ANALYSIS AND OPTIMAL CONTROL OF SUSCEPTIBLE-LATENT-BREAKING-OUT-COUNTERMEASURE COMPUTER VIRUS MODEL

MOHAMMED SALEM MOHAMMED BABUSAIL

FACULTY OF ENGINEERING
UNIVERSITY OF MALAYA
KUALA LUMPUR

2019

ANALYSIS AND OPTIMAL CONTROL OF SUSCEPTIBLE-LATENT-BREAKING-OUT-COUNTERMEASURE COMPUTER VIRUS MODEL

MOHAMMED SALEM MOHAMMED BABUSAIL

DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF INDUSTRIAL ELECTRONICS AND CONTROL ENGINEERING

FACULTY OF ENGINEERING
UNIVERSITY OF MALAYA
KUALA LUMPUR

2019

UNIVERSITY OF MALAYA

ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: Mohammed Salem Mohammed Babusail

Matric No: KQC170006

Name of Degree: Master of Industrial Electronics and Control Engineering

Title of Project Research Report:

ANALYSIS AND OPTIMAL CONTROL OF SUSCEPTIBLE-LATENT-BREAKING-OUT-COUNTERMEASURE COMPUTER VIRUS MODEL

Field of Study: Mathematical Modeling and Optimal control

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This Work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature Date:

Subscribed and solemnly declared before,

Witness's Signature Date:

Name:

Designation:

ABSTRACT

Nowadays, our lives rely significantly on technologies and communications between these technologies from manufacturing industries downward to daily activities which made networks become bigger and it is continuously growing more and more where this gives viruses opportunity to spread faster causing a real threat to human. One of the methods researchers working on it to prevent spreading of viruses is to understand how these viruses propagate in a network via building mathematical models that represent virus propagation. This research project proposes a new SLBC (Susceptible-Latent-Breaking-out-Countermeasure) virus propagation model and studies its invariant, equilibrium, and stability. In addition, finds the optimal control system for the model. Lastly, some examples are presented to study virus prevalence over different conditions.

Keywords: computer virus model, optimal control, Pontryagin maximum/minimum principle

ABSTRAK

Pada masa kini, kehidupan kita bergantung kepada teknologi dan komunikasi antara teknologi-teknologi ini daripada industri pengilangan sehingga ke aktiviti harian yang menjadikan rangkaian lebih luas dan terus berkembang dengan pesat yang membuka peluang kepada virus untuk disebarkan lebih cepat sekaligus menyebabkan ancaman yang nyata kepada manusia. Salah satu kaedah yang penyelidik-penyelidik gunakan untuk mencegah penyebaran virus adalah untuk memahami bagaimana virus-virus ini disebarkan dalam satu-satu rangkaian melalui penciptaan model matematik yang menyerupai penyebaran virus. Projek penyelidikan ini mencadangkan model penyebaran virus SLBC (Susceptible-Latent-Breakingout-Countermeasure) yang baru dan mengaji invarian, keseimbangan dan kestabilannya. Di samping itu, penyelidikan itu turut mengaji sistem kawalan optimum untuk model itu. Akhir sekali, beberapa contoh dibentangkan untuk mengkaji kelaziman virus dalam keadaan yang berbeza.

Kata kunci: model virus komputer, kawalan optimum, maksimum Pontryagin / prinsip minimum Pontryagin.

ACKNOWLEDGEMENTS

First, I give thanks to ALLAH for protection and the ability to do this work and complete this research.

Special thanks to my supervisor, Associate Professor Jeevan Kanesan, who encouraged and directed me. His challenges brought this work towards a completion. It is with his supervision that this work came into existence. Also, thanks to Professors, lecturers, and all workers at University of Malaya.

I wish to extend a huge thank you to my parents, brothers, sisters, and all members of my family for providing me continuous support and encouragement throughout my years of study. This accomplishment would not have been possible without them

Finally, I thank all who in one way or another contributed to the completion of this research project. Thank you.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

CHAPTER 1: INTRODUCTION

1.1 Introduction

This chapter presents generally information about why this subject has been chosen. It starts with background of a problem, definitions, main paths for solving this problem, and reasons why one of these paths has been preferred. In addition, problem statement, objectives, and scope of this work are determined. At the end of this chapter, it is mentioned how this thesis organized.

1.2 Background

We are in the cloud data age where computers and microelectronics communication technology make science of information technology develops rapidly. This played an important role in the living ways of human beings from basic daily life to industry sector (Liang, 2010). At the end, we are making bigger and bigger computer network providing an opportunity for computer viruses and worms to propagate and spreading faster causing a real threat for smooth and normal operation by either damaging data or stealing sensitive information (Ray et al., 2007).

1.2.1 Malware, Virus, and Worm

The general term 'malware' is defined as the unwelcomed and dangerous program normally attached to a junk mail or a code spreading in the internet and try to reach a computer through deception, masquerade as innocent (Pérez García, Alfonso-Cendón, Sánchez González, Quintián, & Corchado, 2018). Malware can perform a variety of harms to the hosted computer: deleting data or files, stealing information, or destroying operating systems. Mostly, malware operates in background, so operators do not notice it. Types of malware include computer virus, computer worms, ransomware, and trojan horses where all types can be classified to self-replicating and not self-replicating (M. Zhang, Liu, Chen, & Li, 2018). Computer virus and worm are of the class self-replicating.

The term ‘computer virus’ originated after Cohen’s program which infects computers, replicates itself, and spreads to other computers (Cohen, 1987). It attaches itself to a non-malicious software and when this hosted software is activated, the virus starts copies itself to other files and programs. Whereas worms have same functionality of virus except they do not need to be attached to other software where they can stand alone (Del Rey & Sánchez, 2012). Dormant period is the period when virus reach a host software before the host software runs but as the host software runs, the virus enters latency period. In latent period the virus tries to spread and infect as much as possible of files, programs and other computers before it breaks out ‘breaking-out period’. Breaking-out period stays till the virus is wiped (X. Yang & Yang, 2012).

1.2.2 Options to Encounter Viruses

Researchers are trying in different directions to encounter spreading and emerging of viruses. According to (White, 1998) there are four directions where researchers are working on. One of these methods is by developing new viruses then from that point develop new detection techniques. This method does not guarantee the extent of damages. Second method uses an analysis center where each time new virus appears in the network will be sent to the center to invent new cure then automatically will be deployed worldwide. However, always there will be a lag between the cure and the virus as well as the center has to handle so many requests and some them may not be real. Third of these, using anti-viruses where this method requires security companies to find viruses and their cures before they spread also customers have to update their anti-virus program as fast as possible. Clearly there will be a huge lag in this method.

Finally, computer virus propagation modeling where researchers study birth and death rates and connections between computers through internet network, emails, media, … etc. Virus propagation still ambiguous and incomplete (White, 1998).

1.2.3 Advantages of Computer Virus Modeling

There are many reasons making modeling of computer virus important. First, it gives a visualization of extent of threats can happen due these viruses and understand new propagation techniques (Staniford, Paxson, & Weaver, 2002). Second, researchers take advantage of these models to create containment and disinfection approaches without the needs to do experiments by releasing the virus and test the approaches so expose network to risk (Whalley et al., 2000). Third, models combined with accurate network structure can lead to locate failures in network infrastructure. In addition to, describe features and symptoms of computer virus and use them as early detection (Serazzi & Zanero, 2003).

1.3 Problem Statement

Internet is becoming part of all aspects of life and has brought huge benefits to human society. However, this makes spreading of digital viruses faster so causing threats to development and inflicting large economic losses. Therefore, network security researchers have been concerning about how can effectively suppress spreading of digital viruses. Mathematical modeling of computer viruses' propagation is considered as a feasible approach to the assessment of prevalence of digital viruses.

1.4 Objectives of Research

The main aim of this research project is to stop spreading of computer virus in Networks. This can be reached via these objectives:

1. Establish a mathematical model for computer virus's propagation.
2. To analyze the new model.
3. To optimize trade-off between countermeasure cost and virus prevalence.

1.5 Scope of Study

This work will build a new mathematical model for propagation of computer viruses where all the model depends on probabilities. All work will be in calculations and simulations, no real experiment, so the model will combine some advantages of existing models and import new assumptions.

1.6 Thesis Organization

This chapter has given the introduction of the topic, explained the problem statement, and determined the research project objectives. The rest of this work is organized as follows, chapter two contains literature review of topic. Methodology and implementation of the model are in chapter three. Chapter four shows simulation results and discussions. Finally, conclusions and recommendations for future work presented in chapter five.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This chapter starts with some examples of computer viruses and their financial losses. Then it presents how epidemic spreads with some examples of existing models. Moreover, a quick glance on system analysis is presented at the end of this chapter.

2.2 History of Viruses' Threats

For example, in March 1999, a virus called Melissa attacked some big companies and forced them to shut down their e-mail systems, making an estimated loss of $800 million. In May 2000, "ILOVEYOU" virus was hidden in an e-mail headed 'ILOVEYOU' starts outbreak in Asia spreading to Europe then USA. The virus caused damage of estimated $15 billion by infecting 45 million computers in 20 countries (Norton_Team, 2016). Gives estimation of losses due to The Code Red worm equal to $2.6 billion in two months only in 2001 (Berghel, 2001).

In 2003, the Blaster worm infected 100,000 Microsoft windows systems which costs millions without considering recovery efforts (Bailey, Cooke, Jahanian, & Watson, 2005). Fastest spreading computer worm is known as Slammer or Sapphire where it infected almost all vulnerable hosts (>90%) in less than ten minutes. It spread through internet and made big financial losses in transportation, and government institutions (Moore et al., 2003). According to the Britch Security Firm, in 2004, MyDoom virus caused over $26.1 billion (Zhu, Yang, & Ren, 2012).

The worm known as Downadup, Conficker, or Kido, first discovered in 2008, has infected over than 9 million computers with full administrator right also resets restore points of computer to make it harder to recover (BBC, 2009). "Shamoon" destroyed data of more than 30000 computers of Saudi Arabia oil's company 'ARAMCO', causing the company 17 days of offline work where all reports, contracts, shipping, and supplies process to be on papers and transmission via interoffice mail or fax page by page (Pagliery, 2015).

2.3 Epidemic Spreading Process

Network representation shows relationship or connection between parts of a system or individuals of a population. Many economical, biological, technological, and other systems have pair-wise dependencies through their subsystems. Network representation uses nodes and links between nodes to represent components and relationship between them. For example, social network represents individuals by nodes and friendships by links (Kephart & White, 1992).

Epidemic spreading is one of the dynamics over networks. A mathematical epidemic model describes how infections spread in the network. Propagation models have led to successful results in prevention and predication of epidemics. However, this is not only applicable in biology, computer viruses mimic these biological viruses. From that point, researchers started using biological models as models for computer viruses but that was considered a start where modified and newly models appeared (Meisel, Pappas, & Zhang, 2010).

The beginning of modeling study started by dividing population into several different groups or called compartments and the interaction between each compartment depends on specific rates not necessary all compartments are interchangeable directly or in both forward and backward. For example, SIR compartment model, Susceptible-Infected-Recovered, a susceptible computer node get infected by virus at specific infectious rate and infected node becomes recovered after cured at specific curing rate. in this model assumed recovered computer will not be susceptible again neither infected. Whereas, other models suppose recovered nodes will lose immunity over time, no recovered compartment, or introducing other compartments (Darabi Sahneh, 2014).

Compartments models studied epidemic over homogenous population and did not provide details about the effect of network structure/topology so new approaches has emerged as (Moreno, Pastor-Satorras, & Vespignani, 2002) proposed a network with heterogenous node degree distribution also (Pastor-Satorras & Vespignani, 2001) did the study over scale-free network. These approached showed that interconnection between nodes play an important role in the spreading of an epidemic. To explore role of contact in more details an individual- based models have appeared like (Wang, Chakrabarti, Wang, & Faloutsos, 2003). The contact between nodes in a network is considered a static dynamic where contacts will not change with time. This is because dynamic of virus is faster than dynamic of existence of nods which is result of shorter average lifetime of epidemic compared to lifetime of individuals (Youssef & Scoglio, 2011) The link between two connected nodes will take value one and link of not connected nodes will take value zero.

2.4 Existing Models

The beginning of computer virus modeling was through (Kephart & White, 1992) then many models exist with different strategies to capture propagation of computer virus in reality and prevent spreading of viruses.

