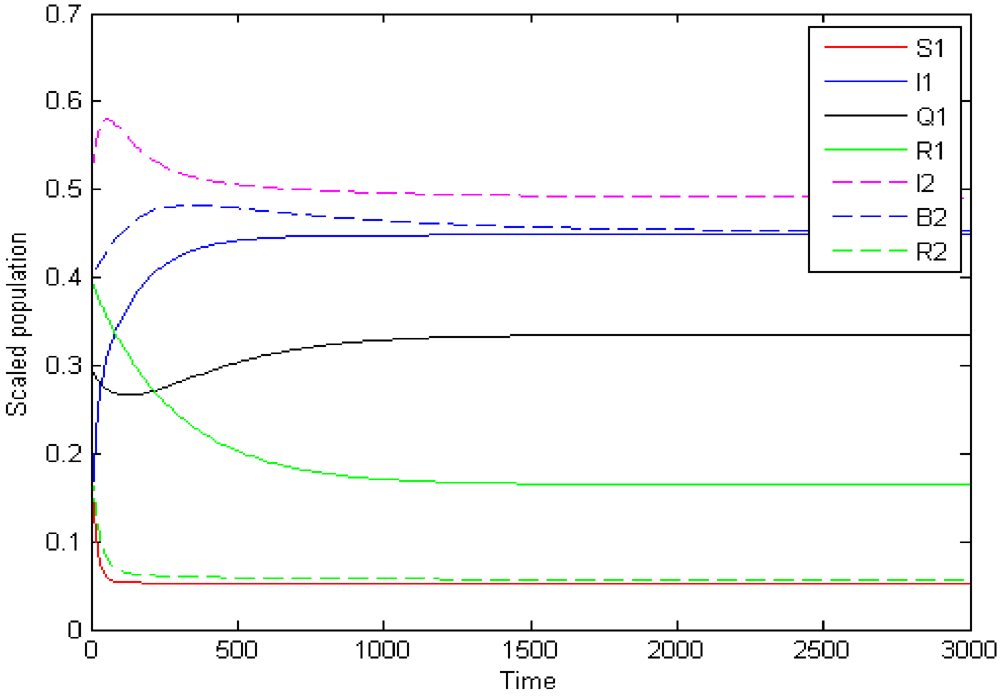

Figure 3.3: Graph between node density and time for set B with initial population (0.2, 0.1, 0.3, 0.4, 0.5, 0.4, 0.2)

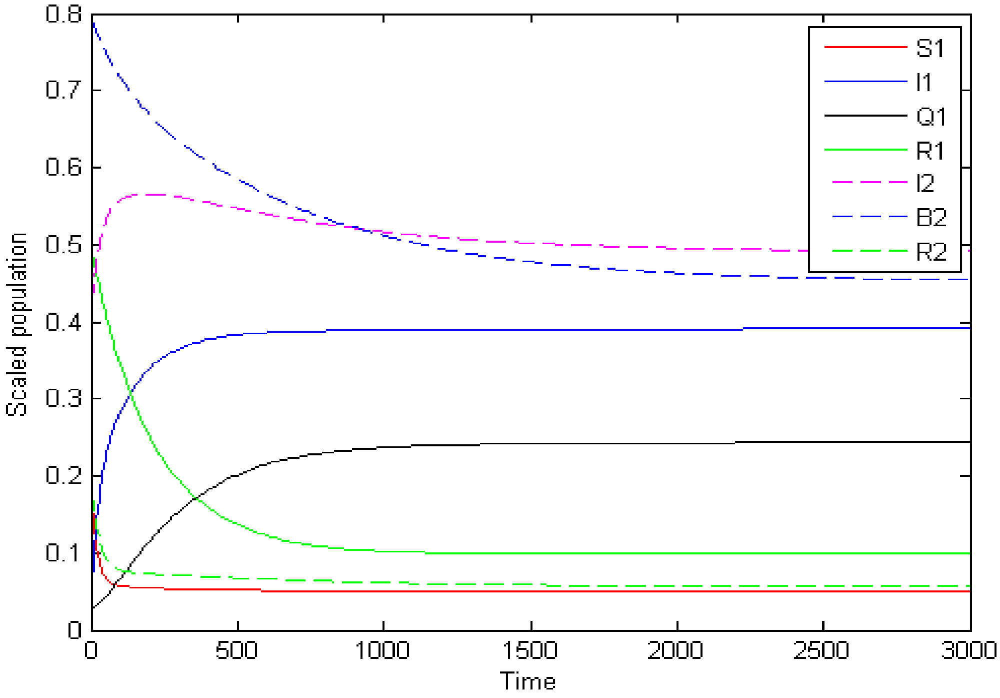

Figure 3.4: Graph between node density and time for set B with initial population (0.2, 0.01, 0.03, 0.5, 0.4, 0.8, 0.2)

