CAPITAL UNIVERSITY OF SCIENCE AND
TECHNOLOGY, ISLAMABAD

Dynamic Analysis of Epidemic Computer Virus Models

by

Zaheer Masood

A thesis submitted in partial fulfillment for the
degree of Doctor of Philosophy

in the

Faculty of Engineering
Department of Electrical Engineering

2020

Dynamic Analysis of Epidemic Computer Virus Models

By

Zaheer Masood

(PE141009)

Dr. Steve S. H. Ling, Senior Lecturer

University of Sydney, Sydney, Australia

(Foreign Evaluator 1)

Dr. Ibrahim Develi, Professor

Erciyes University, Kayseri, Turkey

(Foreign Evaluator 2)

Dr. Raza Samar

(Thesis Supervisor)

Dr. Noor Muhammad Khan

(Head, Department of Electrical Engineering)

Dr. Imtiaz Ahmed Taj

(Dean, Faculty of Engineering)

DEPARTMENT OF ELECTRICAL ENGINEERING

CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

ISLAMABAD

2020

DEDICATED TO MY PARENTS

CAPITAL UNIVERSITY OF SCIENCE & TECHNOLOGY
ISLAMABAD

Expressway, Kahuta Road, Zone-V, Islamabad
Phone:+92-51-111-555-666 Fax: +92-51-4486705
Email: info@cust.edu.pk Website: https://www.cust.edu.pk

CERTIFICATE OF APPROVAL

This is to certify that the research work presented in the thesis, entitled "**Dynamic Analysis of Epidemic Computer Virus Models**" was conducted under the supervision of **Dr. Raza Samar**. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the **Department of Electrical Engineering, Capital University of Science and Technology** in partial fulfillment of the requirements for the degree of Doctor in Philosophy in the field of **Electrical Engineering.** The open defence of the thesis was conducted on **September 02, 2020.**

Student Name : Zaheer Masood (PE141009)

The Examination Committee unanimously agrees to award PhD degree in the mentioned field.

Examination Committee :

(a) External Examiner 1: Dr. Muhammad Anwaar Manzar
Professor
Hamdard University, Islamabad

(b) External Examiner 2: Dr. Aneela Zameer Jaffery
Professor
PIEAS, Islamabad

(c) Internal Examiner : Dr. Muhammad Tahir
Assistant Professor
CUST, Islamabad

Supervisor Name : Dr. Raza Samar
Professor
CUST, Islamabad

Name of HoD : Dr. Noor Muhammad Khan
Professor
CUST, Islamabad

Name of Dean : Dr. Imtiaz Ahmed Taj
Professor
CUST, Islamabad

AUTHOR'S DECLARATION

I, **Zaheer Masood (Registration No. PE141009)**, hereby state that my PhD thesis titled, '**Dynamic Analysis of Epidemic Computer Virus Models**' is my own work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/ world.

At any time, if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my PhD Degree.

Z. Masood.

(**Zaheer Masood**)

Dated: 2 September, 2020

Registration No : PE141009

PLAGIARISM UNDERTAKING

I solemnly declare that research work presented in the thesis titled "**Dynamic Analysis of Epidemic Computer Virus Models**" is solely my research work with no significant contribution from any other person. Small contribution/ help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/ cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of PhD Degree, the University reserves the right to withdraw/ revoke my PhD degree and that HEC and the University have the right to publish my name on the HEC/ University Website on which names of students are placed who submitted plagiarized thesis.

Z. Masood.

(**Zaheer Masood**)

Dated: 2. September, 2020

Registration No : PE141009

List of Publications

It is certified that following publication(s) have been made out of the research work that has been carried out for this thesis:-

1. **Masood, Zaheer** and Majeed, Khalid and Samar, Raza and Raja, Muhammad Asif Zahoor, "Design of Epidemic Computer Virus Model with Effect of Quarantine in the Presence of Immunity" *Fundamenta Informaticae*, Vol. 161(3), 2018, PP. 249-73.
2. **Masood, Zaheer** and Samar, Raza and Raja, Muhammad Asif Zahoor, "Design of a Mathematical Model for the Stuxnet Virus in a Network of Critical Control Infrastructure" *Computers & Security*, Vol. 87, 2019, PP. 101565.
3. **Masood, Zaheer** and Samar, Raza and Raja, Muhammad Asif Zahoor, "Design of fractional order epidemic model for future generation tiny hardware implants" *Future Generation Computer Systems*, Vol. 106, 2020, PP 43-54.

Zaheer Masood
(Registration No.PE141009)

Acknowledgements

All praise be to almighty ALLAH who has been bestowing me with his great bounties and enabled me to complete my dissertation. I offer my deepest gratitude to my parents and family who have provided me motivation and relentless support in my entire life. I would like to express my heartiest gratitude to my supervisor Prof. Dr. Raza Samar, Capital University of Science and Technology (CUST) Islamabad. It was a wonderful experience and learning opportunity to work with him as a PhD student. I am really indebted to his kind support and all out help to complete this research work successfully. His continuous encouragement, support and constructive criticism made me able to complete this task. In spite of his administrative and managerial engagements, his dedication, as a supervisor, is highly appreciable. I will always be in debt to him for his efforts to make me a better researcher and a better human being. I would also like to extend my gratitude to the Dean Faculty of Engineering Prof. Dr. Imtiaz Ahmad Taj and Head of Department Prof. Dr. Noor M. Khan and Dr. Fazal ur Rehman for their continuous encouragement and support during the entire span of my stay at CUST. Special thanks to Prof. Dr. Aamer Iqbal Bhatti for technical help and guidance. I am also thankful to Prof. Dr. Muhammad Asif Zahoor Raja for continuous support with devotion and sincerity. I feel honor to express my feeling of appreciation for the support I have received from the members of Research Group, especially, Mr. Khalid Majeed, Dr. Syed Usama, Mr Zohaib Latif who helped me in my research work and documentation of the thesis.

Abstract

In the present arena of digital world and Internet of Things, networks are becoming the target of well-crafted cyber-attacks especially, the incidents related to breach of internal system security and espionage of protected critical information. The computer viruses that can cause serious damage and compromise sophisticated systems have drawn special attention from the research community due to their masked and multifarious attack patterns. Removable storage media plays an important role in the transfer of data and virus to the computers connected to the critical networks. The air-gap between these networks are compromised by exploiting the internal weaknesses of the arrangement, transferring of data through removable storage media, hardware implants and zero-day vulnerabilities in the software / hardware that could be exploited in the real world before its disclosure. Thus, in a computer network virus poses a serious threat to the resource availability, confidentiality and integrity of critical assets. The purpose of this study is to design and upgrade the existing epidemic virus models under different conditions that describe the transmission of malicious computer code in active computer networks. An epidemic virus model that portray the spread of the malicious code in a critical infrastructure with pre-existing immunity and quarantine as an effective control strategy is designed. Due to the rapid spread of computer viruses and delay in the update of antivirus signature database, the role of quarantine as a controlling mechanism has gained importance. An epidemic virus model is designed that depicts the behavior of Stuxnet virus which is an advance persistent threat (APT) type cyber attack, uses unusual methods to attack resources with an intend to access the critical information while remains undetected and require special arrangement for control. Hardware based implants are common in these days gadgets and in computing machines for exploitation. Hardware implant based epidemic model is designed that portray the exploitation of hardware through embedded tiny chip. The control strategy of these compromised nodes are very difficult because they implant backdoors, install malicious utilities, gain admin rights, work as a legitimate program or infect with viruses. Nonlinear mathematical models are considered to analyze the dynamic behavior

of such virus spreads which exploits the inability of antivirus utilities and zero-day bugs of the software / hardware systems. The existence of disease free and endemic equilibrium points are explored in terms of the basic reproduction number R_0 for stability analysis. Numerical simulations are performed to investigate the dynamics of the models using well-established numerical techniques. Fractional order nonlinear models are designed for detailed analysis of the epidemic virus spread in the normal, air-gapped critical networks and hardware based implant vulnerabilities. Numerical experimentation's for fractional order models are performed using Grunwald-Letnikov (GL) based numerical solver and results show that fractional order models provide enrich dynamics by means of supper fast transients as well as supper slow evolutions of the steady-state which are seldomly perceived in integer order counterparts. Models accuracy are evaluated by comparing the results with available observed real data, published results and exact solutions.

Contents

List of Figures

List of Tables

Abbreviations

AMT	Intel Active Management Technology
BCP	Bugged, Compromised and Patched
BIOS	Basic Input Output System
CP	Captuo
CPU	Central Processing Unit
DFE	Disease Free Equilibrium
FDE	Fractional Differential Equation
FO	Fractional Order
FO-SVM	Fractional Order Stuxnet Virus Model
GL	Grunwald-Letnikov
HTTP	Hyper Text Transfer Protocol
IMU_I	Infected, Damaged and Infected Storage Media
IoT	Internet of Things
IPv4	Internet Protocol Version 4
IPU_I	Infected, Damaged and Infected Removable Storage Media
LAN	Local Area Network
ME	Management Engine
ML	Mittag-Leffler
MSEQIR	Immune, Susceptible, Exposed, Quarantine, Infected and Recovered
PLC	Programmable Logic Controllers
RK	Runge-Kutta
RL	Riemann Liouville
SCADA	Supervisory Control and Data Acquisition System

SIP$U_S U_I$	Susceptible, Infected, Damaged, Susceptible removable storage media and Infected removable storage media
SQL	Structured Query Language
SIR	Susceptible, Infected and Recovered
USB	Universal Serial Bus

Symbols

A	Arrival of New Bugged Computers
A_1, A_2	Arrival of New Computers and New Removable Storage Media
b, ρ	Birth Rate of New Nodes, Recovery Rate from Quarantine
R_0	Basic Reproduction Number
${}_aD_t^\alpha$	Derivative Operator where a and t are Bounds of Operation
P, U_S	Damaged, Susceptible removable storage media
d, δ	Death rate, loss of passive immunity
$\Gamma(\cdot)$, C	Gamma Function, Set of Complex Numbers
β, ξ	Infectious Contact Rate, Latent Period
M,S, E, Q, I, R	Immune, Susceptible, Exposed, Quarantine, Infected, Recovered
U_I	Infected removable storage media
J, λ	Jacobian Matrix, Eigen Values
V, F	Matrix for the Rate of Transmission and Rate of Infection
r_1, r_1	Natural removal rate of Computers and Removable Devices
c_1, c_2	Net Rate of Change of Population of Computers and Removable Devices
α, h, t	Order of Fractional Derivative, Step size, Time

φ	Quarantine Recovery Rate of Exposed Individuals
γ	Recovery Rate from Infectious Class
M_0, S_0, E_0, Q_0, I_0	Represents Initial Conditions
β_1	Rate of Infection Transfer from Infected Computers to Susceptible
β_2	Rate of Infection Transfer from Infected Removable Devices to Susceptible Computers
D_1-D_5	Represents Determinants
σ	Temporary Immunity Rate due to Patches and Virus Signature Update
N, η	Total Population, Loss of Immunity Rate
$E_{\alpha,\beta}$	Two Parameters Based ML Function
K_0, K^*	Virus Free Equilibrium Point, Endemic Equilibrium Point

Chapter 1

Introduction

This chapter introduces the research work carried out in this thesis. Firstly, background and motivation for this work is developed and then the research problem and research objectives are clearly defined. Novel contributions of this research work which adds to the existing knowledge are summarized. This chapter concludes with an overview of the thesis.

1.1 Background and Motivation

Motivation of this research is to design and upgrade virus models by considering the multifarious pattern of virus attack and their spreads in the computer networks. The designed models provides an effective platform for remediation of Stuxnet virus, tiny hardware implants vulnerabilities, zero day attacks, treatment of hardware vulnerabilities, reduce system endemic vulnerabilities and can be used for pre-emptive antivirus software design.

Maintaining database of virus signatures is very difficult due to high creation rate of new viruses with complicated updating mechanisms, especially for isolated critical networks. It is observed that quarantine and immunity can play an important role in the situation where virus signature and patch

updates are difficult, especially in remote locations or bandwidth and resource limited systems. Due to the availability of two recovery mechanisms immunity and quarantine, recovery of infectious nodes can be better and crashing of nodes due to infection may come out to be low. A model with detail analysis is required for investigating this. The inclusion of quarantine class may reduce the chances of the system becoming endemic.

Limited study regarding role of removable storage media in the spread of virus that compromise the air-gap in critical networks is available. Investigation did not establish a link of virus spread to critical industrial networks through removable storage devices.

To understand the in-depth analysis of Stuxnet virus model for fast transients and slow evolutions, fractional order model analysis is required to be explored.

The advancement in technologies creates several challenges to the security of the infrastructure of the nations in the presence of vulnerability and the development of smart viruses [1]. The global median dwell time of attackers is decreasing and targeting prey becomes easy due to bugged hardware. Therefore, detailed dynamical analysis of hardware implants and their devastation pattern with control mechanisms looks a promising domain to be investigated by the research community. In this regard, a bugged, compromised and patched (BCP) mathematical model is required which analyzes the spread of the virus and exploitation of system resources in compromised hardware.

1.2 Objectives and Significance

The objective of this study is to answer the question raised in motivation section.

1. Our objective is to extend the Hethcote MSEIR model [2] by developing an MSEQIR model, to study the behavior and impact of virus spread in the presence of immune and quarantine classes.

2. Our goal in this study is to design a mathematical model that depicts the Stuxnet spread in a working environment and its impact on critical infrastructures managed by industrial control computers.
3. Aim of present study is to exploit the rich heritage of fractional dynamics for the development of fractional Stuxnet virus model in order to study the virus spread in supervisory control and data acquisition systems.
4. Detailed dynamical analysis of hardware implants and their devastation pattern with control mechanisms looks a promising domain to be investigated by the research community. In this study, a bugged, compromised and patched (BCP) mathematical model is presented to analyze the spread of the virus and exploitation of system resources in compromised hardware.
5. In this study, a Fractional order BCP based mathematical model is presented to analyze the very fast transients as well as slow evolutions of the virus spread and exploitation of system resources in compromised hardware.
6. Local and global stability analysis of the models are performed at equilibrium points both for virus free and endemic spread scenarios analytically.
7. Simulation and modeling of virus propagation is performed numerically using state of the art standard numerical solvers such as Adams, backward differentiation formula (BDF), implicit and explicit RK and Grunwald-Letnikov(GL) fractional solver.

1.3 Methodology and Techniques

1.3.1 Literature Review

Virus modeling is a vast emerging field, especially computer virus modelling is a new field. However, literature is reviewed extensively in the form of research papers, review articles, thesis and related books regarding virus modeling and related soft computing techniques.

1.3.2 Mathematical Expansion / Up-gradation of the Model

Mathematical modeling is an art of translating complex real phenomena in to tractable mathematical formulations which provide insight behavior of the problem without interaction with the system. Mathematical models of virus propagation are expanded and upgraded using differential equation models. The choice of variables and parameters are well thought-out by considering their role and relation with real world problems. Different environments are created using a diverse combination of variables and parameters to test the real world situations depicting the spread of virus.

1.3.3 Equilibrium Points

Equilibrium of a system is a state in which it does not change, or the rate of change is zero. The equilibrium of a system can be estimated by setting the derivatives to zero. To understand virus behavior, virus spread and disease free equilibrium points are calculated. Disease free and endemic equilibrium points of the model provide further basis for investigation of the virus spread behavior.

1.3.4 Basic Reproduction Number R_0

The basic reproduction number R_0 of the model is calculated which represents the addition of new infection due to an infected individual in the susceptible population. R_0 is the parameter of infection spread measurement, if $R_0 > 1$, infection will grow in the system and if $R_0 < 1$ then infection will die down.

1.3.5 Stability Analysis

To validate the theoretical boundaries of the virus free and endemic spread, stability analysis of the model at virus free and endemic equilibrium points is performed.

Local and global stability studies are carried out to define the boundaries of the model.

1.3.6 Simulations

Numerical simulations are performed to check the accuracy of proposed models using traditional numerical techniques and advanced fractional numerical methods.

1.3.7 Writeup of Papers/Thesis

Simulation results are systematically provided in the articles for possible publication in highly regarded national and international journals and finally when the research contribution was well-established, thesis writeup was performed.

1.4 Research Contributions

The main contributions of this research work added to the existing knowledge of research community are summarized as below:

1. An Immune $M(t)$, Susceptible $S(t)$, Exposed $E(t)$, Quarantine $Q(t)$, Infected $I(t)$ and Recovered $R(t)$ nodes epidemiological based computer virus model $MSEQIR$ is designed by considering the effect of quarantine in the presence of immunity in the field of network and security. This work is also published in a reputed journal [3]
2. A Susceptible nodes $S(t)$, Infected nodes $I(t)$, Damaged nodes $P(t)$, Removable Susceptible storage media $U_s(t)$ and Removable Infected storage media $U_I(t)$ computer virus model $SIPU_sU_I$ is designed with ability to accurately model the security of isolated critical industrial control networks.
3. A fractional order Stuxnet virus model is proposed by exploiting the rich heritage of fractional calculus in the environment of supervisory control and data

acquisition by bridging the air-gap between traditional and critical control network infrastructures.

4. A novel Bugged, Compromised and patched epidemic mathematical model is designed for embedded tiny chip based infiltration within another computer.
5. A Fractional order Bugged, Compromised and patched mathematical model is proposed to analyze the fast transients as well as slow evolutions of the virus spread and exploitation of system resources in compromised hardware.

1.5 Overview of This Thesis

The thesis are organized as follow

Chapter 1, Introduction: This chapter introduces the research work carried out in this thesis. Firstly, background and motivation for this work was developed and then the research problem and research objectives are clearly defined. Novel contributions of this thesis are summarized. This chapter concludes with an overview of the thesis.

Chapter 2, Literature Review: In this chapter introduction of malware types, threats, impact on world security, attacking behavior, mathematical modeling and fractional order modeling are discussed with references in computer network as well as in biology literature. Literature survey in context of research gaps is carried out.

Chapter 3, Role of Quarantine and Immunity in Virus Spread: This chapter presents the role of quarantine and immunity in computer virus spread. Due to the rapid spread of computer viruses and a delay in the update of antivirus signature database, the role of quarantine and immunity has gained great importance.

Chapter 4, Dynamic Analysis of Stuxnet Virus Spread: In this chapter, spread of virus infection due to removable storage media and infected hosts is analyzed. Removable storage media plays an important role in bridging the air-gap between isolated critical networks and commercial networks.

Chapter 5, Fractional Dynamics of Stuxnet Virus Propagation: In this

chapter fractional dynamics of Stuxnet virus spread are analyzed in the regimes of supervisory control and data acquisition environment when the air-gap between traditional and critical control network is bridged. Spread behavior analysis of malicious codes is investigated for distinct orders of fractional derivative in the model.

Chapter 6, Vulnerability Analysis of hardware Implants: This chapter presents the design of an epidemic model that portrays the exploitation of computers by bugs implanted through embedded tiny chips (mini-computer within another computer) such as Intel management engine (ME).

Chapter 7, Fractional Analysis of Hardware Implants Spread: This chapter describes the fractional version of the epidemic model that portrays the exploitation of hardware through embedded tiny chips inside the computer.The firmware level bugs allow escalation of privileges and remote execution of code beneath the operating system for infiltration.

Chapter 8, Conclusion and Future Work: In this chapter conclusion of the thesis results are drawn and suggestions regarding future work are proposed.

Chapter 2

Literature Review

This chapter discuss the literature review of malware types, advance persistent threats, hardware implants, multifarious attacking pattern and impact on world security. Mathematical modeling and fractional order modeling are also discussed with reference to computer networks as well as in biology literature. Literature survey in context of research gaps are identified. Detail of the literature reviews are given below.

2.1 Introduction

Now a days, victory in wars is based on use of superior technologies and equipments. They mostly use automated systems that are combinations of hardware and software. There is no secret that in our societies most infrastructures are dependent on computers and threats to computers cause threats to society. Software normally controls the functionality of hardware and the real war is waged with malicious software or malware. This is a software program whose intent is malicious and covers a wide range of threats including virus, worm, trogan horse, spam and spyware. A virus is a type of malware that requires human effort / click to spread on the system whereas a worm replicates itself without any effort. A trojan horse is not a virus, it is a destructive program that pretends to be a

genuine application and opens backdoors in the target systems. Around 70% of malicious code belongs to the category of trojan horse. Spam is a term used for an abundance of unsolicited bulk emails. Statistics show that currently 70% of email traffic falls under this category. Spyware is a program that collects information covertly and transmits it to specific control stations. On the other hand, adware (like spyware) collects user information and appeared in late 1990s [4].

In the present arena of networked computers, malware poses a serious threat to the resource availability, confidentiality and integrity of computer networks. Electronic mail, sharing of resources in a network environment, use of secondary data carrying devices and special websites are the major source of spread of malicious objects [5, 6] that can erase data, compromise the resources, delay critical processes, open back doors, modify the operations and launch of distributed denial of service attacks [7–9]. Cyber threats in the form of virus, worm, spyware, adware and trojans stealing information or hacking accounts now often happen in sophisticated and technical ways. Nations and individuals are accumulating cyber resources and developing novel methods to exploit the selected targets in an optimal manner [10–12]. The world economy and security depends upon the secure connectivity of the Internet and intranet due to automation of the industrial and economic processes. International conflicts pose serious threats to system security, financial loss, loss of critical information, damage of resources and ruin of critical assets [13–15]. In the present arena, networks are becoming the target of well-crafted cyber-attacks, especially incidents related to breaking of internal systems and espionage of critical information. The air-gap between these systems are mostly compromised by exploiting the internal weaknesses of the arrangement and zero-day exploits in the software / hardware [16, 17]. Zero-day vulnerability are the holes of any software / hardware that could be exploited in the real world before their disclosure and in the absence of any patch [18]. Due to the natural desire of automating every appliance, the use of software has increased enormously. The poor programming approaches and weak software testing methodologies are unable to detect the vulnerabilities and bugs in the codes, that may lead to compromising the whole system and an easy prey for hackers [19]. Bugs could affect

TABLE 2.1: A brief overview of computer malware.

Year	Author	Description	Ref.
2004	Hoglund, G	Exploiting software: How to break code	[20]
2006	Aycock, J	Computer viruses and malware	[4]
2011	Langner, R	Stuxnet: Dissecting a cyberwarfare weapon	[22]
2011	Kesler, B	The vulnerability of nuclear facilities to cyber attack	[24]
2012	Rid, Thomas	Cyber-weapons	[21]
2013	Finifter, M	Empirical Study of Vulnerability Rewards Programs	[23]
2014	Ablon, L	Markets for cybercrime tools and stolen data	[19]
2014	Axelrod, Robert	Timing of cyber conflict	[10]
2014	Sanger, David	NSA devises radio pathway into computers	[25]
2017	Ashibani, Y	Cyber physical systems security challenges	[14]
2017	Ablon, L	Life and Times of Zero-Day Vulnerabilities	[17]
2018	Tounsi, W	Survey on sophisticated cyber attacks	[11]
2018	Van der Walt	Cyber-security detection on social media platforms	[12]
2018	Ullah, F	Data exfiltration	[13]
2018	Hassan, S	Security threats in Bluetooth technology	[15]
2018	Kim, S	Empirical study of cloned vulnerabilities	[16]

everything from small to advanced devices and could be exploited to steal information, insert rootkit, wipe data, manipulate desired results and compromise the critical industrial plants [20]. These bugs are used as tools for cyber war [21] which range from very small programs that just display annoying messages or very complex program that can physical damage the system such as Stuxnet [22]. Cost estimates of valuable zero-day exploits can go over $100,000 [23]. The discovery of new vulnerabilities in known software is very common. It was found that in a three-year period, 2009-2012, more than 400 problems were found in Firefox browser and over 800 were found in Chrome browser [24]. The rapidly growing market of zero-day exploits, demands careful designing and understanding of the spread mechanism of malicious codes.

In the last few years hardware implants and bugs are commonly used for exploitation of the server computers and systems connected to critical plants. Exploitation of implanted hardware is easy and covertly provides a backdoors to access the information and execute desired instructions [25, 26]. Intel Management Engine

(ME) is the creek behind the Intel Active Management technology (AMT) which is present in almost all version of desktops, laptops and servers using Intel chipsets since 2008 [27]. ME 11 is based on Intel Quark x86-based 32bit processor with MINIX 3 operating system, independent from the main processor and operating system [28]. Every modern computer is based on Intel architecture with an Intel management engine (ME) having powered capabilities, full access to operating memory, out-of-band network management and running of CPU independently even in shutdown state (connected with battery or power supply) [29]. These capabilities allow proprietary remote management of the system and allow Intel to implement different features and technologies [30], while on the other side remote management options tempt hackers to target Intel ME for exploitation, installation of backdoors, stealing important information and compromising critical infrastructures [31]. Intel ME is a firmware, stored in a serial peripheral interface (SPI) flash memory along with BIOS using embedded flash file system, with an isolated, powerfull, privileged and stealthy execution environment [32]. Management Engine firmware module uses Huffman encryption algorithm for the security of boot code that makes it quite difficult to re-construct [33]. Intel admitted that the active management technology platform services are vulnerable to multiple security threats which are reported by external security experts [34]. Hacker can attack the machines having AMT features through AMT VNC-server, AMT web-server, AMT HTTP protocol, AMT HTTPS protocol and AMT serial over LAN. Security experts and critics like electronic frontier foundation say that ME is a backdoor with privacy concern and worries of full access to memory without parent CPU knowledge, can send and receive packets independently of operating system and thus have no hurdle of any sort of firewall and antivirus [35, 36].

2.2 Virus Modeling

Advancement in Internet and computer technologies creates a challenge to the security of the critical infrastructure of nations. These challenges also provide an

TABLE 2.2: Overview of hardware bugs.

Year	Author	Description	Ref.
2009	Bozdag, E	Therac-25 and the security of the computer	[27]
2012	Stewin, P	Understanding DMA malware	[29]
2013	Hoekstra, M	Innovative instructions to create trustworthy software solutions	[28]
2013	Stewin, P	Stealthy peripheral-based attacks on the computing platform	[32]
2014	Ruan, X	Safeguarding the Future Security of Intel Management Engine	[30]
2014	Skochinsky, I	Intel ME Secrets	[33]
2017	Ogolyuk, A	Intel Management Engine Attack Vectors	[36]
2017	Ermolov, M	Hacking a Turned-Off Computer	[31]
2017	Averlant, G	Intel and ARM hardware isolation mechanisms	[34]
2018	Robertson, J	The big hack	[26]
2018	Domas, C	Hardware Backdoors in x86 CPUs	[35]

opportunity to devise a controlling strategy. The behavior of virus spread is studied by using epidemiological modeling of virus propagation to safeguard against threat propagation [37, 38]. The control strategies for these malicious codes are inherently complex due to its rapid spread nature and higher birth rate [39, 40]. A mathematical model gives us the flexibility of deep understanding with a simple procedure, as well as, vibrant assessment to solve complex problems. In mathematical modeling, thoughts are translated in to a mathematical language which is very concise and has well defined rules for manipulations. Models are broadly categorized as deterministic and stochastic. In deterministic models random variation are ignored where as stochastic models are more statistical. In this regards, mathematicians, biologist and computer scientists have introduced the concept of models for critical analysis of the behavior of different malicious epidemic viruses such as classical epidemic susceptible, infected and recovered model of Kermack and McKendrick [41], analysis of dengue epidemic behavior [52, 53], malware propagation in mobile computer devices [54], stochastic behaviour analysis models [49], discrete models [46, 47], deterministic models [42, 50], time delay models [44, 51], the effect of quarantine [43, 55], vertical transmission from mother to child and horizontal transmission among same individual generations [48, 56], fuzziness [45, 57], P2P networks [58, 59], a theoretical assessment approach of virus models

TABLE 2.3: Overview of virus models in biology.

Year	Author	Description	Ref.
1932	Kermack	Contributions to the mathematical theory of epidemics	[41]
2002	Srivastava, Ranjan	Stochastic vs. deterministic modeling	[42]
2002	Hethcote, Herbert	Effects of quarantine in six endemic models	[43]
2002	Nelson, Patrick	Mathematical analysis of delay differential equation models	[44]
2004	Jafelice, Rosana	Fuzzy modeling in symptomatic HIV virus infection	[45]
2010	Braverman, E	Discrete delay host macroparasite model	[46]
2010	Zhang, Cun-Hua	Hopf bifurcations in a predator–prey system	[47]
2012	Busenberg, Stavros	Vertically transmitted diseases: models and dynamics	[48]
2016	Amador, Julia	SEIQS stochastic epidemic model with external infection	[49]
2016	Braverman, Elena	Stochastic difference equations with the Allee effect	[50]
2016	Berezansky, Leonid	Boundedness and persistence of delay differential equations	[51]
2017	Alhumaidan, A	Modelling and Analysing Qualitative Biological Models	[38]
2017	Malik, Hafiz Abid	Modeling and analysis of dengue epidemic behavior	[52]
2019	Cai, Yongli	Global transmission dynamics of a Zika virus model	[53]

[60], discontinuous antivirus strategy in a computer virus model [61] and models that discuss the topological aspects of the network [62].

2.3 Fractional Order Modeling

The state of many biological systems at a given time depends on the states of the system at some previous times. So, fractional derivatives are the natural methods for the solution of biological modeling arising in various disciplines. The concept of fractional mathematics was developed towards the end of 19th century. Fractional order system are at-least as stable as their counter part integer order models [63, 64]. The concept of fractional calculus changes the way to see the model and interpret the meaning. In this regards, mathematicians, computer scientists, physicists and biologist have put efforts to design mathematical models to understand the behavior of the viruses or implants such as fractional epidemiological model for computer viruses [65], fractional order delay-varying computer virus propagation model [66], fractional dynamics of computer virus propagation

TABLE 2.4: Computer virus models overview.

Year	Author	Description	Ref.
2004	Serazzi, G	Computer virus propagation models	[5]
2010	Mishra, Bimal	SEIQRS model for the transmission in Computer Network	[55]
2010	Mishra, Bimal	Fuzzy epidemic model for the transmission of worms	[57]
2011	Mishra, Bimal	Dynamic model of worms with vertical transmission	[56]
2013	Wang, XiaoMing	Modeling of malware propagation in mobile wireless networks	[59]
2014	Mishra, Bimal	Dynamic model of worm propagation in computer network	[39]
2014	Haldar, K	Distributed attack on targeted resources in a computer	[58]
2015	Ren, J	Investigation of dynamics of a virus–antivirus model	[8]
2016	Wang, Xu	Virus propagation modeling in large-scale networks	[37]
2016	Yang, L	The optimal dynamic immunization	[7]
2016	Dong, Tao	Impact of discontinuous antivirus strategy in a computer virus	[61]
2017	Xiao, Xi	Design and analysis of SEIQR worm propagation model	[40]
2017	Yang, Lu-Xing	Impact of patch forwarding on the prevalence of computer virus	[60]
2017	Zhang, Tianrui	Dynamic malware containment under an epidemic models	[62]
2017	Ren, J	Compartmental model for computer virus propagation	[6]
2018	Pont, Mara	Modelling the malware propagation in mobile computer devices	[54]

[67], fractional dynamics and control [68], fractional order SEIR model with vertical transmission [69] and other applications of fractional calculus in engineering [70–76].

2.4 Research Gaps

This thesis is concerned with the development of mathematical models for the dynamics of virus spread in network infrastructure and its constant control strategy. Four type of closely related virus models are discussed for integer and fractional order dynamics.

Security holes and zero-day vulnerabilities in operating system and software are still a significant issue and these vulnerabilities can be addressed by introducing the concept of immunization and effective quarantine strategy [77–79]. Isolation from a highly infected individual/element is a known way of controlling disease

TABLE 2.5: An overview of fractional calculus.

Year	Author	Description	Ref.
1998	Podlubny, Igor	Fractional differential equations	[72]
2007	Sabatier, JATMJ	Advances in fractional calculus	[71]
2007	Ahmed,E	Numerical solutions of fractional-order predator-prey models	[64]
2008	Petráš, Ivo	A note on the fractional-order Chua's system	[74]
2008	Scherer, Rudolf	Numerical treatment of fractional heat equations	[76]
2008	Petras, Ivo	Stability of fractional-order systems with rational orders	[63]
2011	Baleanu, Dumitru	Fractional dynamics and control	[68]
2011	Zalp, Nuri	A fractional order SEIR model with vertical transmission	[69]
2011	Petrás, Ivo	Fractional derivatives and fractional integrals	[75]
2014	Pinto, Carla	Fractional dynamics of computer virus propagation	[67]
2014	Machado, JA	On development of fractional calculus	[73]
2016	Ansari, Moien	Fractional order delay-varying computer virus propagation	[66]
2018	Singh, Jagdev	Fractional epidemiological model for computer viruses	[65]

spread in the biological world and the same can be incorporated for computer viruses. Quarantine classes in the computer world have special significance in the scenario where a virus signature database is outdated and the protection of assets from unauthorized exploitation has high impact. Keeping in view of the above facts and research gaps, an epidemic MSEQIR computer virus model is designed that incorporate the quarantine and immunity classes which may reveal the interesting results and address the research gaps.

Removable storage media plays a vital role in the spread of virus that compromise the air-gap in critical networks. Few studies are conducted to observe the effect of removable media in the spread of worm [80–82]. However, these investigation provides theoretical analysis of the models and does not establishes a link with real world virus spread in computer networks / critical industrial networks. So, a research work is required to establish a link between real world viruses (Stuxnet) spread in the air-gapped networks. Stuxnet is an advance presistant threat (APT) type cyber attack, uses unusual methods to attack resources with an intend to access the critical information while remains undetected and require

special arrangement for control and eradication. APT type attack typical establishes different connection points of compromise to target the victim and ensure that cyber-attack can continue in failure of any one point. Attacker removed the evidence of APT occurrence without removing the re-entry path and can easily regain the control of the target system. Therefore, resource mitigation strategy of an organization from APT's are a challenging cyber security research area [83, 84]. To overcome this gap, $SIPU_SU_I$ epidemic model for Stuxnet virus is designed to highlight the behaviour of Stuxnet virus spread that consider several attacking vectors e.g., infection spread due to infected hosts I and infected removable storage media U_I that are further infected from other infection vectors like email, network, file, application vulnerability, infected media, supply chain compromise or human intelligence and deception.

The advancement in technologies creates several challenges to the security of the infrastructure of the nations in the presence of vulnerability and the development of smart viruses [1]. The global median dwell time of attackers is decreasing and targeting prey is becoming easy due to bugged hardware. The firmware level bugs allow escalation of privileges and remote execution of code beneath the operating system for infiltration or completely intervene with computers. Defending against hardware implants are extremely difficult. Despite the lack of supporting evidence and refuting the reports of hardware implants, concerns in the security industry rises that such implants were used by state agencies and advance state actors. NSA,s digital catalogue reveals several sophisticated tools of hardware espionage, which was exposed in Der Spiegel, the German weekly newspaper and these tools were used to conduct the espionage operation around the world [85]. Hardware implants are more feasible due to simplified design and cost effectiveness [86]. Intel ME is the creek behind the Intel Active Management Technology (AMT) which is present in almost all version of desktops, laptops and servers in Intel chipsets since 2008 [27]. Intel admitted that the active management technology platform services are vulnerable to multiple security threats [34]. Security experts and critics like electronic frontier foundation say that ME is a backdoor with privacy concern and worries of full access to memory without parent CPU knowledge, can send and

receive packets independently of operating system and thus have no hurdle of any sort of firewall and antivirus [35, 36]. Therefore, detailed dynamical analysis of hardware implants and their devastation patterns with static control mechanisms is a promising domain to be investigated by the research community. To overcome the gap of hardware implant vulnerabilities, a mathematical model is designed that simulate the vulnerabilities of embedded tiny chip based hardware implants in network infrastructures.

To understand the in-depth analysis of virus spread for fast transients and super slow evolutions, fractional order model provides a comprehensive analysis. Fractional analysis of these models are carried out which provides further control in term of fractional derivative α and tune the models for a wider domain.

Chapter 3

Role of Quarantine and Immunity in Virus Spread

This chapter presents the role of quarantine and immunity in computer virus spread. Due to the rapid spread of computer viruses and a delay in the update of antivirus signature database, the role of quarantine and immunity gained importance.

3.1 Introduction

In the present arena of Internet of Things (IoT) that comprises of computers, digital / mechanical machines, medical devices, critical systems which are interconnected through network and the vulnerability of a single machine compromise the whole network. Malicious code poses a serious threat to the resource availability, confidentiality and integrity of the network. Automatic mitigation for known viruses are performed relatively with ease, but very hard in the case of unknown malicious object and have to rely on behavior based tedious anomaly detection techniques [87–89]. Therefore, it is essential that a better control strategy may be devised to eradicate the malicious code from spreading on network.

Maintaining database of virus signatures is very difficult due to high creation rate

as compared to limited known applications/files. On-demand virus scans are performed rarely due to high utilization of resources and consequently slow execution of the working applications. Resultantly, dormant viruses tend to have a long life [90, 91]. On the other hand, virus removing applications are also not trouble free because some of them consume more resources while others take a longer time. Therefore, many user attempts to disable them, if they have limited resource system. Organization network uses a limited number of white applications and securing these applications from virus using patch update (Immunization) or segregation from the outer world (Quarantine) are an effective strategy to control the virus or zero day attacks.

Security holes and zero-day vulnerabilities in the operating system and software are still a significant issue and these vulnerabilities can be addressed by introducing the concept of immunization and effective quarantine strategy [77–79]. Isolation from highly infected individual/element is a known way of controlling disease spread in the biological world and the same can be incorporated for computer viruses. Quarantine classes in the computer world have special significance in the scenario where a virus signature database is outdated and the protection of assets from unauthorized exploitation has high impact. Keeping in view of the above illustrated facts, our objective is to extend the Hethcote MSEIR model [2] by developing an MSEQIR model, to study the behavior and impact of virus spread in the presence of immunity and quarantine classes. The potential highlights of the proposed virus model design are summarized as:

1. A novel epidemiological base computer virus model MSEQIR is designed by considering the effect of quarantine in the presence of immunity in the field of network and security.
2. Jacobian linearization matrix approach with an associated reproduction number verified the virus free and endemic stability of the proposed model.
3. Numerical simulation study of MSEQIR model is performed with real life parameters and results shows that the model mimic the situation viably.
4. The designed model provides an effective platform for utilization of zero day attacks, reduce system endemic vulnerability and can be used for pre-emptive

antivirus software design.

3.2 Design Methodology

In this section, we describe the formulation of the proposed virus model in terms of Immune $M(t)$, Susceptible $S(t)$, Exposed $E(t)$, Quarantine $Q(t)$, Infected $I(t)$ and Recovered $R(t)$ scenarios in the field of computers network and information security. The overview of the designed scheme is presented in figure 3.1.

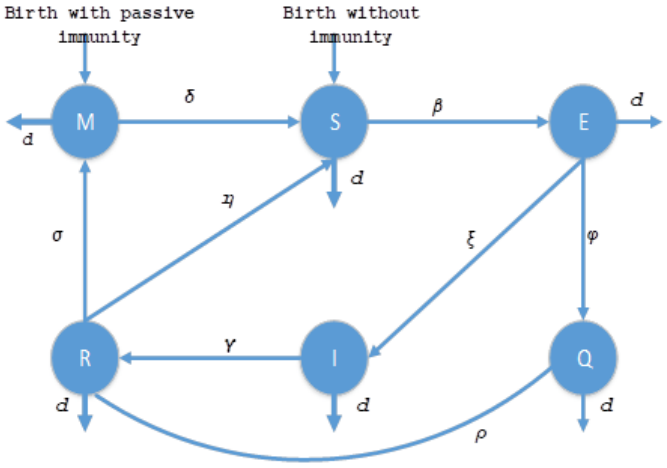


FIGURE 3.1: Schematic flow of proposed MSEQIR model

3.2.1 The Epidemic MSEQIR Virus Model

The Epidemic MSEQIR Virus Model having total population size $N(t)$ which is the sum of Immune $M(t)$, Susceptible $S(t)$, Exposed $E(t)$, Quarantine $Q(t)$, Infected $I(t)$ and Recovered $R(t)$ computer nodes i.e. mathematically: $N = M + S + E + Q + I + R$. In the model, we assume that few system attains passive immunity through patch and virus signature database update while others are susceptible to infection. Dynamic behavior and spread of the virus from different classes of the model are depicted in figure 3.2. The transmission of MSEQIR model with standardized incidence rate is expressed by system of differential equations. The interaction between uninfected systems with infected is widely known as the mass action principle that describes the mathematical perspective of the rate at which

a virus can infect an uninfected cell [92]. The mass action incidence rule also suggests that the rate of interaction between virus and virus free cells is directly proportional to the product of participating classes [93].

Temporary immunities are present in the real life situation that arises in biology as well as in the computer network world. However, these immunities are yet not incorporated as a separate class in epidemic computer models. Aim of the present investigate is to design and analyze a MSEQIR model with effect of quarantine and immunities in the presence of other classes. Workflow of the proposed model is illustrated in figure 3.2.

$$\frac{dM}{dt} = b(N - S) + \sigma R - (\delta + d)M, \tag{3.1}$$

$$\frac{dS}{dt} = bS + \delta M + \eta R - \frac{\beta SI}{N} - dS, \tag{3.2}$$

$$\frac{dE}{dt} = \frac{\beta SI}{N} - (\xi + \varphi + d)E, \tag{3.3}$$

$$\frac{dQ}{dt} = \varphi E - (d + \rho)Q, \tag{3.4}$$

$$\frac{dI}{dt} = \xi E - (d + \gamma)I, \tag{3.5}$$

$$\frac{dR}{dt} = \gamma I + \rho Q - (d + \sigma + \eta)R. \tag{3.6}$$

The initial conditions are given as follows:

$$M(0) = M_0,\ S(0) = S_0,\ E(0) = E_0,\ Q(0) = Q_0,\ I(0) = I_0,\ R(0) = R_0.$$

In this epidemic computer virus model as given in equations (3.1) to (3.6), the parameter b represents the birth rate of new computers node, d represents the death rate, δ represents loss of passive immunity, β the infectious contact rate, ξ is latent period, φ represents quarantine recovery rate of exposed individuals, ρ is recovery rate from quarantine, γ is recovery rate from infectious class, σ represents temporary immunity rate due to patches and virus signature update and η is loss of immunity rate. In this model, we assume that some node got temporary immunity after security patches and antivirus software signature database update, while others are again susceptible to infection. In the most models, temporary immunity are not considered. It is important to note that all parameter values in

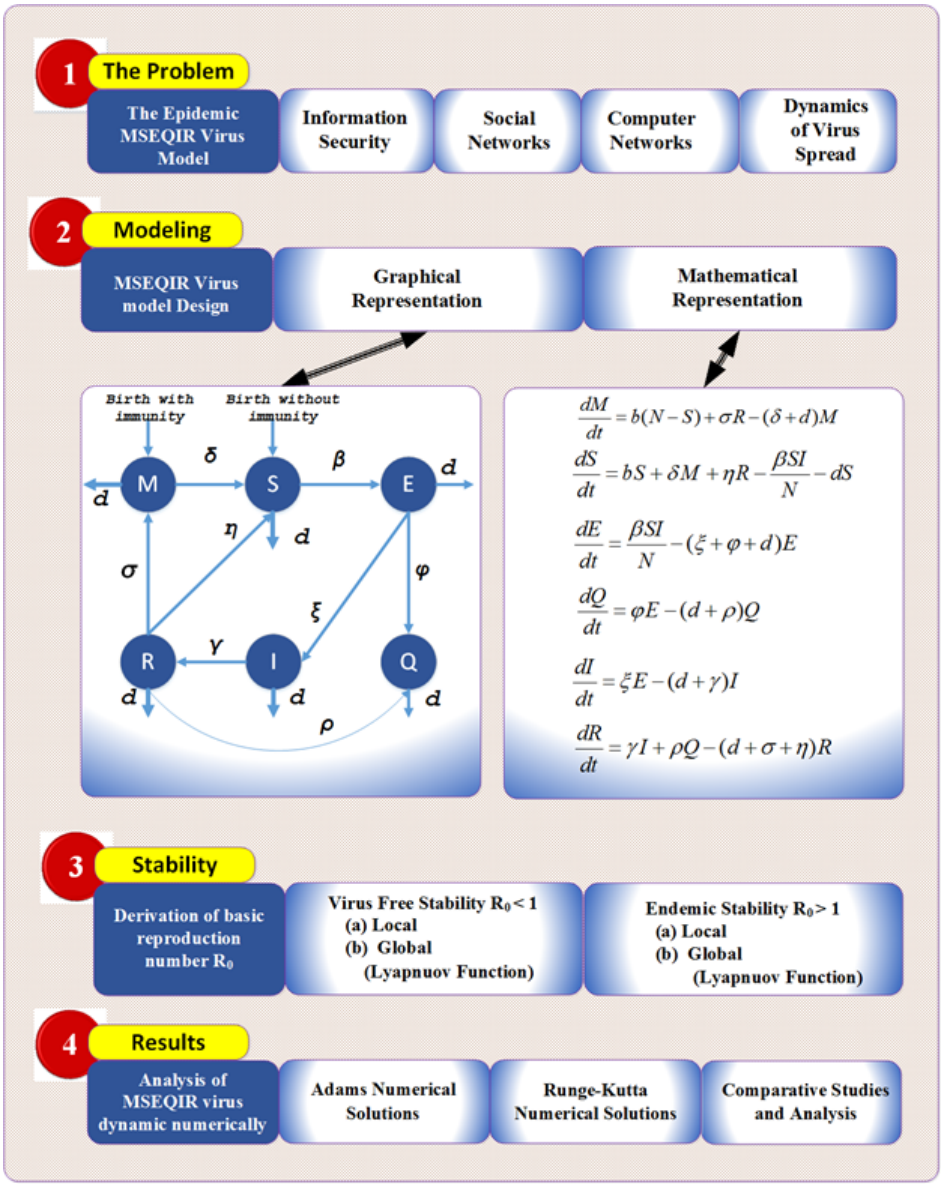


FIGURE 3.2: Schematic workflow of proposed scheme

this model are assumed to be positive.