Computer models can be categorized, based on the topology of propagation, into two classes: homogenous and heterogenous models (Zhu & Cen, 2017). Homogenous models assume the propagation network as fully connected. In fact, an infected computer will spread to any random vulnerable computer in the network such models SLBS (Susceptible, Latent, Breaking out, Susceptible) by (L.-X. Yang, Yang, Zhu, & Wen, 2013) and SEIRS (Susceptible, Exposed, Infected, Recovered, Susceptible) by (Dong, Wang, & Liao, 2016). In contrast heterogenous models suppose that virus in an infected computer can transfer only through contacted computers which means through direct topological neighbor. For Example, (L.-X. Yang & Yang, 2014) studied the behavior of SI (Susceptible, Infected) model over simple scale-free network where he assumes existing of two degrees K, number of connections that a computer has. Homogenous and heterogenous models have provided a significant impact in understanding detailly and qualitatively how and when computer viruses outbreak.

Majority of viruses have quite long propagation period before breaking out which called latent period. The distinctive characteristic of viruses in this phase is its infectious ability where they be at high infectivity (C. Zhang, 2018). So, he examined a multilayer SLBS model using individual-based (node-based) where each node has its state to be investigated alone which gives more details about individuals. In this model he assumed only infected nodes can be cured, no latent nodes be cured. Moreover, transition from latent to break-out is homogenous.

(Z. Zhang & Wang, 2017) proposed SLBQRS (Susceptible, Latent, Breaking, Quarantined-Recovered, Susceptible) compartment model with time delay due to the cleaning process of the anti-virus programs and did stability analysis of the model. Then (Zhao & Bi, 2017) add time delay to move from latent period of virus to be breaking out also investigated properties of Hopf bifurcation of the model. Quarantine compartment introduces concerns about increasing in quarantine rate leads to reducing threshold R_0 in which increasing probability of virus domination.

Countermeasure compartment is considered one of the strategies to suppress virus spreading in computers networks since CMC (countermeasure Competing) strategy by (Chen & Carley, 2004). A countermeasure is an action or method to suppress or reduce potential threats to computers servers, operating system, information system, or networks. Countermeasure tools include anti-virus software and firewalls. Recently, (X. Zhang & Gan, 2018) used SICS (Susceptible-Infected-Countermeasure-Susceptible) model with dynamic countermeasures, not disseminated with a constant rate, where taking into account topology of the network. It is a degree compartment model which divides nodes into compartments each with different degrees. Furthermore, they found the optimal control to minimize both density of infected computers and the total budget for countermeasures. One of disadvantages of these models include absence of latent period.

2.5 Network Topology

According to (Barabási & Bonabeau, 2003; Faloutsos, Faloutsos, & Faloutsos, 1999), Internet, World-Wide-Web, and social connections are a scale-free network where distribution of node linkages follow power law distribution where the network does not have a scale or uniform distribution. In fact, more nodes have less connections except some nodes which have huge number of links.

2.6 System Analysis

Mathematical models have to be analyzed before they have been applied to investigate characteristics of trajectories (solutions) of the system. These analysis shows how a system will behave in different conditions and that include its stability, critical points, invariant, and others.

2.6.1 Positive Invariance

When designing dynamical models, it has to reveal if these models start from an initial point within a set will stay inside the set for all time t. Positive invariant can be expressed mathematically as:

Let dynamical system $\frac{dx(t)}{dt} = f(x(t))$. $x \in R^n$ with initial point x_0 and trajectory $x(t, x_0)$.

A subset $\vartheta \subset R$ to be a positive invariant set if for all $x_0 \in \vartheta \implies x(t) \in \vartheta$, $\forall\, t \geq 0$ (Benzaouia, 2012)

2.6.2 Equilibrium Points

Equilibrium points in differential equations are considered constants solutions to the differential equations (Boyce, DiPrima, & Meade, 2017).

$$\frac{dx}{dt} = f(t, x) \qquad (1)$$

Point $x^*(t) \in R^n$ is called equilibrium point if $f(t, x) = 0$, $\forall\ t$.

2.6.3 Stability Theory

Describes stability of the trajectory of differential equations due small perturbations of initial conditions. For instance, for equilibrium point x^* and for every small > 0 , exists $\delta > 0$ such that:

1. Stable: for a nearby initial condition will stay indefinitely close to the equilibrium point.
2. $||x(t_0) - x^*|| < \varepsilon \quad \forall\, t > t_0 \quad ||x(t) - x^*|| < \delta$
3. Asymptotically stable: nearby initial condition will converge to the equilibrium point.
4. $||x_0 - x^*|| < \varepsilon \qquad t \to \infty \quad ||x(t) - x^*|| = 0\ or\ x(t) \to x^*$
5. Global asymptotically stable: any initial condition will converge to the unique equilibrium point (Murray, 2017)

$$\forall\ x_0\ and\ \ t \to \infty \qquad ||x(t) - x^*|| = 0\ or\ \ x(t) \to x^*$$

2.7 Optimal Control

Optimal control, it is an extension from the calculus of variations, whereas the optimal control dealing with maximization or minimization to find the optimum result. Mainly the optimal control problem consisting of two kind of functions:

a. Cost Function or Objective Function
b. Dynamical system or states functions: that's describe the behaviors of the states with time.

Simply, the optimal control is finding the optimum control that maximize/minimize the cost function at the same time achieving any constraints like control constraint, state constraint, and time constraint.

The optimal control method basically classified into two approaches, direct and indirect methods. Each method could be solved by different numerical methods like direct single shooting, dynamic programing, and in-direct single shooting. However, some tries to find optimal control used un-conventional methods, like using PID controller (Proportional-Integral-Derivative) or using linear time varying approximation (LTV) (Itik, Salamci, & Banks, 2009; Khadraoui et al., 2016).

Direct method converts the optimal control problem to non-linear programing problem. It starts by discretizing the control problem, after that using non-linear programing techniques to solve the problem. It is called stochastic approach.

On the other hand, direct method converts the optimal control problem to boundary value problem by building Hamiltonian equation, then using Pontryagin maximum/minimum principle. It is called deterministic approach.

2.8 Summary

A virus propagation model that simulate real-world situations has to be a node-based model because many real-world networks were showed to have a highly structured property and a node-based model will show behavior of each computer in the network. additionally, the model has to be heterogenous where it is not fully connected. Besides, virus does not break-out 'disrupt' immediately after it infects a computer, this called latent period, it should be long and highly infectious too. Applying countermeasure will be an advantage to the model where it helps in finding optimal control strategy. The model can be supported by some analysis like invariant, equilibrium, and stability.

CHAPTER 3: METHODOLOGY

3.1 Introduction

From previous chapter, some important specifications are determined to represent computer virus's propagation. In this chapter, these specifications are used to build a new mathematical model. At the beginning, the model is established step by step. Then, invariant, equilibrium, and stability analyses of the model are performed.

3.2 Computer Virus Modeling

From the literature review in previous chapter, a new model has a combination of advantages of existing models with some improvements can be obtained. First of all, most viruses have a latent period before breaking out where its infectious rate in this period is high. This requires existing of latent compartment in the new model with high infectious rate. Second, computers do not become infected uniformly, infectiousness is not homogenous through the network. This can be represented as a not fully connected network. Third, same as infectiousness, countermeasure must not be applied for all the network uniformly or randomly. In addition, the goal is to optimize this process where least costs of anti-viruses applied and least of infected computers. Consequently, an optimal control problem has to be solved. Last but not least, breaking-out of latent computers does not occur instantly and this has been modeled by different options, for example, implying a constant time period before computer breaks-out or a constant rate. In this work, a new strategy has been suggested which implies that viruses breaking-out rate will be affected by how many neighbors have been infected because if virus breaks-out, user will use anti-virus, format his computer, disconnect from internet, or shut-down the computer to save his remaining files or his work process so stop virus from spreading through the network which result in removing the virus, so if viruses break-out before infecting much of neighbors, viruses will vanish and will not be an epidemic threats network so in the new model will let breaking-out compartment not infectious and will not be treated.

It is assumed that the network has a population of N nodes (computers) labeled 1, 2, 3, …, N. Connections between these nodes will be unvaried. $A = (a_{ij})_{N\times N}$ denote the adjacency matrix of the network $a_{ij} = a_{ji}$ and $a_{ij} = 0 \;\forall\; i = j$. Thus A is irreducible.

The new model has four compartments, Susceptible, Latent, Breaking-out, Countermeasure, SLBC. So, each node has one of four possible states and each will be given a probability as $S_i(t)$, $L_i(t)$, $B_i(t)$, and $C_i(t)$, which represents probability node i at time t to be susceptible, latent, Breaking-out, and countermeasures respectively. Then, $S_i(t) + L_i(t) + B_i(t) + C_i(t) = 1, 1 \le i \le N$.

Let us impose set of assumptions about state transitions of nodes, it is shown Figure 3.1:

- Due to contact with latent node j, susceptible node i becomes latent by $\beta \sum_j a_{ij} L_j(t)$. β is a positive infectious rate.
- Susceptible node i becomes countermeasures by a vaccination rate γ_i. $\underline{\gamma_i} \le \gamma_i \le \overline{\gamma_i}$
- Latent node becomes breaking-out by $\rho \sum_j a_{ij}(1 - S_j)$. ρ is a positive breaking-out rate.
- Due to applied treatment, a latent node becomes a countermeasure by a treatment rate α_i . $\underline{\alpha_i} \le \alpha_i \le \overline{\alpha_i}$

These state transitions assumptions can be explained mathematically as follows, with Δt be a very small-time interval:

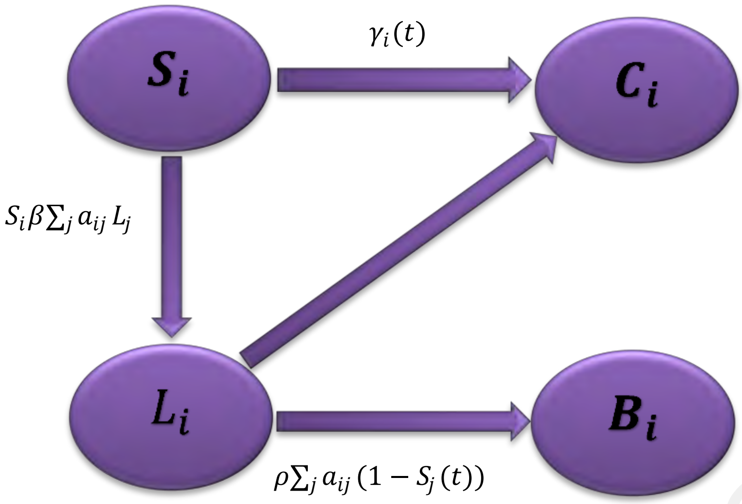


Figure 3.1 Diagram for state transition assumptions.

$\Pr\{i \text{ is latent at time } t + \Delta t \mid i \text{ is susceptible at time } t\} = \beta\Delta t\sum_j a_{ij}L_j(t) + o(\Delta t)$

$\Pr\{i \text{ is countermeasures at time } t + \Delta t \mid i \text{ is susceptible at time } t\} = \gamma_i\Delta t\sum_j a_{ij}L_j(t) + o(\Delta t)$

$\Pr\{i \text{ is breaking} - \text{out at time } t + \Delta t \mid i \text{ is latent at time } t\} = \rho\Delta t\sum_j a_{ij}(1 - S_j) + o(\Delta t)$

$\Pr\{i \text{ is countermeasures at time } t + \Delta t \mid i \text{ is latent at time } t\} = \alpha_i + o(\Delta t)$

$\Pr\{i \text{ is breaking} - \text{out at time } t + \Delta t \mid i \text{ is susceptible at time } t\} = o(\Delta t)$

Remaining state transitions will be same as last one, equal $o(\Delta t)$.