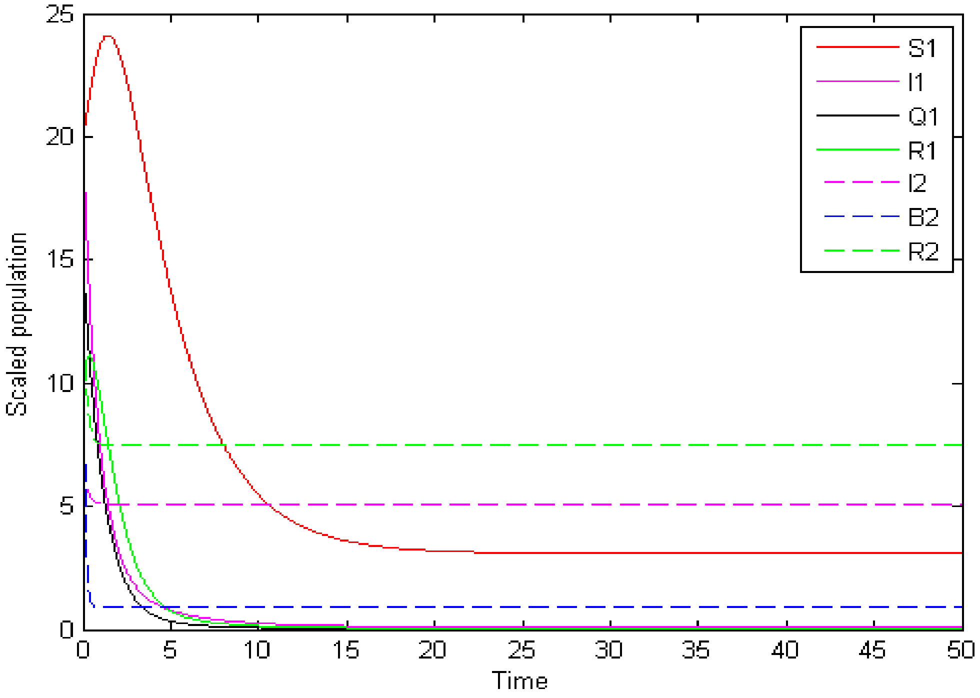

Figure 3.5: Graph between node density and time for set C with initial population (20, 20, 15, 10, 10, 20, 10)

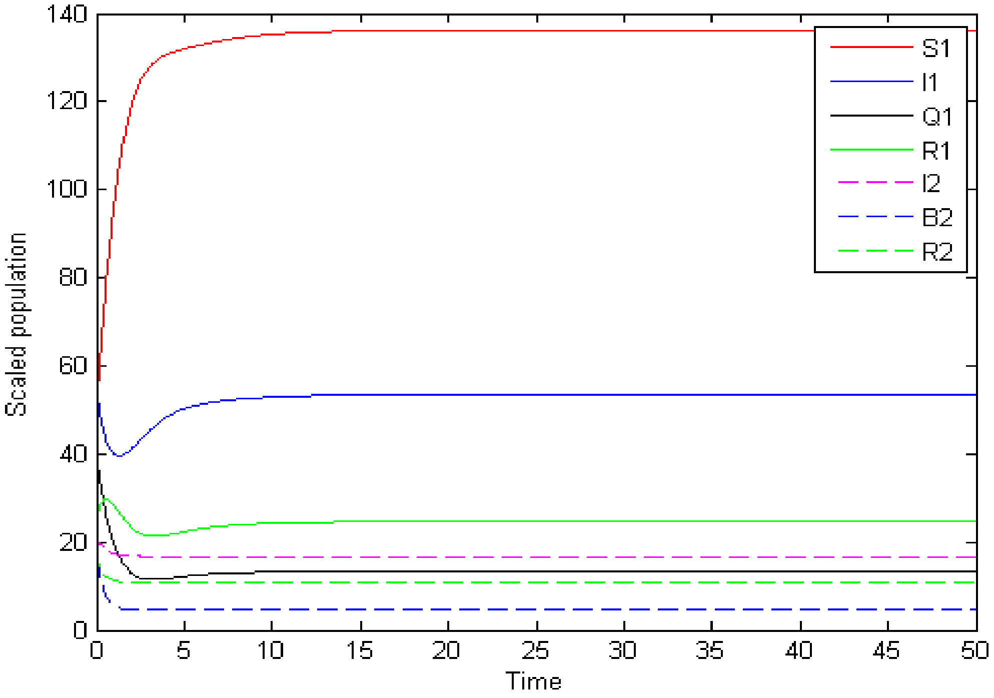

Figure 3.6: Graph between node density and time for set D with initial population (50, 55, 40, 25, 10, 20, 25)

that E_1 is the feasible steady state, i.e., malicious code free equilibrium is stable.

The graph shown in figure 3.3 is plotted according to parameter set B with initial population (0.2, 0.01, 0.3, 0.4, 0.4, 0.4 and 0.2). In the figure 3.3 node density of all classes at steady state are greater than zero and E_1 and E_2 are possible feasible states. Since R_{01}>1, it can be observed from the figure 3.3 that E_2 is the stable steady state, i.e., malicious codes will be present in long run.

The graph shown in figure 3.4 is plotted according to parameter set B with initial population (0.2, 0.01, 0.03, 0.5, 0.4, 0.8 and 0.2). Similarly, it can be concluded that E_2 is the feasible steady states, i.e., malicious objects will be present in long run.

The graph shown in figure 3.5 is plotted according to parameter set C with initial population (20, 20, 15, 10, 10, 20 and 10). It can be seen that the density of $\tilde{S}_1$, $\tilde{I}_2$, $\tilde{B}_2$ and $\tilde{R}_2$ classes at steady state node are greater than zero, and E_1 is possible feasible state. Since $\tilde{R}_0$ <1, it can be observed from the figure3.5 that E_1 is the stable steady state, i.e., malicious code free equilibrium is stable.

The graph shown in figure 3.6 is plotted according to parameter set D with initial population (50, 55, 40, 25, 10, 20 and 25). In the figure 3.6 at steady state node density of all classes are greater than zero. In this figure at steady state node density of all classes are greater than zero and both states, E_1 and E_2, are feasible. Since $\tilde{R}_0$>1, it can be assured that E_2 is the stable steady state, i.e., Malicious codes will be present in long run.

3.4.2 Special Cases

In this subsection, we will study the dynamics of system, when the internal security, i.e., both anti-virus coefficient, m_1 and firewall coefficient, m_2 are zero.