New Computer Nodes having passive immunity and susceptibility are added in M and S classes respectively, node moves from class M to class S at the rate of δ which is represented by the immunity lost rate, nodes from class S moves to class E when they are exposed with infectious class I, nodes from class E move to class Q at quarantine rate φ and to class I for latent period ξ, nodes from class Q and I move to recovered class R based on the recovery rate of these nodes from both classes, class R nodes move to M and S classes based on its susceptibility and immunity due to virus and patch definition update.

Lemma 1. Let us consider the following two systems [94]

$$\frac{dw}{dt} = F(t, w), \frac{dz}{dt} = g(z),$$

where $(w, z) \in \Re^n$, F and g are continuous function satisfying a local Lipschitz condition in any compact set $W \in \Re^n$ and $F(t, w) \to g(w)$ as $t \to \infty$ so that second system is the limit version of the first. Let $\phi(t, t_0, w_0)$ and $\varphi(t, t_0, z_0)$ be the solutions of these systems and $e \in W$ is locally asymptotally stable equilibrium of the limit system and its attractive region is given as:

$L(e) = \{z \in W \,|\varphi(t, t_0, z_0) \to e,\ t \to \infty\}$

Let L_ϕ be the omega limit set of $\phi(t, t_0, w_0)$. If $L_\phi \cap L(e) \neq \phi$, then $\lim_{t\to\infty} \phi(t, t_0, w_0) = e$.

3.3 Model Analysis

3.3.1 Basic Reproduction Number R_0

The basic reproduction ratio is the expected number of new cases from infection produced by an infected individual and denoted by R_0. R_0 is the measure of disease spread potential in the population. If $R_0 < 1$, then infected nodes connected to the network in a susceptible environment will not replace themselves and infection will be eliminated. If $R_0 > 1$, then the number of infection will increase rapidly. The meaningful value of R_0 can be obtained by calculating the V and F matrix, where V is a matrix for the rate of transmission and F is a matrix for the rate of infection. Model MSEQIR has three infected classes. So to get R_0, we use only three equations (3.3)- (3.5) from a system of equations (3.1)-(3.6). Linearizing the system (3.3)-(3.5), we obtain.

$$\begin{bmatrix} \frac{dE}{dt} \\ \frac{dQ}{dt} \\ \frac{dI}{dt} \end{bmatrix} = (F - V) \begin{bmatrix} E \\ Q \\ I \end{bmatrix}, F = \begin{pmatrix} 0 & 0 & \beta \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\text{and } V = \begin{pmatrix} d+\xi+\varphi & 0 & 0 \\ -\varphi & d+\rho & 0 \\ -\xi & 0 & \gamma+d \end{pmatrix}.$$

Basic reproduction number R_0 is the dominant eigenvalue of FV^{-1}, that is

$$FV^{-1} = \begin{pmatrix} \dfrac{\beta(d\xi+\xi\rho)}{(d+\rho)(d+\gamma)(d+\xi+\varphi)} & 0 & \dfrac{\beta}{d+\gamma} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$R_0 = \frac{\beta\xi}{(d+\gamma)(d+\xi+\varphi)}.$$

3.3.2 Existence and Stability of Equilibrium

For model MSEQIR in equilibria, the rate of change for each population is zero. For computer virology perspective, we are able to find virus free equilibrium and virus persistence equilibrium. If the value of any population is not zero in equilibrium, it shows that these populations remains existing. If the value of any class at equilibrium is zero ($M = 0$, $S = 0$, $E = 0$, $Q = 0$, $I = 0$, $R = 0$), those classes will extinct in system / biology as time goes to infinity. Thus, if $I = 0$, $E = 0$ at equilibrium, the virus in computer nodes will vanish as time t tends to infinity. If the value of any class is not zero ($M \neq 0$, $S \neq 0$, $E \neq 0$, $Q \neq 0$, $I \neq 0$, $R \neq 0$), those classes are defined as persistent. Thus, if $M \neq 0$, mean that immunity will persist in that equilibrium state and if $I \neq 0$, then the infection will be present in the nodes. Stability analysis accurately determines the type of the system behavior. The birth rate of the population is represented by b and death rate by d. The net rate in change of population may be positive, zero or negative. In this study, we use the case of zero change in population size.

The system (3.1)-(3.6) is defined on the closed, positive invariant set $D = (M, S, E, Q, I, R)$; $M, S, E, Q, I, R > 0$: $M + S + E + Q + I + R = N$, then we explore the stability of the model which possibly have two equilibria, virus free equilibrium $K_0 = (0, N, 0, 0, 0, 0)$ and endemic equilibrium $K^* = (M^*, S^*, E^*,$

Q^*, I^*, R^*).

Theorem 1. System (3.1)-(3.6) has two equilibrium point, virus free equilibrium $K_0 = (M_0, S_0, E_0, Q_0, I_0, R_0) = (0, N, 0, 0, 0, 0)$ and endemic equilibrium $K^* = (M^*, S^*, E^*, Q^*, I^*, R^*)$.

Proof. Solving the system (MSEQIR) of equations (3.1)-(3.6):

$$b(N - S) + \sigma R - (\delta + d)M = 0, \tag{3.7}$$

$$bS + \delta M + \eta R - \frac{\beta SI}{N} - dS = 0, \tag{3.8}$$

$$\frac{\beta SI}{N} - (\xi + \varphi + d)E = 0, \tag{3.9}$$

$$\varphi E - (d + \rho)Q = 0, \tag{3.10}$$

$$\xi E - (d + \gamma)I = 0, \tag{3.11}$$

$$\gamma I + \rho Q - (d + \sigma + \eta)R = 0. \tag{3.12}$$

The equilibrium of the system (3.1)-(3.6) can be obtained by taking all equations of the system equal to zero. Virus free equilibrium is obtained by assuming that viruses are not present in the system and we obtained a unique virus free equilibrium $K_0 = (M_0, S_0, E_0, Q_0, I_0, R_0) = (0, N, 0, 0, 0, 0)$. Endemic equilibrium point is characterized as the point in which infection ($I \neq 0$) is present in the system. The point $K^*= (M^*, S^*, E^*, Q^*, I^*, R^*)$ is an endemic equilibrium point and is given below:

$$M* = -\left(\begin{array}{l} (d+\rho)(d(d+\xi)(d+\eta+\sigma) + (d(d+\eta+\xi) \\ +(d+\xi)\sigma)\gamma) + (d(d+\eta+\rho) + (d+\rho)\sigma)(d \\ +\gamma)\varphi)(d^2 - \beta\xi + \gamma(\xi+\varphi) + d(\xi+\gamma+\varphi) \end{array} \right) \Big/ \Lambda, \tag{3.13}$$

$$S* = ((d+\gamma)(d+\xi+\varphi))/\beta\xi, \tag{3.14}$$

$$E* = -\left(\begin{array}{l} \delta(d+\rho)(d+\eta+\sigma)(d+\gamma)(d^2 \\ -\beta\xi + \gamma(\xi+\varphi) + d(\xi+\gamma+\varphi)) \end{array} \right) \Big/ \Lambda, \tag{3.15}$$

$$Q* = -\left(\begin{array}{l} \delta(d+\eta+\sigma)(d+\gamma)\varphi(d^2 - \beta\xi \\ +\gamma(\xi+\varphi) + d(\xi+\gamma+\varphi)) \end{array} \right) \Big/ \Lambda, \tag{3.16}$$

$$I* = -\left(\begin{array}{l} \delta(d+\rho)(d+\eta+\sigma)(d^2-\beta\xi \\ +\gamma(\xi+\varphi)+d(\xi+\gamma+\varphi)) \end{array} \right) \Big/ \Lambda, \tag{3.17}$$

$$R* = -\left(\begin{array}{l} \delta(\xi(d+\rho)\gamma+\rho(d+\gamma)\varphi)(d^2 \\ -\beta\xi+\gamma(\xi+\varphi)+d(\xi+\gamma+\varphi)) \end{array} \right) \Big/ \Lambda. \tag{3.18}$$

where, parameter Λ of equations (3.13) to (3.18) is given as:

$$\Lambda = \beta\xi \left(\begin{array}{l} d^4+\delta\rho\left(\xi\left(\begin{array}{l}(\eta+\sigma)+\\(\eta+\xi+\sigma)\gamma\end{array}\right)\right)+\delta\left(\eta+\rho+\sigma\right)\gamma\varphi+\rho\sigma\gamma(\xi+\varphi)+ \\ d^3\left(\begin{array}{l}\delta+\eta+\xi+\rho\\+\sigma+\gamma+\varphi\end{array}\right)+d^2\left(\begin{array}{l}\xi\rho+\xi\sigma+\rho\sigma+\xi\gamma+\rho\gamma+\sigma\gamma\\+(\rho+\sigma+\gamma)\varphi+\eta(\xi+\rho+\gamma\\+\varphi)+\delta(\eta+\xi+\rho+\sigma+\gamma+\varphi)\end{array}\right)+ \\ d\left(\begin{array}{l}\varphi\left(\begin{array}{l}\eta\xi\rho+\xi\rho\sigma+\eta\rho\gamma+\xi\rho\gamma+\xi\sigma\gamma\\+\rho\sigma\gamma+(\rho\sigma+(\eta+\rho+\sigma)\gamma\end{array}\right)+\\ \delta\left(\begin{array}{l}(\rho\sigma+\rho\gamma+\sigma\gamma+\xi(\rho+\sigma+\gamma)+\\(\rho+\sigma+\gamma)\varphi+\eta(\xi+\rho+\gamma+\varphi\end{array}\right)\end{array}\right) \end{array} \right).$$

Hence, the proof is proved.

Virus free stability of the system (3.1)-(3.6) are analyzed by taking its Jacobian. In real life, nearly all systems are nonlinear and to understand the behavior of nonlinear system, it is important to linearize the system. This process of linearization approximates the nonlinear system to the nearest linear system at equilibrium points. We compute the Jacobian matrix in order to linearize the system. Analysis of the Eigenvalues of the Jacobian matrix determines the stability of the system.

Theorem 2. Disease-free equilibrium (DFE) is locally asymptotically stable in D, if $R_0 < 1$ and unstable for $R_0 > 1$.

Proof. The disease free equilibrium (DFE) is locally asymptotically stable, if it is stable and local attractive. According to Theorem 1, the dynamic system (3.1)-(3.6) has virus free equilibrium point $K_0 = (M_0, S_0, E_0, Q_0, I_0, R_0) = (0, N, 0, 0, 0, 0)$. The Jacobian matrix at virus free equilibrium point K_0 is

$$J(D_0) = \begin{pmatrix} -d-\delta & -b & 0 & 0 & 0 & \sigma \\ \delta & 0 & 0 & 0 & -\beta & \eta \\ 0 & 0 & -d-\xi-\varphi & 0 & \beta & 0 \\ 0 & 0 & \varphi & -d-\rho & 0 & 0 \\ 0 & 0 & \xi & 0 & -d-\gamma & 0 \\ 0 & 0 & 0 & \rho & \gamma & -d-\eta-\sigma \end{pmatrix}. \quad (3.19)$$

The characteristics equation of the Jacobian matrix (3.19) is

$$|\lambda I - J(D_0)| = 0,$$

$$\begin{vmatrix} d+\delta+\lambda & b & 0 & 0 & 0 & -\sigma \\ -\delta & \lambda & 0 & 0 & \beta & -\eta \\ 0 & 0 & d+\lambda+\xi+\varphi & 0 & -\beta & 0 \\ 0 & 0 & -\varphi & d+\lambda+\rho & 0 & 0 \\ 0 & 0 & -\xi & 0 & d+\lambda+\gamma & 0 \\ 0 & 0 & 0 & -\rho & -\gamma & d+\eta+\lambda+\sigma \end{vmatrix} = 0. \quad (3.20)$$

Updated expression of equation (3.20) is given as:

$$\begin{aligned} &-\beta(d\delta + d\lambda + \delta\lambda + \lambda^2)\xi(d+\lambda+\rho)(d+\eta+\lambda+\sigma) + (d\delta + d\lambda + \delta\lambda \\ &+\lambda^2)(d+\lambda+\rho)(d+\eta+\lambda+\sigma)(d+\lambda+\gamma)(d+\lambda+\xi+\varphi) = 0, \end{aligned} \quad (3.21)$$

and the corresponding Eigenvalues are given as:

$$\begin{aligned} \lambda_1 &= -d, \\ \lambda_2 &= -\delta, \\ \lambda_3 &= -d-\rho, \\ \lambda_4 &= -d-\eta-\sigma, \\ \lambda_5 &= \tfrac{1}{2}(-2d-\xi-\gamma-\varphi-\sqrt{4\beta\xi+\xi^2-2\xi\gamma+\gamma^2+2\xi\varphi-2\gamma\varphi+\varphi^2}), \\ \lambda 6 &= \tfrac{1}{2}(-2d-\xi-\gamma-\varphi+\sqrt{4\beta\xi+\xi^2-2\xi\Upsilon+\gamma^2+2\xi\varphi-2\gamma\varphi+\varphi^2}). \end{aligned} \quad (3.22)$$

Eigenvalues of (λ_1 - λ_5) of the above characteristic equation (3.22) are less than zero and the eigenvalue of λ_6 is less than zero for $R_0 < 1$. Since

$R_0 = \frac{\beta\xi}{(d+\gamma)(d+\xi+\varphi)} < 1.$

Hence according to stability criteria, if $R_0 < 1$, K_0 is locally asymptotically stable and converse the system may have one unstable point and K_0 become unstable. Thus, the theorem claim stands.

Theorem 3. K_0 is globally asymptotically stable with respect to D, if $R_0 < 1$, otherwise unstable.

Proof. Let us define a following candidate Lyapunov function.

$$L(t) = \xi E(t) + (d + \xi + \varphi) I(t). \tag{3.23}$$

Taking the derivative of the Lyapunov function in (3.23) we have.

$$\begin{aligned} \dot{L}(t) &= \xi \dot{E}(t) + (d + \xi + \varphi) \dot{I}(t), \\ &= \xi[\tfrac{\beta SI}{N} - (\xi + \varphi + d) E] + (d + \xi + \varphi)[\xi E - (\gamma + d) I], \\ &= [\xi \tfrac{\beta S}{N} - (\xi + \varphi + d)(\gamma + d)] I, \\ &\leq [\xi\beta - (\xi + \varphi + d)(\gamma + d)] I. \end{aligned} \tag{3.24}$$

Thus, $R_0 = \frac{\beta\xi}{(d+\gamma)(d+\xi+\varphi)} < 1$, implies that $\dot{L}(t) < 0$ within D. According to LaSalle Invariance Principle K_0 equilibrium point is globally asymptotically stable for $R_0 < 1$. Hence, claimed result obtained.

To investigate the endemic equilibrium stability of the point K^*= (M^*, S^*, E^*, Q^*, I^*, R^*), Obviously $I^* \geq 0$, and thus $N \geq S^*$, so that $R_0 = \frac{\beta\xi}{(d+\gamma)(d+\xi+\varphi)} \geq 1$.

Theorem 4. K^* is locally asymptomatically stable with respect to D, if $R_0 > 1$.

Proof. Now to investigate the endemic equilibrium stability of the point K^*= (M^*, S^*, E^*, Q^*, I^*, R^*), obviously $I^* \geq 0$, is only possible when $R_0 > 1$ and thus $N \geq S^*$, so that

$R_0 = \frac{\beta\xi}{(d+\gamma)(d+\xi+\varphi)} \geq 1$,

$$I^* = -\begin{pmatrix} \delta(d+\rho)(d+\eta+\sigma)(d^2 - R_0(d+\gamma)(d+\xi+\varphi) \\ +\gamma(\xi+\varphi) + d(\xi+\gamma+\varphi)) \end{pmatrix} \Big/ \Lambda$$

Simplifying the expression for $I^* \geq 1$, when $R_0 > 1$.

$$I^* = -\begin{pmatrix} \delta(d+\rho)(d+\eta+\sigma)(d^2 - R_0(d^2 + d\gamma + d\xi + d\varphi + \gamma\xi + \gamma\varphi) \\ +d\gamma + d\xi + d\varphi + \gamma\xi + \gamma\varphi) \end{pmatrix} \Big/ \Lambda$$

. For simplification, we use $K = d\gamma + d\xi + d\varphi + \gamma\xi + \gamma\varphi$, then

$$I^* = -\big(\delta(d+\rho)(d+\eta+\sigma)(d^2 - R_0(d^2+K) + K)\big)/\Lambda.$$

By simplifying the above relation, we have

$$I^* = -\big(\delta(d+\rho)(d+\eta+\sigma)(1-R_0)(d^2+K)\big)/\Lambda.$$

So, it is concluded that when $R_0 > 1$, we have $I^* \geq 1$.

Accordingly, endemic stability point $K^*= (M^*, S^*, E^*, Q^*, I^*, R^*)$ is positive for $R_0 > 1$, so the relations in (3.13) to (3.18) are also positive as given below:

$$\begin{aligned}
M^* &= -\begin{pmatrix} ((d+\rho)(d(d+\xi)(d+\eta+\sigma) + (d(d+\eta+\xi) + (d+\xi)\sigma)\gamma) \\ (d(d+\eta+\rho) + (d+\rho)\sigma)(d+\gamma)\varphi)((1-R_0)(d^2+K) \end{pmatrix} \Big/ \Lambda, \\
S^* &= \frac{(d+\gamma)(d+\xi+\varphi)}{\beta\xi}, \\
E^* &= -\big(\delta(d+\rho)(d+\eta+\sigma)(d+\gamma)(1-R_0)(d^2+K)\big)/\Lambda, \\
Q^* &= -\big(\delta(d+\eta+\sigma)(d+\gamma)\varphi((1-R_0)(d^2+K)\big)/\Lambda, \\
I^* &= -\big(\delta(d+\rho)(d+\eta+\sigma)((1-R_0)(d^2+K)\big)/\Lambda, \\
R^* &= -\big(\delta(\xi(d+\rho)\gamma + \rho(d+\gamma)\varphi)((1-R_0)(d^2+K)\big)/\Lambda.
\end{aligned}$$

The endemic equilibrium point $K^*= (M^*, S^*, E^*, Q^*, I^*, R^*)$ and the Jacobian matrix at the endemic point is

$$J(D^*) = \begin{pmatrix}
-d-\delta & -b & 0 & 0 & 0 & \sigma \\
\delta & -I^*\beta & 0 & 0 & -S^*\beta & \eta \\
0 & I^*\beta & -d-\xi-\varphi & 0 & S^*\beta & 0 \\
0 & 0 & \varphi & -d-\rho & 0 & 0 \\
0 & 0 & \xi & 0 & -d-\gamma & 0 \\
0 & 0 & 0 & \rho & \gamma & -d-\eta-\sigma
\end{pmatrix}. \tag{3.25}$$

For simplicity, we use

$A = d+\delta$, $B = d+\xi+\varphi$, $C = d+\rho$,$D = d+\gamma$, $E = d+\eta+\sigma$, $F = I^*\beta$, $G = S^*\beta$,

then (3.25) is given as:

$$J(D^*) = \begin{pmatrix} -A & -b & 0 & 0 & 0 & \sigma \\ \delta & -F & 0 & 0 & -G & \eta \\ 0 & F & -B & 0 & G & 0 \\ 0 & 0 & \varphi & -C & 0 & 0 \\ 0 & 0 & \xi & 0 & -D & 0 \\ 0 & 0 & 0 & \rho & \gamma & -E \end{pmatrix}. \tag{3.26}$$

The characteristic equation of Jacobian matrix (3.26) is

$$|\lambda I - J(D^*)| = \begin{vmatrix} \lambda + A & b & 0 & 0 & 0 & -\sigma \\ -\delta & \lambda + F & 0 & 0 & G & -\eta \\ 0 & -F & \lambda + B & 0 & -G & 0 \\ 0 & 0 & -\varphi & \lambda + C & 0 & 0 \\ 0 & 0 & -\xi & 0 & \lambda + D & 0 \\ 0 & 0 & 0 & -\rho & -\gamma & \lambda + E \end{vmatrix} = 0. \tag{3.27}$$

Equation (3.27) in its simplified form is as follows:

$$\begin{aligned} &\lambda^6 + \lambda^5(A + B + C + D + F + E) + \lambda^4(AB + AC + AD + AF + EA + \\ &BC + BD + BF + EB + CD + CF + EC + d\delta + DF + ED + EF - G\xi) + \\ &\lambda^3(ABC + ABD + ABF + EAB + ACD + ACF + EAC + ADF + EAD + \\ &\mathrm{e}AF - AG\xi + BCD + BCF + \mathrm{e}BC + Bd\delta + BDF + EBD + EBF + Cd\delta + \\ &CDF + ECD + ECF - CG\xi + \mathrm{e}d\delta + d\delta D + EDF - EG\xi) + \\ &\lambda^2(ABCD + ABCF + EABC + ABDF + EABD + \mathrm{E}ABF + ACDF + \\ &EACD + EACF - ACG\xi + EADF - EAG\xi + BCd\delta + BCDF + EBCD + \\ &EBCF + EBd\delta + Bd\delta D + EBDF + ECd\delta + Cd\delta D + ECDF - ECG\xi + \\ &Ed\delta D - d\delta G\xi - F\eta\xi\Upsilon - F\eta\rho\varphi) + \lambda(ABCDF + EABCD + EABCF + \\ &EABDF + EACDF - EACG\xi - AF\eta\xi\Upsilon - AF\eta\rho\varphi + EBCd\delta + BCd\delta D + \\ &EBCDF + EBd\delta D + ECd\delta D - Cd\delta G\xi - CF\eta\xi\Upsilon - Ed\delta G\xi - DF\eta\rho\varphi - \\ &\delta F\xi\sigma\Upsilon - \delta F\rho\sigma\varphi) + EABCDF - ACF\eta\xi\Upsilon - ADF\eta\rho\varphi + EBCd\delta D - \\ &ECd\delta G\xi - C\delta F\xi\sigma\Upsilon - \delta DF\rho\sigma\varphi = 0. \end{aligned} \tag{3.28}$$

To solve the equation (3.28), we apply the Hurwitz criteria by considering the general characteristic equation of a system is written below:

$$a_0 s^n + a_1 s^{n-1} + a_2 s^{n-2} + a_3 s^{n-3} \cdots \ a_{n-1} s^1 + a_n = 0. \tag{3.29}$$

There are n determinants in nth order equation (3.29), e.g., D_1, D_2, D_3 and D_5 are the first, second, third and fifth determinants of the characteristic equation (3.29), respectively, as:

$$\begin{aligned} D_1 &= a_1 \\ D_2 &= \begin{vmatrix} a_1 & a_3 \\ a_0 & b_2 \end{vmatrix} \\ &= a_1 a_2 - a_3 a_0, \\ D_3 &= \begin{vmatrix} a_1 & a_3 & a_5 \\ a_0 & a_2 & a_4 \\ 0 & a_1 & a_3 \end{vmatrix} \\ &= a_3(a_1 a_2 - a_0 a_3) - a_1(a_1 a_4 - a_0 a_5), \end{aligned} \tag{3.30}$$

and

$$\begin{aligned} D_5 &= \begin{vmatrix} a_1 & a_3 & a_5 & a_7 & a_9 \\ a_0 & a_2 & a_4 & a_6 & a_8 \\ 0 & a_1 & a_3 & a_5 & a_7 \\ 0 & a_0 & a_2 & a_4 & a_6 \\ 0 & 0 & a_1 & a_3 & a_5 \end{vmatrix} \\ &= a_1 \begin{vmatrix} a_2 & a_4 & a_6 & a_8 \\ a_1 & a_3 & a_5 & a_7 \\ a_0 & a_2 & a_4 & a_6 \\ 0 & a_1 & a_3 & a_5 \end{vmatrix} - a_0 \begin{vmatrix} a_3 & a_5 & a_7 & a_9 \\ a_1 & a_3 & a_5 & a_7 \\ a_0 & a_2 & a_4 & a_6 \\ 0 & a_1 & a_3 & a_5 \end{vmatrix}. \end{aligned}$$

According to Lienard-Chipart stability criteria [95], a polynomial with real positive coefficients has roots in left half plane if and only if either all even number

determinants are positive or all odd number of determinants are positive. Now equating the coefficients of general characteristics equation, we get

$$
\begin{aligned}
a_0 &= 1,\\
a_1 &= A+B+C+D+E+F,\\
a_2 &= AB+AC+BC+AD+BD+CD+AE+BE+CE+DE+AF\\
&\quad +BF+CF+DF+EF+d\delta-G\xi,\\
a_3 &= ABC+ABD+ACD+BCD+ABE+ACE+BCE+ADE\\
&\quad +BDE+CDE+ABF+ACF+BCF+ADF+BDF+CDF\\
&\quad +AEF+BEF+CEF+DEF+Bd\delta+Cd\delta+dD\delta+dE\delta-AG\xi\\
&\quad -CG\xi-EG\xi,\\
a_4 &= ABCD+ABCE+ABDE+ACDE+BCDE+ABCF\\
&\quad +ACDF+BCDF+ABEF+ACEF+BCEF+ADEF\\
&\quad +CDEF+BCd\delta+BdD\delta+CdD\delta+BdE\delta+CdE\delta\\
&\quad -ACG\xi-AEG\xi-CEG\xi-dG\delta\xi-F\eta\xi\Upsilon-F\eta\rho\varphi\\
&\quad +ABDF+BDEF+dDE\delta,\\
a_5 &= ABCDE+ABCDF+ABCEF+ABDEF+ACDEF+BCDEF\\
&\quad +BCdD\delta+BCdE\delta+BdDE\delta+CdDE\delta-ACeG\xi-CdG\delta\xi\\
&\quad -dEG\delta\xi-AF\eta\xi\Upsilon-CF\eta\xi\Upsilon-F\delta\xi\sigma\Upsilon\\
&\quad -AF\eta\rho\varphi-DF\eta\rho\varphi-F\delta\rho\sigma\varphi,\\
a_6 &= ABCDEF+BCdDE\delta-CdEG\delta\xi-ACF\eta\xi\Upsilon-CF\delta\xi\sigma\Upsilon\\
&\quad -ADF\eta\rho\varphi-DF\delta\rho\sigma\varphi.
\end{aligned}
$$

From equation (3.30)

$D_1 = a_1 = A+B+C+D+E+F,$

for

$A = d+\delta,\ B = d+\xi+\varphi,\ C = d+\rho,\ D = d+\gamma,$

$E = d+\eta+\sigma,\ F = I^*\beta,\ G = S^*\beta,$

thus $D_1 > 0.$

Similarly

$$D_2 = a_1a_2 - a_3a_0,$$

$$\begin{aligned}D_2 &= C^2D + CD^2 + C^2\mathrm{E} + 2CDE + D^2E + C\mathrm{E}^2 + D\mathrm{E}^2 + C^2F + 2CDF + D^2F \\ &\quad + 2CEF + 2DEF + \mathrm{E}^2F + CF^2 + DF^2 + EF^2 + B^2(C + D + \mathrm{e} + F) \\ &\quad + A^2(B + C + D + E + F) + dF\delta + A((B + C + D + E + F)^2 + d\delta) \\ &\quad - (D + F)G\xi + B((C + D + E + F)^2 - G\xi),\end{aligned}$$

$$\begin{aligned}D_2 &= C^2D + CD^2 + C^2E + 2CDE + D^2E + C\mathrm{E}^2 + D\mathrm{E}^2 + C^2F + 2CDF + D^2F \\ &\quad + 2CEF + 2DEF + \mathrm{E}^2F + CF^2 + DF^2 + EF^2 + B^2(C + D + E + F) \\ &\quad + A^2(B + C + D + E + F) + dF\delta + A((B + C + D + E + F)^2 + d\delta) \\ &\quad + B(C + D + E + F)^2 - S^*\beta\xi(D + F + B),\end{aligned}$$

$$\begin{aligned}D_2 &= C^2D + CD^2 + C^2E + 2CDE + D^2E + C\mathrm{E}^2 + D\mathrm{E}^2 + C^2F + 2CDF + D^2F \\ &\quad + 2CEF + 2DEF + \mathrm{E}^2F + CF^2 + DF^2 + EF^2 + B^2(C + D + E + F) \\ &\quad + A^2(B + C + D + E + F) + dF\delta + A((B + C + D + E + F)^2 + d\delta) \\ &\quad + B(C + D + E + F)^2 - \frac{\beta\xi}{R_0}(D + F + B).\end{aligned}$$

Because $R_0 > 1$, therefore $D_2 > 0$. And for third determinant, we get

$$D_3 = a_3(a_1a_2 - a_0a_3) - a_1(a_1a_4 - a_0a_5),$$

$$D_3 = a_3(D_2) - a_1(a_1a_4 - a_0a_5),$$

$$\begin{aligned}D_3 &= ABD^2d\delta + AB^2Dd\delta + 2A^2BDd\delta + ABE^2d\delta + ACD^2d\delta + AB^2Ed\delta \\ &\quad + AC^2Dd\delta + 2A^2BEd\delta + 2A^2CDd\delta + 2ABF^2d\delta + 2AB^2Fd\delta \\ &\quad + 2A^2BFd\delta + ACE^2d\delta + AC^2Ed\delta + 2A^2CEd\delta + 2ACF^2d\delta + 2AC^2Fd\delta \\ &\quad + 2A^2CFd\delta + ADE^2d\delta + AD^2Ed\delta + 2A^2DEd\delta + 2BCF^2d\delta + BC^2Fd\delta \\ &\quad + B^2CFd\delta + 2ADF^2d\delta + B^2D^3 + B^3D^2 + 2A^2B^2D^2 + 2A^2B^2E^2 \\ &\quad + 2A^2C^2D^2 + 2A^2B^2F^2 + 2B^2C^2D^2 + 2A^2C^2F^2 + 2B^2C^2E^2 + 2A^2D^2E^2 \\ &\quad + 2B^2C^2F^2 + 2A^2D^2F^2 + 2A^2E^2F^2 + 2B^2D^2F^2 + 2C^2D^2E^2 + 2B^2E^2F^2 \\ &\quad + 2C^2D^2F^2 + 2C^2E^2F^2 + AB^3D + BCD^3 + B^3CD + BD^3E + B^3DE \\ &\quad + BD^3F + B^3DF + AB^2C^3 + AB^3C^2 + A^2BC^3 + A^2B^3C \\ &\quad + A^3B^2C + AB^2D^2 + A^2BD^2 + A^2B^2D + AB^2D^3 + AB^3D^2\end{aligned}$$

$$
\begin{aligned}
&+ A^2BD^3 + A^2B^3D + A^3BD^2 + A^3B^2D + AB^3E^2 + AC^2D^3 + AC^3D^2 \\
&+ A^2BE^3 + A^2CD^3 + A^2C^3D + A^3BE^2 + A^3CD^2 + A^3B^2E + A^3C^2D \\
&+ A^2B^3F + A^3BF^2 + A^3B^2F + BC^2D^2 + B^3CD^2 \\
&+ B^2C^2D + AC^2E^3 + AC^3E^2 + BC^2D^3 + BC^3D^2 + A^2C^3E \\
&+ A^3CE^2 + A^3C^2E + B^2CD^3 + B^2C^3D + AC^3F^2 + A^2CF^3 \\
&+ A^2C^3F + A^3CF^2 + A^3C^2F + BC^3E^2 + B^2CE^3 + B^2C^3E \\
&+ B^3CE^2 + B^3C^2E + AD^2E^3 + AD^3E^2 + A^2DE^3 + A^2D^3E + A^3DE^2 \\
&+ A^3D^2E + BC^2F^3 + BC^3F^2 + B^2CF^3 + B^2C^3F + B^3CF^2 \\
&+ B^3C^2F + AD^2F^3 + AD^3F^2 + A^2DF^3 + A^2D^3F + A^3DF^2 \\
&+ A^3D^2F + BD^2E^2 + B^2DE^2 + 3B^2D^2E + BD^2F^2 + B^2DF^2 + B^2D^2F \\
&+ AE^2F^3 + AE^3F^2 + BD^2F^3 + BD^3F^2 + A^2EF^3 + A^2E^3F \\
&+ A^3EF^2 + A^3E^2F + B^2DF^3 + B^2D^3F + B^3DF^2 \\
&+ B^3D^2F + CD^2E^3 + CD^3E^2 + C^2DE^3 + C^2D^3E \\
&+ C^3DE^2 + C^3D^2E + BE^2F^3 + BE^3F^2 + CD^2F^3 + B^2E^3F + B^3EF^2 \\
&+ B^3E^2F + C^2DF^3 + C^2D^3F + C^3DF^2 + C^3D^2F + CE^2F^3 + CE^3F^2 \\
&+ C^2EF^3 + C^3E^2F + DE^2F^3 + DE^3F^2 + D^2EF^3 + D^2E^3F \\
&+ B^3Fd\delta + C^3Fd\delta + D^3Fd\delta + E^3Fd\delta + 4ABC^2D^2 + 4AB^2CD^2 \\
&+ 4AB^2C^2D + 4A^2BCD^2 + 4A^2BC^2D + 4A^2B^2CD + 4AB^2C^2E \\
&+ 4A^2BCE^2 + 4A^2BC^2E + 4ABC^2F^2 + 4AB^2CF^2 + 4AB^2C^2F \\
&+ 4A^2BCF^2 + 4A^2BC^2F + 4A^2B^2CF + 3ABD^2E^2 + 4AB^2D^2F \\
&+ 3AB^2DE^2 + 3AB^2D^2E + 3A^2B^2DE + 4ABD^2F^2 + 4AB^2DF^2 \\
&+ 4A^2BDF^2 + 4A^2BD^2F + 4A^2B^2DF + 4ACD^2E^2 + 4AC^2DE^2 \\
&+ 4A^2CD^2E + 4A^2C^2DE + 4ABE^2F^2 + 4AC^2DF^2 + 4AC^2D^2F \\
&+ 4A^2BEF^2 + 4A^2CDF^2 + 4A^2CD^2F + 4A^2B^2EF + 3BC^2DE^2 \\
&+ 3BC^2D^2E + 3B^2CDE^2 + 3B^2CD^2E + 3B^2C^2DE + 4ACE^2F^2 \\
&+ 4AC^2EF^2 + 4AC^2E^2F + 4BCD^2F^2 + 4BC^2DF^2 + 4BC^2D^2F \\
&+ 4A^2CEF^2 + 4A^2CE^2F + 4A^2C^2EF + 4B^2CDF^2 + 4B^2CD^2F \\
&+ 4B^2C^2DF + 4BCE^2F^2 + 4BC^2EF^2 + 4BC^2E^2F + 4B^2CEF^2
\end{aligned}
$$

$$+ 4B^2CE^2F + 4B^2C^2EF + 4ADE^2F^2 + 4AD^2E^2F + 4A^2DEF^2$$
$$+ 4A^2DE^2F + 3B^2DEF^2 + 3B^2DE^2F + 3B^2D^2EF + 4CDE^2F^2$$
$$+ 4CD^2EF^2 + 4CD^2E^2F + 4C^2DEF^2 + 4C^2DE^2F + 4C^2D^2EF$$
$$+ F^3\Upsilon\eta\xi + F^3eta\rho\varphi + A^2C^2d\delta + ADd^2\delta^2 + 2ABD^3F$$
$$+ ABG^2\xi^2 + ABd^2\delta^2 + A^2B^2d\delta + ACd^2\delta^2 + A^2D^2d\delta + AEd^2\delta^2 + A^2E^2d\delta$$
$$+ BFd^2\delta^2 + B^2F^2d\delta + CFd^2\delta^2 + C^2F^2d\delta + DFd^2\delta^2 + D^2F^2d\delta + EFd^2\delta^2$$
$$+ E^2F^2d\delta + ABCD^2 + ABC^2D + AB^2CD + A^2BCD + 2ABCD^3$$
$$+ 2ABC^3D + 2AB^3CD + 2A^3BCD + 2ABCE^3 + 2ABC^3E + 2AB^3CE$$
$$+ 2A^3BCE + 2ABCF^3 + 2ABC^3F + 2AB^3CF + 2A^3BCF + ABDE^2$$
$$+ ABD^2E + AB^2DE + A^2BDE + ABDE^3 + ABD^3E + AB^3DE$$
$$+ 2A^3BDE + ABDF^2 + ABD^2F + AB^2DF + A^2BDF + 2ABDF^3$$
$$+ 2AB^3DF + 2A^3BDF + 2ACDE^3 + 2ACD^3E + 2AC^3DE + 2A^3CDE$$
$$+ 2ACDF^3 + 2ACD^3F + 2AB^3EF + 2AC^3DF + 2A^3BEF + 2A^3CDF$$
$$+ BCD^2E + BC^2DE + B^2CDE + BCDE^3 + BCD^3E + 2BC^3DE$$
$$+ B^3CDE + BCDF^2 + BCD^2F + BC^2DF + B^2CDF + 2ACEF^3$$
$$+ 2ACE^3F + 2AC^3EF + 2BCDF^3 + 2BCD^3F + 2BC^3DF + 2A^3CEF$$
$$+ 2B^3CDF + 2BCEF^3 + 2BCE^3F + 2BC^3EF + 2B^3CEF + 2ADEF^3$$
$$+ 2ADE^3F + 2AD^3EF + 2A^3DEF + BDEF^2 + BDE^2F + BD^2EF$$
$$+ B^2DEF + 2BDEF^3 + BDE^3F + BD^3EF + B^3DEF + 2CDEF^3$$
$$+ 2CDE^3F + 2CD^3EF + 2C^3DEF + 7ABCDE^2 + 7ABCD^2E$$
$$+ 7AB^2CDE + 7A^2BCDE + 8ABCDF^2 + 8ABCD^2F + 8ABC^2DF$$
$$+ 8A^2BCDF + 8ABCEF^2 + 8ABCE^2F + 8ABC^2EF + 8AB^2CEF$$
$$+ 7ABDEF^2 + 7ABDE^2F + 7ABD^2EF + 7AB^2DEF + 7A^2BDEF$$
$$+ 8ACDE^2F + 8ACD^2EF + 8AC^2DEF + 8A^2CDEF + 7BCDEF^2$$
$$+ 7BCD^2EF + 7BC^2DEF + 7B^2CDE + 2A^2DFd\delta + BD^2Fd\delta$$
$$+ BD^2Ed\delta + B^2DEd\delta + 2AEF^2d\delta + 2AE^2Fd\delta + 2BDF^2d\delta + 2A^2EFd\delta$$
$$+ B^2DFd\delta + 2BEF^2d\delta + BE^2Fd\delta + 2CDF^2d\delta + CD^2Fd\delta + B^2EFd\delta$$
$$+ C^2DFd\delta + 2CEF^2d\delta + CE^2Fd\delta + C^2EFd\delta + 2DEF^2d\delta + DE^2Fd\delta$$

$$
\begin{aligned}
&+ D^2EFd\delta + AF^2\Upsilon\eta\xi + CF^2\Upsilon\eta\xi + 2DF^2\Upsilon\eta\xi + D^2F\Upsilon\eta\xi + 2EF^2\Upsilon\eta\xi \\
&+ E^2F\Upsilon\eta\xi + F^2Gd\delta\xi + AF^2eta\rho\varphi + 2BF^2eta\rho\varphi + B^2Feta\rho\varphi \\
&+ DF^2eta\rho\varphi + 2EF^2eta\rho\varphi + E^2Feta\rho\varphi + ABCDE + ABCDF \\
&+ 2ABCDd\delta + 2ABCEd\delta + 4ABCFd\delta + ABDEd\delta + 4ABDFd\delta \\
&+ 2ACDEd\delta + 4ABEFd\delta + 4ACDFd\delta + BCDEd\delta + 4ACEFd\delta \\
&+ 2BCEFd\delta + 4ADEFd\delta + BDEFd\delta + 2CDEFd\delta + ABF\Upsilon\eta\xi \\
&+ ADF\Upsilon\eta\xi + AEF\Upsilon\eta\xi + 2BDF\Upsilon\eta\xi + 2BEF\Upsilon\eta\xi + CDF\Upsilon\eta\xi \\
&+ 2DEF\Upsilon\eta\xi + 2ABGd\delta\xi + 2ADGd\delta\xi + AFGd\delta\xi + BFGd\delta\xi \\
&+ DFGd\delta\xi - EFGd\delta\xi + ABFeta\rho\varphi + ACFeta\rho\varphi + 2BCFeta\rho\varphi \\
&+ BDFeta\rho\varphi + 2BEFeta\rho\varphi + CDFeta\rho\varphi + 2CEFeta\rho\varphi + DEFeta\rho\varphi \\
&- AC^2G\xi - A^2CG\xi - BC^3G\xi - A^3DG\xi - BD^2G\xi - B^2DG\xi - A^3FG\xi \\
&- BE^3G\xi - C^3DG\xi - C^3FG\xi - DE^3G\xi - E^3FG\xi + AB^3d\delta + AC^3d\delta \\
&+ AD^3d\delta - BD^2d\delta - B^2Dd\delta - A^2B^2G\xi + BCG^2\xi^2 \\
&+ ADG^2\xi^2 - A^2D^2G\xi + AFG^2\xi^2 - A^2F^2G\xi + BEG^2\xi^2 + CDG^2\xi^2 \\
&- C^2D^2G\xi + CFG^2\xi^2 - C^2F^2G\xi + DEG^2\xi^2 - D^2E^2G\xi + EFG^2\xi^2 \\
&- ABC^2G\xi - 2AB^2CG\xi - A^2BCG\xi - 2ABD^2G\xi - 2AB^2DG\xi \\
&- 2ACD^2G\xi - 2AB^2EG\xi - AC^2DG\xi - A^2BEG\xi - A^2CDG\xi \\
&- 2AB^2FG\xi - 2A^2BFG\xi + ACE^2G\xi + AC^2EG\xi - 2BCD^2G\xi \\
&+ A^2CEG\xi - 2B^2CDG\xi - 2ACF^2G\xi - A^2CFG\xi - BCE^2G\xi \\
&- ADE^2G\xi - 2AD^2EG\xi - A^2DEG\xi - 2BCF^2G\xi - 2BC^2FG\xi \\
&- 2B^2CFG\xi - 2ADF^2G\xi - 2AD^2FG\xi - 2A^2DFG\xi - 3BDE^2G\xi \\
&- B^2DEG\xi - 2AEF^2G\xi - AE^2FG\xi - BDF^2G\xi - BD^2FG\xi \\
&- B^2DFG\xi - CDE^2G\xi - 2CD^2EG\xi - C^2DEG\xi - 2BEF^2G\xi \\
&- 2BE^2FG\xi - 2CDF^2G\xi - 2CD^2FG\xi - 2B^2EFG\xi - 2C^2DFG\xi \\
&- CE^2FG\xi - C^2EFG\xi + ABC^2d\delta + AB^2Cd\delta + 2A^2BCd\delta \\
&- 2DE^2FG\xi - 2D^2EFG\xi + 2AD^2Fd\delta - ABCG\xi + ABDG\xi - ACDG\xi \\
&- ACEG\xi + BCDG\xi - ACFG\xi + BDEG\xi - BDFG\xi + ABDd\delta \\
&- BCDd\delta - BDEd\delta + BDFd\delta - 4ABCDG\xi - ABCEG\xi
\end{aligned}
$$

$$
\begin{aligned}
&- 5ABDEG\xi - 5ABDFG\xi - ACDEG\xi - 4ABEFG\xi - 4ACDFG\xi \\
&- ACEFG\xi - 5BCDFG\xi - 4BCEFG\xi - 4ADEFG\xi - 4BDEFG\xi \\
&- AF\Upsilon\delta\sigma\xi - BF\Upsilon\delta\sigma\xi - CF\Upsilon\delta\sigma\xi - DF\Upsilon\delta\sigma\xi - EF\Upsilon\delta\sigma\xi - AF\delta\rho\sigma\varphi \\
&- BF\delta\rho\sigma\varphi - CF\delta\rho\sigma\varphi - DF\delta\rho\sigma\varphi - EF\delta\rho\sigma\varphi + 15ABCDEF \\
&- B^2D^2 - F^2\delta\rho\sigma\varphi - F^2\Upsilon\delta\sigma\xi F - BD^2d\delta + 2A^2B^2C^2 + 2A^2C^2E^2 \\
&+ ABD^3 + AB^2E^3 + A^2B^3E + AB^2F^3 + AB^3F^2 + AB^2F^3 + AB^3F^2 \\
&+ A^2BF^3 + A^3BC^2 + A^2BF^3 + BC^2E^3 + B^3C^2D + AC^2F^3 + A^2CE^3 \\
&+ B^2EF^3 + C^2E^3F + C^3EF^2 + D^3EF^2 + D^3E^2 + AE^3d\delta + B^2F\Upsilon\eta\xi \\
&+ 4ABC^2E^2 + 4AB^2CE^2 + 4A^2B^2CE + 3A^2BDE^2 + 3A^2BD^2E \\
&+ 4AB^2EF^2 + 4A^2BE^2F + 4A^2C^2DF + 3BCD^2E^2 + 4AD^2EF^2 \\
&+ 2CF^2eta\rho\varphi + CD^3F^2 + B^2CD^2 + 4AB^2E^2F + 4AC^2D^2E - AC^2FG\xi \\
&+ 4A^2D^2EF + 3BDE^2F^2 + 3BD^2EF^2 - ABE^2G\xi + 4ACD^2F^2 \\
&+ 2ABEF^3 + 2ABE^3F + BCDE^2 + 7ABC^2DE + 8AB^2CDF \\
&+ 8A^2BCEF + 8ACDEF^2 + 7BCDE^2F + BDE^2d\delta \\
&+ C^2Feta\rho\varphi + ABDEF + BCDEF + 2BCDFd\delta + BCF\Upsilon\eta\xi \\
&+ CEF\Upsilon\eta\xi - CFGd\delta\xi + AEFeta\rho\varphi - A^3BG\xi - B^2C^2G\xi - B^2E^2G\xi \\
&- E^2F^2G\xi F - 2A^2BDG\xi - 2ABF^2G\xi - 2BC^2DG\xi - BC^2EG\xi \\
&- 2B^2CEG\xi - BD^2EG\xi - A^2EFG\xi - 2CEF^2G\xi - 2DEF^2G\xi \\
&- 5BCDEG\xi - 4ABCFG\xi - 4CDEFG\xi + 2D^2E^2F^2 + 4A^2CDE^2 \\
&+ 3BD^2E^2F.
\end{aligned}
$$