If all above transitions are divided by dt and $\Delta t \to 0$, then:

$$\left.\begin{aligned}
\frac{dS_i(t)}{dt} &= -S_i(t)\beta\sum_j a_{ij}L_j(t) - S_i(t)\gamma_i(t) \\
\frac{dL_i(t)}{dt} &= S_i(t)\beta\sum_j a_{ij}L_j(t) \; - \; L_i(t)\rho\sum_j a_{ij}(1 - S_j(t)) \; - \; L_i(t)\alpha_i(t) \\
\frac{dB_i(t)}{dt} &= L_i(t)\rho\sum_j a_{ij}(1 - S_j(t)) \\
\frac{dC_i(t)}{dt} &= S_i(t)\gamma_i(t) \; + \; L_i(t)\alpha_i(t)
\end{aligned}\right\} \quad \textbf{(2)}$$

With initial conditions

$$(S_1(0), \dots, S_N(0), L_1(0), \dots, L_N(0), B_1(0), \dots, B_N(0), C_1(0), \dots, C_N(0))^T \epsilon\, \breve{\Omega}$$

Where

$\breve{\Omega} = \{(S_1, \dots, S_N, L_1, \dots, L_N, B_1, \dots, B_N, C_1, \dots, C_N)^T \epsilon R_+^{4N} | S_i + L_i + B_i + C_i = 1, i = 1,2, \dots N$

Admissible control set:

$$\mathcal{U} = \{u(t) \in (L^2[0,T])^{2N} | \; \underline{\gamma_i} \le \gamma_i(t) \le \overline{\gamma_i} \;, \underline{\alpha_i} \le \alpha_i(t) \le \overline{\alpha_i} \;, \;\; 1 \le i \le N \}$$

Let: $\tilde{X}(t) = (S_1, \dots, S_N, L_1, \dots, L_N, B_1, \dots, B_N, C_1, \dots, C_N)^{\,T}$

$$\frac{d\breve{X}(t)}{dt} = F(\tilde{X}(t), u(t))$$

3.3 Model Analysis

Three analyses have been done in this part. Positive invariant, equilibrium, and stability are proved below. They are as follow:

3.3.1 Positive Invariant

Wants to prove that the system will stay in the set $\breve{\Omega}$ with any initial point inside the set:

$$\tilde{X}(0) \in \breve{\Omega} \quad implies \;\; \tilde{X}(t) \in \breve{\Omega} \quad \forall \;\; t \geq 0$$

According to (Yorke, 1967), let a smooth dynamical system $\frac{dX(t)}{dt} = F(X(t))$ defined at least in a compact set ϑ. ϑ is positive invariance if any point x in the boundary of ϑ is pointing into ϑ.

Let $\partial\breve{\Omega}$ denotes the boundary of system (1) where it consists of the 5N hyperplanes:

$$H_i = \{(S_1, \dots, S_N, L_1, \dots, L_N, B_1, \dots, B_N, C_1, \dots, C_N)^T \in \Omega \mid S_i = 0\}, \quad 1 \leq i \leq N$$

$$H_{N+i} = \{(S_1, \dots, S_N, L_1, \dots, L_N, B_1, \dots, B_N, C_1, \dots, C_N)^T \in \Omega \mid L_i = 0\}, \quad 1 \leq i \leq N$$

$$H_{2N+i} = \{(S_1, \dots, S_N, L_1, \dots, L_N, B_1, \dots, B_N, C_1, \dots, C_N)^T \in \Omega \mid B_i = 0\}, \quad 1 \leq i \leq N$$

$$H_{3N+i} = \{(S_1, \dots, S_N, L_1, \dots, L_N, B_1, \dots, B_N, C_1, \dots, C_N)^T \in \Omega \mid C_i = 0\}, \quad 1 \leq i \leq N$$

$$H_{4N+i} = \{(S_1, \dots, S_N, L_1, \dots, L_N, B_1, \dots, B_N, C_1, \dots, C_N)^T \in \Omega \mid S_i + L_i + B_i + C_i = 1\}, \quad 1 \leq i \leq N$$

For $1 \leq i \leq N$, H_i , H_{N+i} , H_{2N+i} , H_{3N+i} , $and \;\; H_{4N+i}$ have

$$n_i = (0, \dots, 0, -1\,, 0, \dots, 0)^T,$$

$$n_{N+i} = (0, \dots, 0, -1, 0, \dots, 0)^T,$$

$$n_{2N+i} = (0, \dots, 0, -1, 0, \dots, 0)^T,$$

$$n_{3N+i} = (0, \dots, 0, -1, 0, \dots, 0)^T, and$$

$$n_i = (0, \dots, 0, 1, 0, \dots, 0, 1, 0, \dots, 0, 1, 0, \dots, 0)^T$$

as their respective outer normal vectors.

Let $x^* = (S_1^*, \dots, S_N^*, L_1^*, \dots, L_N^*, B_1^*, \dots, B_N^*, C_1^*, \dots, C_N^*)$ be a smooth point of $\partial\Omega$. It is distinguished among 5 possibilities:

Case 1: some $S_i^* = 0$, $0 < i < N$, then $< F(x^*), n_i >= 0$

Case 2: some $L_i^* = 0$, $0 < i < N$, then $< F(x^*), n_{N+i} >= 0$

Case 3: some $B_i^* = 0$, $0 < i < N$, then $< F(x^*), n_{2N+i} >= -L_i(t)\rho\sum_j a_{ij}(1 - S_j) \leq 0$

Case 4: some $C_i^* = 0$, $0 < i < N$, then $< F(x^*), n_{3N+i} >= -S_i(t)\gamma_i - \alpha_i L_i(t) \leq 0$

Case 5: some $S_i^* + L_i^* + B_i^* + C_i^* = 1$, $0 < i < N$, then $< F(x^*), n_{4N+i} >= 0$

Combining above discussion prove that $\breve{\Omega}$ is positive invariant set.

3.3.2 Equilibrium Points

Equilibrium points impose the system to keep the states forever as the system is entered these states. This requires all differential equations to be zero and this happens only when all latent and susceptible nodes are equal to zero.

$F(X(t)) = 0$ if only if $\quad L_i = S_i = 0 \quad \forall \quad 0 < i \leq N$

3.3.3 Stability

Because the system is nonlinear ordinary differential system, the eigenvalues of the system to determine its stability cannot be directly found. Equilibrium point is considered a solution for the system and the Jacobian matrix at the equilibrium point is used to check stability.

Before building Jacobian matrix, system (1) will be reduced to simplify stability analysis. Obviously, system (1) does not depend on $\dot{B}_i$ and $\dot{C}_i$, uncoupled equations, differential equations $\dot{S}_i$and $\dot{L}_i$ can be solved without solving $\dot{B}_i$ and $\dot{C}_i$. Therefore, if this initial condition $S_i + L_i + B_i + C_i = 1$ is guaranteed and system equations $\frac{dS_i(t)}{dt} + \frac{dL_i(t)}{dt} + \frac{dB_i(t)}{dt} + \frac{dB_i(t)}{dt} = 0$ then explore stability at equilibrium points of S_i and L_i is enough.

Our reduced system

$$\left.\begin{aligned}\frac{dS_i(t)}{dt} &= -S_i(t)\beta\textstyle\sum_j a_{ij}L_j(t) - S_i(t)\gamma_i(t)\\ \frac{dL_i(t)}{dt} &= S_i(t)\beta\textstyle\sum_j a_{ij}L_j(t) - L_i(t)\rho\textstyle\sum_j a_{ij}(1 - S_j(t)) - L_i(t)\alpha_i(t)\end{aligned}\right\} \quad \textbf{(3)}$$

Let: $X(t) = (S_1, \dots, S_N, L_1, \dots, L_N)^T$ where $X_N = S_N$, $X_{2N} = L_N$

$$\frac{dX(t)}{dt} = F(X(t))$$

Jacobian matrix: $\left.\begin{bmatrix} \frac{df_1}{dx_1} & \cdots & \frac{df_1}{dx_{2N}} \\ \vdots & \ddots & \vdots \\ \frac{df_{2N}}{dx_1} & \cdots & \frac{df_{2N}}{dx_{2N}} \end{bmatrix}\right|_{S_i = L_i = 0}$

For this model:

$$\left.\frac{df_i}{dx_i}\right|_{S=L=0} = \frac{d}{dS_i}\left(\frac{dS_i}{dt}\right)\Big|_{S=L=0} = \left|-\beta\textstyle\sum_j a_{ij}L_j(t) - \gamma_i\right|_{S=L=0} = -\gamma_i \;\;,\; \forall \quad 1 \le i \le N$$

$$\left.\frac{df_i}{dx_m}\right|_{S=L=0} = \frac{d}{dS_m}\left(\frac{dS_i}{dt}\right)\Big|_{S=L=0} = 0 \;,\; \forall \;\; i \neq m \quad 1 \le i \le N \;\;,\;\; 1 \le m \le N$$

$$\left.\frac{df_i}{dx_m}\right|_{S=L=0} = \frac{d}{dL_p}\left(\frac{dS_i}{dt}\right)\Big|_{S=L=0} = 0 \;,\; \forall \quad 1 \le i \le N \;,\; N+1 \le m \le 2N \;,\; 1 \le p \le N$$

$$\left.\frac{df_i}{dx_m}\right|_{S=L=0} = \frac{d}{dS_m}\left(\frac{dL_p}{dt}\right)\Big|_{S=L=0} = 0 \;,\forall \;\; N+\;1 \le i \le 2N \;,\; 1 \le m \le N \;,\; 1 \le p \le N$$

$$\left.\frac{df_m}{dx_m}\right|_{S=L=0} = \frac{d}{dL_i}\left(\frac{dL_i}{dt}\right)\Big|_{S=L=0} = -\rho\textstyle\sum_j a_{ij} \;-\; \alpha_i \;,\; \forall \;\; 1 \le i \le N \;,\;\; N+1 \le m \le 2N$$

$$\left.\frac{df_i}{dx_m}\right|_{S=L=0} = \frac{d}{dL_p}\left(\frac{dL_p}{dt}\right)\Big|_{S=L=0} = 0 \,,\; \forall \;\; i \neq m \quad N+1 \le i \le 2N \;,\; N+1 \le m \le 2N \;\;,\; 1 \le p \le N$$

To make easy to understand, Jacobian matrix will be divided into this form:

$\begin{bmatrix} A & B \\ C & D \end{bmatrix}$, A, B, C, and D all $N \times N$ matrices.

Then, from the above equations, it can be built A, B, C, and D matrices as follow:

$$A = \begin{bmatrix} -\gamma_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & -\gamma_N \end{bmatrix} \qquad B = C = \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix}$$

$$D = \begin{bmatrix} -\rho\sum_j a_{1j} \;-\; \alpha_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & -\rho\sum_j a_{Nj} \;-\; \alpha_N \end{bmatrix}$$

The eigenvalues λ of the system can obtained from the following formula:

$|\lambda I - A| = 0$, the determinant of λ multiplied by the identity matrix I, A in this case is the Jacobian matrix at equilibrium point.

$$A = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

$$\left|\lambda I - \begin{bmatrix} A & B \\ C & D \end{bmatrix}\right| =$$

$$\left|\begin{matrix} \begin{bmatrix} \lambda + \gamma_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda + \gamma_N \end{bmatrix} & \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix} & \begin{bmatrix} \lambda + \rho \sum_j a_{1j} + \alpha_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda + \rho \sum_j a_{Nj} + \alpha_N \end{bmatrix} \end{matrix}\right|$$

$$=(\lambda + \gamma_1)(\lambda + \gamma_2) \ldots (\lambda + \gamma_N)(\lambda + \rho \textstyle\sum_j a_{1j} + \alpha_1)(\lambda + \rho \sum_j a_{2j} + \alpha_2) \ldots (\lambda + \rho \sum_j a_{Nj} + \alpha_N) = 0$$

$$\Rightarrow \lambda_i = -\gamma_i \text{ or } \lambda_m = -\rho \textstyle\sum_j a_{ij} - \alpha_i \qquad 1 \leq i \leq N \ , \ N+1 \leq m \leq 2N$$

As γ_i, α_i, ρ are nonnegative, all eigenvalues are negative. As a result, the system is asymptotically stable.

3.4 Study of The Optimal Control

In this section the optimal control of the following cost/objective function will be studied.

$$minimize_{u(.)\in\mathcal{U}} \ J(u(.)) = \int_0^T L(x(t), u(t)) \, dt \qquad \textbf{(4)}$$

$$L(x(t), u(t)) = \textstyle\sum_i \left(B_i + \frac{1}{2} p \gamma_i(t) + \frac{1}{2} q \alpha_i(t)\right) \qquad (5)$$

$$\left.\begin{aligned}
\frac{dS_i(t)}{dt} &= -S_i(t)\beta\textstyle\sum_j a_{ij}L_j(t) - S_i(t)\gamma_i(t) \\
\frac{dL_i(t)}{dt} &= S_i(t)\beta\textstyle\sum_j a_{ij}L_j(t) \; - \; L_i(t)\rho\textstyle\sum_j a_{ij}(1 - S_j(t)) \; - \; L_i(t)\alpha_i(t) \\
\frac{dB_i(t)}{dt} &= \; L_i(t)\rho\textstyle\sum_j a_{ij}(1 - S_j(t))
\end{aligned}\right\} \quad \textbf{(6)}$$

$$x = (S_1, \dots, S_N, L_1, \dots, L_N, B_1, \dots, B_N)^{\,T}$$

$$f(x, u) = \frac{dx}{dt}$$

$$\mathcal{U} = \{u(.) \in (L^2[0, T])| \; \underline{\gamma_i} \leq \gamma_i(.) \leq \overline{\gamma_i} \;, \underline{\alpha_i} \leq \alpha_i(.) \leq \overline{\alpha_i} \;, \; 1 \leq i \leq N\,\}$$

3.4.1 Existing of optimal control

To examine existing of optimal control for problem (3) & (4), (Kamien & Schwartz, 2012; Liberzon, 2011) mentioned if the problem satisfies the following six conditions and the system is positive invariant then there is existing an optimal control solution.

a. There is $u(.) \in \mathcal{U}$ such that system (3) is solvable,
b. $\mathcal{U}$ is convex,
c. $\mathcal{U}$ is closed,
d. $f(x, u)$ is bounded by a linear function in x,
e. $L(x, u)$ is convex in $\mathcal{U}$, and
f. $L(x, u) \geq c_1\|u\|_2^{\mathcal{P}} + c_2$ for some $\mathcal{P} > 1$, $c_1 > 0$.