Figures 3.7, 3.8, 3.9 and 3.10 are plotted with same parameters that are given in Set A, B, C and D respectively in the table 3.4.1 except the controlling parameters. However, it can be seen that without controlling factors, the scaled population of Susceptible nodes deviates and decreases with respect to time and similarly, the infected population grows.

From all the graphs, it is observed that the natures of graphs are similar to the earlier graphs with respect to time, for all the values of basic reproduction number. So, it can be concluded that the qualitative features of the model don't change due to change in controlling coefficients.

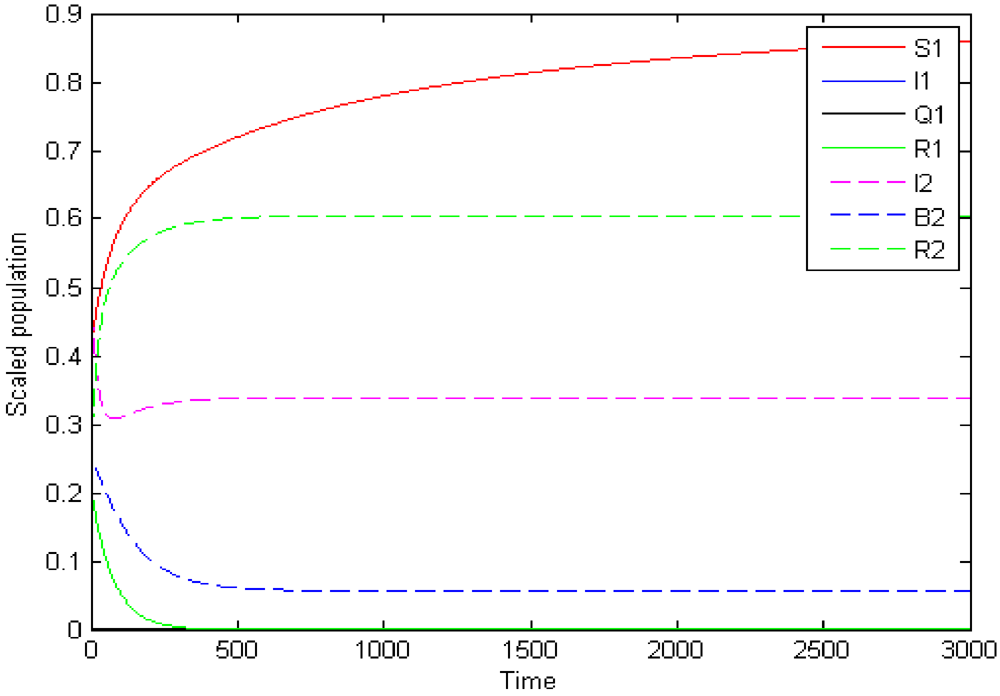

Figure 3.7: Graph between Node Density and Time for set A with initial population (0.4 0.02 0.02 0.2 0.50 0.25 0.25)

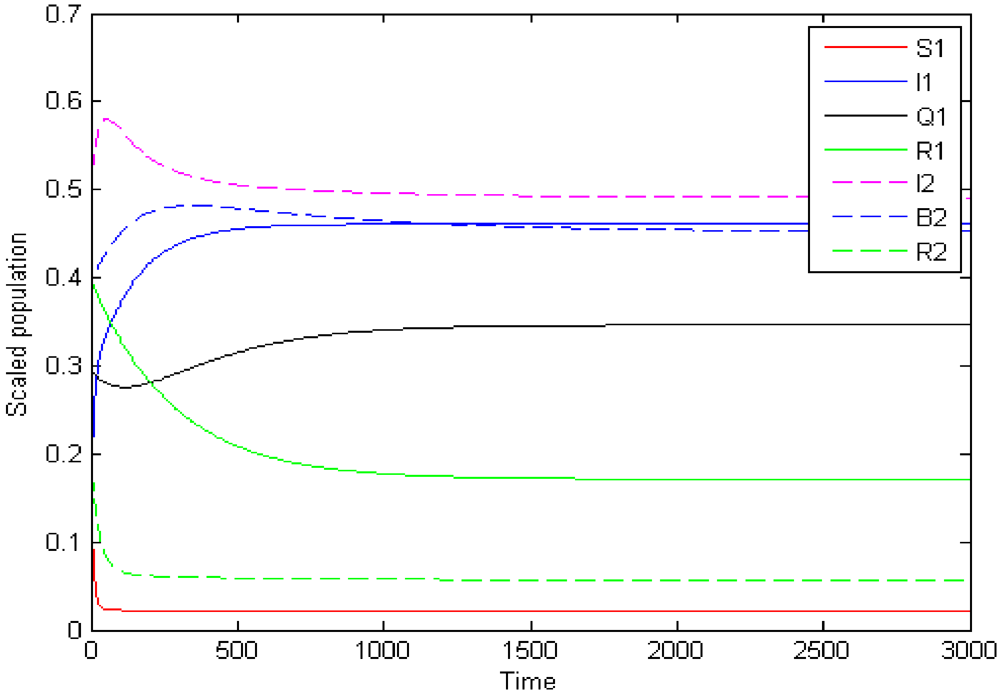

Figure 3.8: Graph between Node Density and Time for set B with initial population (0.2 0.1 0.3 0.4 0.5 0.4 0.2)