Due to the complexity of algebraic expression for determinant D_3, we use numeric values to prove that the D_3 is positive for $R_0 > 1$. Details of numerical procedures are available in the appendix 10, which shows that $D3 > 0$. Similarly, in case of fifth determinant, we may split the information as:

$D_5 = D_{5,1} + D_{5,2} + D_{5,3} + D_{5,4} + D_{5,5} + D_{5,6}$

where

$$
\begin{aligned}
D_{5,1} = \; &- (\delta(BCdDE - C\xi(dEG + F\sigma\Upsilon) - DF\rho\sigma\varphi) + AF(BCDE \\
&- \eta(C\xi\Upsilon + D\rho\varphi)))(CDE + CDF + CEF + DEF + Cd\delta + dD\delta
\end{aligned}
$$

$$
\begin{aligned}
&+ dE\delta + B(EF + D(E + F) + C(D + E + F) + d\delta) - CG\xi - EG\xi \\
&+ A(DE + DF + EF + C(D + E + F) + B(C + D + E + F) \\
&- G\xi))\,[(C^2D + CD^2 + C^2E + 2CDE + D^2E + C\mathrm{E}^2 \\
&+ DE^2 + C^2F + 2CDF + D^2F + 2CEF \\
&+ 2DEF + E^2F + CF^2 + DF^2 + EF^2 + B^2(C + D + E + F) \\
&+ A^2(B + C + D + E + F) + dF\delta + A(B^2 + C^2 \\
&+ D^2 + 2DE + E^2 + 2DF + 2EF + F^2 + 2C(D + E + F) + 2B(C \\
&+ D + E + F) + d\delta) - DG\xi - FG\xi + B(C^2 + D^2 + E^2 \\
&+ 2\mathrm{e}F + F^2 + 2D(E + F) + 2C(D + E + F) - G\xi))(CDE \\
&+ CDF + CEF + DEF + Cd\delta + dD\delta + dE\delta + B(EF \\
&+ D(E + F) + C(D + E + F) + d\delta) - CG\xi - EG\xi + A(DE \\
&+ DF + EF + C(D + E + F) + B(C + D + E + F) - G\xi)),
\end{aligned}
$$

$$
\begin{aligned}
D_{5,2} = &-(A + B + C + D + E + F)(-ABCDE - ABCDF - ABCEF \\
&- ABDEF - ACDEF - BCDEF - BCdD\delta - BCdE\delta - BdDE\delta \\
&- CdDE\delta + ACEG\xi + CdG\delta\xi + d\mathrm{e}G\delta\xi + AF\eta\xi\Upsilon + CF\eta\xi\Upsilon + F\delta\xi\sigma\Upsilon \\
&+ AF\eta\rho\varphi + DF\eta\rho\varphi + F\delta\rho\sigma\varphi + (A + B + C + D + E + F)(CDEF \\
&+ CdD\delta + CdE\delta + dDE\delta + B(DEF + dD\delta \\
&+ dE\delta + C(EF + D(E + F) + d\delta)) - CEG\xi - dG\delta\xi \\
&+ A(CDE + CDF + CEF + DEF + B(EF + D(E + F) + C(D \\
&+ E + F)) - CG\xi - EG\xi) - F\eta\xi\Upsilon - F\eta\rho\varphi))] - (A + B + C \\
&+ D + E + F)C^2D + CD^2 + C^2E + 2CDE + D^2E \\
&+ CE^2 + DE^2 + C^2F + 2CDF + D^2F + 2CEF \\
&+ 2DEF + E^2F + CF^2 + DF^2 + EF^2 + B^2(C + D + E + F) \\
&+ A^2(B + C + D + E + F) + dF\delta + AB^2 + C^2 + D^2 \\
&+ 2D\mathrm{e} + E^2 + 2DF + 2EF + F^2 + 2C(D + E + F),
\end{aligned}
$$

$$
\begin{aligned}
D_{5,3} = &-(\delta(BCdDE - C\xi(dEG + F\sigma\Upsilon) - DF\rho\sigma\varphi) + AF(BCDE
\end{aligned}
$$

$$
\begin{aligned}
&- \eta(C\xi\Upsilon + D\rho\varphi)))((CDE + CDF + CEF + DEF + Cd\delta + dD\delta \\
&+ dE\delta + B(EF + D(E + F) + C(D + E + F) + d\delta) \\
&- CG\xi - EG\xi + A(DE + DF + EF + C(D + E + F) \\
&+ B(C + D + E + F) - G\xi))\,((C^2D + CD^2 + C^2E + 2CDE \\
&+ D^2E + C\mathrm{E}^2 + DE^2 + C^2F + 2CDF + D^2F \\
&+ 2CEF + 2DEF + E^2F + CF^2 + DF^2 + EF^2 + B^2(C + D \\
&+ E + F) + A^2(B + C + D + E + F) + dF\delta + A(B^2 \\
&+ C^2 + D^2 + 2DE + E^2 + 2DF + 2EF + F^2 + 2C(D + E + F) \\
&+ 2B(C + D + E + F) + d\delta) - DG\xi - FG\xi + B(C^2 + D^2 + E^2 \\
&+ 2\mathrm{e}F + F^2 + 2D(E + F) + 2C(D + E + F) - G\xi))(CDE \\
&+ CDF + CEF + DEF + Cd\delta + dD\delta + dE\delta \\
&+ B(EFD(E + F) + C(D + E + F) + d\delta) - CG\xi \\
&- EG\xi + A(DE + DF + EF + C(D + E + F) + B(C + D + E \\
&+ F) - G\xi)) - (A + B + C + D + E + F)(\\
&- ABCDE - ABCDF - ABCEF - ABDEF - ACDEF \\
&- BCDEF - BCdD\delta - BCdE\delta - BdDE\delta - CdDE\delta \\
&+ ACEG\xi + CdG\delta\xi + d\mathrm{e}G\delta\xi + AF\eta\xi\Upsilon + CF\eta\xi\Upsilon \\
&+ F\delta\xi\sigma\Upsilon + AF\eta\rho\varphi + DF\eta\rho\varphi + F\delta\rho\sigma\varphi + (A + B \\
&+ C + D + E + F)(CDEF + CdD\delta + CdE\delta + dDE\delta \\
&+ B(DEF + dD\delta + dE\delta + C(EF + D(E + F) + d\delta)) \\
&- CEG\xi - dG\delta\xi + A(CDE + CDF + CEF + DEF \\
&+ B(EF + D(E + F) + C(D + E + F)) - CG\xi - EG\xi) \\
&- F\eta\xi\Upsilon - F\eta\rho\varphi))) - (A + B + C + D + E + F)((C^2D + CD^2 \\
&+ C^2E + 2CDE + D^2E + CE^2 + DE^2 + C^2F + 2CDF \\
&+ D^2F + 2CEF + 2DEF + E^2F + CF^2 + DF^2 + EF^2 \\
&+ B^2(C + D + E + F) + A^2(B + C + D + E \\
&+ F) + dF\delta + A(B^2 + C^2 + D^2 + 2D\mathrm{e} + E^2 + 2DF + 2EF + F^2 \\
&+ 2C(D + E + F) + 2B(C + D + E + F) + d\delta) - DG\xi - FG\xi
\end{aligned}
$$

$$
\begin{aligned}
&+ B(C^2 + D^2 + E^2 + 2EF + F^2 + 2D(E + F) + 2C(D + E + F) \\
&- G\xi))(CdDE\delta + B(dDE\delta + C(DEF + dD\delta \\
&+ dE\delta)) - CdG\delta\xi - dEG\delta\xi - CF\eta\xi\Upsilon - F\delta\xi\sigma\Upsilon \\
&- DF\eta\rho\varphi - F\delta\rho\sigma\varphi + A(B(DEF + C(EF + D(E + F))) + C\mathrm{e}(DF \\
&- G\xi) - F\eta(\xi\Upsilon + \rho\varphi))) - (A + B + C + D + E + F)^2(\delta(BCdDE \\
&- C\xi(dEG + F\sigma\Upsilon) - DF\rho\sigma\varphi) + AF(BCDE - \eta(C\xi\Upsilon + D\rho\varphi))))),
\end{aligned}
$$

$$
\begin{aligned}
D_{5,4} = &+ (CdDE\delta + B(dDE\delta + C(DEF + dD\delta + dE\delta)) - CdG\delta\xi - dEG\delta\xi \\
&- CF\eta\xi\Upsilon - F\delta\xi\sigma\Upsilon - DF\eta\rho\varphi - F\delta\rho\sigma\varphi + A(B(DEF \\
&+ C(EF + D(E + F))) + CE(DF - G\xi) - F\eta(\xi\Upsilon + \rho\varphi))) \\
&(-ABCDE - ABCDF - ABCEF - ABDEF - ACE\mathrm{e}F \\
&- BCDEF - BCdD\delta - BCdE\delta - BdDE\delta - CdDE\delta \\
&+ ACEG\xi + CdG\delta\xi + dEG\delta\xi + (CD + CE + DE \\
&+ CF + DF + EF + B(C + D + E + F) + A(B + C + D + E \\
&+ F) + d\delta - G\xi)(CDE + CDF + CEF + DEF \\
&+ Cd\delta + dD\delta + dE\delta + B(EF + D(E + F) + C(D + E + F) \\
&+ d\delta) - CG\xi - EG\xi + A(DE + DF + EF \\
&+ C(D + E + F) + B(C + D + E + F) - G\xi)) \\
&+ AF\eta\xi\Upsilon + CF\eta\xi\Upsilon + F\delta\xi\sigma\Upsilon + AF\eta\rho\varphi + DF\eta\rho\varphi + F\delta\rho\sigma\varphi),
\end{aligned}
$$

$$
\begin{aligned}
D_{5,5} = &(CdDE\delta + B(dDE\delta + C(DEF + dD\delta + dE\delta)) - CdG\delta\xi - dEG\delta\xi \\
&- CF\eta\xi\Upsilon - F\delta\xi\sigma\Upsilon - DF\eta\rho\varphi - F\delta\rho\sigma\varphi + A(B(DEF \\
&+ C(EF + D(E + F))) + CE(DF - G\xi) - F\eta(\xi\Upsilon + \rho\varphi))) - (CDEF \\
&+ CdD\delta + CdE\delta + dDE\delta + B(DEF + dD\delta + dE\delta + C(EF \\
&+ D(E + F) + d\delta)) - CEG\xi - dG\delta\xi + A(CDE + CDF \\
&+ CEF + DEF + B(EF + D(E + F) + C(D + E + F)) - CG\xi \\
&- EG\xi) - F\eta\xi\Upsilon - F\eta\rho\varphi)[(CDE + CDF + CEF + DEF + Cd\delta
\end{aligned}
$$

$$
\begin{aligned}
&+ dD\delta + dE\delta + B(EF + D(E + F) + C(D + E + F) + d\delta) - CG\xi \\
&- EG\xi + A(DE + DF + EF + C(D + E + F) + (B(C + D + E + F) \\
&- G\xi))^2 - (A + B + C + D + E + F)(CdDE\delta + B(dDE\delta + C(DEF \\
&+ dD\delta + dE\delta)) - CdG\delta\xi - dEG\delta\xi - CF\eta\xi\Upsilon - F\delta\xi\sigma\Upsilon - DF\eta\rho\varphi \\
&- F\delta\rho\sigma\varphi + A(B(DEF + C(EF + D(E + F))) + CE(DF \\
&- G\xi) - F\eta(\xi\Upsilon + \rho\varphi)))),
\end{aligned}
$$

$$
\begin{aligned}
D_{5,6} = &+ (A + B + C + D + E + F)((CDEF + CdD\delta + CdE\delta + dDE\delta \\
&+ B(DEF + dD\delta + dE\delta + C(EF + D(E + F) + d\delta)) - CEG\xi \\
&- dG\delta\xi + A(CDE + CDF + CEF + DEF + B(EF + D(E \\
&+ F) + C(D + E + F)) - CG\xi - EG\xi) - F\eta\xi\Upsilon - F\eta\rho\varphi)((CD \\
&+ CE + DE + CF + DFEF + B(C + D + E + F) + A(B + C \\
&+ D + E + F) + d\delta - G\xi)(CDE + CDF + CEF + DEF + Cd\delta \\
&+ dD\delta + dE\delta + B(EF + D(E + F) + C(D + E + F) + d\delta) - CG\xi \\
&- EG\xi + A(DE + DF + EF + C(D + E + F)B(C + D + E + F) \\
&- G\xi)) - (A + B + C + D + E + F)(CDEF + CdD\delta + CdE\delta + dDE\delta \\
&+ B(DEF + dD\delta + dE\delta + C(EF + D(E + F) + d\delta)) - CEG\xi - dG\delta\xi \\
&+ A(CDE + CDF + CEF + DEF + B(EF + D(E + F) + C(D + E \\
&+ F)) - CG\xi - EG\xi) - F\eta\xi\Upsilon - F\eta\rho\varphi)) + (CDEF + CdD\delta + CdE\delta \\
&+ dDE\delta + B(DEF + dD\delta + dE\delta + C(EF + D(E + F) + d\delta)) \\
&- CeG\xi - dG\delta\xi + A(CDE + CDF + CEF + DEF + B(EF + D(E \\
&+ F) + C(D + E + F)) - CG\xi - EG\xi) - F\eta\xi\Upsilon - F\eta\rho\varphi)(CdDE\delta \\
&+ B(dDE\delta + C(DEF + dD\delta + dE\delta)) - CdG\delta\xi - dEG\delta\xi - CF\eta\xi\Upsilon \\
&- F\delta\xi\sigma\Upsilon - DF\eta\rho\varphi - F\delta\rho\sigma\varphi + A(B(DEF + C(EF \\
&+ D(E + F))) + CE(DF - G\xi) - F\eta(\xi\Upsilon + \rho\varphi))) \\
&- (CDE + CDF + CEF + DEF + Cd\delta + dD\delta + dE\delta + B(EF \\
&+ D(E + F) + C(D + E + F) + d\delta) - CG\xi - EG\xi + A(DE + DF
\end{aligned}
$$

$$+ EF + C(D + E + F) + B(C + D + E + F) - G\xi))(\delta(BCdDE$$
$$- C\xi(dEG + F\sigma\Upsilon) - DF\rho\sigma\varphi) + AF(BCDE - \eta(C\xi\Upsilon + D\rho\varphi)))$$
$$- (CD + CE + DE + CF + DF + EF + B(C + D + E + F)$$
$$+ A(B + C + D + E + F) + d\delta - G\xi)((CD + CE + DE + CF$$
$$+ DF + EF + B(C + D + E + F) + A(B + C + D + E + F) + d\delta - G$$
$$* \xi)(CdDE\delta + B(dDE\delta + C(DEF + dD\delta + dE\delta)) - CdG\delta\xi - dEG\delta\xi$$
$$- CF\eta\xi\Upsilon - F\delta\xi\sigma\Upsilon - DF\eta\rho\varphi - F\delta\rho\sigma\varphi + A(B(DEF + C(EF + D(E$$
$$+ F))) + CE(DF - G\xi) - F\eta(\xi\Upsilon + \rho\varphi))) - (A + B + C + D + E$$
$$+ F)(\delta(BCdDE - C\xi(dEG + F\sigma\Upsilon) - DF\rho\sigma\varphi) + AF(BCDE$$
$$- \eta(C\xi\Upsilon + D\rho\varphi)))))].$$

Due to the complexity of algebraic expression for determinant D_5, we use numeric values to prove that the D_5 is positive for $R_0 > 1$. Details of numerical procedures are available in the appendix 10, which shows that $D5 > 0$. So all roots of the Jacobian matrix are in left half plane for endemic equilibrium points K^* at $R_0 > 1$. According to stability theory, D^* is locally asymptotically stable in D for $R_0 > 1$. This concludes the proof of the theorem.

3.4 Performance Analysis

In this section, we present a set of simulations for proposed MSEQIR model to evaluate the defending mechanism of the model in the presence of immunity and quarantine classes.

3.4.1 Simulation and Results

Adams numerical method is employed to solve and simulate the system of differential equations (3.1)-(3.6) using WOLFRAM MATHEMATICA 12 on 64 bit windows 10 platform. The simulation of differential equation based virus models

are performed under different parameters and initial conditions to evaluate the behavior of the Immune, Susceptible, Exposed, Quarantine, Infected and Recovered Nodes. The results of simulation of the model is compared using known numerical methods.The parameter values used in these simulations agree with the values in real networks in different situations under different operating systems. Error plots of MSEQIR model between Adams with Explicit Runge-Kutta (RK) numerical method are shown in figure 3.3(c, d) for cases 1 and 2, while for cases 3 and 4 are shown in figure 3.4(c, d). In this model, cases 1 and 2 have good built-in control strategies for zero day attacks [96].

3.4.2 Case 1

In this case, MSEQIR model (3.1)-(3.6) behavior is observed by taking the parameters values as follow: the parameters $b = 0.18$, $d = 0.966$, $\delta = 0.715$, $\beta = 0.7$, $\xi = 10$, $\rho = 0.01$, $\varphi = 0.43$, $\sigma = 0.001$, $\eta = 0.001$ and $\gamma = 3.58$ with initial conditions $M(0) = 0.3$, $S(0) = 0.25$, $E(0) = 0.2$, $Q(0) = 0.05$, $I(0) = 0.2$, $R(0) = 0$ and numerical results are shown in figure 3.3(a). The value of R_0 calculated for the said case is 0.13, while from figure 3.3(a), it is observed that the system is asymptomatically stable. Due to an initial increase in immunity and effective antivirus strategy, infection of the nodes decreases rapidly and recovery increases promptly. Interaction of susceptible nodes with infected nodes and decrease in temporary immunity make the system more prone to infection but due to amalgamation of quarantine and immunity, infection will be controlled at earlier stages. Quarantine class plays an important role in the scenario when infection controlling mechanism are fragile or anti-virus signature definition and patch management are outdated. Malicious objects are quarantined and isolated from other resources. The more we quarantine, the lesser we will be infected and the more system will be recovered. When a node updates security through patching, latent period in exposed node reduces exponentially and infection reduces rapidly due to the existence of three in built control process in the model which are immunity, quarantine and hidden antivirus agent.

3.4.3 Case 2

In second case, dynamic behavior of model (3.1)-(3.6) is analyzed by taking the parameters $b = 0.11$, $d = 0.7$, $\delta = 0.715$, $\beta = 0.7$, $\xi = 6.02$, $\rho = 0.026$, $\varphi = 0.586$, $\sigma = 0.168$, $\eta = 0.116$ and $\gamma = 1.95$ with initial conditions $M(0) = 0.3$, $S(0) = 0.25$, $E(0) = 0.2$, $Q(0) = 0.05$, $I(0) = 0.2$, $R\ (0) = 0$ and results are shown in figure 3.3(b). The value of R_0 is equal to 0.21. It is observed that by slightly increasing the values of contact rate, quarantine rate for exposed individuals and recovery rate from quarantine, infection increases slightly and then reduce due to increase in quarantine and recovery rate. Growth of prey (susceptible) decreases slowly even in the presence of predators (infection) due to tight control of update mechanism (immunity and quarantine).

3.4.4 Case 3

The model dynamics is studied by changing the initial conditions and parameter values as: $b = 0.125$, $d = 0.926$, $\delta = 0.3$, $\beta = 0.602$, $\xi = 0.5$, $\rho = 0.001$, $\varphi = 0.106$, $\sigma = 0.068$, $\eta = 0.001$ and $\gamma = 1$ with initial conditions $M(0) = 0.1$, $S(0) = 0.3$, $E(0) = 0.15$, $Q(0) = 0.1$, $I(0) = 0.3$, $R(0) = 0.05$. The calculated value of $R_0 = 0.10$. The numerical results are shown in figure 3.4(a). It is observed that by reducing the initial immunity of nodes, infection of the nodes increases. Due to outdated antivirus signature definition, recovery from quarantine is less and overall node recovery reduces, instead of increasing infection, it reduces rapidly, which shows that quarantine play an important role in the scenarios where patch and virus signature definitions updating take longer or are not possible.

3.4.5 Case 4

In this scenario, system dynamics is studied by changing the tunable parameters with the same initial conditions as in case 3, changed parameter values are $b = 0.16$, $d = 1$, $\delta = 0.464$, $\beta = 1$, $\xi = 0.5$, $\rho = 0.116$, $\varphi = 0.85$, $\sigma = 0.352$, $\eta = 0.001$

and $\gamma = 13.05$ with initial conditions $M(0) = 0.1$, $S(0) = 0.3$, $E(0) = 0.15$, $Q(0) = 0.1$, $I(0) = 0.3$, $R(0) = 0.05$. The dynamic behavior of the model is shown in figure 3.4(b) with $R_0 = 0.01$. It is seen that updating anti-virus software, recovery from infection and quarantine are increased which decreases the number of infectious nodes. Behavior analysis of node in the presence of immunity and quarantine class is performed in figure 3.5(b). It is observed that if the immunity of the system is increased due to software patching and update in operating system, the nodes in quarantine class are decreased and as immunity of the system decreases, increases in quarantine class is observed. Figure 3.5(a) shows the relationship between susceptible and recovered nodes, susceptible nodes depend on the number of recovered nodes and new computer connected to the network. More recovery mean more number of nodes are available for prey (susceptible) and figure 3.5(c) shows the relationship between immunity and susceptible nodes. In figure 3.5(f), initially the number of immune nodes increases due to hardening (or patching), this causes a reduction in the number of recovered nodes. Decreasing the immunity increases the number of susceptible nodes which ultimately increases the number of exposed nodes 3.5(e); this also causes an increase in the number of quarantined nodes 3.5(d). Simulation results agree with the real life circumstances. The predecessor of this model is used in the field of biology and the enhanced version of this model (with inclusion of Quarantine class) has been developed for virus modeling in computer networks. The designed model is novel and simulated with initial conditions and parameters adjusted as per computer network viruses, comparative analysis with biological virus spread is not available.

3.5 Chapter Summary

A MSEQIR dynamic epidemic model has been designed for the transmission of viruses in computer network. The propagation of virus in this model are both horizontal and vertical. We assume that system has temporary immunity and infected nodes will stay in the latent period before they become infectious. The virus free equilibrium of the model is asymptotically stable for $R_0 < 1$ and unstable

for $R_0 > 1$. This model depicts the real situation of the system in the presence of immunity and quarantine. It is observed that quarantine and immunity play an important role in the situation where virus signature and patch update are difficult, especially in remote locations or bandwidth or resource limited systems. Due to the availability of two recovery mechanisms, the immunity and quarantine, recovery of infectious nodes is very high and crashing of node due to infection is low. The proposed model can be effectively utilized for zero day attacks and preparation of pre-emptive antivirus software. The inclusion of quarantine class reduces the chances of the system to become endemic.

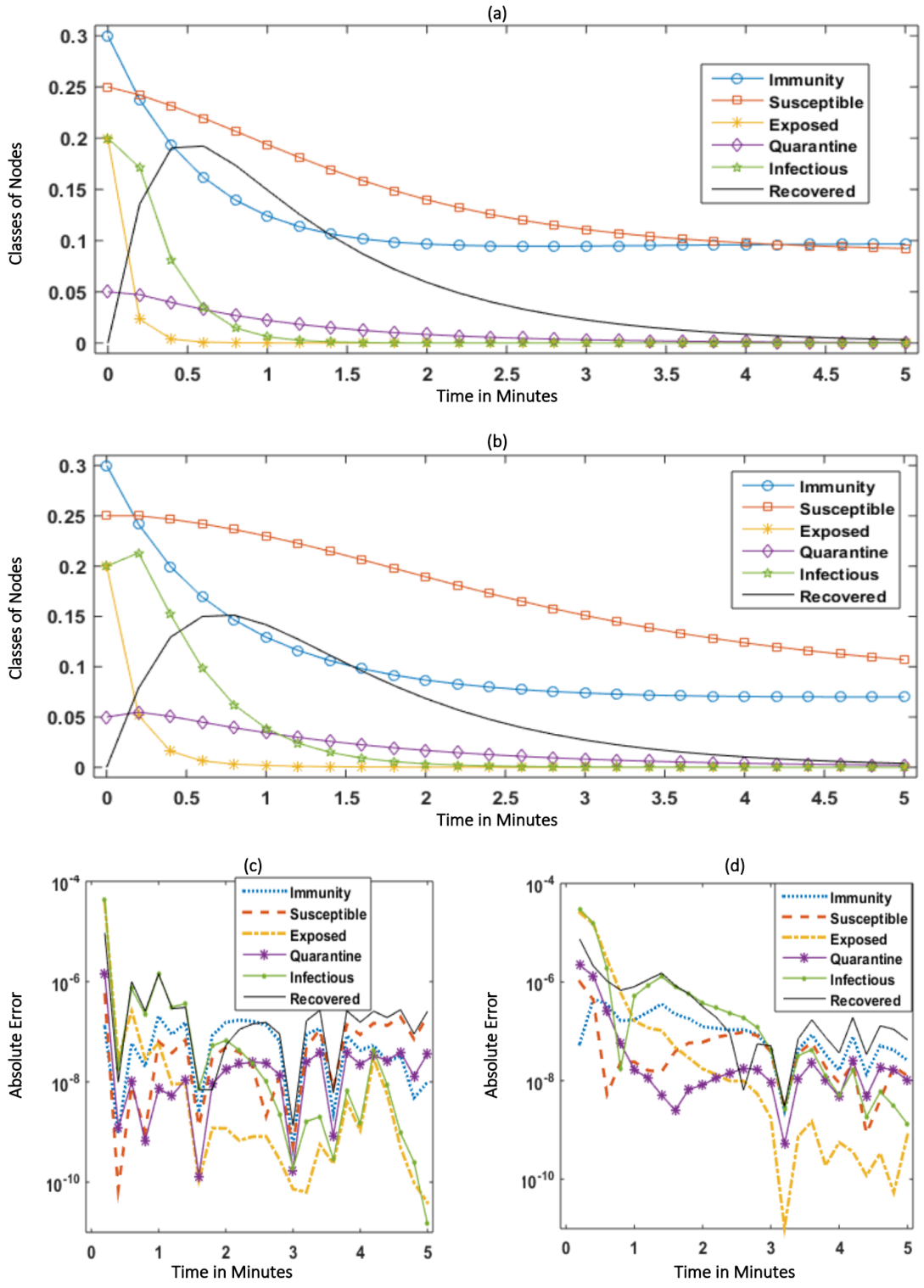


FIGURE 3.3: Dynamic behavior of model (a) Case 1, (b) Case 2, (c) Absolute error of Adams from explicit RK method for Case 1 and (d) Absolute error of Adams from explicit RK method for case 2.

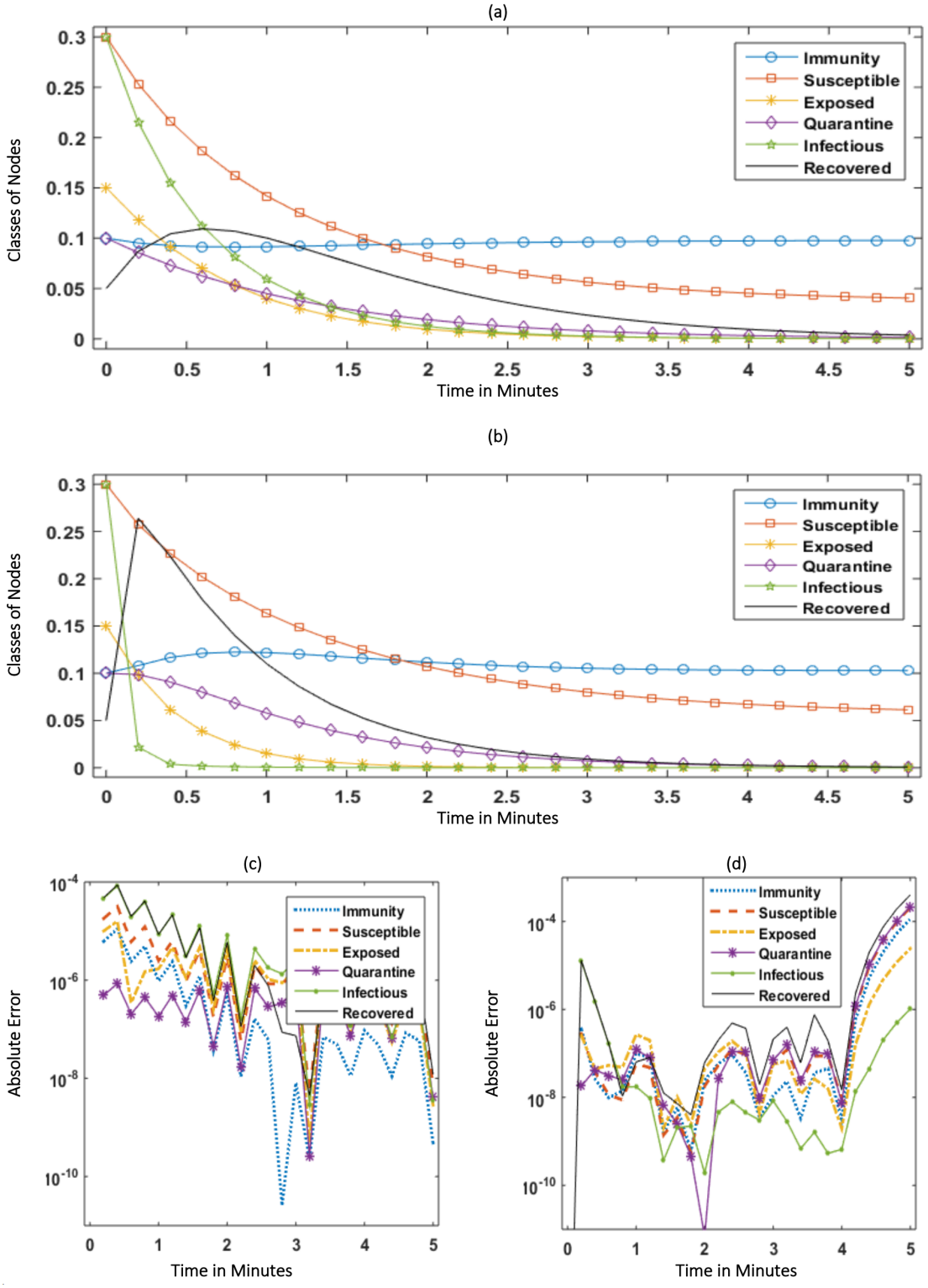
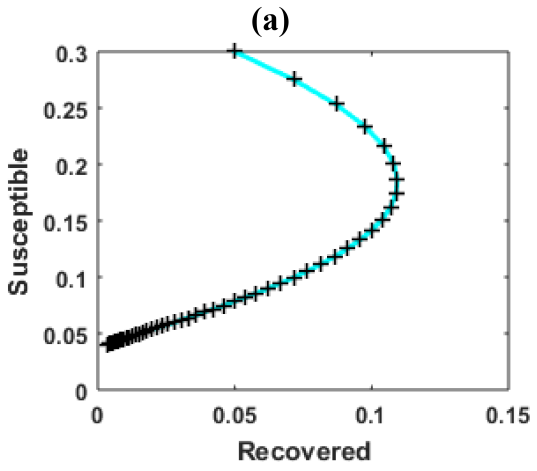
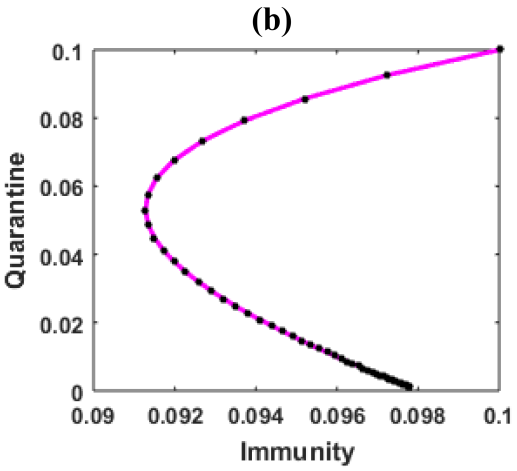


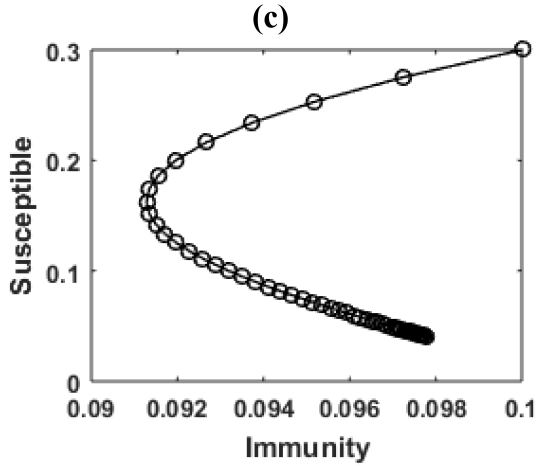
FIGURE 3.4: Dynamic Behavior of model (a) Case 3, (b) Case 4, (c) Absolute error of Adams from RK method for Case 3 and (d) Absolute error of Adams from RK method for case 4.



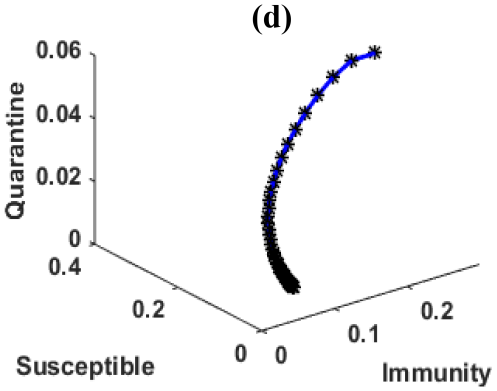
Dynamic behavior of Susceptible, Recovered Node



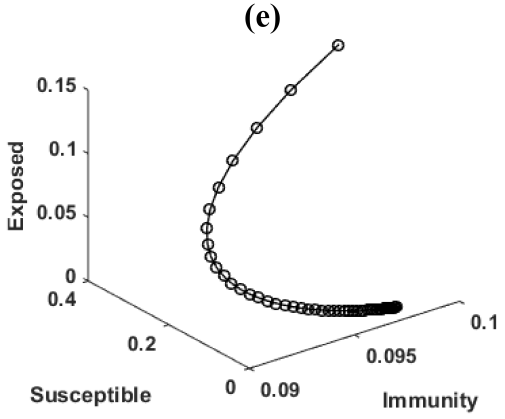
Effect of Immunity on Quarantine



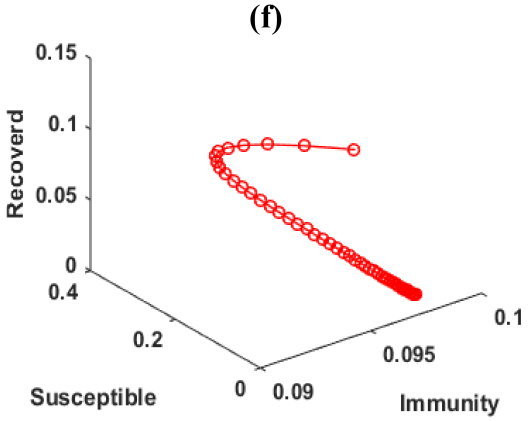
Behavior of immunity Versus Susceptible



Behavior of Immunity, Quarantine and Susceptible Nodes



Behavior of Immunity, Exposed and Susceptible Nodes



Dynamic behavior of Effect of Immunity

FIGURE 3.5: Parameteric plots of different cases of virus model.

Chapter 4

Dynamic Analysis of Stuxnet Virus Spread

4.1 Introduction

In this chapter, spread of virus infection due to removable storage media and infected hosts are analyzed. Removable storage media plays an important role in bridging the air-gap between isolated critical networks and commercial networks. Ease of use and connectivity increases the role of removable storage media in transfering data and virus to the computers connected to critical network (consisting of industrial controllers) which are isolated from main networks. In early 1990s, special hardware and protocols were used in most of the process control mechanisms designed to manage critical systems such as electric grid station, power plant, oil machinery, Radar and water monitoring etc. This makes the whole process simple, however, it also makes the system vulnerable to attack [126]. In March 2007, Idaho National Laboratory conducted an Aurora vulnerability test, which allows the attacker to remotely control the high voltage circuit breaker to destroy the generator by quickly opening and closing the breaker [198]. On January 25, 2003 at 12:30 AM eastern standard time, Slammer started to exploit the vulnerability of Microsoft SQL server and in just ten minutes, it infected about 75,000 servers

worldwide, and only South Korea confronted with half-day internet outage [199]. Process control operators believe that their systems are impenetrable to virus attack firstly due to isolation of their process control systems from the internet, and secondly with the usage of the proprietary protocols for communication. However, many operators replacing their outdated hardware with new one to move towards open protocols and in this process few control systems may connect with Internet unintentionally and makes scenario vulnerable for attack [24]. The air-gap between isolated industrial computer networks and public networks could be bridged by the use of infected removable storage media [200], e.g., Manchester police disconnected from head office for three days due to infection caused by such devices [201]. Stuxnet a 500-kbyte worm, is one of the most complex virus that was primarily written for industrial control systems which can spread using several dimensions but most notorious in this regard are USB devices [138, 202]. The internal design of Stuxnet is very stealthy, complex and hiding ability for large span of time, e.g., Stuxnet virus waits for seventeen months for conducive environment and smartly delay the processes instead of destroying the centrifuges completely [139, 203].

The behaviour of such malicious codes have been conducted by the research community through epidemiology modelling of virus propagation [65, 204]. The control strategies for these sophisticated malicious codes are very difficult due to acquiring a place as a legitimate system process, attaining admin rights, capacity of injecting infectious code in system dynamic link libraries and removing traces [205, 206]. The Stuxnet virus possess all sophisticated virus properties to exploit the zero-day vulnerabilities to target the victims [207, 208]. The advancement in Internet technologies poses great challenges to the security of the critical infrastructure of the nations in the presense of such vulnerability. Therefore, it looks promising to have detailed analysis of dynamic behaviour of these malicious codes and device a controlling strategy to overcome their devastation effectively. Mathematical modelling of malicious code provides us platform for profound understanding of the problem and gives, us a path to devise flexible, stable and robust controlling strategies.

A mathematical model is designed to analyze the behaviour of the Stuxnet type virus, a very refined piece of code, which got the name of first "digital weapon" in news and got the fame a nation versus nation cyber-attack [210]. Our goal in this study is to design a mathematical model that depicts the Stuxnet spread and attacks in a working environment and its impact on critical infrastructures managed by industrial control computers. Few studies are conducted to observe the effect of removable media in the spread of worm [80–82], however in these investigations the model behavior is theoretically verified without the use of real data. Additionally, these models did not establish a link with critical industrial computer scenarios. Main contributions of the proposed virus model based on susceptible, infected, removed, susceptible and infected removable storage media ($SIPU_SU_I$) are highlighted as:

1. A novel computer virus model $SIPU_SU_I$ is designed with ability to accurately model the security of isolated critical industrial control networks.
2. Local stability analysis through the basic reproduction number R_0 of the model is ascertained at equilibria points both for virus free and endemic spread scenarios.
3. Validation of the model through global stability analysis with Lyapunov function further esteblishes its worth.
4. Numerical simulation is performed to test the accuracy of the model for Stuxnet virus, results shows that the model matches the actual situation with reasonable accuracy.