Proofs:

a. It is approved above that Ω is positively invariant for $x(0) \in \Omega$. Also, here $f(x, \bar{u})$ is continuously differentiable. Hence, following the Continuation

Theorem for differential equations (Robinson, 2012), there is $u(.) \in \mathcal{U}$ such that system (4) is solvable.

b. The admissible set $\mathcal{U}$ is convex. Let

$$u(.)^{(1)} = (\gamma_1(.)^{(1)}, \dots, \gamma_N(.)^{(1)}, \alpha_1(.)^{(1)}, \dots, \alpha_N(.)^{(1)})^T \in \mathcal{U}$$

$$u(.)^{(2)} = (\gamma_1(.)^{(2)}, \dots, \gamma_N(.)^{(2)}, \alpha_1(.)^{(2)}, \dots, \alpha_N(.)^{(2)})^T \in \mathcal{U}$$

$$0 < \mathcal{G} < 1$$

As $(L^2[0,T])^{2N}$ is a real vector space, then

$$(1-\mathcal{G})u(.)^{(1)} + \mathcal{G}u(.)^{(2)} \in (L^2[0,T])^{2N}$$

Can be illustrated as:

$$\underline{\gamma} \leq (1-\mathcal{G})\gamma_i(.)^{(1)} + \mathcal{G}\gamma_i(.)^{(2)} \leq \overline{\gamma} \quad , \quad \underline{\alpha} \leq (1-\mathcal{G})\alpha_i(.)^{(1)} + \mathcal{G}\alpha_i(.)^{(2)} \leq \overline{\alpha}$$

(Rudin, 1964), So admissible set $\mathcal{U}$ is convex.

c. The admissible set $\mathcal{U}$ is closed. Let

$$u(.) = (\gamma_1(.), \dots, \gamma_N(.), \alpha_1(.), \dots, \alpha_N(.))^T$$

$$u^{(n)}(.) = ({\gamma_1}^{(n)}(.), \dots, {\gamma_N}^{(n)}(.), {\alpha_1}^{(n)}(.), \dots, {\alpha_N}^{(n)}(.))^T$$

$u(.)$ is a limit point in $\mathcal{U}$ and $u^{(n)}(.)$ is a sequence of points in $\mathcal{U}$. It is known from completeness of $(L^2[0,T])^{2N}$ that

$$\lim_{n\to\infty} u^n(.) = u(.) \in (L^2[0,T])^{2N}$$

So, by observing the following, $\mathcal{U}$ is closed

$$\underline{\gamma} \leq \gamma_i(.) = \lim_{n\to\infty} {\gamma_i}^n(.) \leq \overline{\gamma} \qquad \underline{\alpha} \leq \alpha_i(.) = \lim_{n\to\infty} {\alpha_i}^n(.) \leq \overline{\alpha}$$

d. $f(x,u)$ is bounded by a linear function in x.

Can be proved by observation of $f(x,u)$ as follow

$$-S_i\beta\sum_j a_{ij} - S_i\overline{\gamma_i} \leq -S_i\beta\sum_j a_{ij}L_j - S_i\gamma_i \leq -S_i\underline{\gamma_i}$$

$- L_i(t)\rho\sum_j a_{ij} - L_i(t)\overline{\alpha_i} \leq S_i(t)\beta\sum_j a_{ij}L_j(t) - L_i(t)\rho\sum_j a_{ij}(1-S_j) - L_i(t)\alpha_i \leq S_i(t)\beta\sum_j a_{ij}$

$$0 \leq L_i\rho\sum_j a_{ij}(1-S_j) \leq L_i\rho\sum_j a_{ij}$$

Proof is completed.

e. $L(x,u)$ is convex on $\mathcal{U}$. Let

$$u^{(1)}(t) = (\gamma_1{}^{(1)}(t),\dots,\gamma_N{}^{(1)}(t),\alpha_1{}^{(1)}(t),\dots,\alpha_N{}^{(1)}(t))^T \in \mathcal{U}$$

$$u^{(2)}(t) = (\gamma_1{}^{(2)}(t),\dots,\gamma_N{}^{(2)}(t),\alpha_1{}^{(2)}(t),\dots,\alpha_N{}^{(2)}(t))^T \in \mathcal{U}$$

$L\left(x,(1-\mathcal{G})u^{(1)}(t)+\mathcal{G}u^{(2)}(t)\right) = \sum_i\left[B_i + \frac{1}{2}p\left[(1-\mathcal{G})\gamma_i{}^{(1)}(t)+\mathcal{G}\gamma_i{}^{(2)}(t)\right]^2 + \frac{1}{2}q\left[(1-\mathcal{G})\alpha_i{}^{(1)}(t)+\mathcal{G}\alpha_i{}^{(2)}(t)\right]^2\right] \leq \sum_i\left[B_i + \frac{1}{2}p\left[(1-\mathcal{G})\left[\gamma_i{}^{(1)}(t)\right]^2 + \mathcal{G}\left[\gamma_i{}^{(2)}(t)\right]^2\right] + \frac{1}{2}q\left[(1-\mathcal{G})\left[\alpha_i{}^{(1)}(t)\right]^2 + \mathcal{G}\left[\alpha_i{}^{(2)}(t)\right]^2\right]\right] \leq (1-\mathcal{G})L(x,u^{(1)}(t)) + \mathcal{G}L(x,u)$

(Rudin, 1964), Proof is complete.

f. $L(x,u) \geq c_1\|u\|_2^{\mathcal{P}} + c_2$, for some $\mathcal{P} > 1$, $c_1 > 0$, c_2

Proof. Let $c_1 = \frac{min_i\{p,q\}}{2}$, $\mathcal{P} = 2$, $c_2 = 0$, $\Longrightarrow \frac{min_i\{p,q\}}{2} \times \|u\|_2^2 \leq L(x,u)$

From (a. to f.) the optimal control problem (3) and (4) has an optimal control solution.

3.4.2 Optimality System

After making sure that the optimal control problem (3) & (4) has an optimal solution, here deriving of the optimal control system will be done. First of all, Hamiltonian equation will be established. Then, find co-states and controller conditions for the optimal problem.

$$H = L(x,u) + \sum_i \lambda_i f_i(x,u) = L\big(x(t),u(t)\big) + \sum_i \lambda_i \frac{dS_i}{dt} + \sum_i \mathcal{Y}_i \frac{dL_i}{dt} + \sum_i \mathcal{Z}_i \frac{dB_i}{dt}$$

$$\begin{aligned} H = {} & \sum_i \left(B_i + \frac{1}{2}p\gamma_i(t) + \frac{1}{2}q\alpha_i(t)\right) + \sum_i \lambda_i \left(-S_i(t)\beta \sum_i a_{ij}L_j(t) - S_i(t)\gamma_i(t)\right) \\ & + \sum_i \mathcal{Y}_i \left(S_i(t)\beta \sum_j a_{ij}L_j(t) - L_i(t)\rho \sum_j a_{ij}\left(1 - S_j(t)\right) \right. \\ & \left. - L_i(t)\alpha_i(t) \right) + \sum_i \mathcal{Z}_i \left(L_i(t)\rho \sum_j a_{ij}\big(1 - S_j(t)\big) \right) \end{aligned}$$

λ_i , $\mathcal{Y}_i$, and $\mathcal{Z}_i$ for $1 \le i \le N$, all are co-states. Hamiltonian function has the variables S_i , L_i , B_i , λ_i , $\mathcal{Y}_i$, $\mathcal{Z}_i$, γ_i , and α_i. (Liberzon, 2011) Pontryagin Minimum Principle says there are functions $\lambda_i^*(t)$, $\mathcal{Y}_i^*(t)$, and $\mathcal{Z}_i^*(t)$ such that

$$\frac{d\lambda_i^*}{dt} = -\frac{\partial H^*}{\partial S_i} = \lambda_i\beta \sum_j a_{ij}L_j + \lambda_i\gamma_i - \mathcal{Y}_i\beta \sum_j a_{ij}L_j - \rho \sum_j a_{ij}L_j\mathcal{Y}_j + \rho \sum_j a_{ij}L_j\mathcal{Z}_i$$

$$\begin{aligned} \frac{d\mathcal{Y}_i^*}{dt} = -\frac{\partial H^*}{\partial L_i} = {} & \beta \sum_j a_{ij}S_j\lambda_j - \beta \sum_j a_{ij}S_j\mathcal{Y}_j + \mathcal{Y}_i\rho \sum_j a_{ij}\big(a - S_j\big) + \mathcal{Y}_i\alpha_i \\ & - \mathcal{Z}_i\rho \sum_j a_{ij}(1 - S_j) \end{aligned}$$

$$\frac{d\mathcal{Z}_i^*}{dt} = -\frac{\partial H^*}{\partial B_i} = -1$$

By using the optimality condition:

$$H^* = H(S^*(.), L^*(.), B^*(.), \lambda^*(.), \mathcal{Y}^*(.), \mathcal{Z}^*(.), u^*(.))$$
$$= \min_{u(.)\in\mathcal{U}} H(S^*(.), L^*(.), B^*(.), \lambda^*(.), \mathcal{Y}^*(.), \mathcal{Z}^*(.), u(.))$$

then $u(.)$ For $1 \le i \le N\,,\ 1 \le t \le T$ By either

$$\frac{\partial H(S,L,B,\lambda,\mathcal{Y},\mathcal{Z})}{\partial \gamma_i} = p\gamma_i^*(t) - \lambda_i(t)S_i(t) = 0 \implies \gamma_i^* = \frac{1}{p}\lambda_i(t)S_i(t)$$

or $\gamma_i^* = \overline{\gamma_i}$ or $\gamma_i^* = \underline{\gamma_i}$

$$\frac{\partial H(S,L,B,\lambda,\mathcal{Y},\mathcal{Z})}{\partial \alpha_i} = q\alpha_i^* - \mathcal{Y}_i(t)L_i(t) = 0 \implies \alpha_i^* = \frac{1}{p}\mathcal{Y}_i(t)L_i(t)$$

or $\alpha_i^* = \overline{\alpha_i}$ or $\alpha_i^* = \underline{\alpha_i}$

Combining the above equations, the optimality system will be as below:

$$\left.\begin{array}{l}
\frac{dS_i(t)}{dt} = -S_i(t)\beta\sum_j a_{ij}L_j(t) - S_i(t)\gamma_i(t) \\[2ex]
\frac{dL_i(t)}{dt} = S_i(t)\beta\sum_j a_{ij}L_j(t) \; - \; L_i(t)\rho\sum_j a_{ij}(1 - S_j(t)) \; - \; L_i(t)\alpha_i(t) \\[2ex]
\frac{dB_i(t)}{dt} = \; L_i(t)\rho\sum_j a_{ij}(1 - S_j(t)) \\[2ex]
\frac{d\lambda_i(t)}{dt} = (\lambda_i(t) - \mathcal{Y}_i(t))\beta\sum_j a_{ij}L_j(t) + \rho\sum_j a_{ij}L_j(t)(\mathcal{Z}_j(t) - \mathcal{Y}_j(t)) + \lambda_i(t)\gamma_i(t) \\[2ex]
\frac{d\mathcal{Y}_i(t)}{dt} = \beta\sum_j a_{ij}S_j(t)(\lambda_j(t) - \mathcal{Y}_j(t)) + (\mathcal{Y}_i(t) - \mathcal{Z}_i(t))\rho\sum_j a_{ij}\left(1 - S_j(t)\right) + \\
\mathcal{Y}_i(t)\alpha_i(t) \\[2ex]
\frac{d\mathcal{Z}_i(t)}{dt} = -1 \\[2ex]
\gamma_i(t) = \max\{\min\left\{\frac{1}{p}\lambda_i(t)S_i(t)\,, \overline{\gamma_i}\right\}, \underline{\gamma_i}\} \qquad\qquad 1 \le i \le N \\[2ex]
\alpha_i(t) = \max\{\min\left\{\frac{1}{p}\mathcal{Y}_i(t)L_i(t)\,, \overline{\alpha_i}\right\}, \underline{\alpha_i}\} \qquad\qquad 0 \le t \le T \\[2ex]
\text{Transversality conditions} \quad \lambda_i(T) = 0\;,\; \mathcal{Y}_i(T) = 0\;,\; \mathcal{Z}_i(T) = 0
\end{array}\right\} \quad \textbf{(7)}$$

3.5 Summary

At his point, a new SLBC computer virus's propagation model is built and analyzed. Its invariant and stability around equilibrium point are proved. Finally, the optimality system is derived.