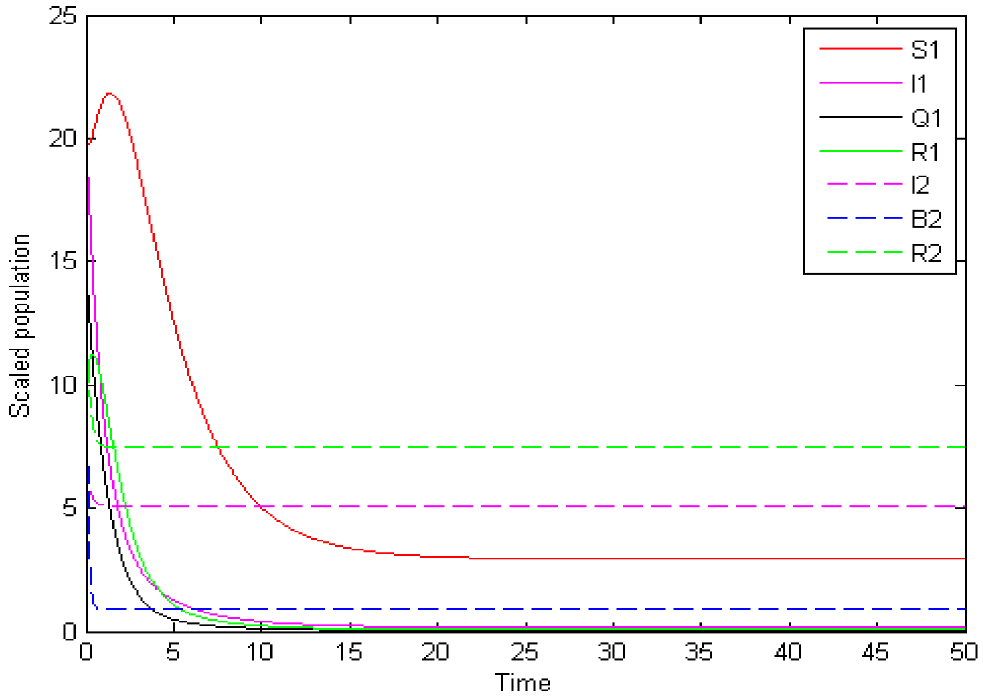

Figure 3.9: Graph between Node Density and Time for set C with initial population (20 20 15 10 10 20 10)

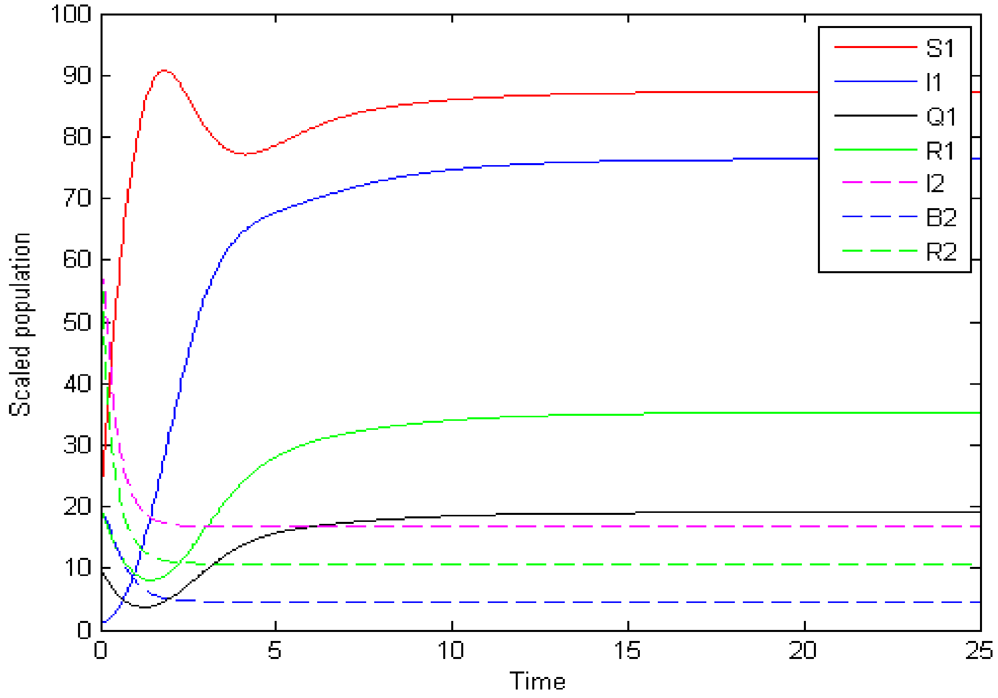

Figure 3.10: Graph between Node Density and Time for set D with initial population (20 1 10 20 50 20 75)

3.5 Estimation of media coverage factor (firewall security coefficient)

Firewall is the computer network security system that observes and controls the entering and outgoing traffic of the network based on predetermined security patterns and policies. The firewall critically makes a barrier between a trusted as well as secure internal computer network and malicious users that are assumed not to be secure or trusted.

3.5.1 Order of Rule Enforcement

The traffic through the particular network connection is examined by the firewall. The firewall monitors every connection and then the rules for various factors, i.e., IP Address, Port, Domain name, keywords, etc. are enforced sequentially. The firewall observes every connection and compares that link for the consistency with service, data and destination. If the connection is valid, then firewall applies that particular rule otherwise, it checks for the next matching rule in its predefined Rule base.

3.5.2 Firewall rule priority

Because firewall rules that possess possible conflicts can be determined, it is important to figure out the sequence in which the rules are executed.

3.5.3 Authenticated bypass

Authenticated bypass is the rule which enables user to create rules for Firewall with Advanced Security that blocks incoming traffic unless it is from a specified trusted computer or user. These rules should allow the propagation of matched network traffic otherwise it would not be given access. A separate security rule for establishment of connection would be used for the network traffic authentication. These patterns and policies are used to allow access to any computer to an authorized troubleshooting devices and network administrators [2].

3.5.4 Block connection

These rules restrict all matched incoming network traffic if it is found suspicious according to these rules.