4.1.1 An Overview of Stuxnet Virus

Stuxnet, a complex virus that mainly targets industrial control systems, uses four zero-day vulnerabilities to attack and have capability to hide itself from antivirus programs. Stuxnet uses two stolen digital certificates to show itself as a legitimate program with deep knowledge of targeted Siemens supervisory control and data acquisition (SCADA) systems. Stuxnet was discovered in June 2010, and it was used to attack the Iranian nuclear enrichment plant at Natanz as shown in

Figure 4.1. The facility at Natanz consists of centrifuge in a cascaded manner in which, the output of one centrifuge piped through the input of the second and so on. Stuxnet has several built-in malicious modules that makes it a sophisticated cyber weapon. The virus exploits four zero-day vulnerabilities, changes system libraries, attacks step7 (Siemens SCADA system), installs signed drivers, hides its presence, clears logs and runs remote procedure call server for communication with its control center and version update [122]. The components of the the virus are graphically shown in Figure 4.2. Stuxnet virus spreads in the system by an infected USB connected to the system and after infecting the first computer, further attacks the network by exploiting different vulnerabilities. The ultimate target of the virus was a machine connected to the centrifuges and managed by the programmable logical controllers (PLCs), a special purpose computers. Typically, such computers are not connected to the Internet and usually work in stand-alone environment. Therefore, Stuxnet uses other transmission methods via USBs to reach the target computers. The vulnerability caused by USBs is common, e.g., in China 26% infections were due to USB malware in year 2009, that exploit the auto-run features of windows [201]. Different Stuxnet versions use different exploits, the latest version uses a Windows LNK vulnerability; older versions use the 'autorun.inf' file vulnerability as shown in Figure 4.3. Stuxnet searches the target Siemens WinCC, an interface used to control the SCADA systems, by connection to SQL database using hardcoded passwords and uploads the infected version. Then, Stuxnet spreads in networks via network shares, windows print spooler MS 10-061 zero-day vulnerability, server message block used for file sharing, zero-day MS 08-067 vulnerability, etc. Stuxnet infects the Siemens SIMATIC Step7 programs that are opened on infected computers. Stuxnet uses built-in peer to peer networks for update of older versions on the local network. Each copy starts remote procedure call service and listens to connection and all connected nodes update themselves. Stuxnet also tries to contact with command and control servers by sending data in encrypted form [22]. Stuxnet is not really harmful for ordinary users, however uses them as a medium to reach the target, i.e., the Siemens PLCs [211]. The virus hides itself from plant operators by installing rootkit on

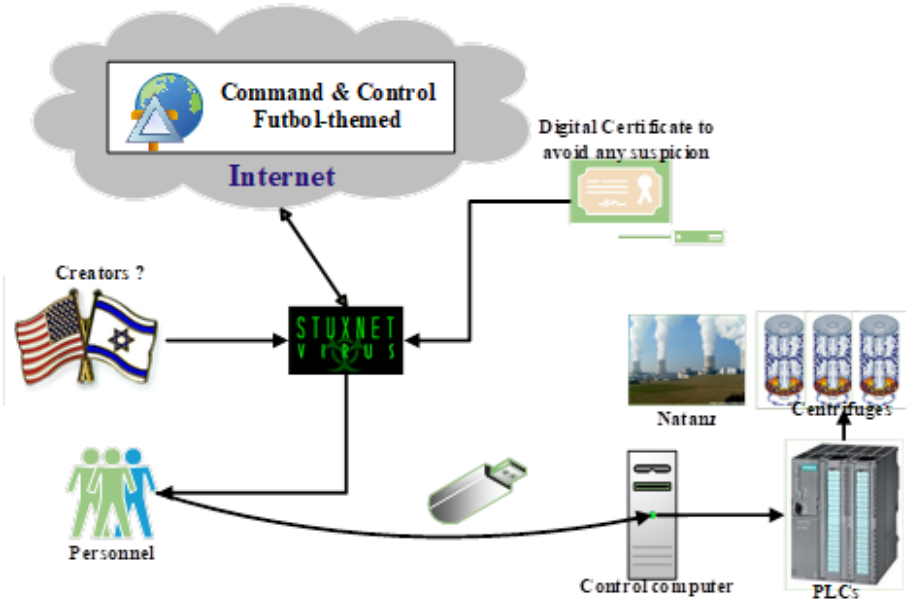


FIGURE 4.1: Overview of Stuxnet

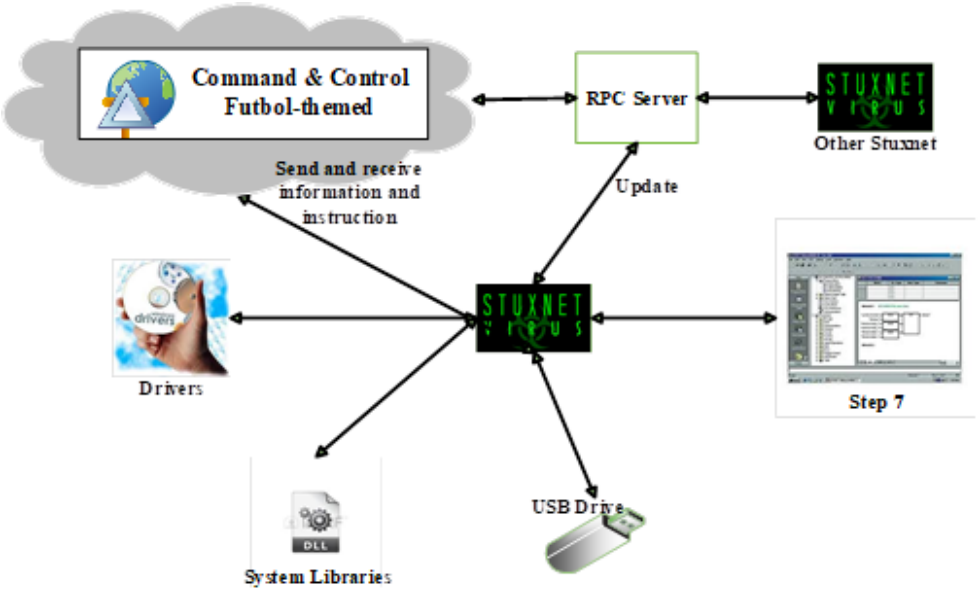


FIGURE 4.2: Stuxnet components

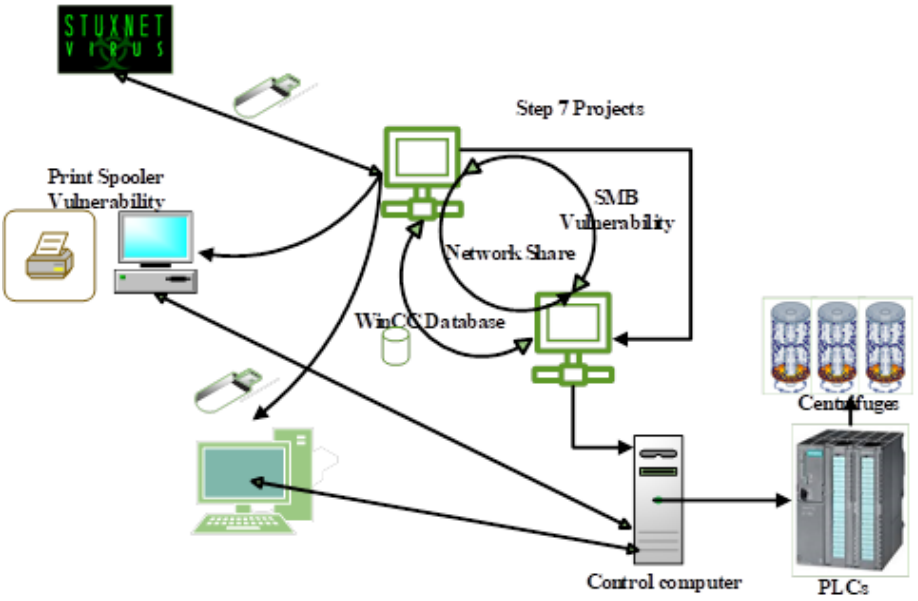


FIGURE 4.3: Different Methods that Stuxnet uses to exploit its target

the infected computers and PLCs. The Stuxnet attack destroyed 1,000 centrifuges out of the 5,000 operating at the Natanz facility [121]. Similar cyber-attacks have evolved a lot over the years for criminal and terrorist entities and also by states as weapons. They can be used not only to gather information, but also to destroy infrastructures.

4.2 The Epidemic Model for Stuxnet Virus

In this section, necessary description for the formulation of $\mathrm{SIPU_SU_I}$ mathematical model is presented as shown in Figure 4.4. The total population $N(t)$ is partitioned into Susceptible nodes, Infected nodes, Damaged nodes and represented by $S(t)$, $I(t)$ and $P(t)$, respectively. The USB susceptible and USB infected media is denoted by $U_s(t)$, and $U_I(t)$, respectively, with $N = S + I + P$ and $U = U_s + U_I$. In this configuration, all computers (networked or stand-alone) which are not infected by the virus fall under the category of susceptible computers. Infected computers are those that are infected due to network sharing or by connecting removable storage media, i.e., USBs. Damaged computers are those that are temporarily unable to perform their desired function and thus removed from the setup.

Susceptible removable storage media are those that are virus free but can become the prey of infection if connected with infected nodes. Infected removable storage media are the main source of infection spread in the network due to weak firmware security and plug and play features of USB devices. Let A_1 be the arrival of new computers and A_2 be the arrival of removable storage devices, ρ is the damage rate due to virus infection caused in control computers, connected to PLCs. β_1 and β_2 denotes the rate of infection transfer from infected computers to susceptible computers on the network and from infected removable devices to susceptible computers, respectively. The natural removal (death) rates of computers and removable devices from the network are represented by r_1 and r_2 respectively. The probability of finding susceptible computers on network in Internet protocol version 4 (IPv4) scheme is $S/2^{32}$ (the total number of computers in IPv4 are 2^{32}). Removable storage devices are the major source of virus spread in air gapped critical industrial networks, they bridge the gaps and provide the environment for predators to target their prey [212]. In this chapter, we model the spread of virus, especially Stuxnet [213, 214] in critical networks through removable storage media and infected computers. Data flow in the model is shown in Figure 4.5, while the following differential equations describe the propagation of the Stuxnet virus:

$$\begin{aligned}
\frac{dS}{dt} &= A_1 - \frac{\beta_1 S(t) I(t)}{2^{32}} - \frac{\beta_2 S(t) U_I(t)}{N(t)} - r_1 S(t), \\
\frac{dI}{dt} &= \frac{\beta_1 S(t) I(t)}{2^{32}} + \frac{\beta_2 S(t) U_I(t)}{N(t)} - \rho I(t) - r_1 I(t), \\
\frac{dP}{dt} &= \rho I(t) - r_1 P(t), \\
\frac{dU_s}{dt} &= A_2 - \frac{\beta_2 U_s(t) I(t)}{N} - r_2 U_s(t), \\
\frac{dU_I}{dt} &= \frac{\beta_2 U_s(t) I(t)}{N} - r_2 U_I(t),
\end{aligned} \tag{4.1}$$

while the associated initial conditions are given as follows:
$S(0) = S_0$, $I(0) = I_0$, $P(0) = P_0$, $U_s(0) = Us_0$, $U_I(0) = U_{I0}$.

$$\frac{dN}{dt} = A_1 - r_1 N, \tag{4.2}$$

$$\frac{dU}{dt} = A_2 - r_2 U,$$

where the arrival rate of the new nodes is represented by A_1 and death rate by r_1, while A_2 represents the arrival rate of new removable storage devices and r_2 their removal rate. Accordingly, the net rate of change of the population is given by $c_1 = A_1 - r_1$ and $c_2 = A_2 - r_2$ which may be positive, zero or negative. Solving

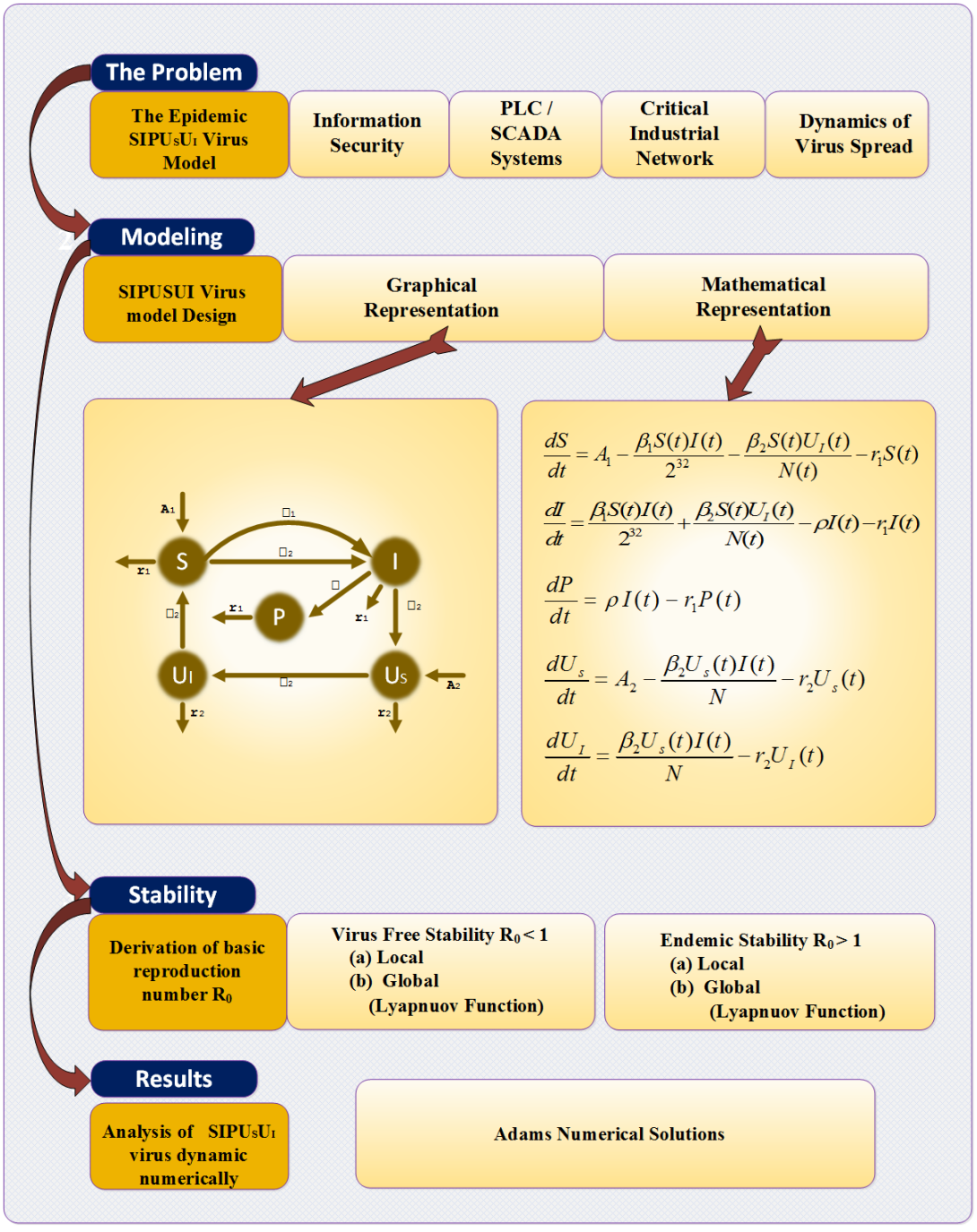


FIGURE 4.4: Graphical abstract of proposed $SIPU_SU_I$ model

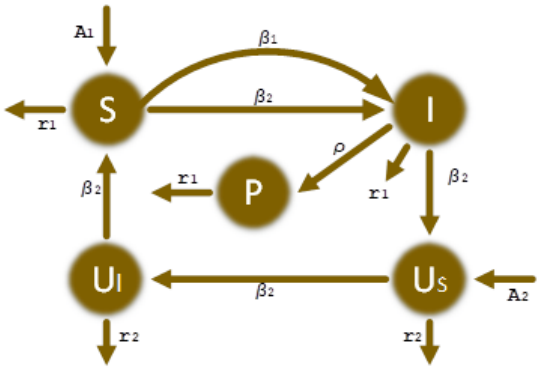


FIGURE 4.5: Schematic flow of proposed SIPU$_S$U$_I$ model

set of equations (4.2), we get

$$N(t) \to \frac{A_1}{r_1} \triangleq N^*, \, t \to \infty, \tag{4.3}$$

$$U(t) \to \frac{A_2}{r_2} \triangleq U^*, \, t \to \infty.$$

The system of equations (4.1) can be written in simplified or reduced form as:

$$\begin{aligned} \frac{dI}{dt} =& \frac{\beta_1(N(t) - I(t) - P(t))I(t)}{2^{32}} + \frac{\beta_2(N(t) - I(t) - P(t))U_I(t)}{N(t)} \\ & - \rho I(t) - r_1 I(t), \\ \frac{dP}{dt} =& \rho I(t) - r_1 P(t), \\ \frac{dU_I}{dt} =& \frac{\beta_2(U(t) - U_I(t))I(t)}{N(t)} - r_2 U_I(t). \end{aligned} \tag{4.4}$$

Where

$$N(t) = N^* + (N(0) - N^*)e^{-r_1 t},$$

and

$$U(t) = U^* + (U(0) - U^*)e^{-r_2 t}.$$

Using equation (4.3) in system (4.4) one have a limit system (IPUI) as [140]:

$$\begin{aligned} \frac{dI}{dt} =& \frac{\beta_1(N^* - I - P)I}{2^{32}} + \frac{\beta_2(N^* - I - P)U_I}{N^*} - \rho I - r_1 I, \\ \frac{dP}{dt} =& \rho I - r_1 P, \end{aligned} \tag{4.5}$$

$$\frac{dU_I}{dt} = \frac{\beta_2(U^* - U_I)I}{N^*} - r_2 U_I.$$

4.3 Model Analysis

4.3.1 Basic Reproduction Number (R_0)

The basic reproduction number is defined as the advent of a new infection caused by an infected individual and denoted by R_0. R_0 is the parameter of infection spread, if $R_0 > 1$, then infection spreads rapidly in the system and if $R_0 < 1$ then infected individuals will not be able to spread the infection and die down. Different methods are used to calculate the basic reproduction number R_0 in epidemiology modeling [215]. Detail of R_0 calculation with next generation matrix is also given in appendix 10.

Model $\mathrm{SIPU_SU_I}$ has been reduced to three classes as given in equation (4.5) and only two classes are infected. The essential condition for occurrence of an epidemic is that the number of infected nodes should increase with the assumption that at the beginning all populations are susceptible.

$$\text{For } \frac{dI}{dt} > 0, \text{we have}$$

$$\frac{\beta_1(N^* - I - P)I}{2^{32}} + \frac{\beta_2(N^* - I - P)U_I}{N^*} - \rho I - r_1 I > 0,$$

$$\text{In case } \frac{dU_I}{dt} > 0,$$

$$\frac{\beta_2(U^* - U_I)I}{N^*} - r_2 U_I > 0,$$

Assuming that all the population should be susceptible, we may write the above expression as:

$$\frac{\beta_1 N^* I}{2^{32}} + \frac{\beta_2 N^* U_I}{N^*} - \rho I - r_1 I > 0,$$

$$\frac{\beta_2 U^* I}{N^*} - r_2 U_I > 0.$$

Simplifying above relation, we have

$$\frac{\beta_1 N^*}{(\rho + r_1)2^{32}} + \frac{\beta^2{}_2 U^*}{r_2 N^*(\rho + r_1)} > 1.$$

Accordingly,

$$R_0 = \frac{\beta_1 N^*}{2^{32}(\rho + r_1)} + \frac{\beta^2{}_2 U^*}{r_2 N^*(\rho + r_1)}. \tag{4.6}$$

4.3.2 Equilibria Studies

The model IPU_I in set of equations (4.5) has two equilibrium points; virus free point at which no virus exists in the system and endemic equilibria point, at which infection spread in the system. Virus free equilibria point for system (4.5) is K_0= $(I, P, U_I) = (0, 0, 0)$ and endemic equilibria point is $K^* = (I^*, P^*, U_I^*)$ for R_0> 1. The set of equations (4.5) for endemic equilibria analysis are written as:

$$\begin{aligned} \frac{\beta_1(N^* - I - P)I}{2^{32}} + \frac{\beta_2(N^* - I - P)U_I}{N^*} - \rho I - r_1 I = 0, \\ \rho I - r_1 P = 0, \\ \frac{\beta_2(U^* - U_I)I}{N^*} - r_2 U_I = 0. \end{aligned} \tag{4.7}$$

Solving set of equations (4.7), we will get expression for the endemic equilibrium point (I^*, P^*, U_I^*) as:

$$I^* = \frac{\sqrt{b^2 - 4ac} - b}{2a}, \tag{4.8}$$

$$P^* = \frac{\rho}{r_1} I^*, \tag{4.9}$$

$$U_I{}^* = \frac{\beta_2 U^*}{\beta_2 I^* + r_2 N^*} I^*, \tag{4.10}$$

where

$$a = \frac{(\rho + r_1)\beta 1 \beta 2}{2^{32} r_1 N^*}, c = (\rho + r_1)(1 - R_0) r_2,$$

$$b = \frac{\beta_2(\rho + r_1)(1 - R_0)}{N^*} + \frac{\beta_2{}^3 U^*}{N^* r_2} + \frac{\beta_1(r_2)\beta_2{}^2 U^*}{2^{32} r_1}(\rho + r_1).$$

From equation (4.8), the condition $I^* > 0$ is only possible whenever the value of $R_0 > 1$.

4.3.3 Disease Free Equilibria

Theorem 4.1. Disease-free equilibrium (DFE) is locally asymptotically stable in K_0, if $R_0 < 1$.

Proof. The system is locally asymptotically stable at DFE point $K_0 = (I, P, U_I) = (0, 0, 0)$. Consider the Jacobian matrix of function with components:

$$\begin{aligned} f_1(I, P, U_I) &= \tfrac{\beta_1(N^*-I-P)I}{2^{32}} + \tfrac{\beta_2(N^*-I-P)U_I}{N^*} - \rho I - r_1 I, \\ f_2(I, P, U_I) &= \rho I - r_1 P, \\ f_3(I, P, U_I) &= \tfrac{\beta_2(U^*-U_I)I}{2^{32}} - r_2 U_I, \end{aligned}$$

is given as:

$$J(I, P, U_I) = \begin{pmatrix} \frac{\partial f_1}{\partial I} & \frac{\partial f_1}{\partial P} & \frac{\partial f_1}{\partial U_I} \\ \frac{\partial f_2}{\partial I} & \frac{\partial f_2}{\partial P} & \frac{\partial f_2}{\partial U_I} \\ \frac{\partial f_3}{\partial I} & \frac{\partial f_3}{\partial P} & \frac{\partial f_3}{\partial U_I} \end{pmatrix}.$$

Therefore, the Jacobian matrix of K_0 DFE point is given as:

$$DFE(K_0) = \begin{pmatrix} \frac{\beta_1 N^*}{2^{32}} - \rho - r_1 & 0 & \beta_2 \\ \rho & -r_1 & 0 \\ \frac{\beta_2 U^*}{N^*} & 0 & -r_2 \end{pmatrix}. \tag{4.11}$$

To find the Eigenvalues, the characteristic equation of above matrix is

$$|\lambda I - DFE(K_0)| = \begin{vmatrix} \lambda - \frac{\beta_1 N^*}{2^{32}} + \rho + r_1 & 0 & -\beta_2 \\ -\rho & \lambda + r_1 & 0 \\ -\frac{\beta_2 U^*}{N^*} & 0 & \lambda + r_2 \end{vmatrix} = 0,$$

and in simplify form as:

$$(\lambda + r_1)\left[\left(\lambda - \frac{N^*\beta_1}{2^{32}} + \rho + r_1\right)(\lambda + r_2) - \frac{{\beta_2}^2 U^*}{N^*}\right] = 0,$$

while the corresponding Eigenvalues are

$$\begin{aligned}
&\lambda_1 = -r_1, \\
&\left[\left(\lambda+\rho+r_1-\tfrac{N^*\beta_1}{2^{32}}\right)(\lambda+r_2)-\tfrac{{\beta_2}^2U^*}{N^*}\right]=0, \\
&(\lambda+r_2)(\rho+r_1)\left(1-\tfrac{N^*\beta_1}{2^{32}(\rho+r_1)}\right)-\tfrac{{\beta_2}^2U^*}{N^*}=0.
\end{aligned} \tag{4.12}$$

The equation (4.12) using (4.6) is written as:

$$\begin{aligned}
&1-\left(\tfrac{N^*\beta_1}{2^{32}(\rho+r_1)}+\tfrac{{\beta_2}^2U^*}{N^*r_2(\rho+r_1)}\right)>0, \\
&1-R_0>0.
\end{aligned} \tag{4.13}$$

If $R_0 < 1$, then the corresponding equation (4.13) is positive, which show that all Eigenvalues of the system (4.12) are in a negative half plane, so the system is asymptotically stable for points K_0 when $R_0 < 1$. This completes the proof.

Theorem 4.2. If $R_0 < 1$, then the point K_0 is globally asymptotically stable, otherwise unstable.

Proof. Let us consider the following Lyapunov function.

$$L(I,P,U_I) = I + \frac{\beta_1}{2^{33}\rho}P^2 + \frac{\beta_2}{r_2}U_I. \tag{4.14}$$

The function is always positive in R^3, for $R^3 = (I,\ P,\ U_I)$ and $(I > 0,\ P > 0,\ U_I > 0)$.

Taking the derivative of the Lyapunov function (4.14) we get

$$\begin{aligned}
\dot{L}(I,P,U_I) &= \dot{I}+\frac{2\beta_1}{2^{33}\rho}P\dot{P}+\frac{\beta_2}{r_2}\dot{U}_I, \\
\dot{L}(I,P,U_I) &= \frac{\beta_1(N^*-I-P)I}{2^{32}}+\frac{\beta_2(N^*-I-P)U_I}{N^*}-\rho I-r_1I \\
&\quad+\frac{\beta_1PI}{2^{32}}+\frac{r_1\beta_1P^2}{2^{32}\rho}+\frac{{\beta_2}^2U^*I}{N^*r_2}-\frac{{\beta_2}^2U_1I}{N^*r_2}-\beta_2U_1, \\
&= \left(\frac{\beta_1N^*}{2^{32}}+\frac{{\beta_2}^2U^*}{N^*r_2}-\rho-r_1\right)I-\frac{\beta_1I^2}{2^{32}}-\frac{\beta_2(P+I)U_I}{N^*} \\
&\quad-\frac{r_1\beta_1P^2}{2^{32}\rho}-\frac{{\beta_2}^2P^2U_II}{N^*r_2}, \\
&= \left((\rho+r_1)\left(\frac{\beta_1N^*}{2^{32}(\rho+r_1)}+\frac{{\beta_2}^2U^*}{N^*r_2(\rho+r_1)}\right)-\rho-r_1\right)I
\end{aligned}$$

$$
\begin{aligned}
&- \frac{\beta_1 I^2}{2^{32}} - \frac{\beta_2 (P+I) U_I}{N^*} - \frac{r_1 \beta_1 P^2}{2^{32}\rho} - \frac{{\beta_2}^2 P^2 U_I I}{N^* r_2}, \\
&= (\rho + r_1)(R_0 - 1) I - \frac{\beta_1 I^2}{2^{32}} - \frac{\beta_2 (P+I) U_I}{N^*} \\
&- \frac{r_1 \beta_1 P^2}{2^{32}\rho} - \frac{{\beta_2}^2 U_I I}{N^* r_2}.
\end{aligned}
$$

Thus, $R_0 < 1$, implies that $\dot{L}(t) \leq 0$ and K_0 is the only invariant set of system (4.7) for $\dot{L}(t) = 0$. According to LaSalle Invariance Principle K_0 is globally asymptotically stable, hence this proves the theorem. Therefore, K_0 equilibrium point is globally asymptotically stable for $R_0 < 1$.

4.3.4 Endemic Stability

To investigate the endemic equilibrium of the point K^*= (I^*, P^*, U_I^*), for $R_0 > 1$ and obviously for $I^* \geq 0$, we have to find its local and global stability for $R_0 > 1$.

Theorem 4.3 K^* is locally asymptotically stable, if $R_0 > 1$.

Proof. Consider the function $f : R^3 \to R^3$ with components and Jacobian matrix as:

$$
\begin{aligned}
f_1(I^*, P^*, U_I^*) &= \tfrac{\beta_1 (N^* - I^* - P^*) I^*}{2^{32}} + \tfrac{\beta_2 (N^* - I^* - P^*) U_I^*}{N^*} - \rho I^* - r_1 I^*, \\
f_2(I^*, P^*, U_I^*) &= \rho I^* - r_1 P^*, \\
f_3(I^*, P^*, U_I^*) &= \tfrac{\beta_2 (U^* - U_I^*) I^*}{2^{32}} - r_2 U_I^*,
\end{aligned}
$$

$$
J(I^*, P^*, U_I^*) = \begin{pmatrix}
\frac{\partial f_1}{\partial I^*} & \frac{\partial f_1}{\partial P^*} & \frac{\partial f_1}{\partial U_I^*} \\
\frac{\partial f_2}{\partial I^*} & \frac{\partial f_2}{\partial P^*} & \frac{\partial f_2}{\partial U_I^*} \\
\frac{\partial f_3}{\partial I^*} & \frac{\partial f_3}{\partial P^*} & \frac{\partial f_3}{\partial U_I^*}
\end{pmatrix}.
$$

The endemic equilibrium point K^*= (I^*, P^*, U_I^*) and the Jacobian matrix at the endemic point is given below

$$
J(K^*) = \begin{pmatrix}
\frac{\beta_1 (N^* - 2I^* - P^*)}{2^{32}} - \frac{\beta_2 {U_I}^*}{N^*} - \rho - r_1 & -\frac{\beta_1 I^*}{2^{32}} - \frac{\beta_2 {U_I}^*}{N^*} & \frac{\beta_2 (N^* - I^* - P^*)}{N^*} \\
\rho & -r_1 & 0 \\
\frac{\beta_2 (U^* - {U_I}^*)}{N^*} & 0 & \frac{\beta_2 I^*}{N^*} - r_2
\end{pmatrix}. \tag{4.15}
$$

Characteristic equation of the above Jacobian is

$$= |\lambda I - J(K^*)| = 0,$$

$$\begin{vmatrix} \lambda - \frac{\beta_1 N^*}{2^{32}} + \frac{\beta_1(2I^*+P^*)}{2^{32}} + \frac{\beta_2 {U_I}^*}{N^*} + \rho + r_1 & \frac{\beta_1 I^*}{2^{32}} + \frac{\beta_2 {U_I}^*}{N^*} & -\frac{\beta_2(N^*-I^*-P^*)}{N^*} \\ -\rho & \lambda + r_1 & 0 \\ -\frac{\beta_2(U^*-{U_I}^*)}{N^*} & 0 & \lambda + \frac{\beta_2 I^*}{N^*} + r_2 \end{vmatrix} = 0,$$

and simplifies as:

$$\begin{aligned} &\lambda^3 + (b_{11} + b_{22} + b_{33})\lambda^2 + (b_{11}b_{22} + b_{11}b_{33} + b_{22}b_{33} - b_{12}b_{21} \\ &-b_{13}b_{31})\lambda + b_{11}b_{22}b_{33} - b_{12}b_{21}b_{33} - b_{13}b_{31}b_{22} = 0, \end{aligned} \tag{4.16}$$

where

$$\begin{aligned} &b_{11} = -\tfrac{\beta_1 N^*}{2^{32}} + \tfrac{\beta_1(2I^*+P^*)}{2^{32}} + \tfrac{\beta_2 {U_I}^*}{N^*} + \rho + r_1, \quad b_{12} = \tfrac{\beta_1 I^*}{2^{32}} + \tfrac{\beta_2 {U_I}^*}{N^*}, \\ &b_{21} = -\rho, \quad b_{23} = 0, \quad b_{22} = r_1, \quad b_{13} = -\tfrac{\beta_2(N^*-I^*-P^*)}{N^*}, \\ &b_{31} = -\tfrac{\beta_2(U^*-{U_I}^*)}{N^*}, \quad b_{33} = \tfrac{\beta_2 I^*}{N^*} + r_2, \quad b_{32} = 0. \end{aligned}$$

To analyze the stability of system (4.16), we use Hurwitz criteria as reported in [216, 218]. To overview Hurwitz criteria, let us consider the general characteristic equation of a system.

$$b_0 s^n + b_1 s^{n-1} + b_2 s^{n-2} + b_3 s^{n-3} \cdots \; b_{n-1} s^1 + b_n = 0,$$

with n determinants in nth order equation and the first three determinants, i.e., D_1, D_2 and D_3, of the said characteristic equation is as:

$$D_1 = b_1,$$

$$D_2 = \begin{vmatrix} b_1 & b_3 \\ b_0 & b_2 \end{vmatrix} = b_1 b_2 - b_3 b_0,$$

$$D_3 = \begin{vmatrix} b_1 & b_3 & b_5 \\ b_0 & b_2 & b_4 \\ 0 & b_1 & b_3 \end{vmatrix} = b_3(b_1 b_2 - b_0 b_3) - b_1(b_1 b_4 - b_0 b_5).$$

Now equating the coefficient of general characteristics equation with (4.16), we have

$$
\begin{aligned}
b_0 &= 1,\\
b_1 &= b_{11} + b_{22} + b_{33},\\
b_2 &= b_{11}b_{22} + b_{11}b_{33} + b_{22}b_{33} - b_{12}b_{21} - b_{13}b_{31},\\
b_3 &= b_{11}b_{22}b_{33} - b_{12}b_{21}b_{33} - b_{13}b_{31}b_{22},\\
b_4 &= 0,\\
b_5 &= 0,
\end{aligned}
$$

$$
\begin{aligned}
D_1 &= b_1 = b_{11} + b_{22} + b_{33},\\
&= -\tfrac{\beta_1 N^*}{2^{32}} + \tfrac{\beta_1(2I^*+P^*)}{2^{32}} + \tfrac{\beta_2 {U_I}^*}{N^*} + \rho + r_1 + r_1 + \tfrac{\beta_2 I^*}{N^*} + r_2,\\
&= \tfrac{\beta_2(N^*-I^*-P^*){U_I}^*}{N^*I^*} + \tfrac{\beta_2 {U_I}^*}{N^*} + \tfrac{\beta_1 I^*}{2^{32}} + r_1 + \tfrac{\beta_2 I^*}{N^*} + r_2,\\
&> 0.
\end{aligned}
$$

$$
\begin{aligned}
D_2 &= b_1b_2 - b_3b_0,\\
D_2 &= (b_{11} + b_{22} + b_{33})(b_{11}b_{22} + b_{11}b_{33} + b_{22}b_{33} - b_{12}b_{21}\\
&\quad - b_{13}b_{31}) - b_{11}b_{22}b_{33} + b_{12}b_{21}b_{33} + b_{13}b_{31}b_{22},\\
&= {b^2}_{11}b_{22} + {b^2}_{11}b_{33} + b_{11}b_{22}b_{33} - b_{11}b_{12}b_{21} - b_{11}b_{13}b_{31}\\
&\quad + b_{11}{b^2}_{22} + b_{11}b_{22}b_{33} + {b^2}_{22}b_{33} - b_{22}b_{12}b_{21} - b_{22}b_{13}b_{31}\\
&\quad + b_{11}b_{22}b_{33} + b_{11}{b^2}_{33} + b_{22}{b^2}_{33} - b_{33}b_{12}b_{21} - b_{33}b_{13}b_{31}\\
&\quad - b_{11}b_{22}b_{33} + b_{33}b_{12}b_{21} + b_{22}b_{13}b_{31},
\end{aligned}
$$

$$
\begin{aligned}
D_2 &= {b^2}_{11}b_{22} + {b^2}_{11}b_{33} + b_{11}{b^2}_{22} + b_{22}{b^2}_{33} + b_{11}{b^2}_{33} + {b^2}_{22}b_{33}\\
&\quad +2b_{11}b_{22}b_{33} - b_{11}b_{12}b_{21} - b_{11}b_{13}b_{31} - b_{22}b_{12}b_{21}\\
&\quad -b_{33}b_{13}b_{31},\\
&> (b_{11}b_{33} - b_{13}b_{31})(b_{11} + b_{33}),\\
&> \left\{\left(\tfrac{\beta_1(N^*-I^*-P^*)}{2^{32}} + \rho + r_1\right) r_2 - \tfrac{{\beta^2}_2(N^*-I^*-P^*)(U^*-{U_I}^*)}{{N^*}^2}\right\}(b_{11} + b_{33}),\\
&= \left\{\left(\tfrac{\beta_1(N^*-I^*-P^*)I^*}{2^{32}} + \rho I^* + r_1 I^* - \tfrac{\beta_2(N^*-I^*-P^*){U_I}^*}{N^*}\right)\tfrac{r_2}{I^*}\right\}(b_{11} + b_{33}),\\
&= 0.
\end{aligned}
$$

$$
\begin{aligned}
D_3 &= b_3(b_1b_2 - b_0b_3),\\
D_3 &= b_3(D_2),
\end{aligned}
$$

using values of b_3

$$\begin{aligned} D_3 = &(b_{11}b_{22}b_{33} - b_{12}b_{21}b_{33} - b_{13}b_{31}b_{22})((b_{11} + b_{22} \\ &+ b_{33})(b_{11}b_{22} + b_{11}b_{33} + b_{22}b_{33} - b_{12}b_{21} \\ &- b_{13}b_{31}) - b_{11}b_{22}b_{33} + b_{12}b_{21}b_{33} + b_{13}b_{31}b_{22}), \\ =&(b_{11}b_{22}b_{33} - b_{12}b_{21}b_{33} - b_{13}b_{31}b_{22})D_2, \\ >&(b_{11}b_{33} - b_{13}b_{31})b_{22}D_2, \\ >&0. \end{aligned}$$

Thus, all the values of D_1, D_2 and D_3 are positive, so all the Eigenvalues of the equation (4.16) are in the left half plane. If $R_0 > 1$ then there exists an endemic equilibrium point K^* which is locally asymptotically stable. This completes the proof.

Theorem 4.4 Endemic equilibrium point K^* is globally asymptotically stable, if $R_0 > 1$.

Proof. Let for ease, we consider the five dimensional Lyapunov function as:

$$\begin{aligned} L(S, I, P, U_s, U_I) = &(S - S^* - S^* \ln \frac{S}{S^*}) + (I - I^* - I^* \ln \frac{I}{I^*}) \\ &+ \frac{S^* {U_I}^*}{I^* {U_s}^*}(U_s - {U_s}^* - {U_s}^* \ln \frac{U_s}{{U_s}^*}) \\ &+ \frac{S^* {U_I}^*}{I^* {U_s}^*}(U_I - {U_I}^* - {U_I}^* \ln \frac{U_I}{{U_I}^*}). \end{aligned} \tag{4.17}$$

Lyapunov function is always positive in R^5. Taking the derivative of (4.17) and inserted the values of parameters we have

$$\begin{aligned} \dot{L}(S, I, P, U_s, U_I) = &(1 - \frac{S^*}{S})\dot{S} + (1 - \frac{I^*}{I})\dot{I} + \frac{S^* {U_I}^*}{I^* {U_s}^*}(1 - \frac{{U_s}^*}{U_s})\dot{U}_s \\ &+ \frac{S^* {U_I}^*}{I^* {U_s}^*}(1 - \frac{{U_I}^*}{U_I})\dot{U}_I, \\ = &\left[\begin{array}{l} \frac{\beta_1}{2^{32}}(1 - \frac{S^*}{S})(S^* I^* - SI) + \frac{\beta_2}{N}(1 - \frac{S^*}{S})(S^* {U_I}^* - SU_I) \\ +r_1(1 - \frac{S^*}{S})(S^* - S) \end{array} \right] \\ &+ \left[\frac{\beta_1}{2^{32}}(1 - \frac{I^*}{I})(SI - S^* I) + \frac{\beta_2}{N}(1 - \frac{I^*}{I})(SU_I - \frac{S^* I {U_I}^*}{I^*}) \right] \end{aligned}$$

$$
\begin{aligned}
&+\left[\begin{array}{l}\frac{\beta_2 S^* {U_I}^*}{N I^* {U_s}^*}(1-\frac{{U_s}^*}{U_s})(I^* {U_s}^* - I U_s) + \frac{S^* {U_I}^*}{I^* {U_s}^*}(1-\frac{{U_s}^*}{U_s})(U_I - {U_I}^*) \\ +\frac{r_2 S^* {U_I}^*}{I^* {U_s}^*}(1-\frac{{U_s}^*}{U_s})({U_s}^* - U_s)\end{array}\right] \\
&+\left[\frac{\beta_2 S^* {U_I}^*}{N I^* {U_s}^*}(1-\frac{{U_I}^*}{U_I})(I U_s - I^* {U_s}^* \frac{U_I}{{U_I}^*})\right], \\
&\leq \frac{\beta_1}{2^{32}}\left[\begin{array}{l}2S^* I^* - \frac{{S^*}^2 I^*}{S} \\ -S I^*\end{array}\right] + \frac{\beta_2}{N}\left[\begin{array}{l}2S^* {U_I}^* - \frac{{S^*}^2 {U_I}^*}{S} - \frac{S I^* U_I}{I} + \\ 2S^* {U_I}^* - \frac{S^* I {U_I}^{*2} U_s}{I^* {U_s}^* U_I} - \frac{S^* U_I {}^* U_s {}^*}{U_s}\end{array}\right], \\
&\leq \frac{\beta_2 S^* {U_I}^*}{N}\left[4 - \frac{S^*}{S} - \frac{S I^* U_I}{I S^* {U^*}_I} - \frac{{U^*}_s}{U_s} - \frac{I U_s {U^*}_I}{I^* U_I {U^*}_s}\right], \\
&\leq -2\frac{\beta_2 S^* {U_I}^*}{N}\left(\sqrt[4]{\frac{I^* U_I}{I {U_I}^*}} - \sqrt[4]{\frac{I {U_I}^*}{I^* U_I}}\right)^2, \\
&\leq 0.
\end{aligned}
$$

Which is negative. Hence the system (4.5) at the endemic equilibrium point K^* is globally asymptotically stable for $R_0 > 1$. This proves the theorem.

4.4 Simulation and Results

In this section, results of simulation are presented for $SIPU_SU_I$ model to understand the spread of the virus and the role of removable storage media in virus spread. Adams numerical method is used to solve and simulate the system of differential equations (4.1) for different parameters and initial conditions which are given in tables 4.1 and 4.2. Numerical results are obtained using NDSolve routine for the solution of differential equations using WOLFRAM MATHEMATICA 12 on 64 bit windows 10 platform. Simulation results obtained from the Stuxnet designed $SIPU_SU_I$ virus model are compared using state of the art numerical methods Adams versus BDF. Error analysis of both methods are shown in error plots. To validate the simulation results, we use the real data of Stuxnet virus spread [122, 219, 220] to evaluate the accuracy and convergence of the $SIPU_SU_I$ model. Approximately 100,000 users across 155 countries were infected by the Stuxnet attack and among these 63% were in Iran only. The number of hosts removed (which went down and lost their functionality) because of the Stuxnet attack was approximately 1500 (and 1200 were in Iran only).

Result of case 1 for $SIPU_SU_I$ model is calculated with Adams method which

TABLE 4.1: Parameters used in the simulation of model $SIPU_SU_I$.

Parameter	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
A_1	0.042	0.042	40	100	40	40
A_2	0.042	0.042	40.09	0	40.09	40.09
β_1	0.336	0.4	0.349	0	0.42	0.42
β_2	0.6	0.8	0.681	0.681	0	0
r_1	0.1126	0.19	0.0804	0.0804	0.0804	0.0804
r_2	0.0088	0.027	0.027	0.027	0.027	0.027
ρ	0.00265	0.051	0.0011	0.0011	0.0011	0.0065

TABLE 4.2: Initial values of the parameter used in the simulation of the model $SIPU_SU_I$.

Variables	S	I	P	U_S	U_I
Case 1-2	$2.3 * 10^6$	10000	10	50000	10000
Case 3-6	$2.3 * 10^6$	30000	10	30000	10000

show the dynamic behaviour of the virus spread and its error analysis with backward differentiation formula (BDF) as shown in figure 4.6(a) and (b), respectively. The BDF is a family of multi-step linear numerical methods for ordinary differential equations and especially used for stiff problems. While the results of case 2 given in figure 4.7(a) and (b) shows slight increase in the infection rate of removable storage media due to infected USBs. Model $SIPU_SU_I$ also describes the role of removable storage media for critical system networks, which are usually isolated from the internet. In figure 4.6(a) number of hosts are plotted versus time in months which shows the number of infected hosts due to a Stuxnet global attack, which was approximately 97,000 in 24 months and the number of crashed hosts (industrial systems which got destroyed) was approximately 1500. The total number of removable storage media is assumed to be 60,000 and due to increase in the number of infected hosts, infection in the removable storage media increases.