CHAPTER 4: RESULTS AND DISCUSSION

4.1 Introduction

In this chapter, the properties was discussed in last chapter, like positive invariant and optimality, will be shown. Besides, some examples performed to notice behavior of the model in different scenarios. These examples are divided into two cases. Case 1, the new model will be simulated with zero countermeasure in four examples to see the extent of spreading, effect of changing virus's starting point, immunization effect, and early detection impact. Case 2, compare optimal control solution to constant controls using the cost function to verify effectiveness of the optimal system.

Hint: all the examples below will be in a scale-free Network with 100 nodes. Distribution of node linkages follow power law distribution. Each node supposed to enter the network with four links so each node in the network have at least four connections.

S^*, L^*, B^*, and C^* will denote to average proportion of susceptible, latent, breaking-out, and countermeasure in the network respectively.

$$S^*(t) = \frac{1}{N}\sum_{i=1}^{N} S_i(t)\ , L^*(t) = \frac{1}{N}\sum_{i=1}^{N} L_i(t)\ , B^*(t) = \frac{1}{N}\sum_{i=1}^{N} B_i(t)\ , C^*(t) = \frac{1}{N}\sum_{i=1}^{N} C_i(t)$$

4.2 Equipment

Below simulations were carried out using a laptop with CPU Core i3-4030, 1.9 GHz and memory RAM of 4 GB. MATLAB R2018a was the software used. All the codes for the next examples are placed in Appendix A.

4.3 Case 1

In this part, four examples will exhibit how the computers in the scale-free network will behaves towards different situations. All these examples in case 1. will have zero vaccination and treatment rates (γ and α).

4.3.1 Example 1.

Here the model will be tested with different rates of infection and breaking-out where infection rate is higher than breaking-out rate. Initial values are $S_i(0) = 0.9$, $L_i(0) = 0.1$, and $B_i(0) = C_i(0) = 0$. Figure 4.1 shows $S^*(t)$, $L^*(t)$, and $B^*(t)$ with multiple infection rates β and breaking-out rates ρ. It is clear that the virus will eventually disperse over the whole network.

4.3.2 Example 2.

Now will let virus start from one computer each time of the network to see if there is any distinction between virus start from a popular computer "hub" which has many links and virus start from a computer has low number of connections. Initial values $S_i(0) = 1$, $L_i(0) = 0$, and $B_i(0) = C_i(0) = 0$. For all i except one computer every-time has $S_j(0) = 0$, $L_j(0) = 1$. Figure 4.2 exhibits $S^*(t)$, $L^*(t)$, and $B^*(t)$ in six situations, one-time a node with 39 links/connections be with $L(0) = 1$ and $S(0) = 0$ and another time a node with 29 links be with $L(0) = 1$ and $S(0) = 0$ … etc. It is shown that virus at the end will be infecting all computers with the only different is how fast spreading is. Consequently, in this network topology, virus prevalence does not depend on from which node it starts spreading. Basically, does not matters for virus to hunt either a popular node or any unpopular node. From security point of view, making an administrative computer, in local network, not allowed to use internet for security purposes while other computers free to connect to internet will eventually lead to prevalence of virus as soon as any computer of the local network get infected.

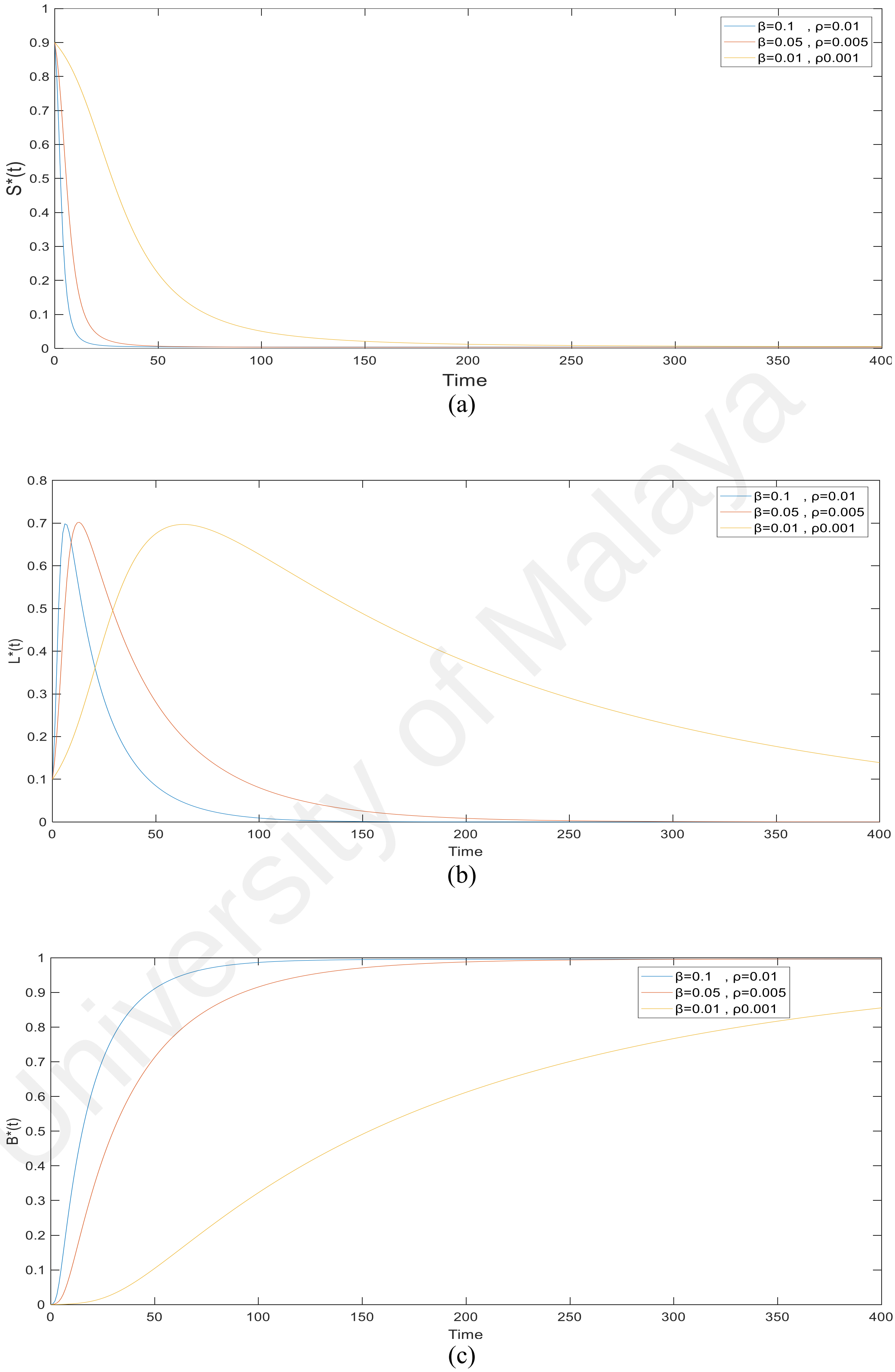


Figure 4.1 Average proportion of (a)Susceptible. (b)Latent. (c)Breaking-out. for different infection and breaking-out rates and zero countermeasure.

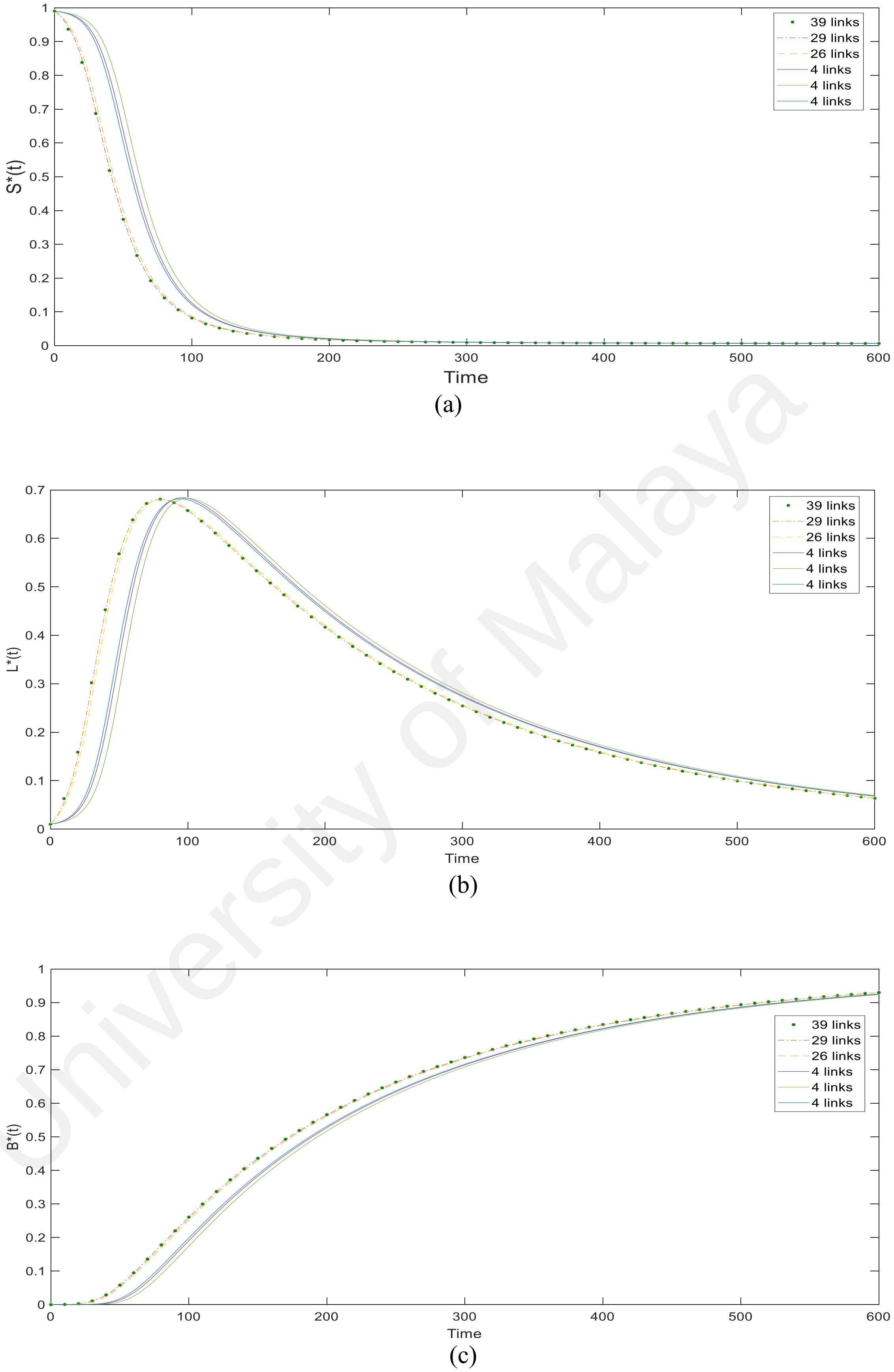


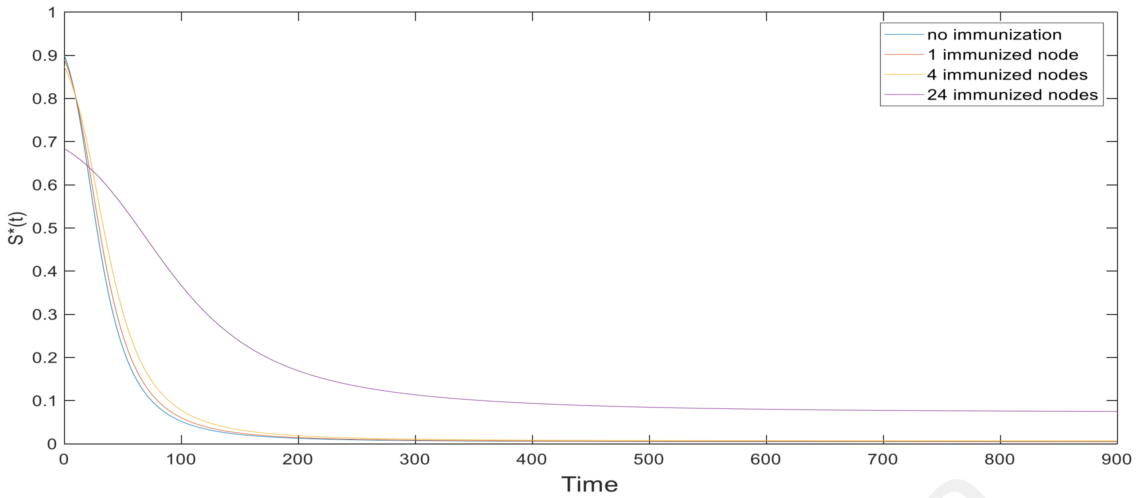
Figure 4.2 Average proportion of (a)Susceptible. (b)Latent. (c)Breaking-out. for various virus starting node depending on node's number of links.