3.5.5 Allow connection

These defined rules allow matched incoming network traffic nevertheless the informational data is nontrust-able. Because the general criterion is to avoid and stop malicious incoming network traffic, there should be a rule for allowance defined to help any network service or program that must accept the incoming traffic. The coefficient of firewall security, 'm' should be dependent upon the types of files(data) under consideration, defined rules of firewall security in firewall rule base and the reliability and efficiency of the software(firewall) [2]. A way of measuring the value m of firewall security is defined as:

$$m = -log_2(a + b - ab) \tag{3.6}$$

Where 'b' measures the response of the data to the determined security rules. For the analysis purpose, some rules can be added certainly by observing the nature of attacker population. Firewall will check those rules firewall rule base when the files or data will be received in targeted class. If these data respond correctly to all rules, then b=0 and if not, then b=1 and it is expected that the rate of malware propagation can be drawn away by proportion 'a', when each received files tolerate the predetermined security rules [2].

From figures 3.11 to 3.14, it can be seen that for the both case of reproduction number, the fraction of infected population decreases with respect to time as the values of firewall and anti-virus coefficients increase.

The work of firewall is just to minimize damage caused by spyware by blocking unauthorized and malicious party access, while antivirus is used for the prevention, detection, and removal of malicious software from the system. So, the effect of antivirus and firewall can be seen by the figures 3.11 to 3.14.

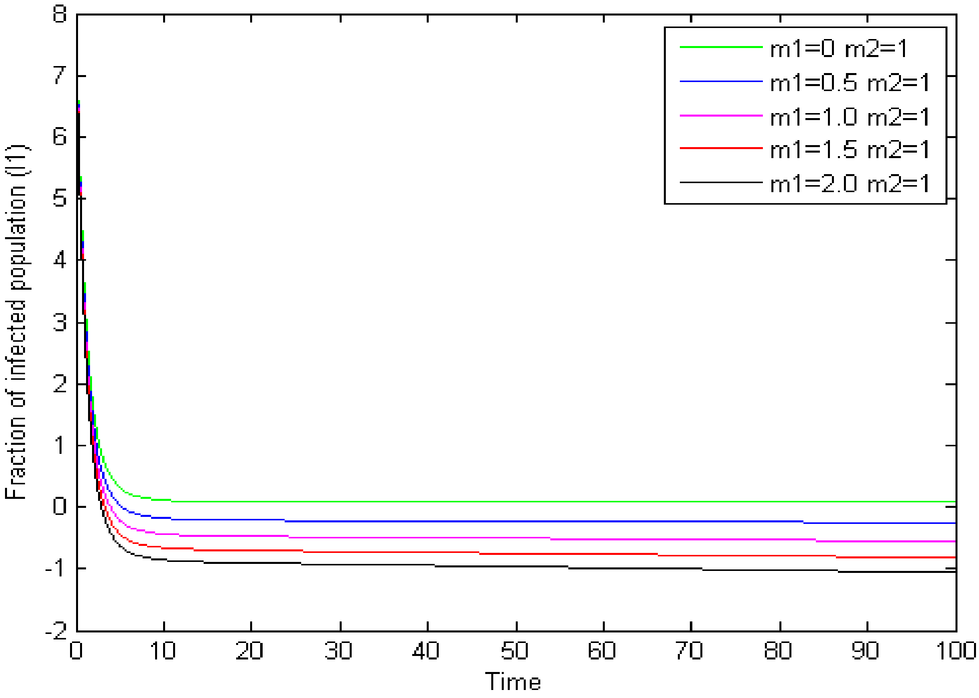

Figure 3.11: Effect of m_1 (antivirus coefficient) on $\tilde{I}_1$ when $\tilde{R}_0 < 1$

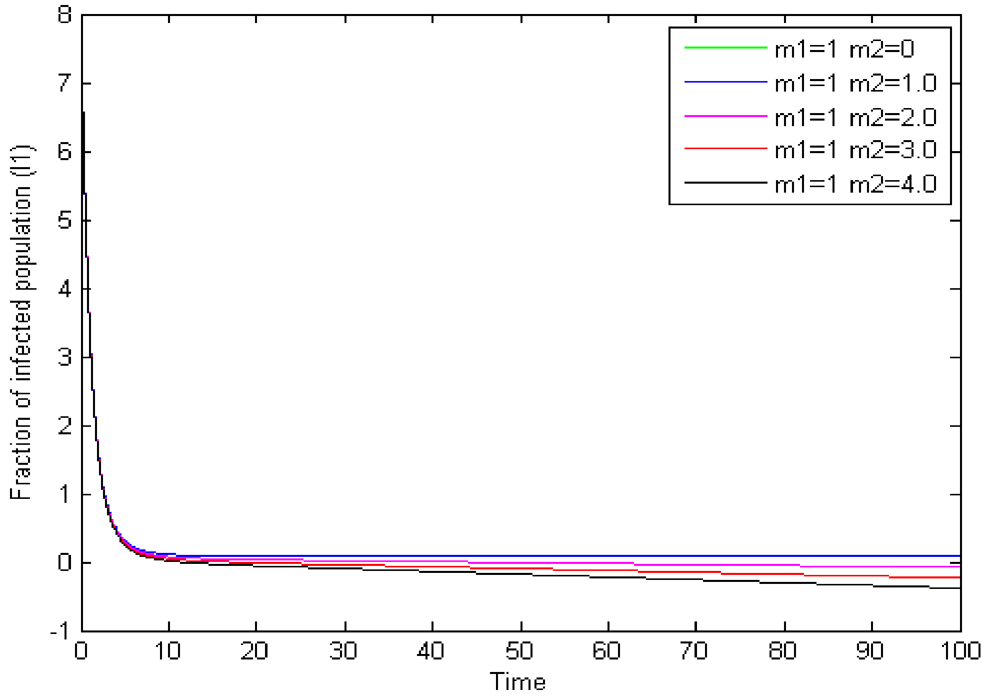

Figure 3.12: Effect of m_2 (firewall coefficient) on $\tilde{I}_1$ when $\tilde{R}_0 < 1$