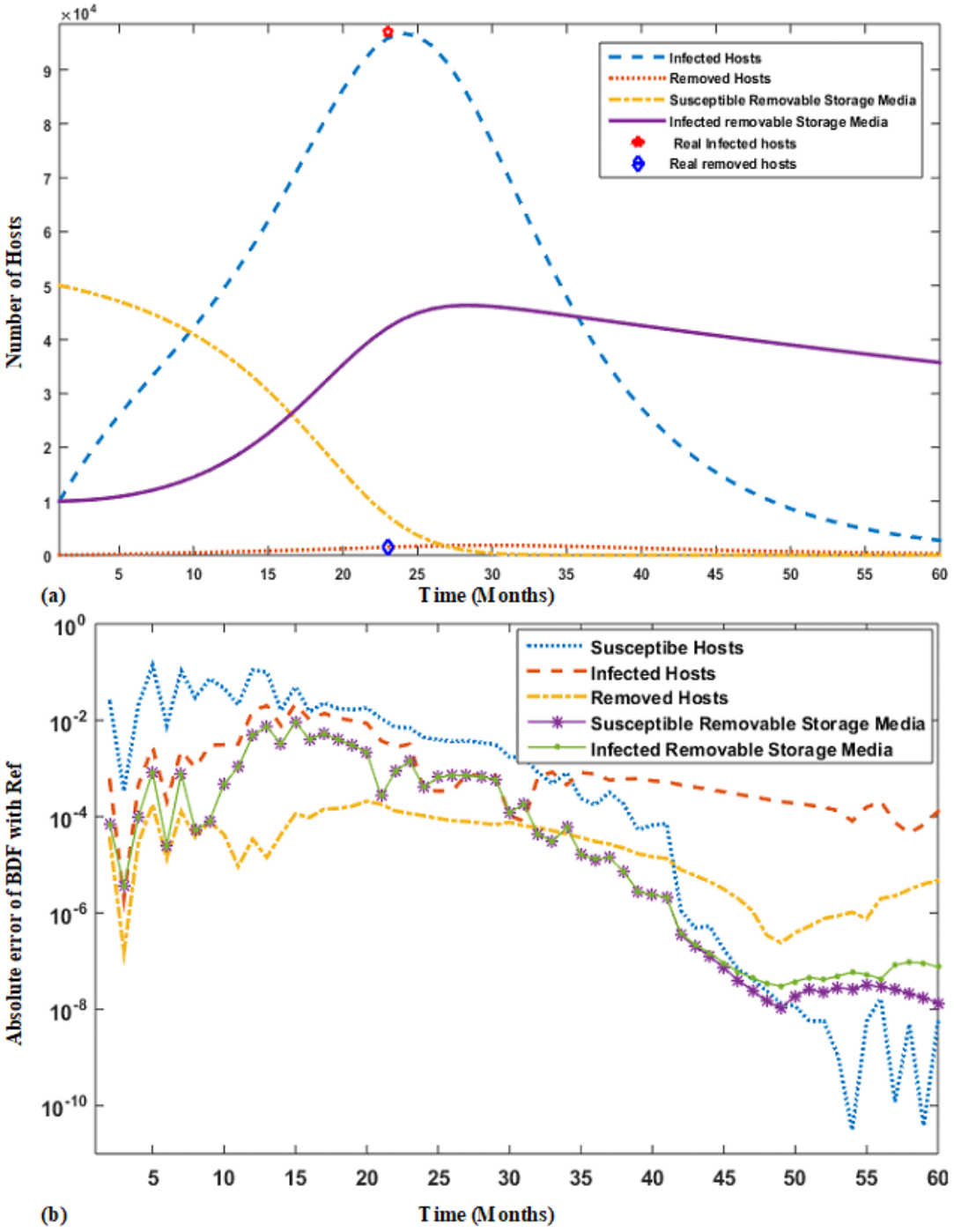


FIGURE 4.6: (a-b) Simulation of virus spread using $SIPU_SU_I$ model with parameters and initial conditions given in tables 4.1,4.2 respectively for case 1 and error analysis of Adams with BDF.

Increase of infection in removable storage media ultimately increase overall infections. In 24 months period infected removable storage media has reached up to 45,000. Camouflage of Stuxnet virus was revealed after 24 months after launching

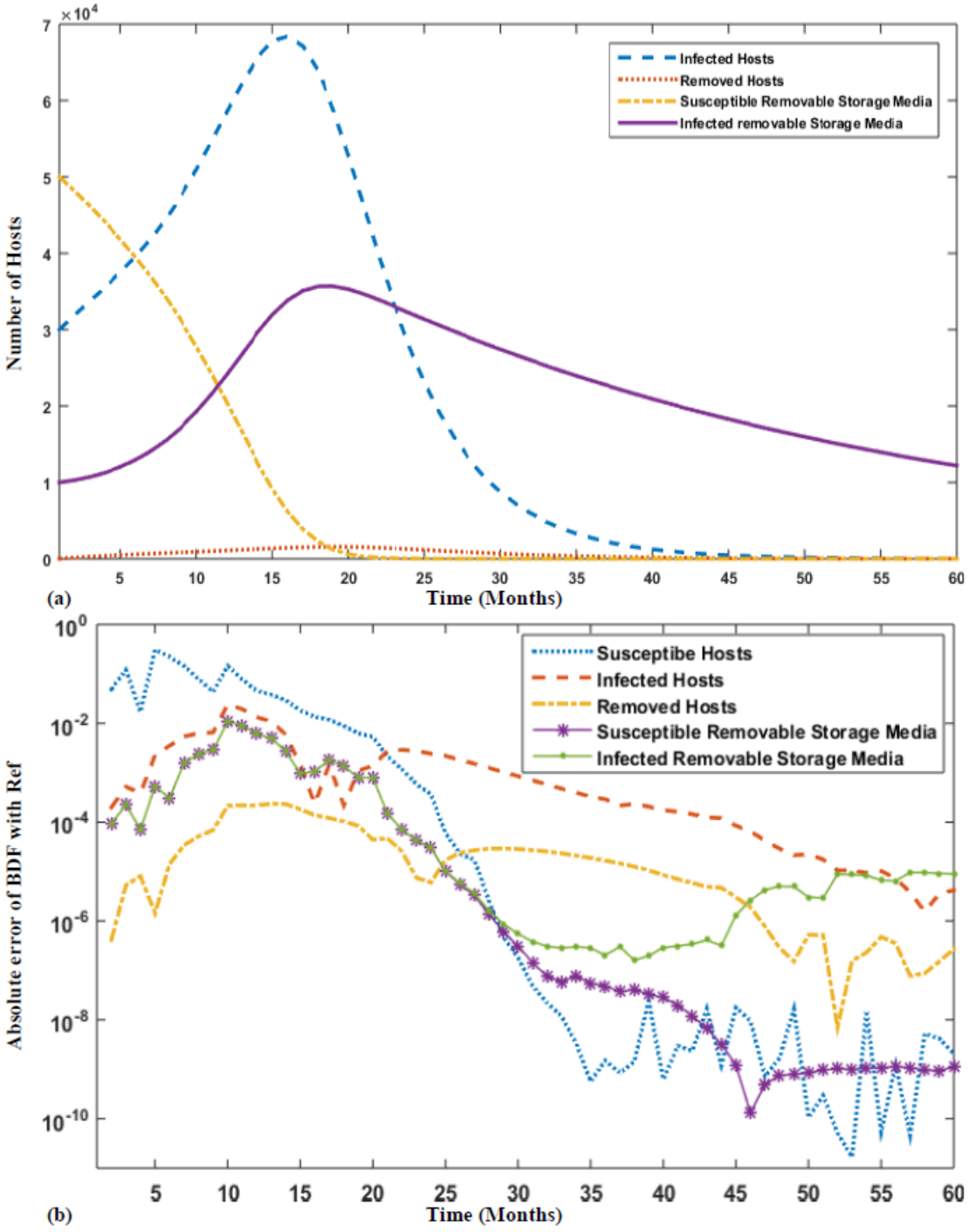


FIGURE 4.7: (a-b) Simulation of virus spread using $SIPU_SU_I$ model with parameters and initial conditions given in tables 4.1,4.2 for case 2 respectively and error analysis of Adams with BDF.

of virus first attack. Decrease in the number of infected hosts and removable storage media is observed after 24 months due to availability of remedial techniques, natural isolation from networks and anti-virus signature update for the Stuxnet virus. The effect of removable storage media can also be analyzed by increasing

the values of infectious contact rate of removable storage media as shown in figure 4.7(a). Number of removable hosts will be increased quickly as compared to figure 4.6(a) by slightly increasing the contact rate of infected removable media. The maximum value of case 1 was achieved in 18 months as compared to 24 months time. Figure 4.7(a) shows that increasing the infectious contact rate of removable storage media also decline the number of infected nodes and infected media earlier as compare to figure 4.6. Sudden increase in the virus malicious activity aggravate the problem which will ultimately conceal the virus camouflage and earlier remedial actions will be required. In figure 4.8(a), we increased the number of new arrived computers and removable storage media to observe the model behavior for Stuxnet virus in 60 months. The number of infected hosts were 92,680, removed hosts were 828 and infected removable storage media were 17870. In figure 4.8(b) infectious contact rate β_1 of susceptible hosts with infected hosts is reduced to zero which has an insignificant effect in the spreading of virus in infected and removed hosts. The difference in the number of infected hosts and infected removable storage media from previous case of figure 4.8(a) is only 50 and 1 respectively. So infectious contact rate of susceptible computers by infected computer has negligible effect on virus spread. In figure 4.9(a) effects of virus spread are analyzed by changing the value of infectious contact rate of susceptible removable storage media β_2 to zero. Figure 4.9(a) shows a major change in the number of infected and removed hosts which are 5005 and 124 respectively. The role of infected removable storage media depicts that controlling its connectivity with susceptible hosts controls the infection of Stuxnet virus in the network. Decreasing β_2 will not only decrease the number of infected hosts but also decrease the number of infected removable media and consequently other hosts also. Limiting the number of removable devices can control the virus spread. In air-gapped network removable storage media play a major role in bridging the gap and normally plant networks which includes SCADA / PLC's type hardware that are isolated from other work networks. Stuxnet is a type of virus that targets the special hardware which controls the plants and this sholuld be isolated from other network. In figure 4.9(b), simulations are performed by slightly increasing the values of ρ, the damage rate

of infectious hosts and keeping values of other parameters fixed. Figure 4.9(b) shows that slight increase in the value of ρ will increase the number of damaged hosts .

Phase portrait of the model $SIPU_SU_I$ as shown in the figure 4.10 (a-f), these shows interesting results. Phase portrait of figure 4.10 (a) is plotted between susceptible hosts, removed hosts and infected removable storage media to depict the behavior of model for case 1. It is observed that curve in this phase portrait is forms a loop, the number of susceptible host decreases slowly due to increase in the number of infected removable storage media. Decrease in the number of susceptible hosts become rapid when infected removable storage media crosses the limit of 10,000 and the susceptible host increases again when infected removable media reaches the limit of 30,000. It illustrates that increase in the number of removable storage media, suddenly increases the infection in the system and reduces the number of susceptible hosts and vice verse due to other controlling factors, like revealing of virus camouflage etc. Phase portrait in figure 4.10(b) which is plotted among susceptible, infected and removed hosts which highlights the relations of these hosts for case 1. As simulation progress in figure 4.10(b), increase in the number of infected and removed nodes are observed. Figure 4.10(b) form a loop which shows the increase / decrease in the number of nodes and infection in the system. Infection spreads in the system due to availability of susceptible nodes and nonavailability of control mechanism. Decrease in the number of susceptible hosts is observed due to natural removal and removal due to infection. Figure 4.10(c) shows that after 20,000 infected hosts, slightly increase in the number of infected hosts will exponentially increase the number of infected removable storage media. Reduction in the number of infected hosts will not reduce the number of infected storage media which highlights the independent role of removable storage media in the spread of the infection. Figure 4.10(d) shows that increase in the number of susceptible hosts decrease the number of infected storage media and vice versa. Infected hosts versus susceptible removable storage are plotted in Figure 4.10(e) which indicates that increase in the number of infected hosts decreases the number of susceptible media exponentially. In figure 4.10 (f), increase in the

number of infected hosts also increases the number of removed hosts. The number of infected hosts were approximately 97,000 at that time and removed hosts were around 1500. These results show that controlling the connectivity of removable storage media, will control the spread of the virus in industrial control computers specifically and partially in other networks, as public networks has different options for its connectivity. For the Stuxnet model, results obtained from the model are validated using published data of Stuxnet virus spread (infection and damage caused throughout the world).

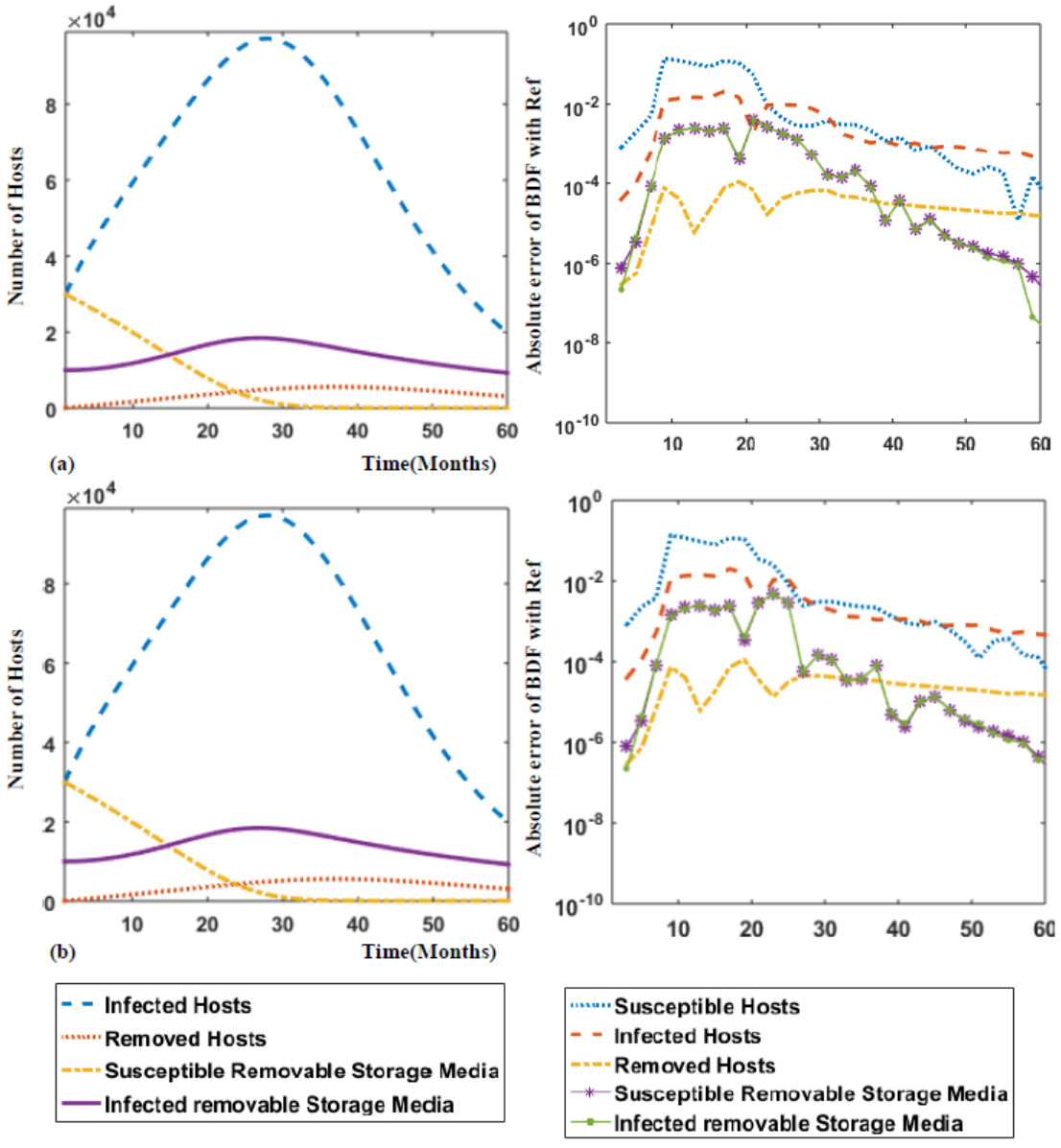


FIGURE 4.8: (a-b) Simulation of virus spread using $SIPU_SU_I$ model with parameters and initial conditions given in table 4.1,4.2 for case 3-4 respectively and error analysis of Adams with BDF.

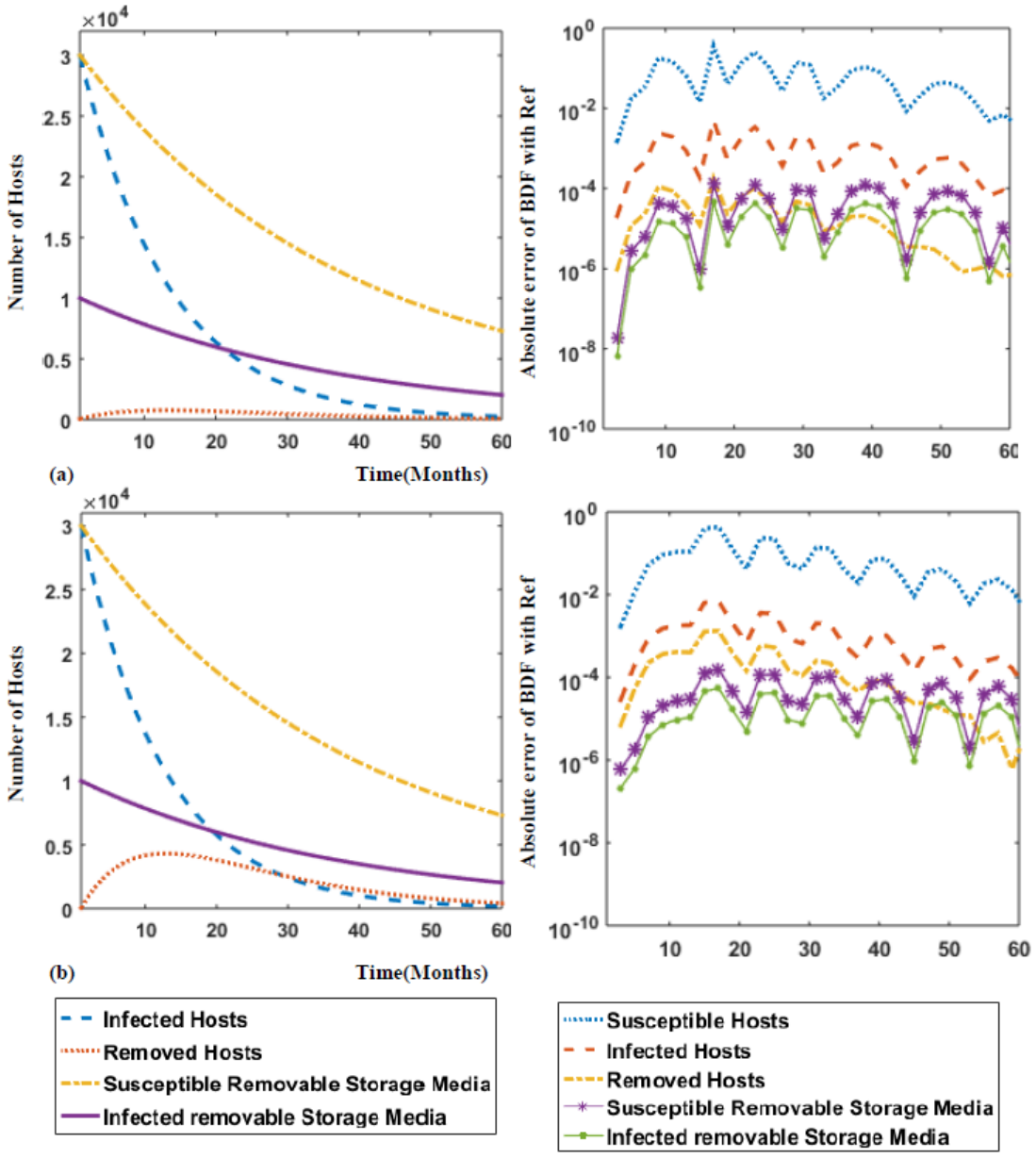
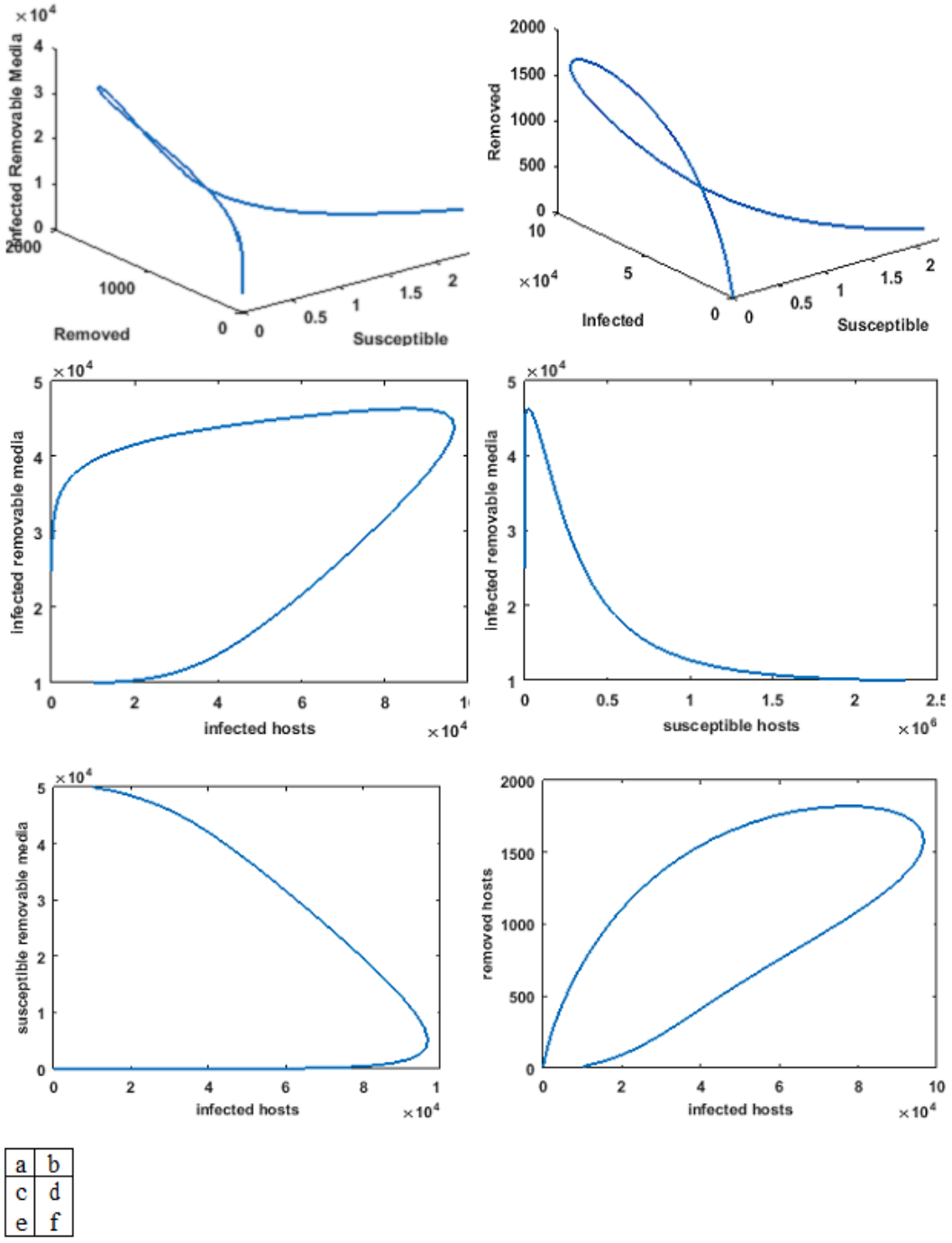


FIGURE 4.9: (a-b) Simulation of virus spread using $SIPU_SU_I$ model with parameters and initial conditions given in table 4.1,4.2 for case 5-6 respectively and error analysis of Adams with BDF.

4.4.1 Control Strategies

In this section, a control strategies for Stuxnet virus propagation model are presented. In reality, control strategies are variable in time and the mathematical theory behind these strategies are called optimal control theory, however control strategies discussed here are constant. It is evident from the results presented that



a	b
c	d
e	f

FIGURE 4.10: (a-f) Phase portrait of virus spread using a $SIPU_SU_I$ model for case 1.

the removable storage media plays an important role in the spread of Stuxnet virus in air-gapped network and necessary interpretation of control strategy are briefly highlighted as follows. As shown in figure 4.7(a); by increasing the value of β_2, the infectious contact rate of removable storage media in case 2 will increase the infection quickly as compare to case 1. The role of β_2 in controlling the infection

is further investigated in cases 5 and 6 with observation that reducing the value of β_2 to 0 exponentially reduces the number of infected hosts for case 5 as shown in figure 4.9(b). It is further noted that infection of virus spread is present in the network but in case of Stuxnet virus that exploits specific hardware thus removal of hardware are not relatively substantial. Increasing the value of parameter ρ, i.e., damage rate due to virus infection, increases the infection due virus in specific hardware which ultimately enhance the damage rate. Controlling the parameter ρ will also control the damage rate of hardware connected with specific devices. Meanwhile, time dependent control preventive policy can be obtained by minimizing the objective function (4.18) for damage rate due to virus infection on specific hardware.

$$J(\rho) = \int_0^T [K_1 U_I(t) + K_2 I(t) + K_3 \frac{\rho^2(t)}{2}]dt. \tag{4.18}$$

The first term $K_1 U_I(t)$ in the objective function represents the number of infected removable storage media and second term $K_2 I(t)$ represents the number of infected hosts. The term $K_3 \frac{\rho^2(t)}{2}$ represents the rate of damaged hosts. Theoretical analysis of the objective function (4.18), can be conducted by interested readers for the Stuxnet virus model through adaptation of similar procedures reported in relevant studies [233, 234].

4.5 Chapter Summary

A $\mathrm{SIPU_SU_I}$ dynamic epidemic model is presented for the transmission of viruses into a standalone computer network through removable storage media. If the infection contact rate $\beta_2 = 0$ for an $\mathrm{SIPU_SU_I}$ model, then it reduces the model to an SIR model. The $\mathrm{SIPU_SU_I}$ model captures the spreading characteristics of a sophisticated digital virus such as the Stuxnet. Mathematical analysis shows that the dynamics of this model is determined through the basic reproduction number R_0. Disease free equilibrium of the model is globally asymptotically stable for $R_0 < 1$ and asymptotic endemic stability is also shown for $R_0 > 1$. To control the

spread of infectious disease one must retain the basic reproduction number less than one. Removable storage media and infectious contact rate play an important role in the extent of viruses spread. Additionally, numerical study is performed with state of the art differential equation solvers for validation of the model on available data for Stuxnet virus as well as number of scenarios for removable storage media and consistently results are found in good agreement with standard solutions and reported statistics.

Chapter 5

Fractional Dynamics of Stuxnet Virus Propagation

In this chapter fractional dynamics of Stuxnet virus spread are analyzed in the regimes of supervisory control and data acquisition environment by bridging the air-gap between traditional and the critical control network infrastructures. Spreading behavior analysis of malicious codes are investigated for distinct order of fractional derivative terms in the model for transient response.

5.1 Introduction

Computer virus is a small program that works on a system without the consent of the users and may cause damage or steal information for the exploitation of the desired targets. In strategic conflicting environments as well as in financial market, the use of computer viruses in network operation as a digital weapon against the desired targets e.g., computer spyware program used as information collection platform in syrian war [118], Shamoon and Stuxnet viruses for cyber incidents [119]. The tools used for cyber war range from very small program that just display annoying messages or a very complex program that can physically damage the system such as Stuxnet [120]. Stuxnet was discovered in June 2010 at Natanz

nuclear enrichment facility in Iran [121]. The name of Stuxnet virus was derived from two keywords in its source code, .stub and mrxnet.sys. Stuxnet virus is a sophisticated piece of code that mainly targets the supervisory control and data acquisition systems, exploits four zero-day vulnerabilities to attack the targeted hosts and uses the advance technique to hide from guard programs. The possibilities of Stuxnet virus spreads in the networks are due to windows print spooler MS 10-061 zero-day vulnerability, network shares and server message block (SMB) file sharing etc. Stuxnet virus monitors the frequency of motors operating centrifuges machines before modification, which must be in range of 807 Hz to 1210 Hz. Stuxnet changes the output frequency for short periods of time to 1410 Hz and then to 2 Hz and then to 1064 Hz. Change in the output frequency of the motors essentially sabotage the working of machines [221]. The Stuxnet virus attack destroyed 1000 centrifuges out of the 5,000 operating at the Natanz nuclear facility in Iran [122]. The purpose of the virus was not just to infect the computers but to cause real world physical damage

Theoretical behavior analysis of the Stuxnet malicious codes can be carried out by the strength of epidemiology modelling of virus propagation [191–193]. The control strategies of these malicious codes are very difficult because they often hide themselves, may exploit zero-day vulnerabilities, gain admin rights and work as a legitimate program. The advancement in technologies, creates several challenges to the security of the critical infrastructure of the nations in the presence of vulnerability and the development of smart viruses. The process of automating every appliance enormously increases the use of software, resultantly the lengthy and complex routines are developed. Eradication of bugs in complex codes / routines are challanging tasks and complete removal of these bugs are impractical, so these software may contain the vulnerabilities which can ultimately compromise the whole system [126]. Therefore, detail dynamical analysis of these malicious codes and their devastation pattern with control mechanisms looks promising domain to be investigated by the research community.

The spread of virus in computer networks has close analogy with the spread of biological viruses in the population. Mathematical modeling of viruses in biology

as well as in computer networks give us profound understanding of the problem and help us to devise a reliable, viable and robust control strategies [127]. It is known that the state of many biological systems at current time depends on the states of the system at previous time. Thus, fractional derivative is the natural method to use in the solution of the biological modeling arising in various disciplines. Besides these, the role of fundamental concepts and underlying theories of fractional calculus has been applied effectively in the modeling of the complex systems in diversified fields with rich dynamics than that of integer counterparts [70, 71]. Keeping in view of these facts, aim of present study is to exploit the rich heritage of fractional dynamics for the development of fractional Stuxnet virus model in order to study the virus spread in supervisory control and data acquisition systems. In this chapter, fractional order mathematical model of Stuxnet virus is presented to analyze the fast transients, super slow evolutions of the virus spread dynamic and attacking pattern on critical infrastructures managed by industrial control computers. The contributions of the proposed fractional Stuxnet virus model is briefly highlighted as:

1. A novel fractional order Stuxnet virus model is proposed by exploiting the rich heritage of fractional calculus in the environment of supervisory control and data acquisition by bridging the air-gap between traditional and the critical control network infrastructures.
2. Local and global stability analysis of Stuxnet virus model is proven at equilibrium points both for virus free and endemic spread.
3. Correctness of the proposed Grunwald-Letnikov based fractional numerical solver is ascertained with close matching results from state of the art Runge-Kutta numerical solver for integer order variants of the model.
4. Numerical experimentations with Grunwald-Letnikov based fractional numerical solver for distinct order of the fractional derivative terms in the system show that fractional order models provide enrich dynamics by means of super-fast transients as well as super slow evolutions of the steady-state.

5.2 Fractional Calculus Fundamentals

5.2.1 Preliminaries

Fractional calculus is the generalization of classical calculus theory of derivatives and integrals of real or complex orders. Fractional calculus is a 300 years old topic in mathematics and the idea of fractional calculus was first listed in the literature with a letter from Leibniz to L'Hostital in 1696. In this letter half derivative term was introduced i.e. the generalization of the derivative operator $D^{\alpha}f()$ while α represents the order of fractional derivative. The development of fractional calculus belonged to the efforts of several scientists like Liouville, Euler, Letnikov, and Riemann [73, 134]. Several definitions of fractional derivative exist while the broadly used are given by Caputo (CP), Grunwald-Letnikov (GL) and Riemann-Liouville (RL) [194]. The GL definition of fractional derivative is as under.

$$ {}_{a}^{GL}D_{t}^{\alpha}f(t) = \lim_{h\to 0}\frac{1}{h^{\alpha}}\sum_{m=0}^{[(t-a)/h]}(-1)^{m}\binom{\alpha}{m}f(t-mh),\ t>a,\ a>0. \tag{5.1} $$

The Caputo's definition of fractional derivatives can be written as

$$ {}_{a}^{CP}D_{t}^{\alpha}f(t) = \frac{1}{\Gamma(n-\alpha)}\int_{a}^{t}\frac{f^{n}(x)}{(t-x)^{\alpha-n+1}}dx, \tag{5.2} $$

for $(n-1<\alpha<n)$, where $\Gamma(\cdot)$ is a gamma function.
The RL definition is given as

$$ {}_{a}^{RL}D_{t}^{\alpha}f(t) = \frac{1}{\Gamma(n-\alpha)}\frac{d^{n}}{dt}\int_{a}^{t}\frac{f(x)}{(t-x)^{\alpha-n+1}}dx. \tag{5.3} $$

For $(n-1<\alpha<n)$, while a and t are the bounds of the operation for ${}_{a}D_{t}^{\alpha}$, Laplace transform method is normally used with CP, GL and-RL fractional derivatives under zero initial conditions as: [74].

$$\pounds\{{}_aD_t^{\pm\alpha}f(t);s\} = s^{\pm\alpha}F(s), \tag{5.4}$$

while the analytical expressions are represented with Mittag-Leffler(ML) type functions [135] introduced by Agarwal and Humbert [136] and is given mathematically as:

$$E_{\alpha,\beta}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(\beta+\alpha k)}, \quad \alpha,\beta,z \in C, \;\; \Re(\alpha) > 0, \Re(\beta) > 0, \tag{5.5}$$

where C represents the set of complex numbers and $E_{\alpha,\beta}$ is two parameter based ML function.

5.2.2 Grunwald-Letnikov Based Numerical Solver for FDEs

Analytical solutions of the fractional differential equations (FDEs) were generally determined through Laplace transformed method (5.4), these expressions are represented by commonly ML function (5.5) while the numerical solutions of the most commonly used method is based on GL definition.

To introduced the numerical solver based on GL [137] for FDEs, Let's consider a general form of FDE along with initial conditions:

$$\begin{aligned} &{}_aD_t^{\alpha}f(t) = f(y(t),t), \\ &y^{(k)}(0) = y_0^{(k)}, k = 0,1,2,\ldots n-1, \end{aligned}$$

where $(n-1 < \alpha < n)$, using equation (5.1), Ivo Petras [75] provided the final recursive expression for GL based numerical solver as:

$$y(t_k) = f(y(t_k),t_k)h^r - \sum_{j=v}^{k} c_j^{(r)} y(t_{k-j}),$$

where

$$c_j^r = \left(1 - \frac{1+r}{j}\right) c_{j-1}^r c_0^r = 1, j = 0,1,\ldots$$

for $t_k = kh$ and h is the step size parameter. Further necessary details of GL based numerical scheme can be seen in [76].

5.3 Model Formulation of Fractional Order Stuxnet Virus

The formulation of fractional order Stuxnet virus model (FO-SVM) is presented here. The detail workflow diagram of the proposed FO-SVM is shown in figure 5.1. The entire FO-SVM is segmented in to five classes; three for computer population, i.e. susceptible $S(t)$, infected $I(t)$ and damaged $M(t)$ while two for removable storage media, i.e. susceptible storage media $U_s(t)$ and infected storage media $U_I(t)$. Total population is represented by $N(t)$, i.e., $N(t) = S(t) + I(t) + M(t)$, while total removable devices $U(t)$, i.e., $U(t) = U_s(t) + U_I(t)$. In rest of the article, the variables with respective to time t, $S(t)$, $I(t)$, $M(t)$, $U_s(t)$, $U_I(t)$, $N(t)$ and $U(t)$ are denoted by S, I, M, U_s, U_I, N and U respectively. Let A_1 and A_2 represent the arrival of new computer nodes and removable storage media respectively, damage rate caused to PLC's due to virus infection is represented by ρ , β_1 is the infectious contact rate of susceptible nodes with infected nodes during network scan and β_2 denotes the infectious contact rate of removable storage media with susceptible computer nodes, r_1 and r_2 are the natural removal (death) rates of computers and removable devices from the network, respectively. The number of nodes in Internet protocol version 4 (IPv4)is 2^{32} and the probability of finding susceptible nodes in IPv4 scheme is $S/2^{32}$. Susceptible nodes can be infected at the rate $\beta_1 SI$ or at $\beta_2 SU_I/N$ while the removable storage media could be infected at rate $\beta_2 U_s I/N$. Removable storage media is the common source of virus spread in critical industrial air gapped networks, which are isolated from normal networks. The removable storage devices facilitate the flow of information to and from the networks that make them as an easy prey for intruders [80]. In this chapter, fractional order virus model is exploited to illustrate the spread of the virus, especially Stuxnet [138, 139] in industrial networks through removable storage media. The flow diagram of proposed model is shown in figure 5.2 while the governing differential equations describe the model and are given mathematically as:

$$D^{\alpha}S = A_1 - \frac{\beta_1 SI}{2^{32}} - \frac{\beta_2 SU_I}{N} - r_1 S,$$

$$
\begin{aligned}
D^{\alpha}I &= \frac{\beta_1 SI}{2^{32}} + \frac{\beta_2 SU_I}{N} - \rho I - r_1 I, \\
D^{\alpha}M &= \rho I - r_1 M, \\
D^{\alpha}U_s &= A_2 - \frac{\beta_2 U_s I}{N} - r_2 U_s, \\
D^{\alpha}U_I &= \frac{\beta_2 U_s I}{N} - r_2 U_I,
\end{aligned} \tag{5.6}
$$

where $\alpha \in [0,1]$ is the order of the fractional derivatives term $D^{\alpha} = d^{\alpha}/dt^{\alpha}$. In case of $\alpha = 1$, the system provided in set of equation (5.6) is transformed to standard first order model of Stuxnet virus propagation. From set of equation (5.6) for the value of $\alpha = 1$ we have

$$
\begin{aligned}
\frac{dN}{dt} &= A_1 - r_1 N, \\
\frac{dU}{dt} &= A_2 - r_2 U.
\end{aligned} \tag{5.7}
$$

The net rate of change of the population is given by $c_1 = A_1 - r_1$ and $c_2 = A_2 - r_2$, and the values of these constants may be positive, zero or negative. Solving the set of equations (5.7), we get

$$
\begin{aligned}
N(t) &\to \frac{A_1}{r_1} \triangleq N^*, \; t \to \infty, \\
U(t) &\to \frac{A_2}{r_2} \triangleq U^*, \; t \to \infty.
\end{aligned} \tag{5.8}
$$

The system of equations (5.6) can be written in simplified or reduced form by incorporating the variable N and U as:

$$
\begin{aligned}
D^{\alpha}I &= \frac{\beta_1 (N - I - M) I}{2^{32}} + \frac{\beta_2 (N - I - M) U_I}{N} - \rho I - r_1 I, \\
D^{\alpha}M &= \rho I - r_1 M, \\
D^{\alpha}U_I &= \frac{\beta_2 (U - U_I) I}{N} - r_2 U_I,
\end{aligned} \tag{5.9}
$$

where

$$
N(t) = N^* + (N(0) - N^*) e^{-r_1 t},
$$

and

$$
U(t) = U^* + (U(0) - U^*) e^{-r_2 t}.
$$

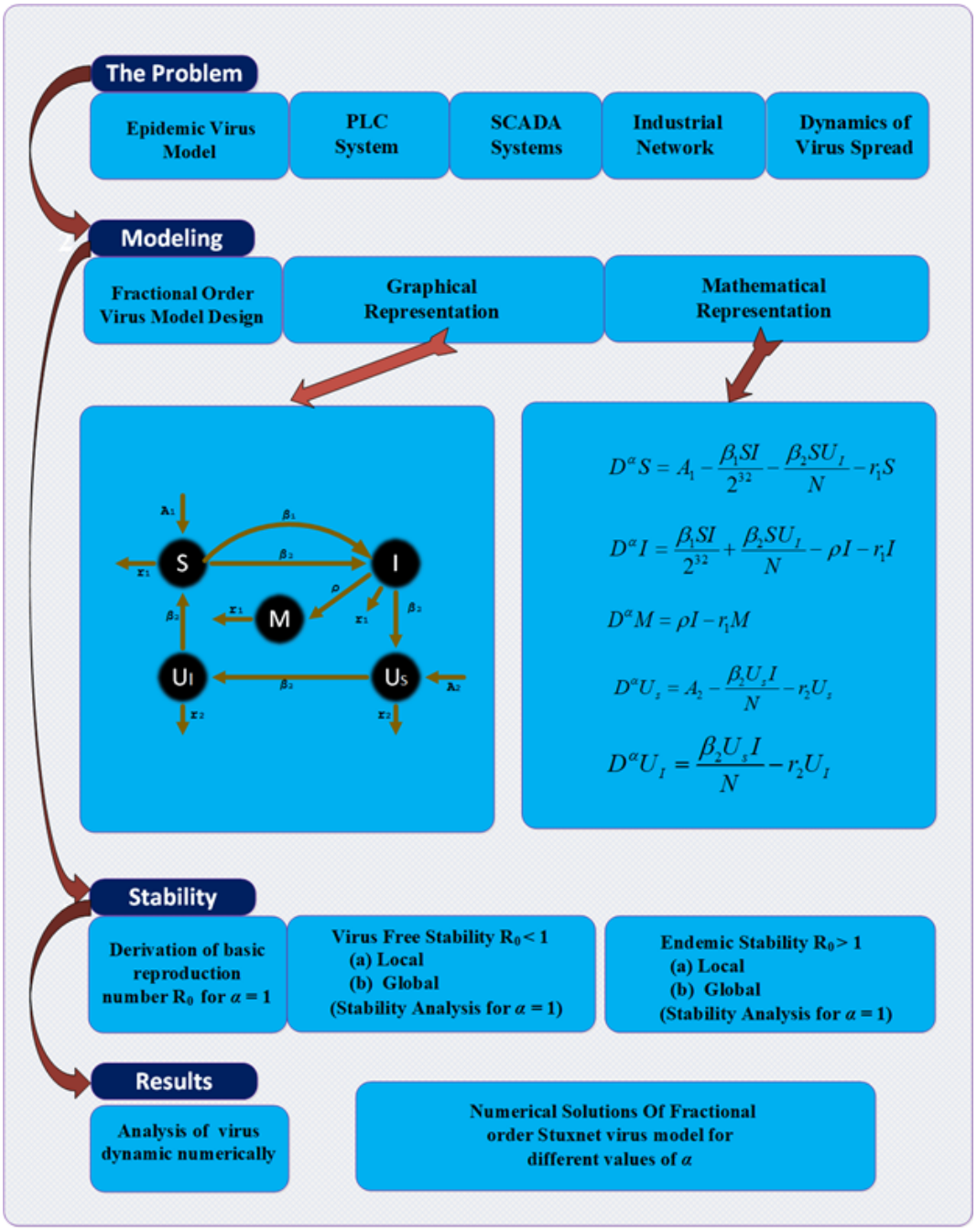


FIGURE 5.1: Graphical overview of schematic for the proposed FO-SVM model

Using equation (5.8) in system (5.9), one may have a limit system (IMU_I) as [140, 141]:

$$\begin{aligned} D^{\alpha}I &= \frac{\beta_1(N^* - I - M)I}{2^{32}} + \frac{\beta_2(N^* - I - M)U_I}{N^*} - \rho I - r_1 I, \\ D^{\alpha}M &= \rho I - r_1 M, \\ D^{\alpha}U_I &= \frac{\beta_2(U^* - U_I)I}{N^*} - r_2 U_I. \end{aligned} \tag{5.10}$$

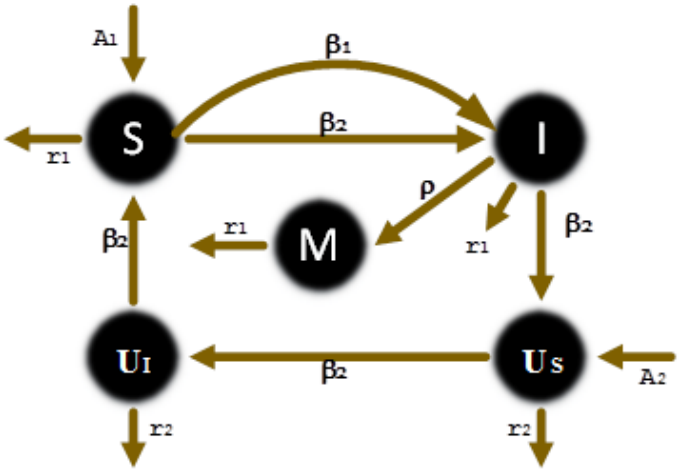


FIGURE 5.2: Schematic flow of proposed FO-SVM model

The equations in set (5.10), represented the reduced model for further investigations.