4.3.3 Example 3

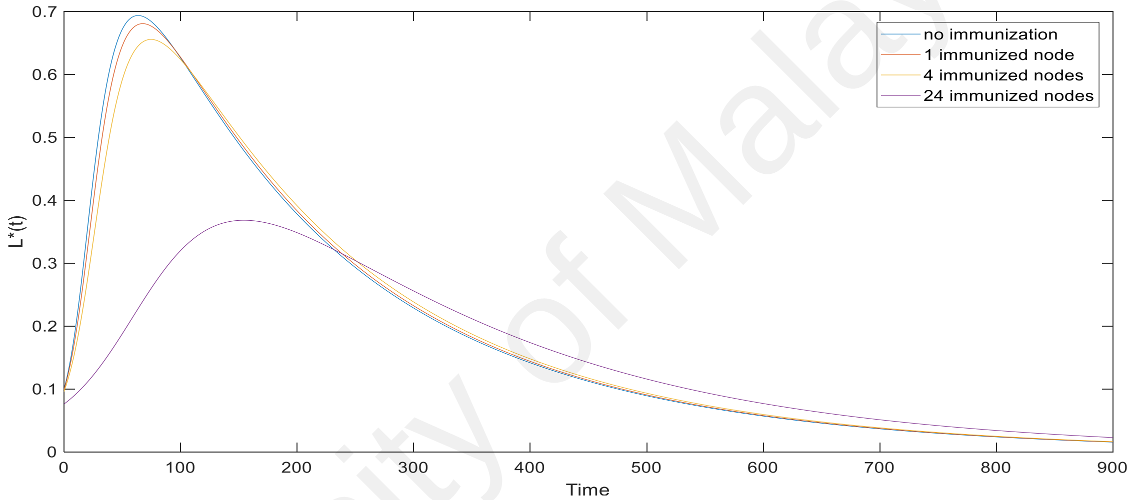
Here, benefits of immunization of hub nodes will be tested. It starts with immunization of one node that has the highest number of connections. Then immunize hubs that have more than twenty connections. Finally, all nodes with ten connections are immunized. Immunization here will be represented by assuming that the node is in the countermeasure compartment since initial values. Figure 4.3 shows the result of simulation in four scenarios. Scenario 1. with no immunized nodes, Scenario 2. The most popular node, with 31 links, is immunized, Scenario 3. highest four hubs (with 31, 28, 21, and 21 links) are immunized, and Scenario 4. all nodes with 10 links and more are immunized (24 nodes immunized, 24% of the network). On the whole, in scale-free network immunization of hubs' nodes will not prevent virus from spreading over rest of the nodes.

4.3.4 Example 4

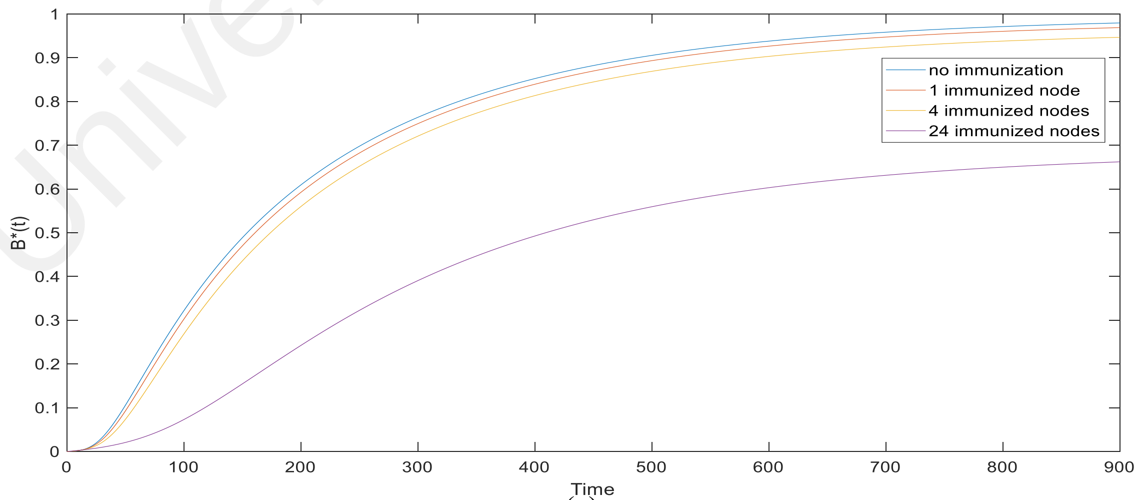
The breaking-out rate will be higher or equal to infection rate. Figure 4.4 shows the result for that. It is noted from the figure that virus will stop spreading without applying countermeasure if the breaking-out rate is higher than infection rate. Here high breaking-out rate can be considered same as an early detection of the virus because if the virus has been detected, either will be treated by user or the computer will be shut-down, so virus not destroying more files, until find solution to it. Consequently, this will prevent virus reaching many computers. Same as in example 2. here virus starting node does not matter in its spreading extent. $\beta = 0.01$ $\rho = 0.001$.



(a)

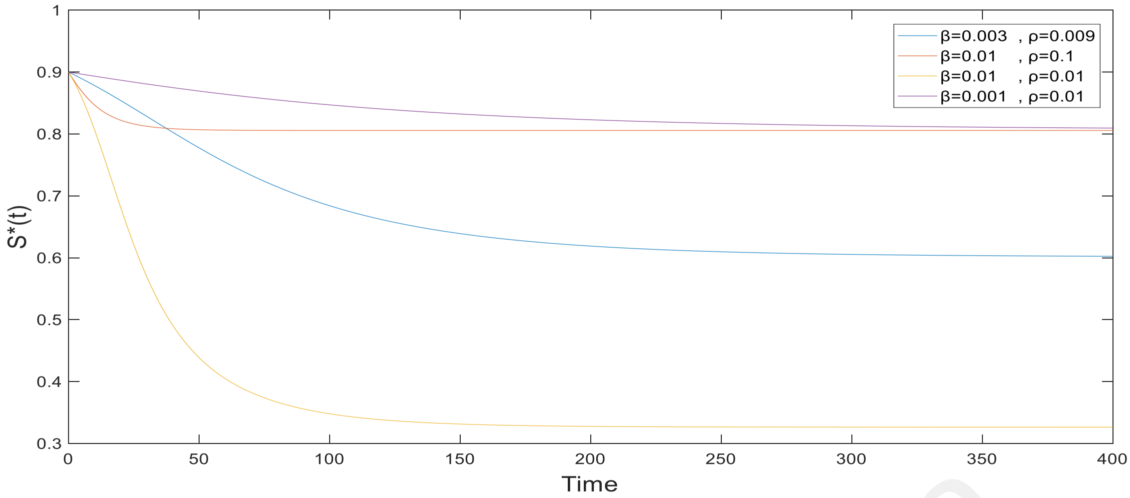


(b)

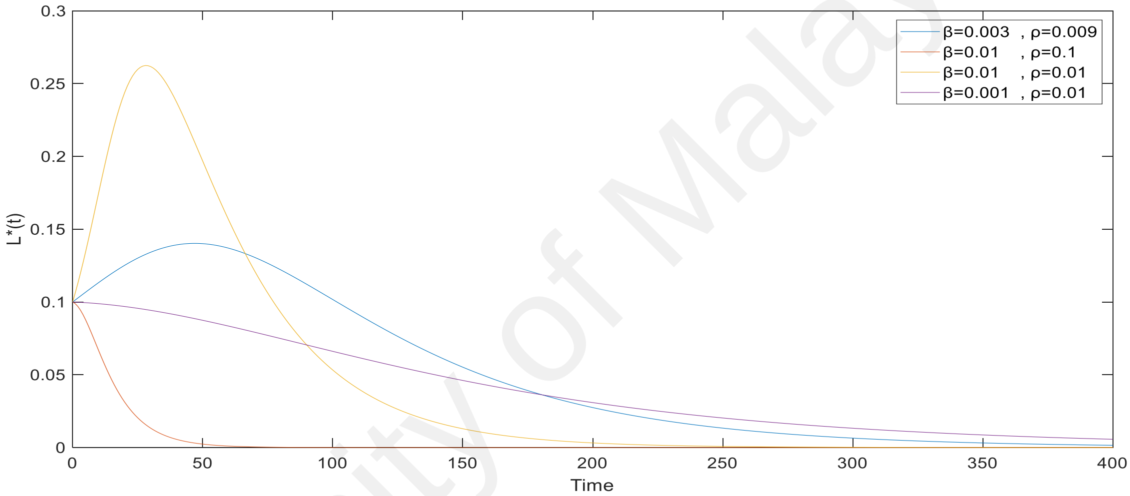


(c)

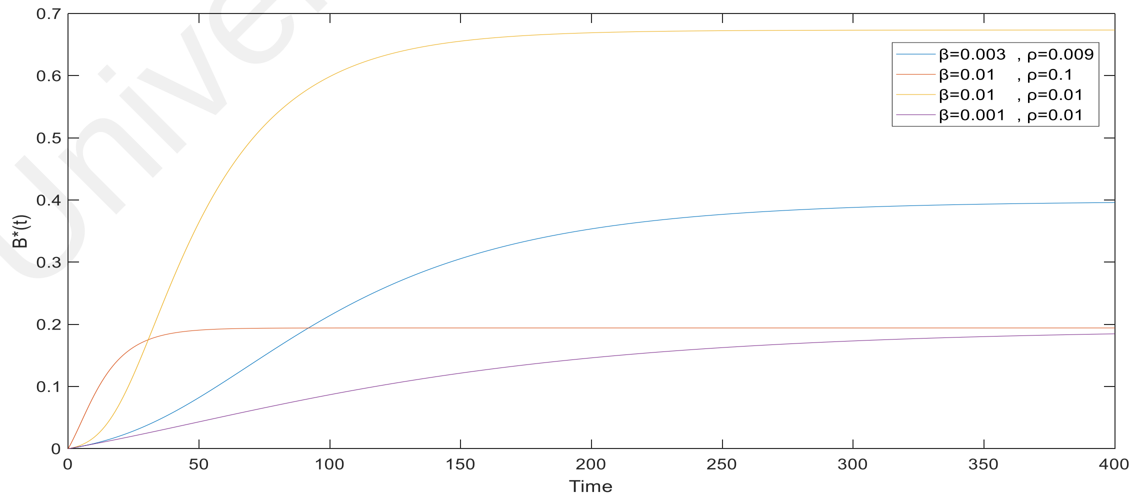
Figure 4.3 Average proportion of (a)Susceptible. (b)Latent. (c)Breaking-out. for immunization of various nodes.



(a)



(b)



(c)

Figure 4.4 Average proportion of (a)Susceptible. (b)Latent. (c)Breaking-out. with breaking-out rate (ρ) higher or equal to infection rate (β).