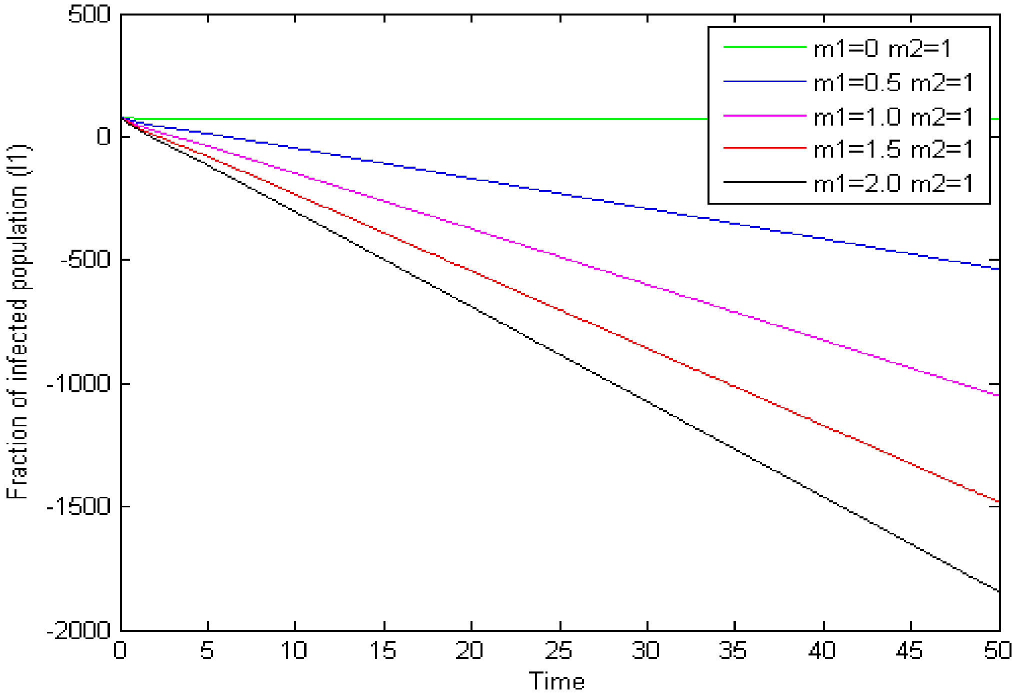

Figure 3.13: Effect of m_1 (antivirus coefficient) on $\tilde{I}_1$ when $\tilde{R}_0 > 1$

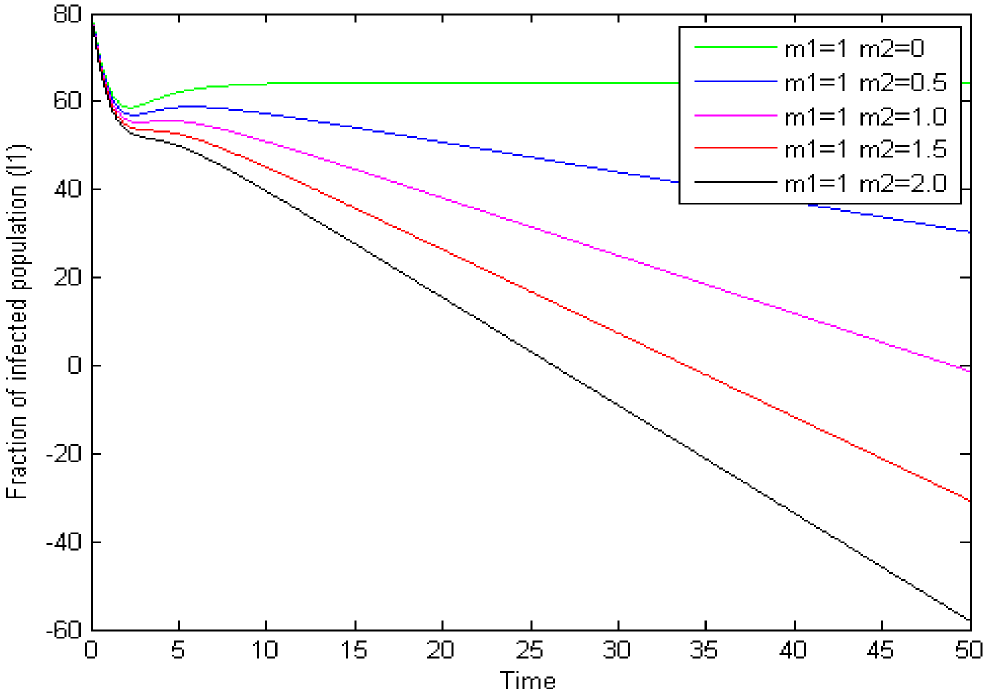

Figure 3.14: Effect of m_2 (firewall coefficient) on $\tilde{I}_1$ when $\tilde{R}_0 > 1$

3.6 Sensitivity Analysis

In this step, normalized forward sensitivity index is used for the sensitivity analysis concerning basic reproduction number. The relative change in a state variable with respect to a bit change in the system parameter is quantified using sensitivity indices. The ratio of the relative variation (or change) in the variable to the relative change in the particular system parameter is defined as the distributed forward sensitivity index of the variable to that particular parameter. The sensitivity index can also be derived using partial derivatives [3]. Let p is a parameter and u is the function of p, a little change δ p to the parameter p and the corresponding change in u as δ u:

$$\delta u = u(p+\delta p) - u(p) = [u(p+\delta p) - u(p)].\frac{\delta p}{\delta p} \equiv \delta p \frac{\partial u}{\partial p}. \tag{3.7}$$

The distributed forward sensitivity index for a variable, u, which depends on a parameter, p, can be defined as:

$$\Upsilon_p^u = \frac{\partial u}{\partial p} \times \frac{p}{u}. \tag{3.8}$$

The prediction and measurement of more sensitive parameter has to be done thoughtfully, because a little change in the parameter will result in relatively huge quantitative change. However, estimation of less sensitive parameter should not require as much practice, since a small change in the parameter, will not lead to huge variation in the quantity.