5.4 Model Analysis

In this section, stability of the model for local, as well as, global are presented through derivation of basic reproduction number R_0 for both disease free and endemic equilibrium points.

5.4.1 Basic Reproduction Number (R_0)

The basic reproduction number is defined as the average of new infection caused by an infected individual in its infectious period and usually represented by R_0. If $R_0 > 1$, then infection will spread rapidly in the system and if $R_0 < 1$ then infection will die down [142].

Reduced version of the model (5.10) has been used for the derivation of R_0. The R_0 is computed on integer order model, i.e., $\alpha = 1$. The essential condition for an epidemic to occur is based on increase in the number of infected nodes with an assumption of initially, susceptible nodes based population.

In case of $D^{\alpha}I > 0$, we have $D^{\alpha}U_I > 0$

$$\frac{\beta_1(N^* - I - M)I}{2^{32}} + \frac{\beta_2(N^* - I - M)U_I}{N^*} - \rho I - r_1 I > 0,$$

and accordingly in case of $D^{\alpha}U_I > 0$, we have

$$\frac{\beta_2(U^* - U_I)I}{N^*} - r_2 U_I > 0.$$

Assuming that all new nodes in the population are susceptible at start, we may write the above expressions as:

$$\frac{\beta_1 N^* I}{2^{32}} + \frac{\beta_2 N^* U_I}{N^*} - \rho I - r_1 I > 0,$$
$$\frac{\beta_2 U^* I}{N^*} - r_2 U_I > 0.$$

Simplifying above relations, we have

$$\frac{\beta_1 N^*}{(\rho + r_1)2^{32}} + \frac{\beta_2^2 U^*}{r_2 N^*(\rho + r_1)} > 1.$$

Accordingly,

$$R_0 = \frac{\beta_1 N^*}{2^{32}(\rho + r_1)} + \frac{\beta_2^2 U^*}{r_2 N^*(\rho + r_1)}. \tag{5.11}$$

The equation (5.11) represents the derived basic reproduction number of the model.

5.4.2 Equilibria Studies

The model (5.10) has two equilibrium points; i.e., virus free and endemic equilibria points. In case of endemic equilibrium point, infection spread in the system.
For equilibria studies, we have

$$D^{\alpha}I = 0, D^{\alpha}M = 0, D^{\alpha}U_I = 0.$$

Virus free equilibria point for system (5.10) is $K_0 = (I,\ M,\ U_I) = (0,\ 0,\ 0)$ and endemic equilibria point is $K^* = (I^*,\ M^*,\ U_I^*)$ for $R_0 > 1$.

The model (5.10) for endemic equilibria analysis is written as:

$$\begin{aligned} \frac{\beta_1(N^*-I-M)I}{2^{32}}+\frac{\beta_2(N^*-I-M)U_I}{N^*}-\rho I-r_1 I=0,\\ \rho I-r_1 M=0,\\ \frac{\beta_2(U^*-U_I)I}{N^*}-r_2 U_I=0. \end{aligned} \tag{5.12}$$

Solving equations in set (5.12), we get expressions for the endemic equilibrium point (I^*, M^*, U_I^*) as:

$$I^*=\frac{\sqrt{b^2-4ac}-b}{2a}, \tag{5.13}$$

$$M^*=\frac{\rho}{r_1}I^*, \tag{5.14}$$

$$U_I^*=\frac{\beta_2 U^*}{\beta_2 I^*+r_2 N^*}I^*, \tag{5.15}$$

where

$$\begin{aligned} a&=\frac{(\rho+r1)\beta1\beta2}{2^{32}r_1N^*},\\ b&=\frac{\beta_2(\rho+r_1)(1-R_0)}{N^*}+\frac{\beta_2^3U^*}{N^*r_2}+\frac{\beta_1(r_2)\beta_2^2U^*}{2^{32}r_1}(\rho+r_1),\\ c&=(\rho+r_1)(1-R_0)r_2. \end{aligned}$$

It is evident from equation (5.13) that the possibility of infection spread i.e., $I^*>0$, is only verified for the value of $R_0>1$.

5.4.3 Disease Free Equilibria

Theorem 4.1. Disease-free equilibrium (DFE) is locally asymptotically stable at K_0, if $R_0<1$.

Proof. The system is locally asymptotically stable at DFE point $K_0=(I,\ M,\ U_I)=(0,\ 0,\ 0)$. Consider the Jacobian matrix of function $f: R^3\to R^3$ with components:

$$D^\alpha I=\frac{\beta_1(N^*-I-M)I}{2^{32}}+\frac{\beta_2(N^*-I-M)U_I}{N^*}-\rho I-r_1 I,$$

$$D^{\alpha}M = \rho I - r_1 M,$$
$$D^{\alpha}U_I = \frac{\beta_2(U^* - U_I)I}{N^*} - r_2 U_I.$$

Therefore, the Jacobian matrix at K_0, DFE point for integer order model (5.10) is given as:

$$DFE(K_0) = \begin{pmatrix} \frac{\beta_1 N^*}{2^{32}} - \rho - r_1 & 0 & \beta_2 \\ \rho & -r_1 & 0 \\ \frac{\beta_2 U^*}{N^*} & 0 & -r_2 \end{pmatrix}. \tag{5.16}$$

To find the Eigenvalues, the characteristic equation of (5.16) is

$$|\lambda I - DFE(K_0)| = \begin{vmatrix} \lambda - \frac{\beta_1 N^*}{2^{32}} + \rho + r_1 & 0 & -\beta_2 \\ -\rho & \lambda + r_1 & 0 \\ -\frac{\beta_2 U^*}{N^*} & 0 & \lambda + r_2 \end{vmatrix} = 0,$$

and simplify as:

$$(\lambda + r_1)\left[\left(\lambda - \frac{N^*\beta_1}{2^{32}} + \rho + r_1\right)(\lambda + r_2) - \frac{\beta_2^2 U^*}{N^*}\right] = 0.$$

While the corresponding Eigenvalues of above relation are

$$\lambda_1 = -r_1,$$
$$\left[\left(\lambda - \tfrac{N^*\beta_1}{2^{32}} + \rho + r_1\right)(\lambda + r_2) - \tfrac{\beta_2^2 U^*}{N^*}\right] = 0.$$

Simplifying the above expression for finding the values of remaining Eigenvalues

$$r_1(\lambda + r_2) + \rho(\lambda + r_2) + \lambda(\lambda + r_2) - (\lambda + r_2)\frac{N^*\beta_1}{2^{32}} - \frac{{\beta_2}^2 U^*}{N^*} = 0,$$
$$\lambda^2 + \lambda\left(r_1 + r_2 + \rho - \frac{N^*\beta_1}{2^{32}}\right) + r_1 r_2 + \rho r_2 - r_2\frac{N^*\beta_1}{2^{32}} - \frac{{\beta_2}^2 U^*}{N^*} = 0,$$
$$\frac{\lambda^2}{r_2(\rho + r_1)} + \frac{\lambda\left(r_1 + r_2 + \rho - \frac{N^*\beta_1}{2^{32}}\right)}{r_2(\rho + r_1)} + \left(1 - \frac{N^*\beta_1}{2^{32}(\rho + r_1)} - \frac{{\beta_2}^2 U^*}{N^* r_2(\rho + r_1)}\right) = 0,$$
$$\frac{\lambda^2}{r_2(\rho + r_1)} + \frac{\lambda}{r_2}\left(\frac{r_2}{\rho + r_1} + \frac{r_1 + \rho}{\rho + r_1} - \frac{N^*\beta_1}{2^{32}(\rho + r_1)}\right) + (1 - R_0) = 0,$$

rearranging the above expression

$$\frac{\lambda^2}{r_2(\rho+r_1)}+\frac{\lambda}{r_2}\left(\frac{r_2}{\rho+r_1}+1-\frac{N^*\beta_1}{2^{32}(\rho+r_1)}\right)+(1-R_0)=0, \tag{5.17}$$

and for $R_0<1$, equation (5.11) can be written as:

$$\frac{N^*\beta_1}{2^{32}(\rho+r_1)}<1-\frac{{\beta_2}^2U^*}{N^*r_2(\rho+r_1)}. \tag{5.18}$$

Using the expression (5.18) in (5.17), make the coefficient positive for $R_0<1$, which show that all Eigenvalues of the system (5.17) are in a negative half plane, so the system is asymptomatically stable for point K_0 when $R_0<1$. If system is stable for the value of $\alpha=1$, it will be stable for the value of $\alpha<1$ as reported in [63]. This completes the proof.

Theorem 4.2. If $R_0<1$, then the point K_0 is globally asymptomatically stable, otherwise unstable.

Proof. Let us consider the following Lyapunov function.

$$L(I,M,U_I)=I+\frac{\beta_1}{2^{33}\rho}M^2+\frac{\beta_2}{r_2}U_I. \tag{5.19}$$

The function is always positive in R^3, for $R^3=(I,M,UI)$ and $(I>0,M>0,UI>0)$. Taking the derivative of the Lyapunov function (19) for α=1 we get

$$D^\alpha L\left(I,M,U_I\right)=D^\alpha I+\frac{2\beta_1}{2^{33}\rho}MD^\alpha M+\frac{\beta_2}{r_2}D^\alpha U_I,$$

$$\begin{aligned}
D^\alpha L(I,M,U_I)&=\frac{\beta_1(N^*-I-M)I}{2^{32}}+\frac{\beta_2(N^*-I-M)U_I}{N^*}-\rho I-r_1I+\frac{\beta_1MI}{2^{32}}\\
&\quad+\frac{r_1\beta_1M^2}{2^{32}\rho}+\frac{{\beta_2}^2U^*I}{N^*r_2}-\frac{{\beta_2}^2U_1I}{N^*r_2}-\beta_2U_1,\\
&=\left(\frac{\beta_1N^*}{2^{32}}+\frac{{\beta_2}^2U^*}{N^*r_2}-\rho-r_1\right)I-\frac{\beta_1I^2}{2^{32}}-\frac{\beta_2(M+I)U_I}{N^*}\\
&\quad-\frac{r_1\beta_1M^2}{2^{32}\rho}-\frac{{\beta_2}^2M^2U_II}{N^*r_2},\\
&=\left((\rho+r_1)\left(\frac{\beta_1N^*}{2^{32}(\rho+r_1)}+\frac{{\beta_2}^2U^*}{N^*r_2(\rho+r_1)}\right)-\rho-r_1\right)I-\frac{\beta_1I^2}{2^{32}}\\
&\quad-\frac{\beta_2(M+I)U_I}{N^*}-\frac{r_1\beta_1M^2}{2^{32}\rho}-\frac{{\beta_2}^2M^2U_II}{N^*r_2},
\end{aligned}$$

$$= (\rho + r_1)(R_0 - 1)I - \frac{\beta_1 I^2}{2^{32}} - \frac{\beta_2(M+I)U_I}{N^*} - \frac{r_1\beta_1 M^2}{2^{32}\rho} - \frac{{\beta_2}^2 U_I I}{N^* r_2}.$$

For $R_0 < 1$, implies that $D^\alpha L \leq 0$ and K_0 is the only invariant set of system (5.12). According to LaSalle Invariance Principle K_0 is globally asymptotically stable, hence this proves the theorem. Therefore, K_0 equilibrium point is globally asymptotically stable for $R_0 < 1$. Additionally, If system is stable for the value of $\alpha = 1$ it will be stable for the value of $\alpha < 1$ as reported in [63].

5.4.4 Endemic Stability

Endemic stability of equilibrium point K^*= (I^*, M^*, U_I^*) is investigated in this section for the values of $R_0 > 1$ and $I^* \geq 0$.

Theorem 4.3. Endemic equilibrium point K^* is locally asymptomatically stable, if $R_0 > 1$.

Proof. Consider the function $f : R^3 \to R^3$ with components and Jacobian matrix for integer order model (5.10) as:

$$\begin{aligned}
D^\alpha I &= f_1(I^*, M^*, U_I^*) = \tfrac{\beta_1(N^*-I^*-M^*)I^*}{2^{32}} + \tfrac{\beta_2(N^*-I^*-M^*)U_I^*}{N^*} - \rho I^* - r_1 I^*,\\
D^\alpha M &= f_2(I^*, M^*, U_I^*) = \rho I^* - r_1 M^*,\\
D^\alpha U_I &= f_3(I^*, M^*, U_I^*) = \tfrac{\beta_2(U^*-U_I^*)I^*}{2^{32}} - r_2 U_I^*,
\end{aligned}$$

$$J(I^*, M^*, U_I^*) = \begin{pmatrix} \frac{\partial f_1}{\partial I^*} & \frac{\partial f_1}{\partial M^*} & \frac{\partial f_1}{\partial U_I^*} \\ \frac{\partial f_2}{\partial I^*} & \frac{\partial f_2}{\partial M^*} & \frac{\partial f_2}{\partial U_I^*} \\ \frac{\partial f_3}{\partial I^*} & \frac{\partial f_3}{\partial M^*} & \frac{\partial f_3}{\partial U_I^*} \end{pmatrix}.$$

The endemic equilibrium point K^*= (I^*, M^*, U_I^*) and the Jacobian matrix at the endemic point is given below for the value of $\alpha = 1$.

$$J(K^*) = \begin{pmatrix} \frac{\beta_1(N^*-2I^*-M^*)}{2^{32}} - \frac{\beta_2 U_I^*}{N^*} - \rho - r_1 & -\frac{\beta_1 I^*}{2^{32}} - \frac{\beta_2 U_I^*}{N^*} & \frac{\beta_2(N^*-I^*-M^*)}{N^*} \\ \rho & -r_1 & 0 \\ \frac{\beta_2(U^*-U_I^*)}{N^*} & 0 & -\frac{\beta_2 I^*}{N^*} - r_2 \end{pmatrix}. \tag{5.20}$$

Characteristic equation of (5.20) is

$$= |\lambda I - J(K^*)| = 0,$$

$$\begin{vmatrix} \lambda - \frac{\beta_1 N^*}{2^{32}} + \frac{\beta_1(2I^*+M^*)}{2^{32}} + \frac{\beta_2 U_I^*}{N^*} + \rho + r_1 & \frac{\beta_1 I^*}{2^{32}} + \frac{\beta_2 U_I^*}{N^*} & -\frac{\beta_2(N^*-I^*-M^*)}{N^*} \\ -\rho & \lambda + r_1 & 0 \\ -\frac{\beta_2(U^*-U_I^*)}{N^*} & 0 & \lambda + \frac{\beta_2 I^*}{N^*} + r_2 \end{vmatrix} = 0,$$

simplifies as:

$$\lambda^3 + (b_{11} + b_{22} + b_{33})\lambda^2 + (b_{11}b_{22} + b_{11}b_{33} + b_{22}b_{33} - b_{12}b_{21} - b_{13}b_{31})\lambda \qquad (5.21)$$
$$+b_{11}b_{22}b_{33} - b_{12}b_{21}b_{33} - b_{13}b_{31}b_{22} = 0,$$

where

$$b_{11} = -\frac{\beta_1 N^*}{2^{32}} + \frac{\beta_1(2I^*+M^*)}{2^{32}} + \frac{\beta_2 U_I^*}{N^*} + \rho + r_1, \quad b_{12} = \frac{\beta_1 I^*}{2^{32}} + \frac{\beta_2 U_I^*}{N^*}, \quad b_{21} = -\rho, b_{23} = 0,$$
$$b_{22} = r_1, \quad b_{13} = -\frac{\beta_2(N^*-I^*-M^*)}{N^*}, \quad b_{31} = -\frac{\beta_2(U^*-U_I^*)}{N^*}, \quad b_{33} = \frac{\beta_2 I^*}{N^*} + r_2, b_{32} = 0.$$

To analyze the stability, we use Hurwitz criteria as reported in [143, 144] for system (5.21). Now equating the coefficient of general characteristics equation with (5.21), we have

$$\begin{aligned} b_0 &= 1, \\ b_1 &= b_{11} + b_{22} + b_{33}, \\ b_2 &= b_{11}b_{22} + b_{11}b_{33} + b_{22}b_{33} - b_{12}b_{21} - b_{13}b_{31}, \\ b_3 &= b_{11}b_{22}b_{33} - b_{12}b_{21}b_{33} - b_{13}b_{31}b_{22}. \end{aligned}$$

Determinants (D_1, D_2 and D_3) of the characteristic equation (5.21) are expressed in Hurwitz process as:

$$\begin{aligned} D_1 &= b_1 = b_{11} + b_{22} + b_{33}, \\ &= -\frac{\beta_1 N^*}{2^{32}} + \frac{\beta_1(2I^* + M^*)}{2^{32}} + \frac{\beta_2 U_I^*}{N^*} + \rho + r_1 + r_1 + \frac{\beta_2 I^*}{N^*} + r_2, \end{aligned}$$

using the value of equation (5.11) for $R_0 > 1$ as:
$\frac{\beta_1 N^*}{2^{32}} + \frac{\beta_2^2 U^*}{r_2 N^*} > \rho + r$, we have

$$D_1 = -\frac{\beta_1 N^*}{2^{32}} + \frac{\beta_1(2I^*+M^*)}{2^{32}} + \frac{\beta_2 U_I^*}{N^*} + \frac{\beta_1 N^*}{2^{32}} + \frac{\beta_2^2 U^*}{r_2 N^*} + r_1 + \frac{\beta_2 I^*}{N^*} + r_2,$$

$$D_1 = \frac{\beta_1(2I^*+M^*)}{2^{32}} + \frac{\beta_2 U_I^*}{N^*} + \frac{\beta_2^2 U^*}{r_2 N^*} + r_1 + \frac{\beta_2 I^*}{N^*} + r_2,$$

$$D_1 > 0,$$

and

$$\begin{aligned}
D_2 &= b_1 b_2 - b_3 b_0,\\
D_2 &= (b_{11}+b_{22}+b_{33})(b_{11}b_{22}+b_{11}b_{33}+b_{22}b_{33}-b_{12}b_{21}-b_{13}b_{31})\\
&\quad - b_{11}b_{22}b_{33}+b_{12}b_{21}b_{33}+b_{13}b_{31}b_{22},\\
&= b_{11}^2 b_{22}+b_{11}^2 b_{33}+b_{11}b_{22}b_{33}-b_{11}b_{12}b_{21}-b_{11}b_{13}b_{31}+b_{11}b_{22}^2+b_{11}b_{22}b_{33}\\
&\quad + b_{22}^2 b_{33}-b_{22}b_{12}b_{21}-b_{22}b_{13}b_{31}+b_{11}b_{22}b_{33}+b_{11}b_{33}^2+b_{22}b_{33}^2-b_{33}b_{12}b_{21}\\
&\quad - b_{33}b_{13}b_{31}-b_{11}b_{22}b_{33}+b_{33}b_{12}b_{21}+b_{22}b_{13}b_{31},\\
D_2 &= b_{11}^2 b_{22}+b_{11}^2 b_{33}+b_{11}b_{22}^2+b_{22}b_{33}^2+b_{11}b_{33}^2+b_{22}^2 b_{33}+2b_{11}b_{22}b_{33}-b_{11}b_{12}b_{21}\\
&\quad - b_{11}b_{13}b_{31}-b_{22}b_{12}b_{21}-b_{33}b_{13}b_{31}.
\end{aligned}$$

The above expression remain positive except for $-b_{13}b_{31}(b_{11}+b_{33})$, D_2 is desired to be positive for $R_0 > 1$, we simply represent the expression as:

$$D_2 = +\text{veterms} + (b_{11}b_{33}-b_{13}b_{31})(b_{11}+b_{33}),$$

$$D_2 = D_{2-1} + D_{2-2},$$

Here, D_{2-1} represent the positive terms in D_2 while the remaining terms represented with D_{2-2}, we have.

$$\begin{aligned}
D_{2-2} &= (b_{11}b_{33}-b_{13}b_{31})(b_{11}+b_{33}),\\
&= \left\{\left(\frac{\beta_1(N^*-I^*-M^*)}{2^{32}}+\rho+r_1\right)r_2 - \frac{\beta_2^2(N^*-I^*-M^*)(U^*-U_I^*)}{N^{*2}}\right\}(b_{11}+b_{33}),\\
&= \left\{\left(\frac{\beta_1(N^*-I^*-M^*)}{2^{32}}+\rho+r_1 - \frac{\beta_2^2(N^*-I^*-M^*)(U^*-U_I^*)}{r_2 N^{*2}}\right)r_2\right\}(b_{11}+b_{33}),\\
&= \left\{\left(\frac{\beta_1(N^*-I^*-M^*)}{2^{32}}+\rho+r_1 - \frac{\beta_2^2(N^*-I^*-M^*)U^*}{r_2 N^{*2}} + \frac{\beta_2^2(N^*-I^*-M^*)U_I^*}{r_2 N^{*2}}\right)r_2\right\}\\
&\quad (b_{11}+b_{33}),\\
&= \left\{\left(\begin{array}{l}\frac{\beta_1(N^*-I^*-M^*)}{2^{32}}+\rho+r_1 - \frac{\beta_2^2 U^*}{r_2 N^*} + \frac{\beta_2^2 I^* U^*}{r_2 N^{*2}} + \frac{\beta_2^2 M^* U^*}{r_2 N^{*2}}\\ +\frac{\beta_2^2(N^*-I^*-M^*)U_I^*}{r_2 N^{*2}}\end{array}\right)r_2\right\}(b_{11}+b_{33}),
\end{aligned}$$

for using the value of $R_0 > 1$ and after simplification, the above expression becomes

$$D_{2-2} > \left\{ \left(\begin{array}{l} \frac{\beta_1(N^* - I^* - M^*)}{2^{32}} + \frac{\beta_1 N^*}{2^{32}} + \frac{\beta^2{}_2 U^*}{r_2 N^*} - \frac{\beta^2{}_2 U^*}{r_2 N^*} \\ + \frac{\beta^2{}_2 I^* U^*}{r_2 N^{*2}} + \frac{\beta^2{}_2 M^* U^*}{r_2 N^{*2}} + \frac{\beta^2{}_2 (N^* - I^* - M^*) {U_I}^*}{r_2 N^{*2}} \end{array} \right) r_2 \right\}$$
$$(b_{11} + b_{33}),$$

$$D_{2-2} > \left\{ \left(\begin{array}{l} \frac{\beta_1(N^* - I^* - M^*)}{2^{32}} + \frac{\beta_1 N^*}{2^{32}} + \frac{\beta^2{}_2 I^* U^*}{r_2 N^{*2}} \\ + \frac{\beta^2{}_2 M^* U^*}{r_2 N^{*2}} + \frac{\beta^2{}_2 (N^* - I^* - M^*) {U_I}^*}{r_2 N^{*2}} \end{array} \right) r_2 \right\}$$
$$(b_{11} + b_{33}),$$

$$D_{2-2} > 0,$$

as a result

$$D_2 > 0.$$

$$D_3 = b_3(b_1 b_2 - b_0 b_3),$$

$$D_3 = b_3(D_2),$$

$$D_3 = \begin{pmatrix} b_{11}b_{22}b_{33} - b_{12}b_{21}b_{33} \\ -b_{13}b_{31}b_{22} \end{pmatrix} \begin{pmatrix} (b_{11} + b_{22} + b_{33})(b_{11}b_{22} + b_{11}b_{33} \\ +b_{22}b_{33} - b_{12}b_{21} - b_{13}b_{31}) \\ - b_{11}b_{22}b_{33} + b_{12}b_{21}b_{33} + b_{13}b_{31}b_{22} \end{pmatrix},$$
$$= (b_{11}b_{22}b_{33} - b_{12}b_{21}b_{33} - b_{13}b_{31}b_{22})D_2,$$
$$> (b_{11}b_{33} - b_{13}b_{31})b_{22}D_2,$$

positivity of the expression $b_{11}b_{33} - b_{13}b_{31}$ for $R_0 > 1$ is already proved for the case D_2, therefore,
$D_3 > 0$.

Thus, all the values of D_1, D_2 and D_3 are positive, so all the Eigenvalues of the equation (5.21) are in the left half plane for $R_0 > 1$, then there exists an endemic equilibrium point K^* which is locally asymptomatically stable. This completes the proof.

5.5 Simulation and Results

In this section, results of numerical simulations for FO-SVM are presented to understand the dynamics of virus spread in critical network infrastructure in the presence of removable storage connectivity which may compromise the air-gap between the networks. Numerical experimentation is conducted for the designed FO-SVM as given in equation (5.6) for different variation of parameters and initial start-up scenarios as mentioned in tables 5.1 and 5.2 respectively. The dynamical behavior of the fractional order (FO) model is studied by varying the non-integer order derivative α using scientific computer programming language MATLAB R2015b 64bit. Most FO differential system lacks exact analytical solutions, so numerical solver based on Grunwald-Letnikov (GL) procedure as described in section 2 is exploited for approximate solution of the model. To establish the working accuracy of GL fractional numerical method, results of GL method is compared with RK method for integer order scenario. Error analysis are shown in error plots which establish the working accuracy of the method. The security firms including Symantec tracked 100,000 infected computers as of September 29, 2010 in the world. Additionally, available real data is used to validate the accuracy and convergence of the model for Stuxnet virus spread. The virus infects approximately 100,000 users from 155 different countries and 63% were in Iran only. The number of hosts that lost functionality (hardware connected to these hosts was damaged due to sudden increase in frequency up to 1410 Hz then decreased to 2 Hz and then again increased to 1064 Hz in spite of normal working range of 807 Hz to 1210 Hz) due to virus attack. Virus operated the machines connected with the hosts at extreme range of frequencies dictated by Stuxnet and caused a physical damage of 1500 centrifuge machines (approximately 1200 in Iran only). Approximately 3,280 unique samples and variants of Stuxnet virus were recorded by Symantec and other security corporations [120, 122, 222].

In order to establish the working accuracy of GL based numerical solvers, results of the scheme are compared with state of the art numerical solver based on Runge-Kutta (RK) method for integer order case of the model. The results

TABLE 5.1: Parameters variation in the simulation of the FO-SVM model.

Parameter	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6	Case 7	Case 8	Case 9
A_1	0.042	0.042	40	100	5600	5600	5600	412	5600
A_2	0.042	0.042	45.7	60	412	412	412	5600	412
β_1	0.6	0.4	0.385	0.4	0.4	0.4	0.745	0.4	0.4
β_2	0.6	0.8	0.795	0.635	0.745	0.745	0.4	0.745	0.004
ρ	0.00265	0.0051	0.001	0.009	0.021	0.8	0.021	0.021	0.021
r_1	0.1126	0.19	0.0804	0.1598	0.1276	0.0804	0.1276	0.1276	0.1276
r_2	0.0088	0.027	0.027	0.027	0.0131	0.0131	0.0131	0.0131	0.0131

TABLE 5.2: Initial values of the parameter used in simulation of the model.

Variables	S	I	M	U_S	U_I
Case 1	$2.3 * 10^6$	10000	10	50000	10000
Case 2	$2.3 * 10^6$	30000	10	50000	10000
Case 3	$2.3 * 10^6$	30000	10	30000	10000
Case 4-9	$2.3 * 10^6$	30000	10	30000	5000

are determined for nine cases of integer order model (5.6) by GL based computing technique for inputs $t \in [0,\ 60]$ with step size $h = 0.001$ (time t taken in months). Numerical solutions of the model on the same inputs are also calculated by the RK method for each variation. Figure 5.3 highlights the model behavior with Stuxnet virus real world data. FO-SVM model results shown in figure 5.3 is calculated using RK method for assuming the value of fractional order $\alpha = 1$. In figure 5.3 number of hosts are plotted versus time in months which shows the number of infected hosts due to a Stuxnet virus global attack. Number of infected hosts are 96,760 (real infected hosts were 100,000) and number of damaged hosts are 1500 (real damaged hosts were 1500) in 23 months time which shows model accuracy for real world virus data as shown in figure 5.3 with red and blue dots respectively.

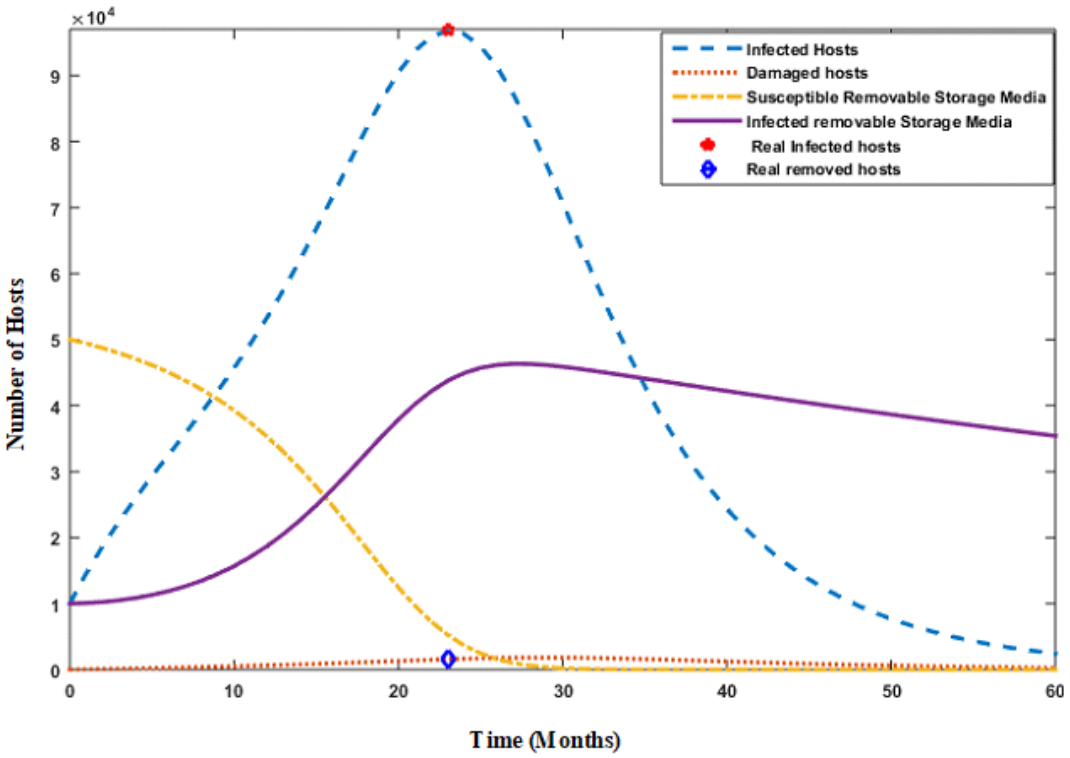


FIGURE 5.3: Simulation of Stuxnet virus spread with available data having parameters A_1=0.042, A_2=0.042, β_1=0.366, β_2=0.6, ρ=0.00265, r_1=0.1126, r_2=0.0088, S=$2.3 * 10^6$, I=10000, M=10, U_s=50000, U_I=10000.

In this case total number of removable storage media are assumed to be 60,000 and due to increase in the number of infected hosts (96,760 after 23 months), infection in removable storage media increases. The number of infected removable storage devices are 43,740 in 23 months. Decrease in the number of infected hosts are observed after 23 months due to availability of remedial techniques, natural isolation from networks and anti-virus signature update for the Stuxnet virus.

In figure 5.4, comparisons of results of both RK numerical solver and GL based method are presented for susceptible hosts S in nine cases. The error analysis based on absolute difference between two approaches are also plotted in figure 5.4 to assess the closeness. Results shows a matching of both solutions up to three decimal place of accuracy. The small values of errors in these plots show that results of GL method are in good agreement with standard RK numerical technique, which establishes the working accuracy of the GL based solver. In figures 5.5 and 5.6, comparison of RK method with GL method are presented for infected nodes I, damaged node M, susceptible removable storage media U_s and infected

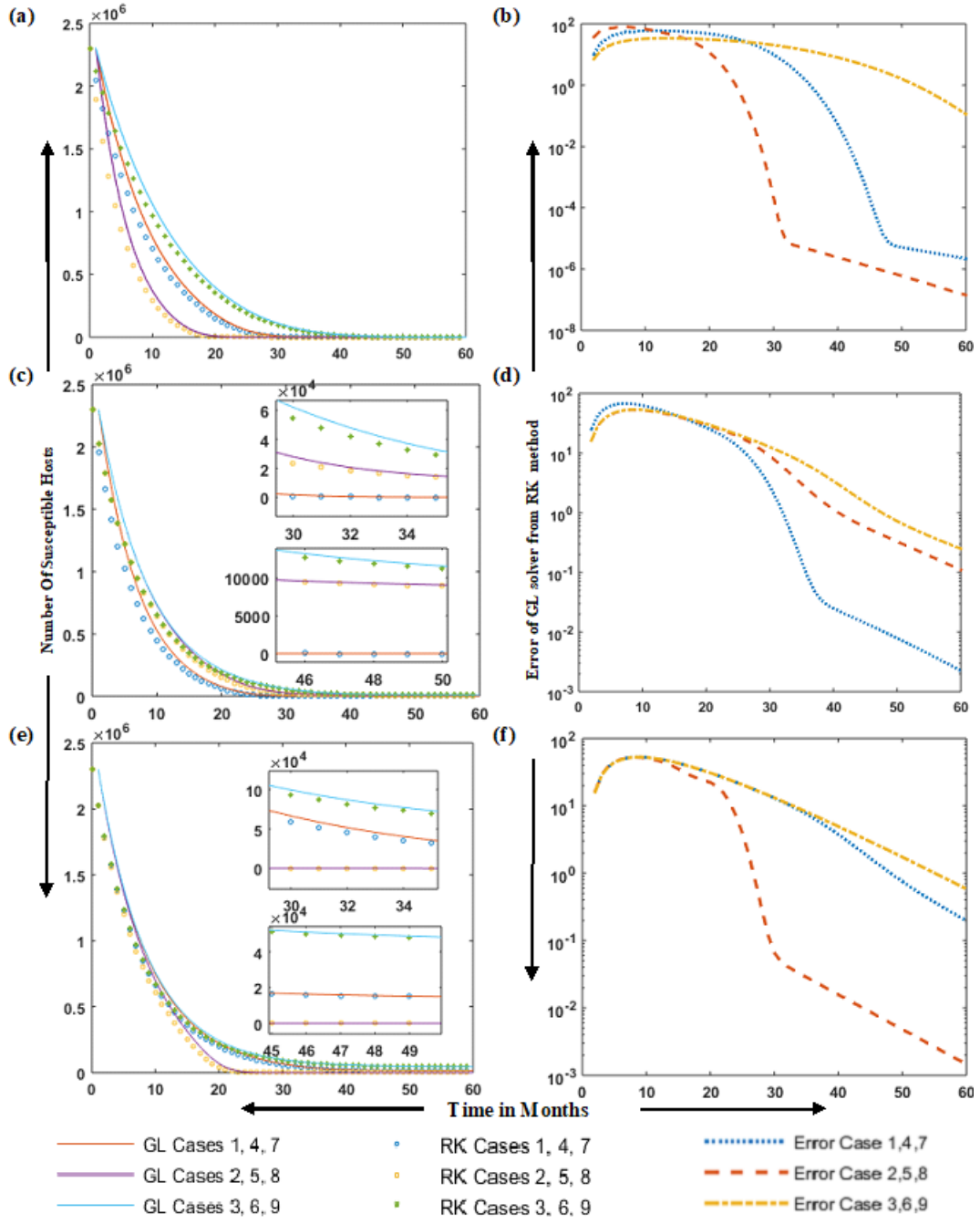


FIGURE 5.4: Comparison of solutions for GL solver from RK method in case of susceptible S hosts; a and b for cases 2 to 4, c and d for cases 5 to 7 while e and f for cases 8 to 10.

removable storage media U_I respectively for nine cases of the model. These nine cases also explain behavior of virus spread in different scenarios. Considering the figures 5.4-5.6 and the different cases simulated, we have the following comments to make. Case 1 shows the behaviour of model (5.6) by increasing the value of infectious contact rate β_1 from 36.6% to 60% (value of β_1 in figure 5.3 is 36.6%).

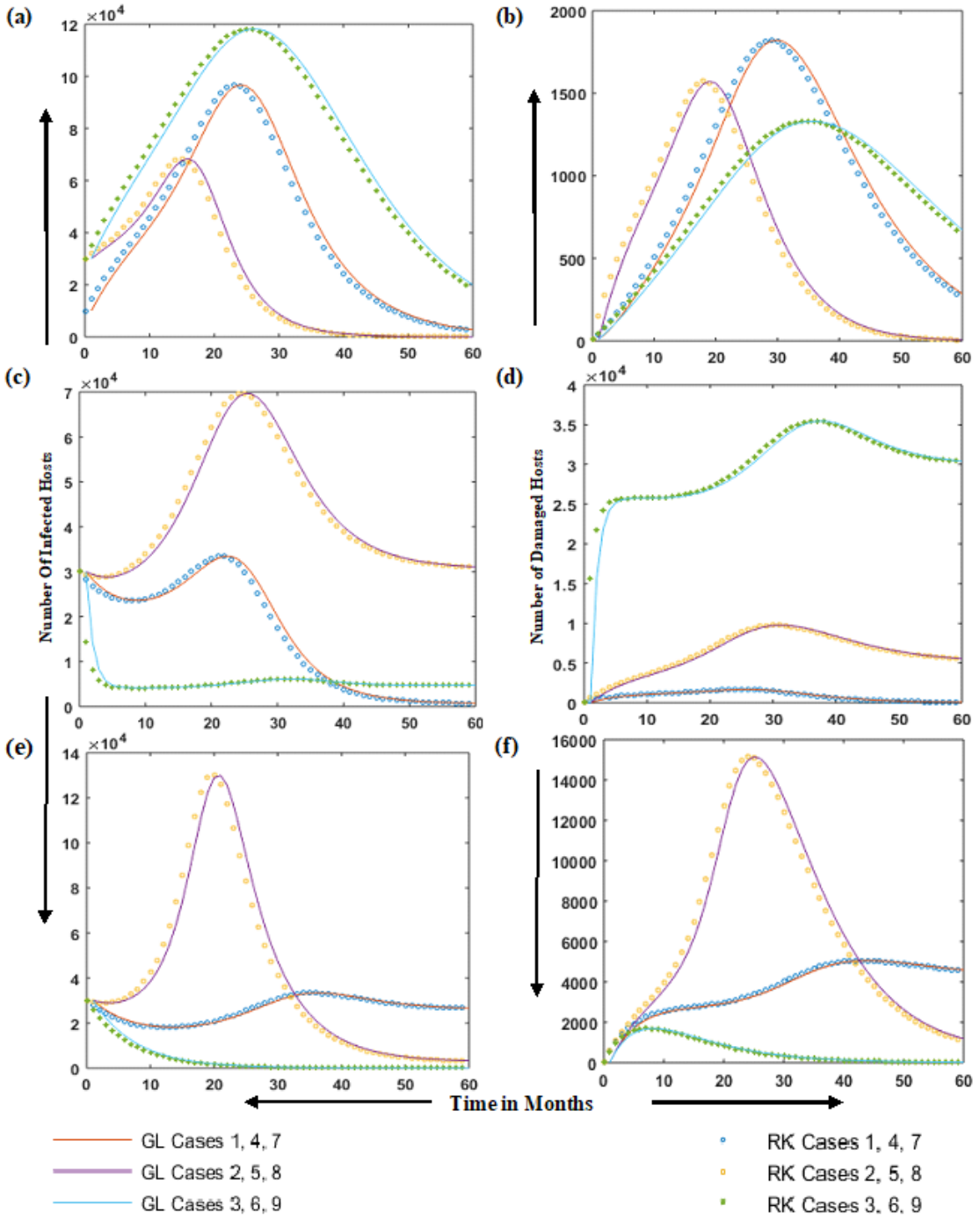


FIGURE 5.5: Comparison of solutions for GL solver from RK method in case of infected hosts I and damaged hosts M; a and b for cases 1 to 3, c and d for cases 4 to 6 while e and f for cases 7 to 9.

It is observed that number of infected hosts in 24 months are 96,760 as shown in figure 5.5a (in figure 5.3, number of infected hosts in 24 months are 96,270) which shows a slight increase in the number of infected hosts. In case 2, number of initial infected hosts are assumed to be 30,000. Increasing the infectious

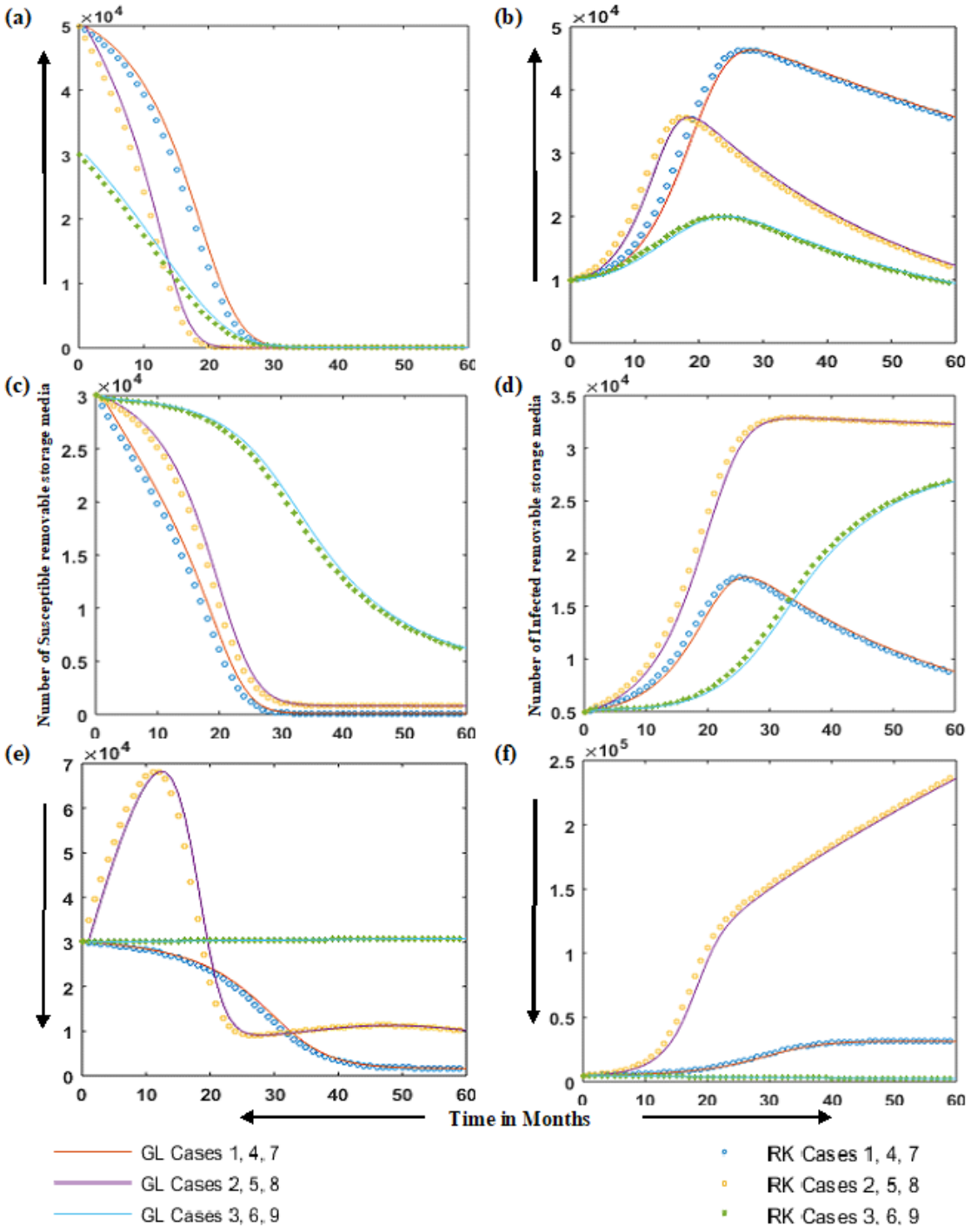


FIGURE 5.6: Comparison of solutions for GL solver from RK method in case of susceptible and infected removable storage media; a and b for cases 1 to 3, c and d for cases 4 to 6 while e and f for cases 7 to 9.

contact rate of removable storage media (in case 2) reduces the number of susceptible hosts rapidly as compared to case 1 (figure 5.4a). However, the number of infected hosts are reduced (figure 5.5a) due to increase in the natural removal rate of hosts and removable storage media r_1 and r_2 (hosts are removed to save from

the Stuxnet attack). In case 3, we reduce the damage rate and the quantity of initial susceptible removable storage media which reduces the number of infected removable storage media (figure 5.6b) and increases the number of infected hosts (figure 5.5a). In case 4, FO-SVM model dynamics are observed by increasing the arrival rate of new nodes and the arrival rate of new removable storage devices as mentioned in tables 5.1 and 5.2. Results shows that even increasing the arrival rate of new hosts and arrival rate of new removable storage media will not spread the infection faster without the presence of a sufficient number of infected removable storage devices as shown in figure 5.5c. In cases 5 and 6, we further increase the values of arrival rate of new nodes as well as removable storage devices for in-depth behavior analysis of the model. Both cases have similar parameters except case 6 which represents higher damage rate (especially, for zero-day vulnerability or for a new virus attack) that increases the quantity of damaged computers and reduces the number of infected computers (removed due to high damage rate) in the networks as compared to case 5. Case 5 shows high number of infected nodes (figure 5.5c) because Stuxnet virus only destroys the machines which have specific hardware (Siemens specific PLCs) and remains dormant till it finds the target. In case 7 values of β_1 and β_2 of case 6 are swapped to observe the behavior of the model. In case 7 value of β_1 is increased and the value of β_2 is decreased as compared to case 6. It is observed that increasing the infectious contact rate β_1 of FO-SVM model does not increase the infection as much (figure 5.5e). However, increasing the value of β_2 (the infectious contact rate of removable storage media with susceptible computer nodes) and A_2 (the arrival of removable storage media) in case 8, will increase the infection in the network. This outlines the role of removable storage media in transferring virus in the air-gapped networks (figure 5.5e). In case 9, value of infectious contact rate of removable storage media with susceptible computer nodes β_2 is reduced which results in the reduction of damaged nodes (figure 5.5f), infected nodes (figure 5.5e) and increase in the number of susceptible storage devices (figure 5.6e). Case 9 further elaborates the scenario already presented in case 8.