4.4 Case 2

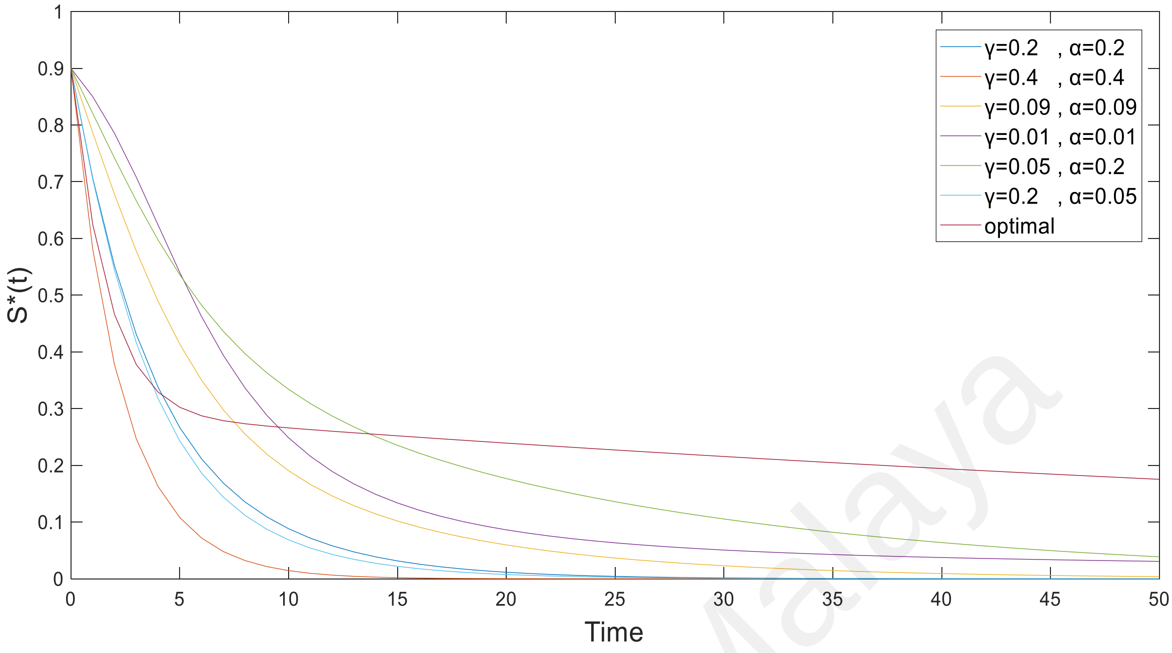
Vaccination and treatment rates (γ and α) will take some values in the next example to compare them with the optimal rates. There is no specific values can be found for these rates but here these rates will take values as: ($0.4 \leq \gamma_i \leq 0.01$, $0.4 \leq \alpha_i \leq 0.01$). the minimum bound (0.01) is chosen because values of ($L(t)$) will not be zero easily as MATLAB decrease the value for many decimals below zero so it is needed that the minimum not to be zero to force virus not to burst again, also agree with (X. Zhang & Gan, 2017). If the maximum rate chosen to be more than (0.4), it makes negligible effect on the virus so for that it is chosen to be (0.4), also similar to (L.-X. Yang, Draief, & Yang, 2016).

4.4.1 Example 5

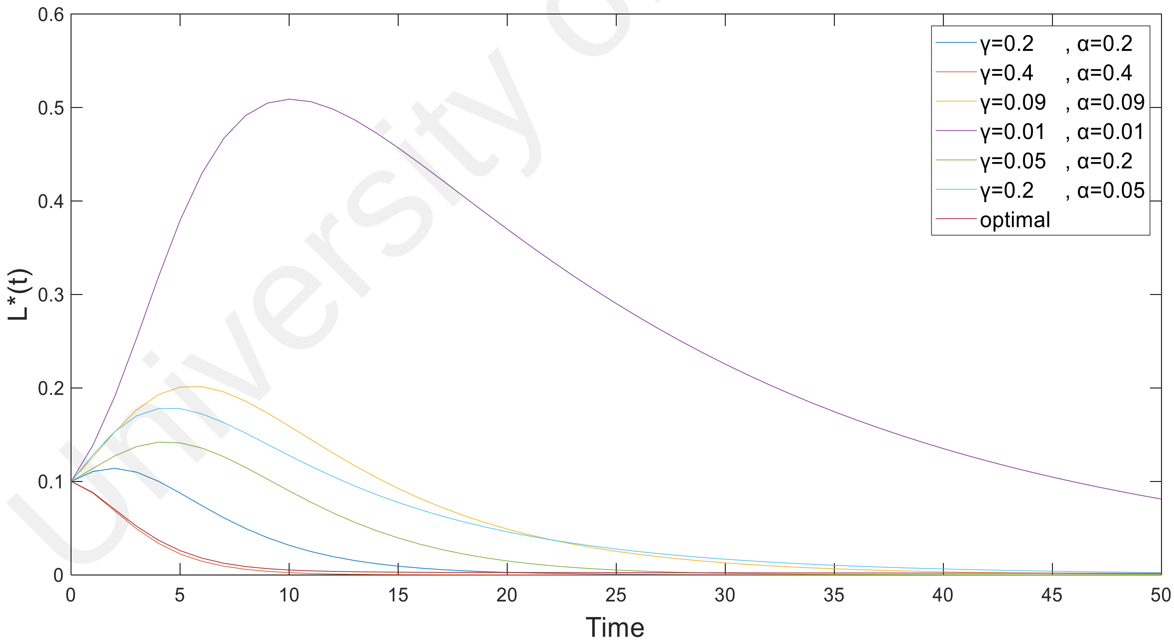
The model will be implemented with infection rate $= 0.05$, breaking-out rate $\rho = 0.009$, various vaccination rate (γ) and treatment rate (α) and finally with the optimal countermeasure. $S^*(t)$ and $L^*(t)$ are shown in Figure 4.5 and $B^*(t)$ and $C^*(t)$ are shown in Figure 4.6. Furthermore, Table 4.1 presents the values of the objective function (J) equation (4) and average proportion of Breaking-out compartment at the end of the time ($B^*(t_f)$) for multiple vaccination and treatment rates. Figure 4.7 illustrates how the average value of optimal vaccination and treatment rates. From that figure, one can notice that vaccination rate, which is for susceptible nodes, does not reach its maximum (0.4) and drops to its minimum after ten seconds unlike the treatment rate, which for latent nodes, starts at maximum (0.4) and stay for a while then reach its minimum after twenty seconds. This may indicate the important of treatment over vaccination and the more focus should be pointed toward latent computers while combating viruses.

Table 4.1 values of the objective function (J) and breaking-out average proportion (B^*) for different countermeasures rates.

	Optimal	$\gamma = 0.2$ $\alpha = 0.2$	$\gamma = 0.4$ $\alpha = 0.4$	$\gamma = 0.09$ $\alpha = 0.09$	$\gamma = 0.01$ $\alpha = 0.01$	$\gamma = 0.05$ $\alpha = 0.2$	$\gamma = 0.2$ $\alpha = 0.05$
$B^*(t_f)$	0.025	0.05	0.025	0.15	0.67	0.07	0.15
J	179.2	400.32	873.63	633.83	2030	404	690

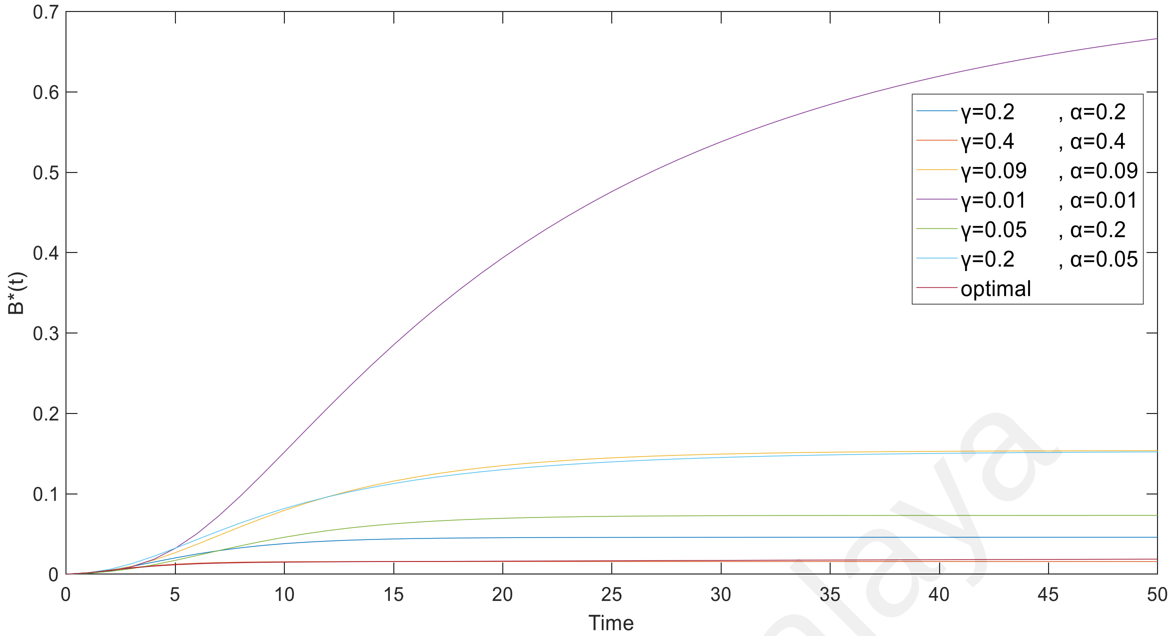


(a)

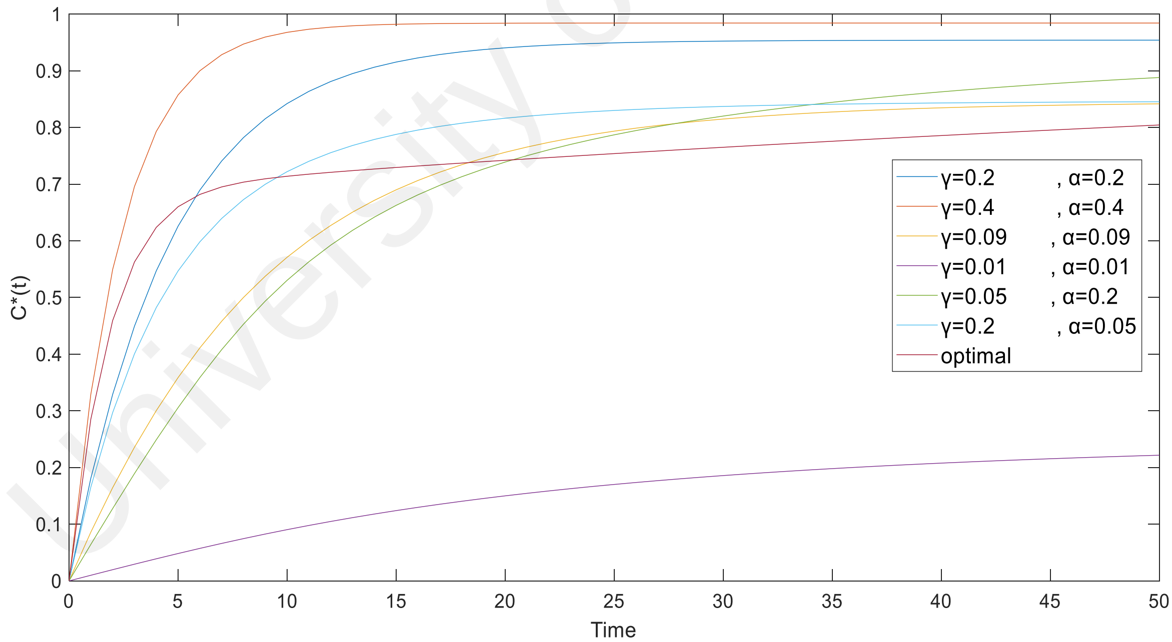


(b)

Figure 4.5 Average proportion of (a)Susceptible. (b)Latent. for different countermeasures rates (vaccination (γ), treatment (α)).