The analytical expressions for sensitivity index of R_0, with respect to each parameter, are derived. The normalized sensitivity indices for parameters are retrieved as given by the following tables.

The sensitivity indices of the basic reproduction numbers R_{01} and R_{02} for all the sets using different parameters are as follows:

1. Distributed sensitivity indices for (non-dimensional) parameters set with respect to R_{01} is shown in table 3.2.

Parameters (y_j)	**Sensitivity** $\Upsilon_{y_j}^{R_{01}}$	$\Upsilon_{y_j}^{R_{01}}$ **Set 1**	$\Upsilon_{y_j}^{R_{01}}$ **Set 2**
b	0	0	0
d_1	0	0	0
β_1	$\frac{\beta_1}{\beta_1+1}$	0.000999	0.0099
β_2	0	0	0
μ	$-\frac{\mu}{d_2+\mu+\eta+1}$	-0.002	-0.00298
λ_0	0	0	0
d_4	0	0	0
b_1	0	0	0
d_3	0	0	0
η	$-\frac{\eta}{d_2+\mu+\eta+1}$	-0.0028	-0.000397
η_1	0	0	0
α	0	0	0
d_2	$-\frac{d_2}{d_2+\mu+\eta+1}$	-0.28	-0.00397
γ	0	0	0
δ	0	0	0
θ	0	0	0

Table 3.2: Distributed sensitivity indices for (non-dimensional) parameters set concerning R_{01}

It is observed that d_2, β_1, μ and η are moderately sensitive and rest are independent of R_{01} . For example, $\Upsilon_{d_2}^{R_{01}}$ for set 1 = -0.28, hence, increasing (decreasing) d_2 by 1 % will decrease (increase) R_{01} by 0.28%.

2. Distributed sensitivity indices for parameters (non-dimensional) set with respect to R_{02} is shown in table 3.3.

Parameters (y_j)	**Sensitivity $\Upsilon_{y_j}^{R_{02}}$**	$\Upsilon_{y_j}^{R_{02}}$ **Set 1**	$\Upsilon_{y_j}^{R_{02}}$ **Set 2**
b	0	0	0
d_1	0	0	0
β_1	0	0	0
β_2	0	0	0
μ	0	0	0
λ_0	$-\frac{\lambda_0}{1+d_2+\lambda_0}$	-0.287	-0.00398
d_4	0	0	0
b_1	0	0	0
d_3	0	0	0
η	0	0	0
η_1	0	0	0
α	0	0	0
d_2	$-\frac{d_2}{1+d_2+\lambda_0}$	-0.0057	-0.000796
γ	0	0	0
δ	0	0	0
θ	0	0	0

Table 3.3: Distributed sensitivity indices for (non-dimensional) parameters set concerning R_{02}

It is observed that λ and d_2 are moderately sensitive, and rest are independent of R_{02} .

3. Distributed sensitivity indices for (dimensional) parameters set with respect to $\tilde{R}_0$ is shown in the table 3.4.

Parameters (y_j)	**Sensitivity** $\Upsilon_{y_j}^{\tilde{R}_0}$	$\Upsilon_{y_j}^{\tilde{R}_0}$ **Set 1**	$\Upsilon_{y_j}^{\tilde{R}_0}$ **Set 2**
b	0	0	0
d_1	0	0	0
$\tilde{\beta}_1$	1	1	1
$\tilde{\beta}_2$	0	0	0
$\tilde{\mu}$	$-\frac{\tilde{\mu}}{\tilde{d}_2+\tilde{\mu}+\tilde{\eta}}$	-0.27	-0.27
$\tilde{\lambda}_0$	0	0	0
$\tilde{d}_4$	0	0	0
$\tilde{b}_1$	0	0	0
$\tilde{d}_3$	0	0	0
$\tilde{\eta}$	$-\frac{\tilde{\eta}}{\tilde{d}_2+\tilde{\mu}+\tilde{\eta}}$	-0.36	-0.36
$\tilde{\eta}_1$	0	0	0
$\tilde{\alpha}$	0	0	0
$\tilde{d}_2$	$-\frac{\tilde{d}_2}{\tilde{d}_2+\tilde{\mu}+\tilde{\eta}}$	-0.36	-0.36
$\tilde{\gamma}$	0	0	0
$\tilde{\delta}$	0	0	0
$\tilde{\theta}$	0	0	0

Table 3.4: Distributed sensitivity indices for (dimensional) parameters set concerning $\tilde{R}_0$

From table, It is observed that $\tilde{d}_2$ and $\tilde{\eta}$, $\tilde{\mu}$ are moderately sensitive and rest are independent of $\tilde{R}_0$. For example, $\Upsilon_{\tilde{d}_2}^{\tilde{R}_0}$ for set 1 = -0.36, hence, increasing (decreasing) $\tilde{d}_2$ by 1% will decrease (increase) $\tilde{R}_0$ by 0.36%.

In the next chapter, the conclusion and the future scope are discussed.