The derivative order $\alpha = 1$ has been presented in the figures 5.4,5.5 and

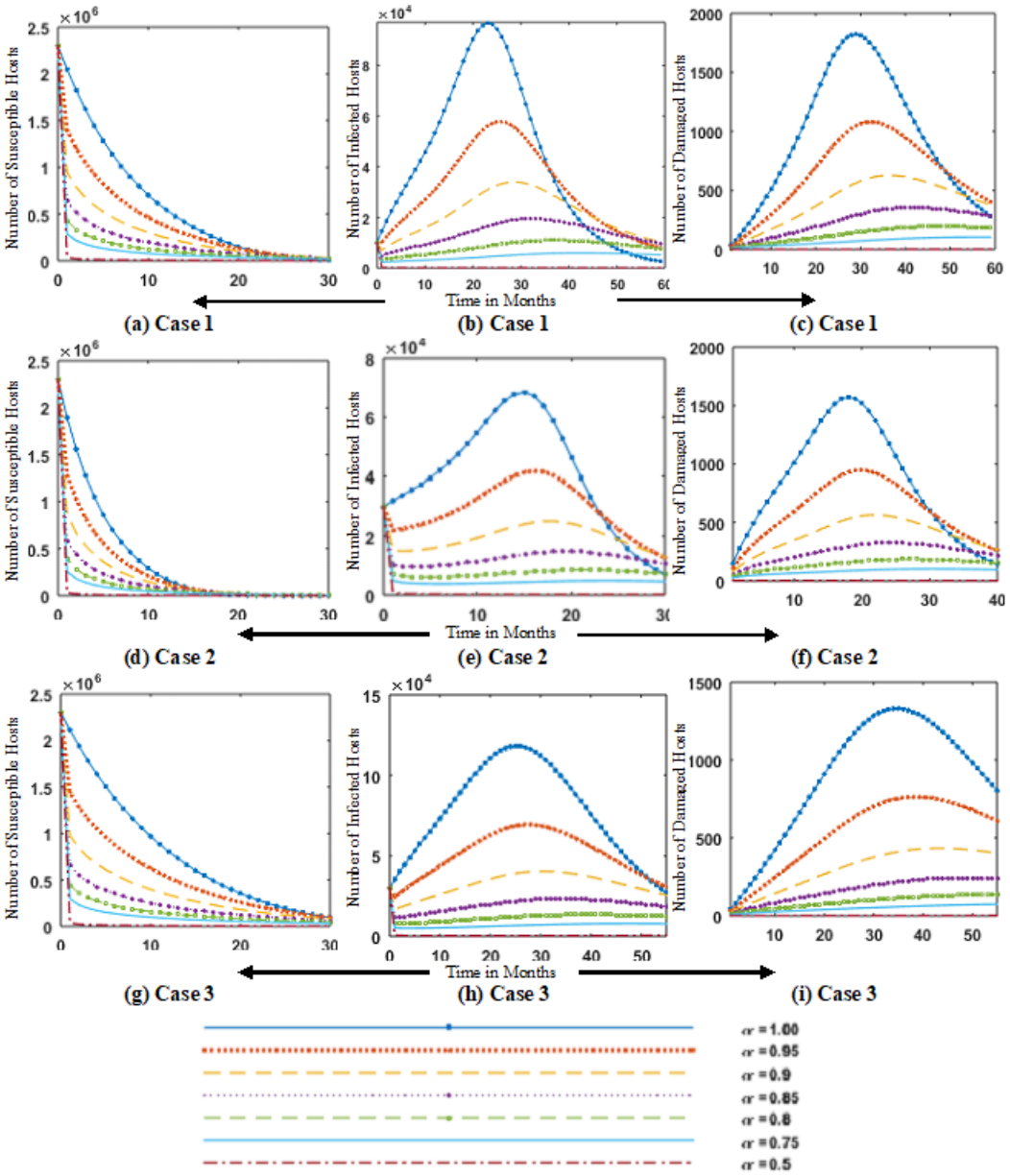


FIGURE 5.7: Dynamics of the susceptible S, infected I and damaged M computers for cases 1 to 3 of FO-SVM for 60-month time t by taking different fractional orders.

5.6. The effect of change in fractional order α has been presented in figures 5.7-5.11. Detailed analysis of FO-SVM model is conducted by changing fractional order α in the system (5.6), such that one may observe fast transients as well as slow evolutions in the dynamics of the model. The fractional order solution of the FO-SVM model for different values of the fractional order α are solved using GL based solver. The solutions are determined for nine cases of FO-SVM by GL based numerical procedure for different fractional orders, i.e., $\alpha = [0.5, 0.75, 0.8,$

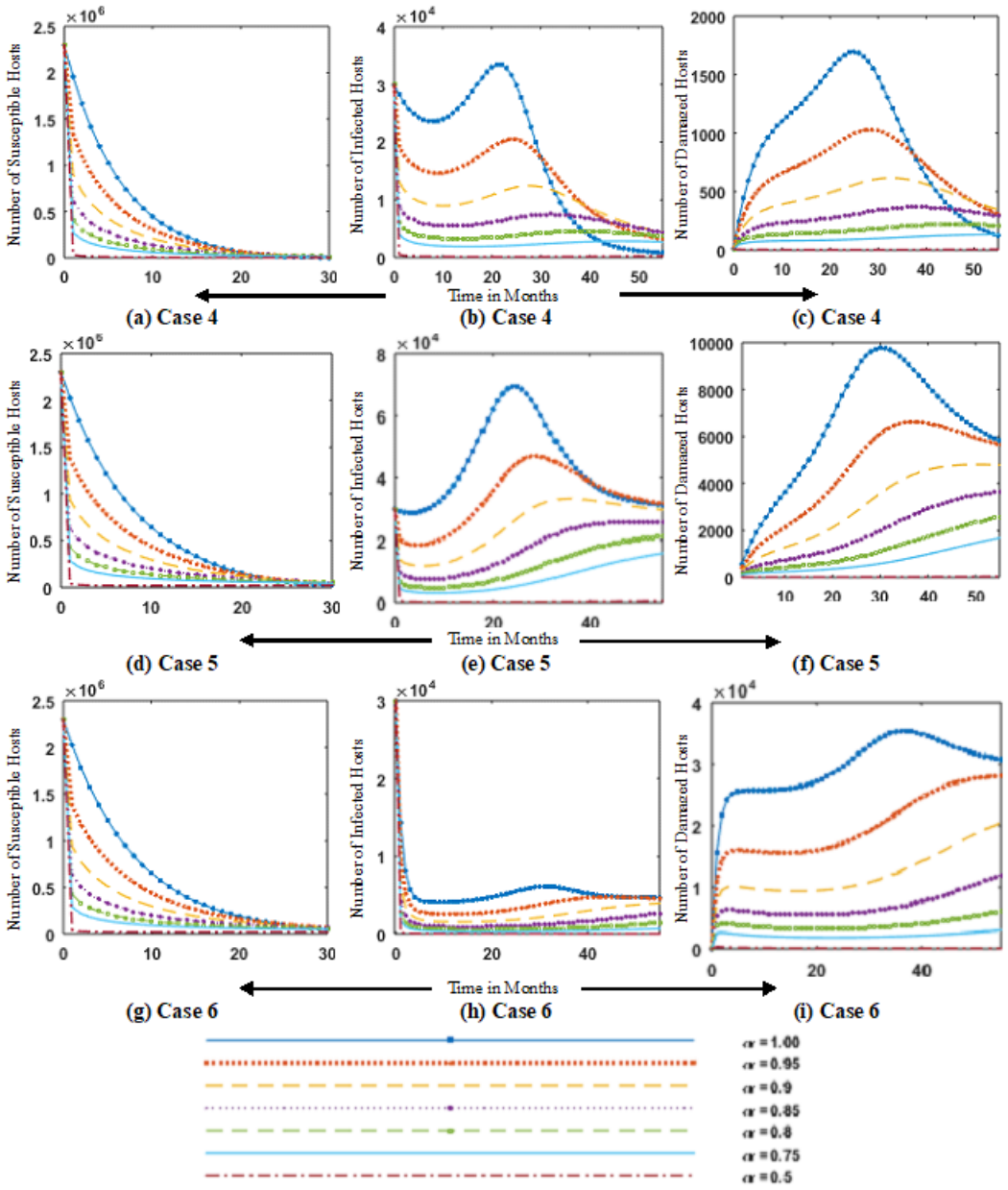


FIGURE 5.8: Dynamics of the susceptible S, infected I and damaged M computers for cases 4 to 6 of FO-SVM for 60-month time t by taking different fractional orders.

0.85, 0.9, 0.95, 1], for the inputs $t \in [0, 60]$ with step size $h = 0.001$. Results for the dynamics of the FO-SVM model in terms of susceptible S, infected I and damaged M computers are plotted in figures 5.7,5.8 and 5.9 for cases 1-3, 4-6 and 7-9 respectively. Susceptible removable storage media U_s and infected removable storage media U_I are plotted in figures 5.10 and 5.11 for cases 1-4 and 5-9 respectively for different values of the fractional order α.

In figure 5.7 number of susceptible, infected and damaged hosts are plotted versus

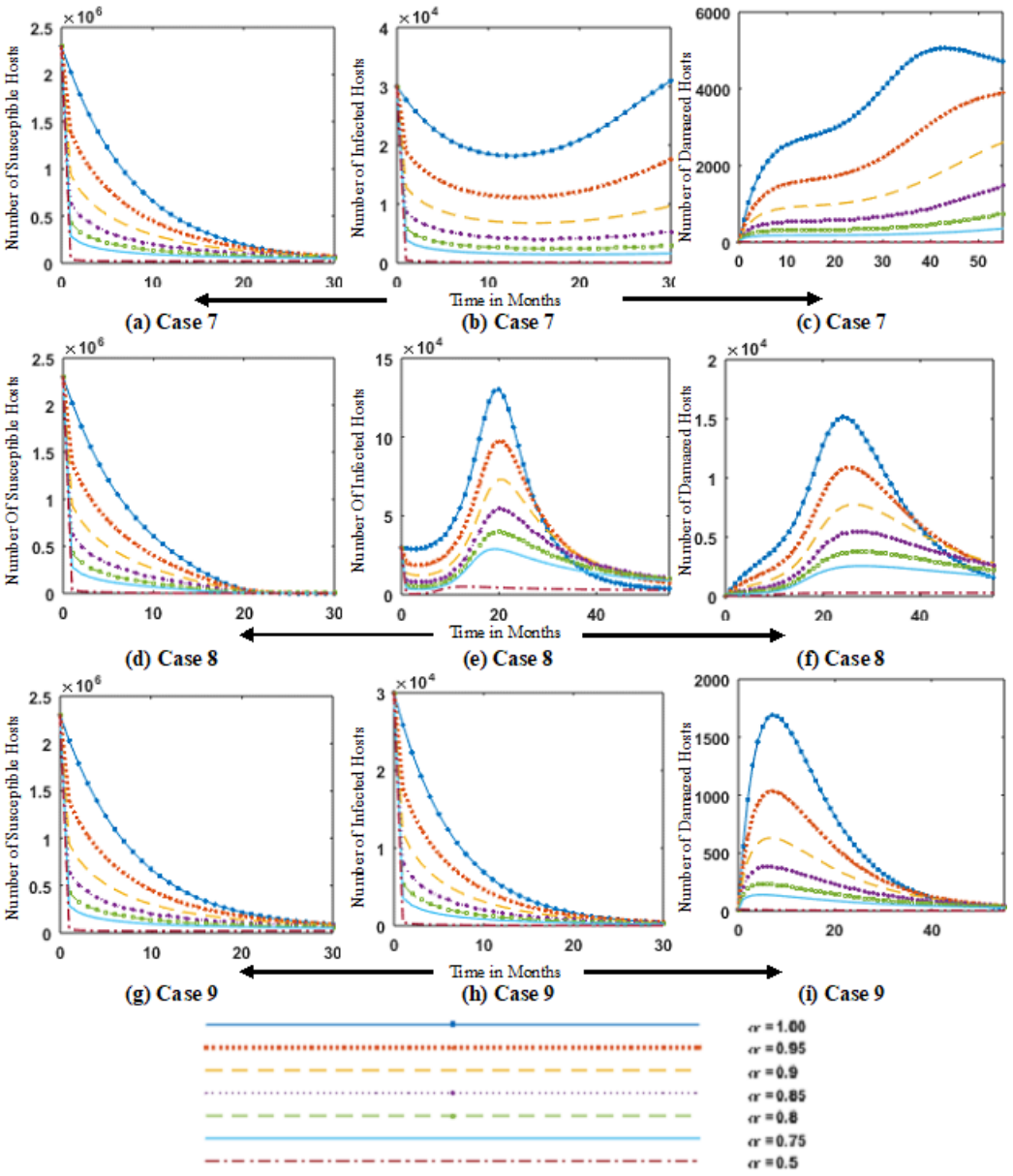


FIGURE 5.9: Dynamics of the susceptible S, infected I and damaged M computers for cases 6 to 9 of FO-SVM for 60-month time t by taking different fractional orders.

time for cases 1-3 with the value of α =[0.5, 0.75, 0.8, 0.85, 0.9, 0.95, 1]. Consistent pattern is observed in the evolution of curves with the value of order α. The value of infected hosts in case 1 with $\alpha = 1$ is 96,760, and for $\alpha = 0.95$, the value of infected hosts are approximately 56,000 for $t = 24$ months as shown in figure 5.7b. In figure 5.7c, the number of damaged hosts (hosts that were connected with specific models of Siemens PLCs) for the value of $\alpha = 0.95$ are 1000 for $t = 30$. **Adjusting the value of α to 0.98 may adjust the number of**

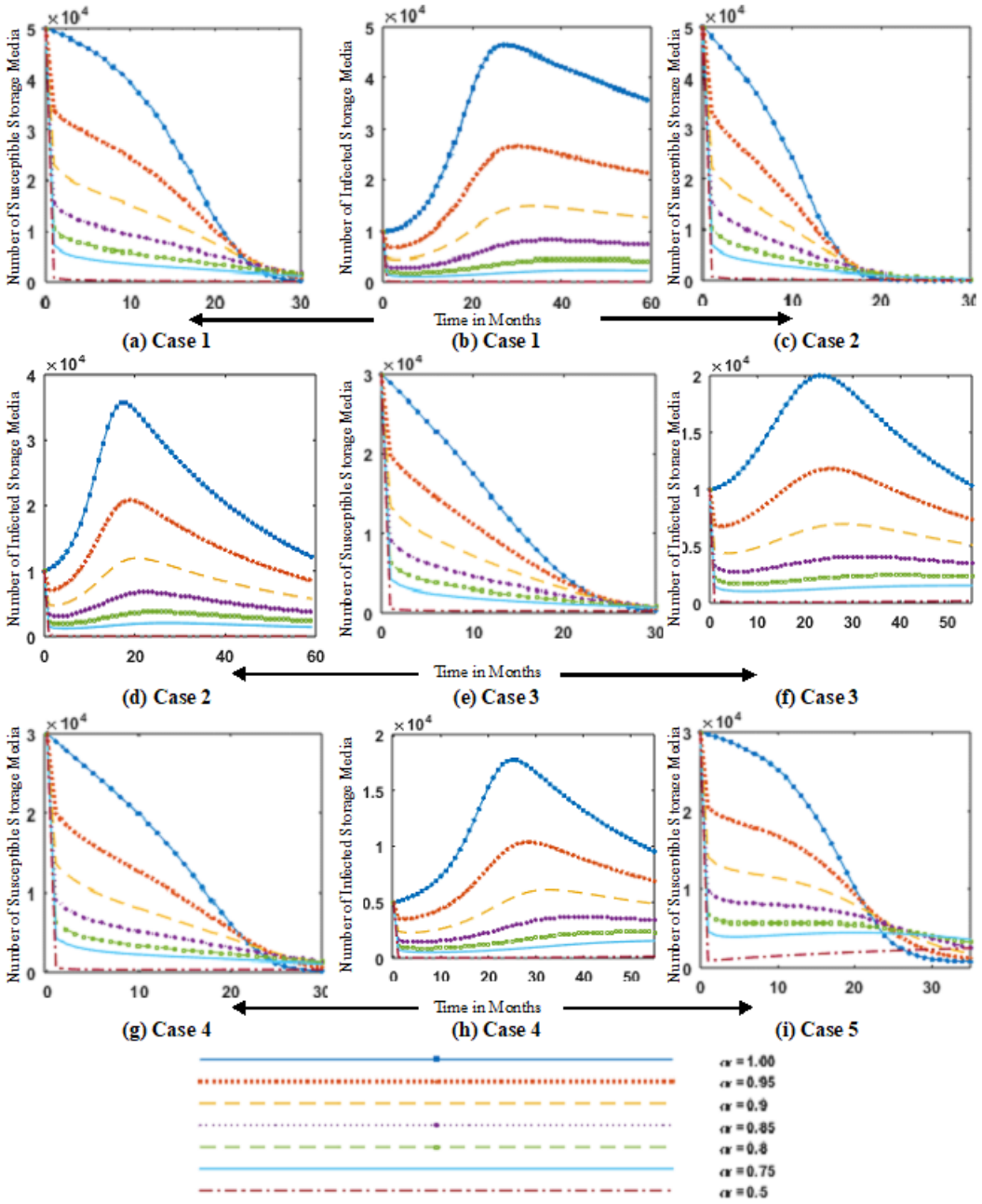


FIGURE 5.10: Dynamics of the susceptible removable storage media U_s and infected removable storage media U_I for 60-month time t, for cases 1 to 5 of FO-SVM by taking different fractional orders.

damaged hosts to 1500, which matches with the real published data of the Stuxnet virus. This illustrate the controllability feature of α for tuning the model. Despite the rapid spread-ability of Stuxnet virus it causes little or no harm to the systems that don't have specific hardware. Figures 5.8 and 5.9 highlight the results for cases 4-6 and 7-9 respectively for variation of fractional order α, which shows that variation in α gives smooth variations in the dynamics. For $\alpha = 0.1$ we

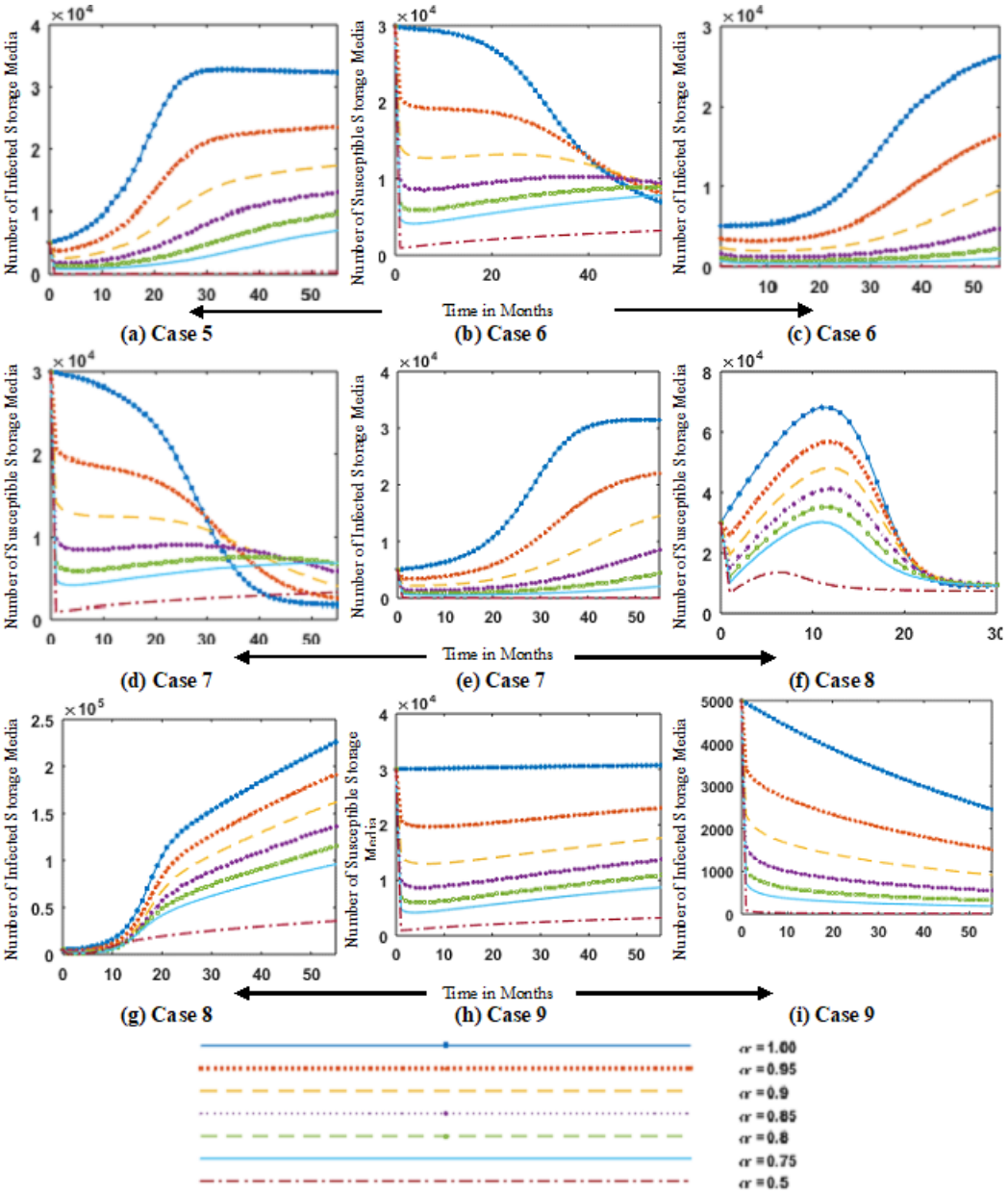


FIGURE 5.11: Dynamics of the susceptible removable storage media U_s and infected removable storage media U_I for 60-month time t, for cases 5 to 9 of FO-SVM by taking different fractional orders.

have the slowest evolution. In figures 5.10 and 5.11 number of susceptible storage media and infected storage media are plotted for case 1-9 against time for different values of fractional order α =[0.5, 0.75, 0.8, 0.85, 0.9, 0.95, 1]. It is observed that tuning the values of α tunes the dynamics of transients as shown in figure 5.10a. The value of susceptible storage media for $t = 1$ and $\alpha = 0.95$ is 35,000 which reduces to 10,000 for $\alpha = 0.8$. For the value of $\alpha = 0.1$, slow change is being observed in the dynamics. Increasing the value of α increases the rate of change

of the variables. Fractional version of the Stuxnet virus model is considered for further virus analysis. The results of the fractional variant are compared with results of the standard integer order derivative model. The fractional model is novel and to establish the working accuracy of GL fractional numerical method, results of GL method are also compared with RK method for integer order scenario. Error analysis are shown in error plots which establish the working accuracy of the method.

5.6 Chapter Summary

A detailed analysis of novel design of fractional order Stuxnet virus model is presented with richer dynamics for the transmission of virus spread in an isolated critical network through removable storage media. The fractional order Stuxnet virus based mathematical models are found at least as stable as integer order models. The value of fractional order α of proposed fractional Stuxnet virus model control the solution reachability toward stead state point more effectively. Additionally, the fractional order system of Stuxnet virus model can tackle the different responses viably, including super slow evolutions and very fast transients, these responses are found in system having long memory characteristics. It is observed that changing the value of α provide a degree of freedom for more general models. More flexibility to be tuned / adjusted to predict new upcoming viruses / trojans and their spread dynamics. Tacking the value of $\alpha = 0.98$ may adjust the number of damaged hosts to 1500 in case 1 which matches the number of damaged caused by Stuxnet virus. The process of transformation of classical model in to a fractional model is very sensitive to the value of order of differentiation α and can be converted to a simple SIR model if we choose the values of infectious contact rate $\beta_2 = 0$. Theoretical analysis of the model capturing the Stuxnet virus spreading characteristics is determined by mathematical derivation of the basic reproduction number R_0 for integer order scenarios. Disease free and endemic equilibrium points of the model is globally asymptotically stable for $R_0 < 1$ and $R_0 > 1$, respectively.

Chapter 6

Vulnerabilities Analysis of Hardware Implants

This chapter presents the design of an epidemic model that portray the exploitation of hardware bug implanted through embedded tiny chip based mini-computer within another computer such as Intel management engine (ME). The succeeding chapter will also present the fractional variation of the proposed model.

6.1 Introduction

A bug in a software is an error, failure, flaw, that can produces an unenviable results, behave in an undesirable way or might allow malicious user to bypass restriction to access the privileged control of the system [159]. Bugs are not viruses but they may allow the installation of backdoor, malware and compromise the whole system, e.g., a patient was died in a radiation therapy in 1980 due to a bug in Therac-25 and a Chinook helicopter was crashed in 1994 due to a code bug in its control computer [161]. Theoretical analysis of the compromised systems are carried out by utilizing the strength of epidemiological modeling of threat propagation [162, 163]. The control strategies of these compromised nodes are very difficult because they implant backdoors, install malicious utilities, gain admin

rights, work as a legitimate program or infect with viruses. Increase in the use of Internet and advancement in fabrication technologies provides an opportunity to implant hardware backdoors which poses a great challenge to the security of system connected with critical infrastructures. Geopolitical tension increases the frequency of attack for compromising enemy country systems, installation of backdoors and sabotaging the critical infrastructure of the opponent [165]. Hardware based implants are common in these days gadgets that would do malicious stuff, subvert the system and possibly control the system to execute the malicious intent. A fully capable computer tiny chip is a size of a pencil point that can compromise the whole infrastructure. Detection of hardware based implants are very difficult which also provides an opportunity for researcher to find a reasonable solution [166–168].

Mathematical model used for the compromised hardware is an effective way to analyze the spread of the malicious code in the infrastructure of any organization. Theoretical analysis of the malicious codes can be carried out by the competency of epidemiology modelling of virus propagation dynamics [131, 174]. The advancement in technologies creates several challenges to the security of the infrastructure of the nations in the presence of vulnerability and the development of smart viruses. [1]. The global median dwell time of attackers are decreasing and targeting prey become easy due to bugged hardware. Therefore, detail dynamical analysis of hardware implants and their devastation pattern with control mechanisms looks promising domain to be investigated by the research community. In this chapter, a bugged, compromised and patched (BCP) mathematical model is presented to analyze the spread of the virus and exploitation of system resources in compromised hardware. The contributions of the proposed BCP model are briefly narrated as follows:

1. A novel BCP based epidemic mathematical model is designed for embedded tiny chip based mini-computer infiltration within another computer type vulnerability.
2. Disease free and endemic equilibria measures are used for theoretical analysis of the BCP epidemic model by derivation of basic reproduction number as well

as global and local stability conditions.

3. Strength of numerical solver based on Runge-Kutta methods is exploited for numerical analysis of BCP model by varying infectious contact rate, loss of immunity rate and efficacy of patching.
4. Results of numerical experimentations for variation of different parameters shows interesting results.

6.2 Model Formulation of BCP System

Mathematical formulation of BCP model is presented here, the entire BCP model is divided into three classes of computer nodes, i.e, bugged $B(t)$, compromised $I(t)$ and patched $P(t)$. Total population is represented as $N(t) = B(t) + C(t) + P(t)$. In rest of the chapter, the variables with respect to time t, i.e., $B(t), C(t), P(t)$ and $N(t)$ are denoted by B, C, P and N, respectively. Let A represents the arrival of new bugged computer nodes, δ represents the loss of immunity, β is the infectious contact rate of bugged nodes with compromised nodes, η represents the inefficiency of patching, γ is the rate at which compromised individuals become patched and d is the natural death rate. After the implant of tiny spy hardware during manufacturing or in transit, the targeted hardware becomes bugged. Bugged nodes have inbuilt holes that can be easily exploited by installing backdoors which can ultimately infect or compromise the whole infrastructure or network. The term $\frac{\beta B(t)C(t)}{N(t)}$ shows that bugged nodes interact with compromised nodes and the probability of becoming compromised also depends on infectious contact rate β. The efficacy of patching is shown in the expression $\frac{\delta\beta P(t)C(t)}{N(t)}$ which represents the interaction of patched nodes with compromised nodes and the probability of compromising the patched nodes depends on the value of δ and β. Due to the diversity of attacking pattern, patching efficiency δ gains pivotal role in system protection. Understanding of bug node behavior is crucial for manipulation of devastation and control strategy. Compromised nodes are more vulnerable because they offer full control of the system as compare to partial infection.

In this chapter, BCP model is exploited to illustrate the spread of infection in

the network through bugged nodes. The schematic workflow of proposed scheme in terms of process block structures and flow diagram of proposed BCP model is shown in figures 6.1 and 6.2 respectively. The governing system of differential equations describe the model dynamics, detail of the model equations are given below:

$$\begin{aligned}
\frac{dB}{dt} &= A - \frac{\beta B(t)C(t)}{N(t)} + \xi P(t) - dB(t), \\
\frac{dC}{dt} &= \frac{\beta B(t)C(t)}{N(t)} + \frac{\delta\beta P(t)C(t)}{N(t)} - \gamma C(t) - dC(t), \\
\frac{dP}{dt} &= \gamma C(t) - \frac{\delta\beta P(t)C(t)}{N(t)} - \xi P(t) - dP(t),
\end{aligned} \tag{6.1}$$

from set of equation (6.1) we have

$$\frac{dN}{dt} = A - dN. \tag{6.2}$$

The net rate of change of the population is given by $c = A - d$ and its values may be positive, zero or negative. The system of equations (6.1) can be reduced by incorporating the variable N and P as:

$$\begin{aligned}
\frac{dC}{dt} &= \frac{\beta(N - P - C)C}{N} - \frac{\delta\beta PC}{N} - \gamma C - dC, \\
\frac{dP}{dt} &= \gamma C - \frac{\delta\beta PC}{N} - \xi P - dP.
\end{aligned} \tag{6.3}$$

The equations in set (6.3), represent the reduced order model for further investigations.

6.3 Model Theoretical Analysis

In this section, analysis of BCP model for local and global stability are presented through basic reproduction number R_0 for both disease free and endemic equilibrium points.

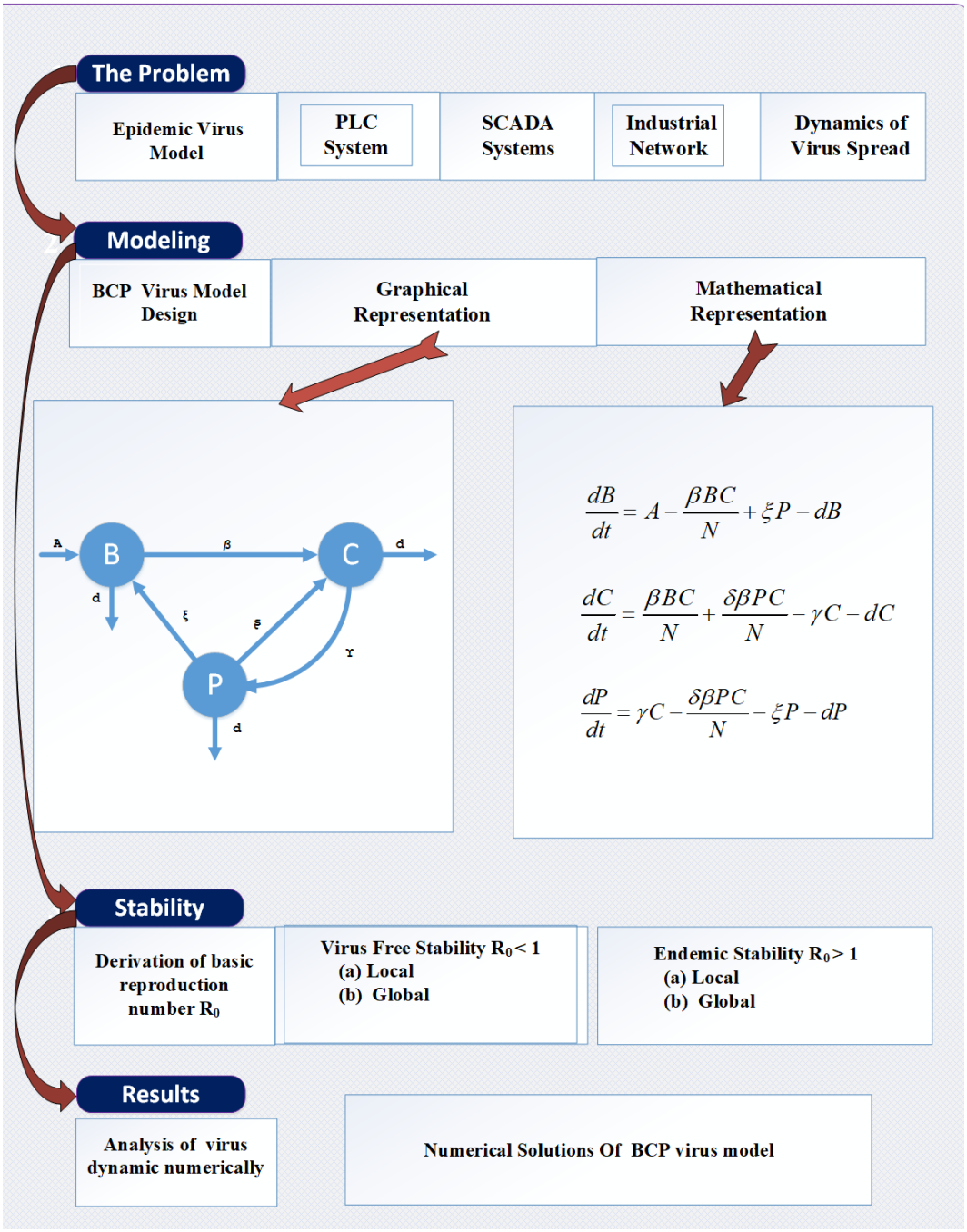


FIGURE 6.1: Graphical overview of schematic for the proposed BCP model

6.3.1 Basic Reproduction Number (R_0)

The basic reproduction number is defined as the average of new infection caused by an infected individual in its infectious period and usually represented by R_0. If $R_0 > 1$, then infection will spread rapidly in the system and if $R_0 < 1$ then infection will die down [181].

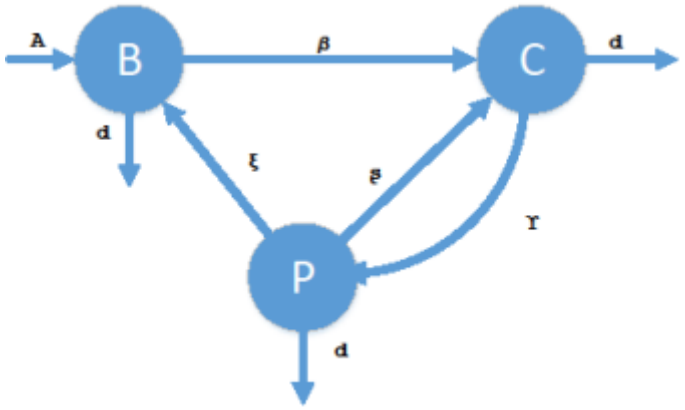


FIGURE 6.2: Schematic flow of proposed BCP model

Reduced version of the model (6.3) has been used for the derivation of R_0. The essential condition for an epidemic to occur, is based on increase in the number of infected nodes with an assumption that initially all populations are susceptible. In case of $\frac{dC}{dt} > 0$, we have

$$\frac{\beta BC}{N} - \frac{\delta\beta(N-B-C)C}{N} - \gamma C - dC > 0.$$

Assuming that all new nodes in the populations are initially susceptible, we may write the above expression as:

$$\begin{aligned} &\tfrac{\beta BC}{N} - \tfrac{\delta\beta(N-B-C)C}{N} - \gamma C - dC > 0, \\ &\tfrac{\beta B}{N} - \tfrac{\delta\beta(N-B-C)}{N} > \gamma + d. \end{aligned}$$

Simplifying above relation, we have

$$\begin{aligned} &\tfrac{\beta B}{N} + \tfrac{\delta\beta N}{N} - \tfrac{\delta\beta B}{N} > \gamma + d, \\ &\beta > \gamma + d, \end{aligned}$$

therefore,

$$\frac{\beta}{\gamma + d} > 1,$$

$$R_0 = \frac{\beta}{\gamma + d}. \tag{6.4}$$

Equation (6.4) represents the model derived basic reproduction number.

6.3.2 Equilibria Studies

The BCP model (6.3) has two equilibrium points; i.e., virus free and endemic equilibria points. In disease free environment, no infection spreads while in case of endemic equilibrium, infection spreads in the system.

In equilibria studies, we have

$$\frac{dC}{dt} = 0, \qquad \frac{dP}{dt} = 0.$$

So, virus free equilibrium point for system (6.3) is $K_0 = (C, P) = (0, 0)$ and endemic equilibrium point is $K^* = (C^*, P^*)$ for $R_0 > 1$.

The model (6.3) for endemic equilibrium analysis is written as:

$$\frac{\beta(N - P - C)C}{N} + \frac{\delta\beta PC}{N} - \gamma C - dC = 0, \tag{6.5}$$

$$\gamma C - \frac{\delta\beta PC}{N} - \xi P - dP = 0.$$

Solving equations (6.5) for endemic equilibrium point, we get the value of endemic point ($C*$, $P*$), detail is avaiable in appendix (**??**)

$$C^* = \frac{\sqrt{b^2 - 4ac} - b}{2a},$$

$$P^* = \frac{\frac{1}{R_0} + C^* - 1}{\delta - 1}. \tag{6.6}$$

where

$a = \delta\beta \qquad b = \delta\beta(\frac{1}{R_0} - 1) + \xi + d - \delta\gamma + \gamma \qquad c = (\frac{1}{R_0} - 1)(\xi + d).$

It is evident from equation (6.6) that the value of $C^* > 0$ is only possible, if the value of $R_0 > 1$.

6.3.3 Disease Free Equilibria

Theorem 5.1 Disease-free equilibrium (DFE) point K_0 is locally asymptotically stable for $R_0 < 1$.

Proof. The system is locally asymptotically stable at DFE point $K_0 = (C, P) = (0, 0)$. Consider the Jacobian matrix of function $f : R^2 \to R^2$ with components:

$$\frac{dC}{dt} = f_1(C, P) = \frac{\beta(N - P - C)C}{N} - \frac{\delta\beta PC}{N} - \gamma C - dC,$$

$$\frac{dP}{dt} = f_2(C, P) = \gamma C - \frac{\delta\beta PC}{N} - \xi P - dP.$$

The Jacobian matrix at disease free equilibrium point $K_0 = (C, P)$ is given below.

$$J(C, P) = \begin{pmatrix} \frac{\partial f_1}{\partial C} \frac{\partial f_1}{\partial P} \\ \frac{\partial f_2}{\partial C} \frac{\partial f_2}{\partial P} \end{pmatrix}.$$

Therefore, the Jacobian matrix at K_0, DFE point for reduced order model (6.3) is given as:

$$DFE(K_0) = \begin{pmatrix} \beta - \gamma - d & 0 \\ \gamma & -\xi - d \end{pmatrix}. \tag{6.7}$$

To find the Eigenvalues, the characteristic equation of (6.7) is

$$|\lambda I - DFE(K_0)| = \begin{vmatrix} \lambda - \beta + \gamma + d & 0 \\ -\gamma & \lambda + \xi + d \end{vmatrix} = 0,$$

which simplifies as:

$$\begin{aligned}
&(\lambda - \beta + \gamma + d)(\lambda + \xi + d) = 0, \\
&\lambda^2 + \lambda(\xi + d - \beta + \gamma + d) + (\xi\gamma + \gamma d + \xi d + d^2 - \beta\xi - \beta d) = 0, \\
&\lambda^2 + (\gamma + d)\lambda \left[\tfrac{\xi}{\gamma+d} + \tfrac{d}{\gamma+d} - \tfrac{\beta}{\gamma+d} + 1\right] + \gamma(\xi + d) + d(\xi + d) - \beta(\xi + d) = 0, \\
&\lambda^2 + (\gamma + d)\lambda \left[\tfrac{\xi}{\gamma+d} + \tfrac{d}{\gamma+d} - R_0 + 1\right] + (\xi + d)(\gamma + d - \beta) = 0,
\end{aligned}$$

further simplifying with R_0

$$\lambda^2 + (\gamma + d)\lambda \left[\frac{\xi}{\gamma + d} + \frac{d}{\gamma + d} + 1 - R_0\right] + (\xi + d)(\gamma + d)(1 - R_0) = 0.$$

All the coefficients in the above equation are positive for the value of $R_0 < 1$, which shows that all Eigenvalues are in left half plane, so the system is asymptotically stable for point K_0 when $R_0 < 1$, which proves the stability of the system.

Theorem 5.2 If $R_0 < 1$, then the point K_0 is globally asymptomatically stable, otherwise unstable.

Proof. Let us consider the following Lyapunov function.

$$L(B, C, P) = K(B + P + C). \tag{6.8}$$

Disease free equilibrium point for equation (6.1) is $(B, C, P) = (\frac{A}{d}, 0, 0)$. The function is always positive in R^3, $R^3 = (B,\ C,\ P)$ and $(B > 0,\ C > 0,\ P > 0)$. Taking the derivative of the Lyapunov function (6.8), we get

$$\dot{L}(B, C, P) = K(\dot{B} + \dot{C} + \dot{P}),$$

$$\begin{aligned}
\dot{L}(B, C, P) &= K[A - \tfrac{\beta BC}{N} + \xi P - dB + \tfrac{\beta BC}{N} + \tfrac{\delta \beta PC}{N} - \gamma C - dC \\
&\quad + \gamma C - \tfrac{\delta \beta PC}{N} - \xi P - dP], \\
\dot{L}(B, C, P) &= K[A - dB - dP - dC], \\
\dot{L}(B, C, P) &= -Kd[C + P].
\end{aligned}$$

For $R_0 < 1$, implies that $\dot{L}(t) \leq 0$ and K_0 is the only invariant set of the system (6.1) for $\dot{L}(t) = 0$. According to LaSalle Invariance Principle K_0 is globally asymptotically stable. This completes the theorem proof.