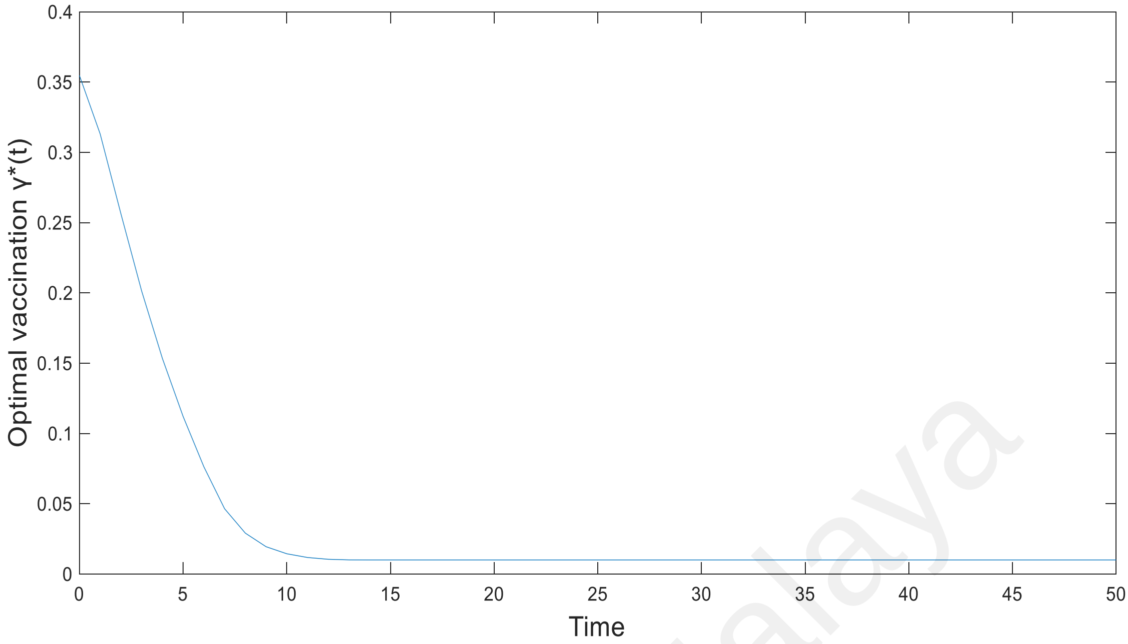


(a)

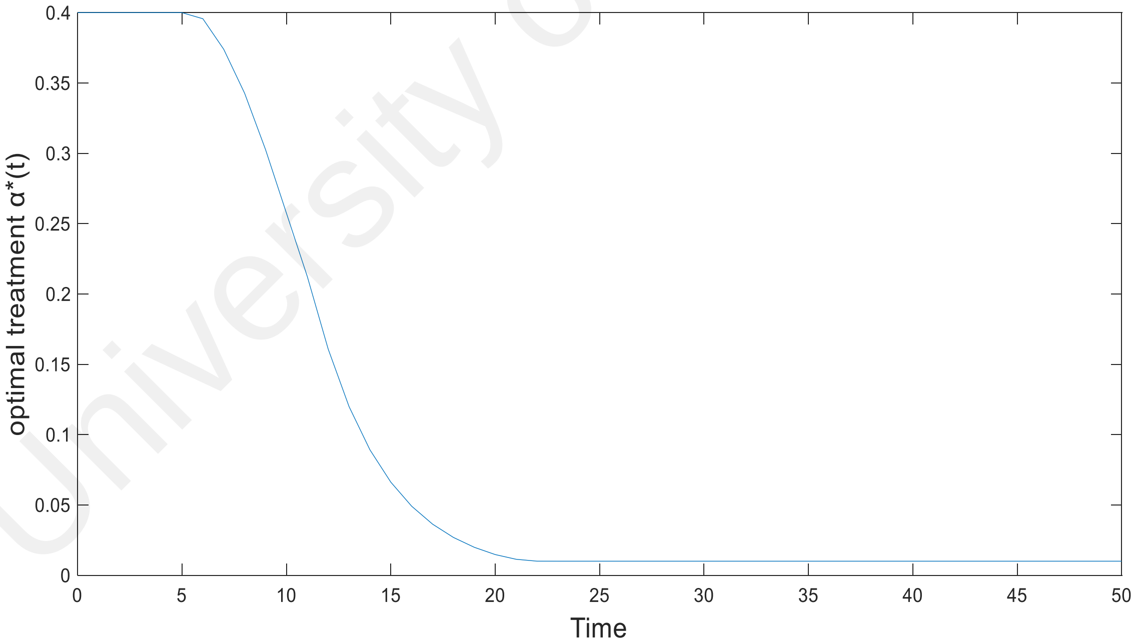


(b)

Figure 4.6 Average proportion of (a)Breaking-out. (b)Countermeasure. for different countermeasures rates (vaccination (γ), treatment (α)).



(a)



(b)

Figure 4.7 Average of optimal countermeasure (a)Vaccination. (b)Treatment. over time.

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

In this research project, a new SLBC (Susceptible-Latent-Breaking-out-Countermeasure) mathematical model for computer virus propagation has been established and its positive invariance, equilibrium point, and stability proved. Optimal control strategy for the model to prevent prevalence of viruses has been built. Moreover, some results appeared throughout some examples conducted on the model and can be concluded as follow: in scale-free network, without countermeasure, viruses will contaminate all the computers in the network despite existing of vaccination nodes and virus's starting point. In addition, effectiveness of the optimal control has been shown through achieving a low level of infections with a low cost of countermeasure.

5.2 Future Work

First, it is worthy to conduct a research on the impact of network topology on the optimal countermeasure strategy. Second, because of impulsive nature of infection and countermeasure, mathematical model and optimal control problem should be transferred to impulsive models. Last but not least, in real-world security level differs from node to another so rates of infection and breaking-out will be different throughout the network.

REFERENCES

Bailey, M., Cooke, E., Jahanian, F., & Watson, D. (2005). The blaster worm: Then and now. *IEEE Security & Privacy, 3*(4), 26-31.

Barabási, A.-L., & Bonabeau, E. (2003). Scale-free networks. *Scientific american, 288*(5), 60-69.

BBC. (2009). Clock ticking on worm attack code. Retrieved from http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/7832652.stm

Benzaouia, A. (2012). *Saturated switching systems* (Vol. 426): Springer Science & Business Media.

Berghel, H. (2001). The Code Red Worm. *Communications of the ACM, 44*(12). doi:10.1145/501317.501328

Boyce, W. E., DiPrima, R. C., & Meade, D. B. (2017). *Elementary Differential Equations and Boundary Value Problems, Loose-Leaf Print Companion*: John Wiley & Sons.

Chen, L.-C., & Carley, K. M. (2004). The impact of countermeasure propagation on the prevalence of computer viruses. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 34*(2), 823-833.

Cohen, F. (1987). Computer viruses. *Computers & Security, 6*(1), 22-35.

Darabi Sahneh, F. (2014). *Spreading processes over multilayer and interconnected networks.* Kansas State University,

Del Rey, A. M., & Sánchez, G. R. (2012). A discrete mathematical model to simulate malware spreading. *International Journal of Modern Physics C, 23*(10), 1250064.

Dong, T., Wang, A., & Liao, X. J. A. M. M. (2016). Impact of discontinuous antivirus strategy in a computer virus model with the point to group. *40*(4), 3400-3409.

Faloutsos, M., Faloutsos, P., & Faloutsos, C. (1999). On power-law relationships of the internet topology. ACM Comp. *Comm. Review, 29*(4).

Itik, M., Salamci, M. U., & Banks, S. P. (2009). Optimal control of drug therapy in cancer treatment. *Nonlinear Analysis: Theory, Methods & Applications, 71*(12), e1473-e1486.

Kamien, M. I., & Schwartz, N. L. (2012). *Dynamic optimization: the calculus of variations and optimal control in economics and management*: Courier Corporation.

Kephart, J. O., & White, S. R. (1992). Directed-graph epidemiological models of computer viruses. In *Computation: the micro and the macro view* (pp. 71-102): World Scientific.

Khadraoui, S., Harrou, F., Nounou, H. N., Nounou, M. N., Datta, A., & Bhattacharyya, S. P. (2016). A measurement-based control design approach for efficient cancer chemotherapy. *Information Sciences, 333*, 108-125.

Liang, Y. M. K. (2010). Introduction to Computer Virus and Preventive Measures [J]. *Computer Study, 1*.

Liberzon, D. (2011). *Calculus of variations and optimal control theory: a concise introduction*: Princeton University Press.

Meisel, M., Pappas, V., & Zhang, L. (2010). A taxonomy of biologically inspired research in computer networking. *Computer Networks, 54*(6), 901-916.

Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., & Weaver, N. (2003). Inside the slammer worm. *IEEE Security & Privacy*(4), 33-39.

Moreno, Y., Pastor-Satorras, R., & Vespignani, A. (2002). Epidemic outbreaks in complex heterogeneous networks. *The European Physical Journal B-Condensed Matter and Complex Systems, 26*(4), 521-529.

Murray, R. M. (2017). *A mathematical introduction to robotic manipulation*: CRC press.

Norton_Team. (2016). The 8 Most Famous Computer Viruses of All Time. Retrieved from https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html

Pagliery, J. (2015). The inside story of the biggest hack in history. *CNN Money, 5*.

Pastor-Satorras, R., & Vespignani, A. (2001). Epidemic dynamics and endemic states in complex networks. *Physical Review E, 63*(6), 066117.

Pérez García, H., Alfonso-Cendón, J., Sánchez González, L., Quintián, H., & Corchado, E. (2018). *International Joint Conference SOCO'17-CISIS'17-ICEUTE'17 León, Spain, September 6–8, 2017, Proceeding*.

Ray, D. A., Ward, C. B., Munteanu, B., Blackwell, J., Hong, X., & Li, J. (2007). *Investigating the Impact of Real-World Factors on Internet Worm Propagation*, Berlin, Heidelberg.

Robinson, R. C. (2012). *An introduction to dynamical systems: continuous and discrete* (Vol. 19): American Mathematical Soc.

Rudin, W. (1964). *Principles of mathematical analysis* (Vol. 3): McGraw-hill New York.

Serazzi, G., & Zanero, S. (2003). *Computer virus propagation models.* Paper presented at the International Workshop on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems.

Staniford, S., Paxson, V., & Weaver, N. (2002). *How to Own the Internet in Your Spare Time.* Paper presented at the USENIX security symposium.

Wang, Y., Chakrabarti, D., Wang, C., & Faloutsos, C. (2003). *Epidemic spreading in real networks: An eigenvalue viewpoint.* Paper presented at the 22nd International Symposium on Reliable Distributed Systems, 2003. Proceedings.

Whalley, I., Arnold, B., Chess, D., Morar, J., Segal, A., & Swimmer, M. (2000). An environment for controlled worm replication and analysis. *IBM TJ Watson Research Center, 37*.

White, S. R. (1998). *Open Problems in Computer Virus Research*. Paper presented at the Virus Bulletin, Munich Germany.

Yang, L.-X., Draief, M., & Yang, X. (2016). The optimal dynamic immunization under a controlled heterogeneous node-based SIRS model. *Physica A: Statistical Mechanics and its Applications, 450*, 403-415. doi:10.1016/j.physa.2016.01.026

Yang, L.-X., & Yang, X. (2014). The spread of computer viruses over a reduced scale-free network. *Physica A: Statistical Mechanics and its Applications, 396*, 173-184. doi:10.1016/j.physa.2013.11.026

Yang, L.-X., Yang, X., Zhu, Q., & Wen, L. (2013). A computer virus model with graded cure rates. *Nonlinear Analysis: Real World Applications, 14*(1), 414-422. doi:10.1016/j.nonrwa.2012.07.005

Yang, X., & Yang, L.-X. (2012). Towards the Epidemiological Modeling of Computer Viruses. *Discrete Dynamics in Nature and Society, 2012*, 1-11.

Yorke, J. A. (1967). Invariance for ordinary differential equations. *Theory of Computing Systems, 1*(4), 353-372.

Youssef, M., & Scoglio, C. (2011). An individual-based approach to SIR epidemics in contact networks. *Journal of theoretical biology, 283*(1), 136-144.

Zhang, C. (2018). Global Behavior of a Computer Virus Propagation Model on Multilayer Networks. *Security and Communication Networks, 2018*, 1-9. doi:10.1155/2018/2153195

Zhang, M., Liu, K., Chen, L., & Li, Z. (2018). State feedback impulsive control of computer worm and virus with saturated incidence. *Math Biosci Eng, 15*(6), 1465-1478.

Zhang, X., & Gan, C. (2017). Optimal and Nonlinear Dynamic Countermeasure under a Node-Level Model with Nonlinear Infection Rate. *Discrete Dynamics in Nature and Society, 2017*, 1-16. doi:10.1155/2017/2836865

Zhang, X., & Gan, C. (2018). Global attractivity and optimal dynamic countermeasure of a virus propagation model in complex networks. *Physica A: Statistical Mechanics and its Applications, 490*, 1004-1018. doi:10.1016/j.physa.2017.08.085

Zhang, Z., & Wang, Y. (2017). Qualitative analysis for a delayed epidemic model with latent and breaking-out over the Internet. *Advances in Difference Equations, 2017*(1). doi:10.1186/s13662-017-1074-9

Zhao, T., & Bi, D. (2017). Hopf bifurcation of a computer virus spreading model in the network with limited anti-virus ability. *Advances in Difference Equations, 2017*(1). doi:10.1186/s13662-017-1243-x

Zhu, Q., & Cen, C. (2017). A Novel Computer Virus Propagation Model under Security Classification. *Discrete Dynamics in Nature and Society, 2017*, 1-11. doi:10.1155/2017/8609082

Zhu, Q., Yang, X., & Ren, J. (2012). Modeling and analysis of the spread of computer virus. *Communications in Nonlinear Science and Numerical Simulation, 17*(12), 5117-5124. doi:10.1016/j.cnsns.2012.05.030