CHAPTER 4

CONCLUSION AND FUTURE SCOPE

4.1 Conclusion

For the analysis, a simplified IBR model with the normalized attack on SIQR model based targeted resources is introduced and analysis is done using theory of stability of ordinary differential equations consolidating rule base of firewall security. The decisive findings of the project are given below:

1. In the introduced model, two equilibrium states are found of which one is malicious codes free equilibrium and other is endemic. Basic reproduction number for the non endemic equilibrium state has been monitored, and malicious code free equilibrium was found stable, when $R_0<1$ and, the endemic equilibrium achieved stability when $R_0>1$. Here, local asymptotic stability is used to justify the result.

2. The coefficient of firewall security m can be defined as

   $$m = -log_2(a + b - ab). \tag{4.1}$$

   Where 'b' measures the reaction of the files to the predetermined security rules. It is considered that the rate of malthreat propagation can be decreased by a proportion 'a', when all received files tolerate the predetermined security rules.

3. It is observed that the basic reproduction number R_0 is not affected by the coefficient of firewall security and hence the features related to quality of the model don't change.

   Hence, it can be concluded that use of rule base defined for firewall security helps to alleviate the issue of propagation of malicious objects such as code in the network by minimizing the level of infected nodes at stable state.

4. The stability of the system is observed using local asymptotic stability method, and numerical simulation has been done to verify analytical results. Finally, most sensitive system parameters related to basic reproduction number are monitored using normalized forward sensitivity index.

The sensitive parameters related to basic reproduction number are observed and shown in table 4.1.

Basic Reproduction Number	Sensitive Parameters
R_{01}	β_1, μ, η
R_{02}	d_2, λ
$\tilde{R}_0$	$\tilde{\beta}_1, \tilde{d}_2, \tilde{\mu}, \tilde{\eta}$

Table 4.1: Sensitive parameters with respect to basic reproduction number

Table 4.2 shows the comparison between the proposed model and the earlier model(Jain, Bhargava, Soni and J. Dhar):

Type of Analysis	Bhargava, Palash, Soni, Dhar	Proposed Model
Total equilibrium states	16	2
Malicious code free equilibrium	4	1
Endemic equilibrium	12	1
Highly sensitive parameters	2 to 4	0
Moderately sensitive parameters	3 to 5	2 to 4

Table 4.2: Comparison Table

4.2 Future Scope

The analysis can be extended by considering time variant recruitment rate and can be modified by using some antidotal nodes finding anti-virus security and susceptible nodes can also be more generalized. In all known epidemic mathematical models, an individual's treatment is done with sovereignty. With the help of this model and analysis, one can implement kill signal procedure through information propagation.

The idea of quarantined nodes can also help an individual of an organization to get rid of some new computer network attacks like ransom-ware etc. Hence, the analysis proposes modified networking structure through which new network attacks can be contaminated and if it is not possible then this structure can minimize the probability of getting an infection for a network.

REFERENCES

[1] Beckley, R., Weatherspoon, C., Alexander, M., Chandler, M., Johnson, A. and Bhatt, G. S.: 2013, Modeling epidemics with differential equation.

[2] Bhargava, A., Soni, D. K., Jain, P. and Dhar, J.: 2016, Dynamics of attack of malicious codes on the targeted network: Effect of firewall, *International Conference on Recent Trends in Information Technology (ICRTIT), 2016*, IEEE, pp. 1–6.

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

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

[5] Fehlberg, E.: 1969, Low-order classical runge-kutta formulas with stepsize control and their application to some heat transfer problems.

[6] Gray, A., Greenhalgh, D., Hu, L., Mao, X. and Pan, J.: 2011, A stochastic differential equation sis epidemic model, *SIAM Journal on Applied Mathematics* **71**(3), 876–902.

[7] Kermack, W. O. and McKendrick, A. G.: 1927, A contribution to the mathematical theory of epidemics, in: Proceedings of the royal society of london a: Mathematical, physical and engineering sciences, *The Royal Society* **115**, 700 – 721.

[8] Kribs-Zaleta, C. M. and Velasco-Hernandez, J. X.: 2000, A simple vaccination model with multiple endemic states, *Mathematical Biosciences* **164**(2), 183–201.

[9] Liu, Y. and an Cui, J.: 2008, The impact of media coverage on the dynamics of infectious disease, *International Journal of Biomathematics* **1**(01), 65–74.

[10] McGraw, G. and Morrisett, G.: 2000, Attacking malicious code: A report to the infosec research council, *IEEE Software* **17**, 33–41.

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

[12] Mishra, B. K. and Jha, N.: 2010, Seiqrs model for the transmission of malicious objects in computer network, *Applied Mathematical Modelling* **34**(3), 710–715.

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

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

[15] Mishra, B. K. and Singh, A. K.: 2011, Two quarantine models on the attack of malicious objects in computer network, *Mathematical Problems in Engineering* **2012**.

[16] Mishra, B. and Saini, D.: 2013a, Mathematical models on computer viruses, pp. 929–936.

[17] Mishra, B. and Saini, D.: 2013b, Seirs epidemic model with delay for transmission of malicious objects in computer network, pp. 1476–1482.

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

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

[20] Sahu, G. P. and Dhar, J.: 2015, 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), 1651–1672.

[21] Wang, F., Yang, Y., Zhao, D. and Zhang, Y.: 2015, A worm defending model with partial immunization and its stability analysis, *Journal of Communnications* **10**(4), 276–283.

[22] Wang, L., Zhou, D., Zhijun Liuand, D. X. and Zhang, X.: 2017, Media alert in an sis epidemic model with logistic growth, *Journal of Biological Dynamics* **11**(sup1), 120–137.