6.3.4 Endemic Stability

In this section endemic stability of the reduced order model at endemic equilibrium point $K^* = (C^*, P^*)$, for $R_0 > 1$ and $C^* \geq 0$ is investigated.

Theorem 5.3 Point K^* is locally asymptomatically stable for $R_0 > 1$.

Proof. Consider the function $f : R^2 \to R^2$ with components and Jacobian matrix for reduced order model (6.5) as:

$$\begin{aligned}
\frac{dC}{dt} &= f_1(C^*, P^*) = \frac{\beta(N - P^* - C^*)C^*}{N} - \frac{\delta \beta P^* C^*}{N} - \gamma C^* - dC^*, \\
\frac{dP}{dt} &= f_2(C^*, P^*) = \gamma C^* - \frac{\delta \beta P^* C^*}{N} - \xi P^* - dP^*.
\end{aligned}$$

Jacobian matrix at endemic equilibrium point $K^* = (C^*, P^*)$ is given below.

$$J(C^*, P^*) = \begin{bmatrix} \frac{\partial f_1}{\partial C^*} & \frac{\partial f_1}{\partial P^*} \\ \frac{\partial f_2}{\partial C^*} & \frac{\partial f_2}{\partial P^*} \end{bmatrix},$$

$$J(K^*) = \begin{pmatrix} \beta - (\gamma + d) - \frac{\beta(P^* + 2C^*)}{N} - \frac{\delta\beta P^*}{N} & -\frac{\beta C^*}{N} - \frac{\delta\beta C^*}{N} \\ \gamma - \frac{\delta\beta P^*}{N} & -\frac{\delta\beta C^*}{N} - \xi - d \end{pmatrix}. \tag{6.9}$$

Characteristic equation of (6.9) is

$$|\lambda I - J(K^*)| = \begin{vmatrix} \lambda - \beta + (\gamma + d) + \frac{\beta(P^*+2C^*)}{N} + \frac{\delta\beta P^*}{N} & \frac{\beta C^*}{N} + \frac{\delta\beta C^*}{N} \\ -\gamma + \frac{\delta\beta P^*}{N} & \lambda + \frac{\delta\beta C^*}{N} + \xi + d \end{vmatrix} = 0,$$

which simplifies as:

$$\lambda^2 + (b_{11} + b_{22})\lambda + (b_{11}b_{22} - b_{12}b_{21}) = 0, \tag{6.10}$$

where

$$\begin{aligned} b_{11} &= -\beta + (\gamma + d) + \tfrac{\beta(P^*+2C^*)}{N} + \tfrac{\delta\beta P^*}{N}, \\ b_{12} &= -\tfrac{\beta C^*}{N} - \tfrac{\delta\beta C^*}{N}, \qquad b_{21} = \gamma - \tfrac{\delta\beta P^*}{N}, \\ b_{22} &= \tfrac{\delta\beta C^*}{N} + \xi + d. \end{aligned}$$

To analyze the stability of system (6.3), we use the Hurwitz criteria as reported in [143, 144]. To overview the Hurwitz criteria, let's consider the general characteristic equation of the system.

$$b_0 s^n + b_1 s^{n-1} + b_2 s^{n-2} + b_3 s^{n-3} \cdots \; b_{n-1} s^1 + b_n = 0,$$

with n determinants in the nth order equation and the first two determinants, i.e., D_1 and D_2 of the said characteristic equation are as:

$$\begin{aligned} D_1 &= b_1, \\ D_2 &= \begin{vmatrix} b_1 & b_3 \\ b_0 & b_2 \end{vmatrix} = b_1 b_2 - b_3 b_0. \end{aligned}$$

Now equating the coefficients of general characteristics equation with equation (6.10), we have

$$b_0 = 1,$$
$$b_1 = b_{11} + b_{22},$$
$$b_2 = b_{11}b_{22} - b_{12}b_{21}.$$

Determinants (D_1 and D_2) of the characteristic equation (6.10) are expressed in Hurwitz process as:

$$D_1 = b_1 = b_{11} + b_{22},$$
$$D_1 = \left(-\beta + \gamma + d + \frac{\beta(P^*+2C^*)}{N} - \frac{\delta\beta P^*}{N}\frac{\delta\beta C^*}{N} + \xi + d\right),$$
$$D_1 = \beta\left[-1 + \frac{1}{R_0} + \frac{P^*}{N}(1-\delta) + \frac{C^*}{N}(2+\delta) + \frac{\xi+d}{\beta}\right].$$

Simplifying the above expression, we get

$$D_1 = \beta\left[-1 + \frac{1}{R_0} - \frac{\frac{1}{R_0}+C^*-1}{\delta-1}(\delta-1) + C^*(2+\delta) + \frac{\xi+d}{\beta}\right],$$
$$D_1 = \beta\left[-C^* + C^*(2+\delta) + \frac{\xi+d}{\beta}\right],$$
$$D_1 = \beta\left[C^*(1+\delta) + \frac{\xi+d}{\beta}\right],$$

where

$$C^* = \frac{\sqrt{b^2-4ac}-b}{2a}, P^* = \frac{\frac{1}{R_0}+C^*-1}{\delta-1},$$

thus

$D_1 > 0$.

Solving determinant D_2:

$$D_2 = b_1b_2 - b_3b_0,$$
$$D_2 = b_1b_2 = (b_{11}+b_{22})(b_{11}b_{22} - b_{12}b_{21}),$$
$$D_2 = D_1(b_{11}b_{22} - b_{12}b_{21}).$$

D_1 is positive, so we neglect it

$$D_2 = b_{11}b_{22} - b_{12}b_{21},$$
$$D_2 = \left(-\beta + (\gamma+d) + \frac{\beta(P^*+2C^*)}{N} - \frac{\delta\beta P^*}{N}\right)\left(\frac{\delta\beta C^*}{N} + \xi + d\right)$$
$$- \left(\frac{\beta C^*}{N} - \frac{\delta\beta C^*}{N}\right)\left(\gamma - \frac{\delta\beta P^*}{N}\right),$$

$$D_2 = -\frac{\gamma\beta C^*}{N} + \frac{\delta\beta^2 P^* C^*}{N^2} + \frac{\gamma\beta C^*}{N} + \frac{\delta^2\beta^2 P^* C^*}{N^2} + \frac{(\gamma+d)\gamma\beta C^*}{N} + (\gamma+d)(\xi+d) + \frac{\delta\beta^2 C^*(P^*+2C^*)}{N^2} + (\xi+d)\frac{\beta(P^*+2C^*)}{N} - \frac{\delta\beta^2 C^*}{N} - \beta(\xi+d) - \frac{\delta^2\beta^2 P^* C^*}{N^2} - \frac{\gamma\beta C^*}{N}(\xi+d).$$

Simplifying the above expression, we get

$$D_2 = -\frac{\gamma\beta C^*}{N} + \frac{\delta\beta^2 P^* C^*}{N^2} + \frac{d\delta\beta C^*}{N} + \frac{\delta\beta^2 P^* C^*}{N} + \frac{2\delta\beta^2 C^{*2}}{N} + (\xi+d)\frac{\beta 2C^*}{N} - \frac{\delta\beta^2 C^*}{N} - \beta(\xi+d),$$

$$D_2 = \gamma + d\left[\begin{array}{l} -\frac{\gamma C^* R_0}{N} + \frac{\delta\beta P^* C^* R_0}{N^2} + \frac{d\delta C^* R_0}{N} + \delta\beta P^* C^* R_0 + \frac{2\delta\beta C^{*2} R_0}{N} \\ +R_0(\xi+d)\frac{\beta 2C^*}{N} - \frac{\delta\beta R_0 C^*}{N} - R_0(\xi+d) \end{array}\right],$$

$$D_2 = \beta\left[\begin{array}{l} -\frac{\gamma C^*}{N} + \frac{\delta\beta P^* C^*}{N^2} + \frac{d\delta C^*}{N} + \frac{\delta\beta P^* C^*}{N} + \frac{2\delta\beta C^{*2}}{N} + (\xi+d)\frac{\beta 2C^*}{N} \\ -\frac{\delta\beta C^*}{N} - (\xi+d) \end{array}\right],$$

$$D_2 = \beta\left[-\frac{\gamma C^*}{N} + \frac{\delta\beta P^* C^*}{N^2} + \frac{d\delta C^*}{N} + \frac{\delta\beta P^* C^*}{N} + (2C^*-1)(\delta\beta C^* + \xi + d)\right],$$

$$D_2 = \beta\left[\frac{C^*(\delta\beta P^* - \gamma)}{N} + \frac{\delta\beta P^* C^*}{N^2} + \frac{d\delta C^*}{N} + (2C^*-1)(\delta\beta C^* + \xi + d)\right].$$

For $R_0 > 1$, compromised nodes increase and the value of D_2 becomes positive, therefore $D_2 > 0$. Thus all the values of D_1 and D_2 are positive, so all the Eigenvalues of the equation (6.10) are in the left half plane for $R_0 > 1$. Thus there exists an endemic equilibrium point K^* which is locally asymptomatically stable. This completes the proof.

6.4 Simulation and Results

Numerical simulations are performed to understand the behavior of the BCP model which may help us to devise controlling mechanisms and eradication strategies. System of equations (6.1) are used in the simulation of the designed BCP model. Numerical simulations for six different cases are studied with variations of parameters and initial thresholds as mentioned in table 6.1. Dynamics of the BCP model is plotted using the well-known Runge-Kutta (RK) method using WOLFRAM MATHEMATICA 12 on 64 bit windows 10 platform and result of the simulations are shown in figure 6.3.

In case 1, figure 6.3a shows that at start of vulnerability when a tiny chip is

implanted in the hardware, limited knowledge about particular hardware vulnerability is present and the exploitation of the hardware is also less. Hence, the number of Compromised nodes are lesser in number and same trend is also observed in Patched nodes (due to new vulnerability, patches are unavailable). In case 2, figure 6.3b slight increase in the infectious contact rate β from 1% to 1.45% causes increase in the number of Compromised nodes. The number of Compromised nodes are 15 in 42 months and in case 1, number of Compromised nodes are 2 in 42 months. In case 3, figure 6.3c all parameter values of case 1 are retained except the value of δ which represents the loss of immunity. The value of δ in case 1 is 34.8% but increasing the value of δ in case 3, causes increase in the number of Compromised nodes i.e., $t = 60.11,\ B = 13.92,\ C = 13.92,\ P = 3.85$. Case 4 figure 6.3d illustrates the behavior of the BCP model by changing the parameter ξ that represents the inefficiency of patching and γ that represent the rate at which Compromised nodes becomes patched. Reducing the value of ξ and γ reduces the number of Bugged nodes and increases the number of Compromised nodes. Decreasing the value of ξ from 12.6% to 0.5% decreases the number of Bugged nodes due to inefficient patching. Reducing the value of γ from 8.4% to 0.5% increases the number of Compromised nodes which highlights the fact that efficient patching controls the number of Bugged nodes. Increasing the value of γ and decreasing the value of ξ reduces the number of Compromised nodes and increases the number of Patched nodes as shown in figure 6.3f for case 6. Case 5 (figure 6.3e) analyzes the variation of parameter γ which is the rate at which Compromised nodes become patched. Increasing the values of γ from 0.5% to 27.4% reduces the number of Compromised nodes and increases the number of Patched nodes. This shows that the hardware bug is now known and effective patching of the bug is also available. Increasing the values of γ creates a slight oscillation after time $t = 38$ in case 6 as shown in figure 6.3f.

Phase portrait of six cases are also shown in figure 6.4 (a) to (f) which illustrates the complete behavior of the BCP model for cases 1-6 respectively. Results depict that limiting the infectious contact rate β will reduce the number of Compromised nodes. Limiting the number of Bugged nodes controls the spread of Compromised

TABLE 6.1: Parameters variation in the simulation of the BCP model.

Parameter	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
A	1.665	1.665	1.665	1.665	1.665	2
β	0.01	0.0145	0.01	0.0145	0.0424	0.0412
δ	0.348	0.348	0.716	0.348	0.348	0.005
γ	0.084	0.084	0.084	0.005	0.274	0.72
ξ	0.126	0.126	0.126	0.005	0.005	0.005
d	0.05	0.05	0.05	0.05	0.05	0.05

nodes which ultimately controls the spread of infection. Phase portrait of figure 6.4a shows that due to nonavailability of information regarding particular hardware implants, number of Bugged nodes increases. After 30 months time hardware exploitation started which increases the number of Compromised nodes. Patch development is also started after the availability of a knowledge about a particular hardware bug. In case 2 small increase in the infectious contact rate β as compared to case 1, increases the number of Compromised nodes as shown in figure 6.4b. In case 3 increasing the value of δ (loss of patching immunity) as compared to case 1, increases the number of Bugged nodes and later (after 40 months) also increases the number of Compromised nodes as shown in phase portrait figure 6.4c. Phase portrait in figure 6.4e is forming a loop which shows that both Compromised and Patched nodes curves extend parallel after the number of Bugged nodes reaches the limit of 20. Oscillatory behavior form a spiral shape in the phase portrait of case 6 after $t = 35$ as shown in figure 6.4f.

6.5 Chapter Summary

In this chapter, BCP model is designed to investigate the spread of malicious code through implanted tiny hardware in a legitimate system. Theoretical analysis of BCP mathematical model for disease free and endemic equilibria points are carried out based on basic reproduction number R_0. Global stability of the model is proved by using Lyapunov functions. It is observed that controlling the infectious contact rate β controls the number of Compromised nodes. Furthermore, controlling the number of Bugged nodes also controls the number of Compromised nodes.

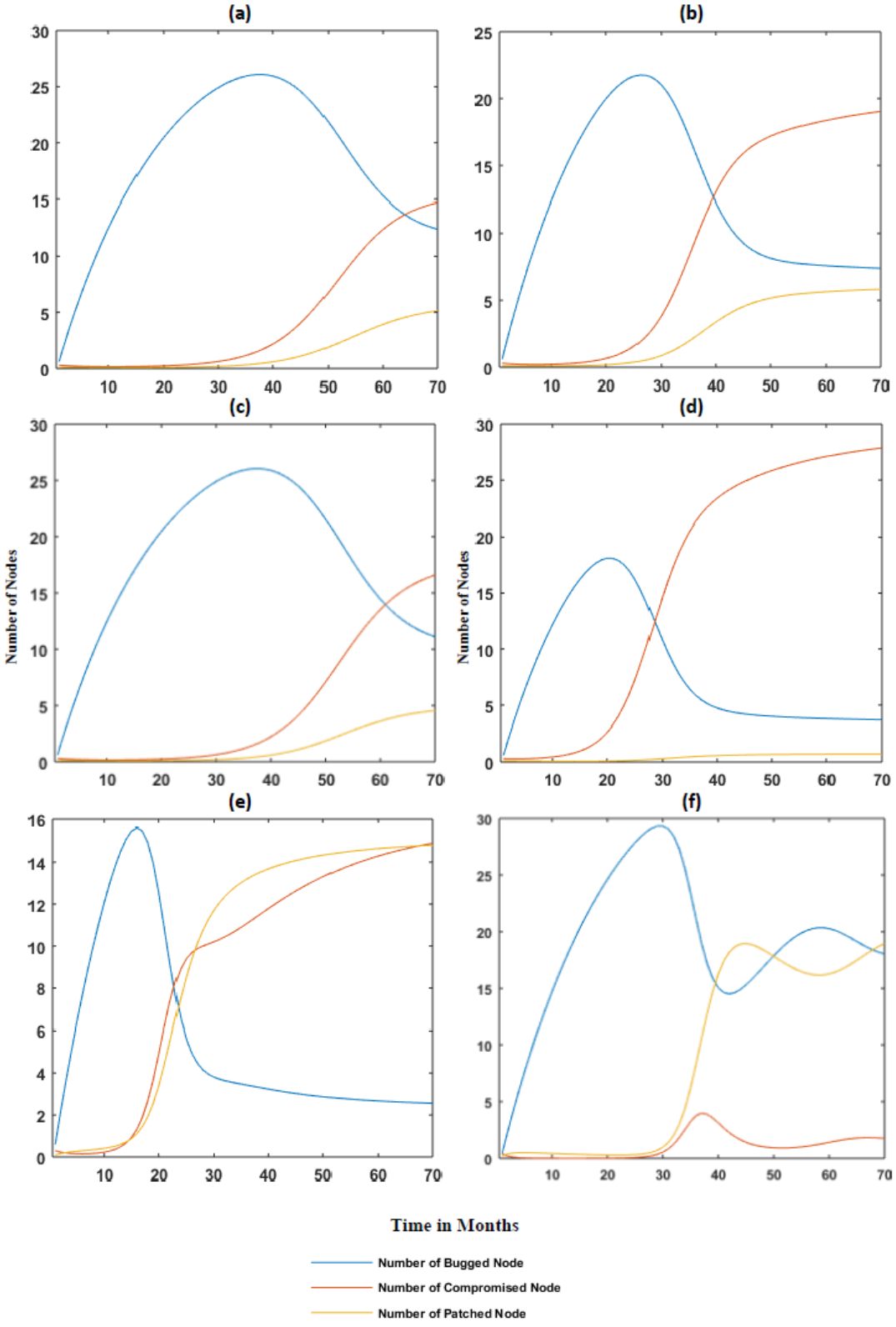


FIGURE 6.3: Solutions of BCP model using RK method for case1 to case6 (a-f) respectively.

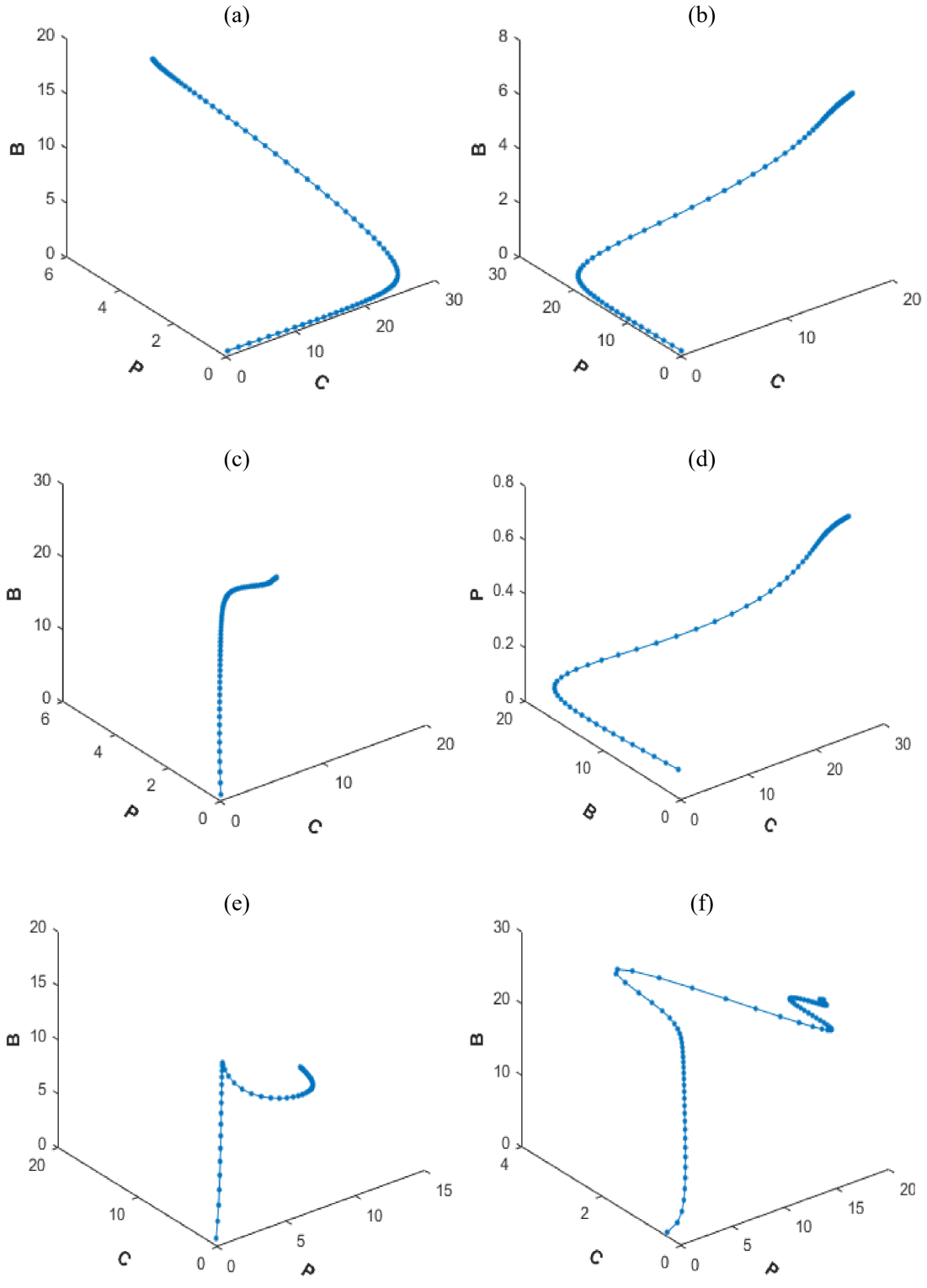


FIGURE 6.4: Phase portrait of bugged, compromised and patched nodes for cases 1 to 6 (a-f) respectively of BCP model.

Chapter 7

Fractional Analysis of Hardware Implants Vulnerabilities

7.1 Introduction

This chapter describes the fractional version of the epidemic model that portrays the exploitation of hardware through embedded tiny chip based implants within another computer.The firmware level bugs allow escalation of privileges and remote execution of code beneath the operating system for infiltration or completely intervention with the computer. Mathematical modeling of compromised hardware provide a platform for profound understanding of the problem and give us a path to devise flexible, stable and robust control strategies. The state of many biological systems at a given time depends on the states of the system at some previous times. Fractional derivatives are a natural method for solution of biological models arising in various disciplines. According to computer crime and security survey 74.3% of total financial loss related to the information incidents are caused due to hardware theft [98]. Trend of hardware implants in future may further increases. Defending against hardware implants is extremely difficult. Despite the lack of supporting evidence and refuting of reports of hardware implants, concerns in the security industry exists that such implants are used by state agencies and advance

state actors. NSA's digital catalogue reveals several sophisticated tools of hardware espionage, which was exposed in Der Spiegel, the German weekly newspaper, these tools were used to conduct espionage operation around the world [85] (Fig 7.1). Physical hardware implant attacks have become easier to conduct and little defense against these implants is available till date. Hardware implants are common due to simplified design and cost effectiveness [86]. Utilization of fractional

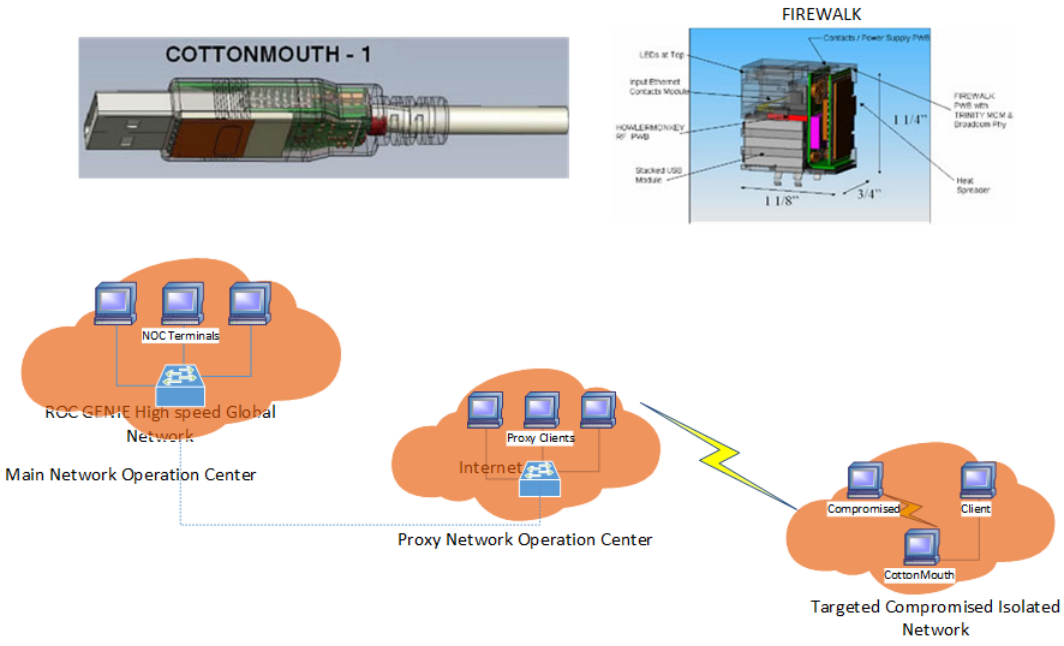


FIGURE 7.1: Digital tools of espionage through hardware implants

calculus concepts and underlying theories to solve complex mathematical models of computer epidemics gives us a more flexible approach as compared to integer order models [74, 175]. A fractional order mathematical model is used for modelling the compromised hardware for effective analysis of the spread of malicious code in the infrastructure of any organization. Theoretical analysis of the compromised nodes can be carried out by epidemiology modelling of virus propagation dynamics [131, 174]. Controlling strategy for tiny hardware implant is very difficult because they are often hidden and create several challenges to security of the infrastructure of the nations. To mimic the problem of hardware implants in computer systems, requirement for a mathematical model to simulate the problem was identified. Therefore, a detailed dynamical analysis of hardware implants and their devastation patterns with control mechanisms looks a promising domain to

be investigated by the research community. The rich heritage of fractional calculus is exploited to develop a fractional order bugged, compromised and patched model (FO-BCP) in order to depict the spread of malicious code in compromised hardware due to bugged nodes. In this study, a FO-BCP based mathematical model is presented to analyze the fast transients as well as super slow evolutions of the virus spread and exploitation of system resources in compromised hardware.

7.2 Fractional Calculus: Preliminaries

Fractional calculus is the generalization of classical calculus theory of derivatives and integrals of real or complex orders, i.e., non-integer order. The idea of half derivative was first introduced by Leibniz in a letter. The development of fractional calculus is the effort of several scientists such as Letnikov, Liouville, Euler and Riemann [177, 178]. Several definitions of fractional derivatives exist while broadly used definitions are given by Caputo (CP), Grunwald-Letnikov (GL) and Riemann-Liouville (RL) [71, 134].

The definition of GL fractional derivative is as under.

$$ {}_{a}^{GL}D_{t}^{\alpha} f(t) = \lim_{h \to 0} \frac{1}{h^{\alpha}} \sum_{j=0}^{[(t-a)/h]} (-1)^{j} \binom{\alpha}{j} f(t - jh), t > a, \alpha > 0. \tag{7.1} $$

For generalization, the derivative operator $D^{\alpha} f(x)$ in which α represents the order of fractional derivative is used.

The Caputo's definition of fractional derivatives can be written as

$$ {}_{a}^{CP}D_{t}^{\alpha} f(t) = \frac{1}{\Gamma(m-\alpha)} \int_{a}^{t} \frac{f^{m}(\tau)}{(t-\tau)^{\alpha-m+1}} d\tau, \tag{7.2} $$

for $(m-1 < \alpha < m)$ and where $\Gamma(\cdot)$ is the gamma function. The RL definition of fractional derivative is given as

$$ {}_{a}^{RL}D_{t}^{\alpha} f(t) = \frac{1}{\Gamma(n-\alpha)} \frac{d^{n}}{dt} \int_{a}^{t} \frac{f(x)}{(t-x)^{\alpha-n+1}} dx, \tag{7.3} $$

for $(n-1<\alpha<n)$, while α and t are the bounds of the operation for ${}_aD_t^{\alpha}$. In rest of the study, we will use the GL definition of fractional derivatives.

7.3 An Overview of Grunwald-Letnikov Numerical Solver of FDE

In this section, necessary description of numerical solver based on the most commonly used definition of Grunwald-Letnikov (GL) fractional derivative is given. The general form of fractional differential equation (FDE) with associated initial conditions is given mathematically as:

$$\begin{aligned} {}_a^{GL}D_t^{\alpha}y(t) &= f(y(t),t), \\ y^{(k)}(0) &= y_0^{(k)}, k=0,1,2,\dots n-1, \end{aligned} \tag{7.4}$$

where $(n-1<\alpha<n)$. Using equation (7.1) in (7.4) we have

$$\frac{1}{h^{\alpha}}\sum_{j=0}^{[(t-a)/h]}(-1)^j\binom{\alpha}{k}y(t-jh)\approx f(y(t),t),$$

simplifying above relation, we have

$$y(t)+\sum_{j=1}^{[(t-a)/h]}(-1)^j\binom{\alpha}{k}y(t-jh)\approx h^{-\alpha}f(y(t),t).$$

In case of discrete input grid in the interval $t\in[0,T]=[0,h,2h,...,Mh=T]$, where h is the step size parameter, so $[0,T]=[t_0=0,t_1,...,t_M=T]$. The grid points in the interval are represented as $t_m=mh$ for $m=0,1,2,...,M$. The above equation is written in discrete from as:

$$y(t_m)+\sum_{j=1}^{m}(-1)^j\binom{\alpha}{j}y(t_m-jh)=h^{-\alpha}f(y(t_m),t_m), m=0,1,2,...M.$$

In simple form,the above relation is written as:

$$y(t_m) + \sum_{j=1}^{m} c_j^{\alpha} y(t_m - jh) = h^{-\alpha} f(y(t_m), t_m), m = 0, 1, 2, ...M,$$

where $c_j^{(\alpha)}$ is defined as:

$$c_j^{\alpha} = (-1)^j \binom{\alpha}{j}, \ and \quad c_0^{\alpha} = 1,$$

$$c_j^{\alpha} = \left(1 - \frac{1+\alpha}{j}\right) c_{j-1}^{\alpha}, j = 0, 1, \ldots$$

Then the recursive relation for GL based numerical solver is given as:

$$y(t_m) = f(y(t_m), t_m)h^{-\alpha} - \sum_{j=1}^{k} c_j^{\alpha} y(t_{m-j}), m = 0, 1, 2, ...M. \tag{7.5}$$

Further necessary details of GL based numerical scheme can be seen in [70, 72].

7.4 Model Formulation of BCP Fractional Order System

Mathematical formulation of FO-BCP model is presented here. The schematic workflow of proposed scheme in terms of process block structures is shown in figure 7.2. The entire BCP model is divided into three classes of computer nodes, i.e, bugged $B(t)$, compromised $C(t)$ and patched $P(t)$. Total population is represented as $N(t) = B(t) + C(t) + P(t)$. In this chapter, the variable with respect to time t, i.e., $B(t), C(t), P(t)$ and $N(t)$ are denoted for simplicity by B, C, P and N, respectively. Let A represent the arrival of new bugged computer nodes, δ represent the loss of immunity, β the infectious contact rate of bugged nodes with compromised nodes, η the inefficiency of patching, γ the rate at which compromised individuals become patched and d the natural death rate. Installation of tiny implants during manufacturing or in transit make hardware bugged and vulnerable to exploit. Bugged nodes compromise the attached peripherals and

connected network. The expression $\frac{\beta B(t)C(t)}{N(t)}$ shows that when compromised nodes interact with bugged nodes and the probability of becoming compromised also depends on infectious contact rate β. The term $\frac{\delta\beta P(t)C(t)}{N(t)}$ represents the interaction of patched nodes with compromised nodes and the probability of compromising the patched nodes depends on the value of δ and β. Due to diversity of attack vectors, parameter δ, efficacy of patching attain pivotal role in system protection. Role of Bugged nodes increases due to behavior is crucial for manipulation of Understanding of bug node behavior is crucial for manipulation of devastation and control strategy. Compromised nodes are more vulnerable because they offer full control of the system as compare to partial infection. Bugged nodes have inbuilt holes that can be easily exploited to install backdoors and compromise the system, which ultimately infects or compromises the whole infrastructure or network. Understanding of bugged node behavior is crucial for manipulation of devastation and control strategy. Compromised nodes are more vulnerable because it offers full control of the system as compare to partial infection.

In this chapter FO-BCP model is exploited to illustrate the spread of the infection in networks through bugged nodes. The flow diagram of proposed BCP model is shown in figure 7.3 while the governing system of differential equations describing the model dynamics are given as:

$$\begin{aligned} D^{\alpha}B(t) &= A - \frac{\beta B(t)C(t)}{N(t)} + \xi P(t) - dB(t), \\ D^{\alpha}C(t) &= \frac{\beta B(t)C(t)}{N(t)} + \frac{\delta\beta P(t)C(t)}{N(t)} - \gamma C(t) - dC(t), \\ D^{\alpha}P(t) &= \gamma C(t) - \frac{\delta\beta P(t)C(t)}{N(t)} - \xi P(t) - dP(t), \end{aligned} \tag{7.6}$$

where $\alpha \in [0,1]$ is the order of the fractional derivative term $D^{\alpha} = {}_{a}^{GL}D_{t}^{\alpha}$. In case of $\alpha = 1$, the system of equations (7.6) is transformed to standard first order model of BCP infection propagation.

From set of equations (7.6) for the value of $\alpha = 1$ we have

$$\frac{dN}{dt} = A - dN. \tag{7.7}$$

The net rate of change of the population is given by $c = A - d$ and its values may be positive, zero or negative. The system of equations (7.6) can be reduced by

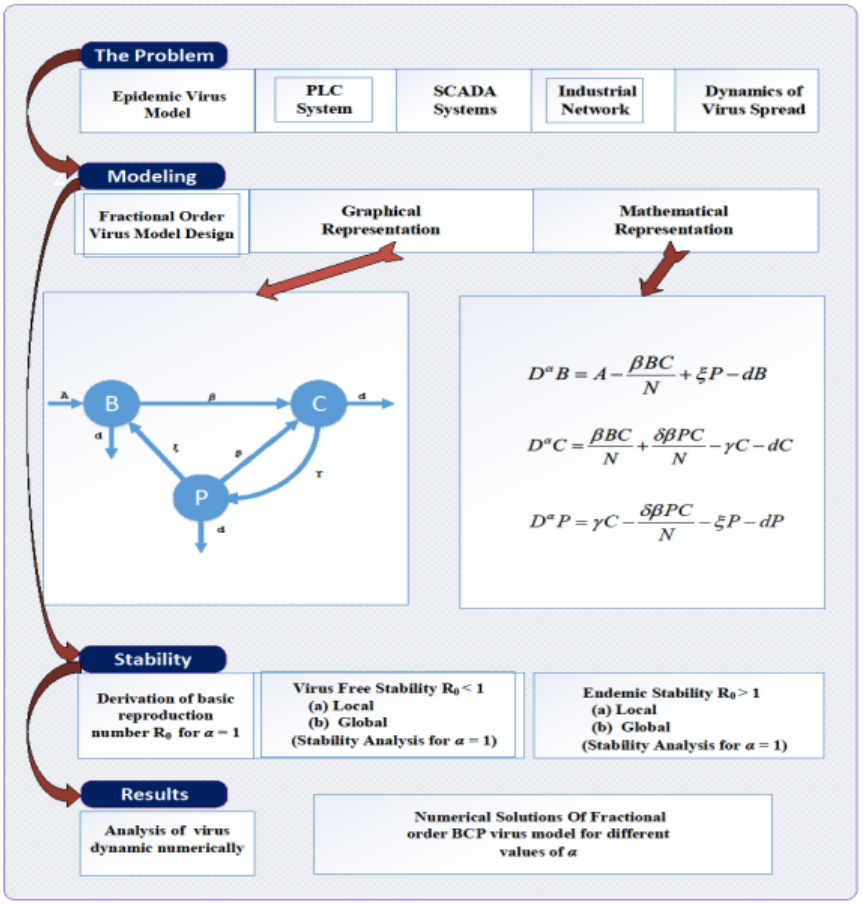


FIGURE 7.2: Graphical overview of schematic for the proposed FO-BCP model

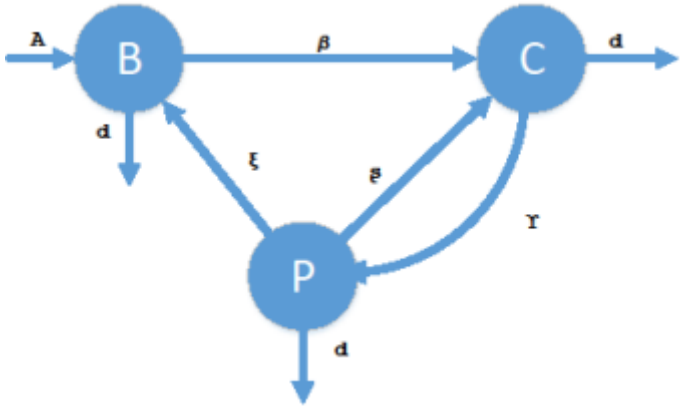


FIGURE 7.3: Schematic flow of proposed FO-BCP model

incorporating the variable N and P as:

$$D^\alpha C = \frac{\beta(N - P - C)C}{N} - \frac{\delta \beta PC}{N} - \gamma C - dC, \tag{7.8}$$

$$D^{\alpha}P = \gamma C - \frac{\delta\beta PC}{N} - \xi P - dP.$$

The equations in set (7.8), represent the reduced fractional order model for further investigation in this chapter.

7.5 Model Analysis

In this section, stability analysis of FO-BCP model for local and global stability is presented through basic reproduction number R_0 for both disease free and endemic equilibrium points.

7.5.1 Basic Reproduction Number (R_0)

The basic reproduction number is defined as the average number of new infection caused by an infected individual in its infectious period in a susceptible population and represented by R_0. If $R_0 > 1$, then infection will spread rapidly in the system and if $R_0 < 1$ then infection will die down [181].

Reduced version of the model (7.8) has been used for the derivation of R_0. Let us calculate R_0 for the integer order model, i.e., $\alpha = 1$. The essential condition for an epidemic to occur is the increase in the number of infected nodes with an initial susceptible population.

In case of $D^{\alpha}C > 0$, we have

$$\frac{\beta BC}{N} - \frac{\delta\beta(N-B-C)C}{N} - \gamma C - dC > 0.$$

Assuming that all new nodes in the population are susceptible at start, we may write the above expressions as:

$$\frac{\beta BC}{N} - \frac{\delta\beta(N-B-C)C}{N} - \gamma C - dC > 0,$$

$$\frac{\beta B}{N} - \frac{\delta\beta(N-B-C)}{N} > \gamma + d.$$

Simplifying above relations, we have

$$\frac{\beta B}{N} + \frac{\delta\beta N}{N} - \frac{\delta\beta B}{N} > \gamma + d,$$

$$\beta > \gamma + d.$$

Accordingly,

$$\frac{\beta}{\gamma + d} > 1,$$

and

$$R_0 = \frac{\beta}{\gamma + d}. \tag{7.9}$$

Equation (7.9) represents the FO-BCP model basic reproduction number.

7.5.2 Equilibria Studies

The FO-BCP model (7.8) has two equilibrium points; i.e., virus free and endemic equilibria points. In disease free environment, no infection spreads and in case of endemic equilibrium point, infection spreads in the system.
For equilibrium, we have

$$D^\alpha C = 0, \qquad D^\alpha P = 0.$$

Virus free equilibrium point for system (7.8) is $K_0 = (C, P) = (0, 0)$ and endemic equilibrium point is $K^* = (C^*, P^*)$ for $R_0 > 1$.
The model (7.8) for endemic equilibrium analysis is written as:

$$\frac{\beta(N - P - C)C}{N} + \frac{\delta\beta PC}{N} - \gamma C - dC = 0, \tag{7.10}$$

$$\gamma C - \frac{\delta\beta PC}{N} - \xi P - dP = 0.$$

Solving equations (7.10) for endemic equilibrium point, we get the value of endemic point (C^*, P^*) as:

$$C^* = \frac{\sqrt{b^2 - 4ac} - b}{2a},$$

$$P^* = \frac{\frac{1}{R_0} + C^* - 1}{\delta - 1}, \tag{7.11}$$

where

$a = \delta\beta, \quad b = \delta\beta(\frac{1}{R_0} - 1) + \xi + d - \delta\gamma + \gamma, \quad c = (\frac{1}{R_0} - 1)(\xi + d).$

It is evident from equation (7.11) that the value of $C^* > 0$ is possible only for $R_0 > 1$.

7.5.3 Disease Free Equilibrium

Theorem 5.1 Disease-free equilibrium (DFE) point K_0 is locally asymptotically stable for $R_0 < 1$.

Proof. The system is locally asymptotically stable at DFE point $K_0 = (C, P) = (0, 0)$. Consider the Jacobian matrix of function $f : R^2 \to R^2$ with components:

$$D^\alpha C = f_1(C, P) = \frac{\beta(N - P - C)C}{N} - \frac{\delta\beta PC}{N} - \gamma C - dC,$$

$$D^\alpha P = f_2(C, P) = \gamma C - \frac{\delta\beta PC}{N} - \xi P - dP.$$

The disease free equilibrium point $K_0 = (C, P)$ and the Jacobian matrix at the disease free point is given below for the value of $\alpha = 1$.

$$J(C, P) = \begin{pmatrix} \frac{\partial f_1}{\partial C} & \frac{\partial f_1}{\partial P} \\ \frac{\partial f_2}{\partial C} & \frac{\partial f_2}{\partial P} \end{pmatrix}.$$

Therefore, the Jacobian matrix at K_0, DFE point for integer order model (6.10) is given as:

$$DFE(K_0) = \begin{pmatrix} \beta - \gamma - d & 0 \\ \gamma & -\xi - d \end{pmatrix}. \tag{7.12}$$

To find the Eigenvalues, the characteristic equation of (7.12) is

$$|\lambda I - DFE(K_0)| = \begin{vmatrix} \lambda - \beta + \gamma + d & 0 \\ -\gamma & \lambda + \xi + d \end{vmatrix} = 0,$$

which can be written as:

$$(\lambda-\beta+\gamma+d)(\lambda+\xi+d)=0,$$
$$\lambda^2+\lambda(\xi+d-\beta+\gamma+d)+(\xi\gamma+\gamma d+\xi d+d^2-\beta\xi-\beta d)=0,$$
$$\lambda^2+(\gamma+d)\lambda\left[\tfrac{\xi}{\gamma+d}+\tfrac{d}{\gamma+d}-\tfrac{\beta}{\gamma+d}+1\right]+\gamma(\xi+d)+d(\xi+d)-\beta(\xi+d)=0,$$
$$\lambda^2+(\gamma+d)\lambda\left[\tfrac{\xi}{\gamma+d}+\tfrac{d}{\gamma+d}-R_0+1\right]+(\xi+d)(\gamma+d-\beta)=0,$$
$$\lambda^2+(\gamma+d)\lambda\left[\tfrac{\xi}{\gamma+d}+\tfrac{d}{\gamma+d}+1-R_0\right]+(\xi+d)(\gamma+d)(1-R_0)=0.$$

The above expression shows that all Eigenvalues are in left half plane for $R_0<1$, so the system is asymptotically stable for point K_0 when $R_0<1$. This proves the stability of system for the value of $\alpha=1$ and system will also remain stable for $\alpha<1$ as reported in [182].

Theorem 5.2 If $R_0<1$, then the point K_0 is globally asymptotically stable, otherwise unstable.

Proof. Let us consider the following Lyapunov function.

$$L(B,C,P)=K(B+P+C). \tag{7.13}$$

Disease free equilibrium point for equation (7.6) is $(B,C,P)=(\frac{A}{d},0,0)$. The function is always positive in R^3, for $R^3=(B,\,C,\,P)$ and $(B>0,\,C>0,\,P>0)$. Taking the derivative of the Lyapunov function (7.13) for $\alpha=1$, we get

$$D^\alpha L\,(B,C,P)=K(D^\alpha B+D^\alpha C+D^\alpha P),$$

$$\begin{aligned}D^\alpha L(B,C,P)&=K[A-\tfrac{\beta BC}{N}+\xi P-dB+\tfrac{\beta BC}{N}+\tfrac{\delta\beta PC}{N}-\gamma C-dC\\&\quad+\gamma C-\tfrac{\delta\beta PC}{N}-\xi P-dP],\\D^\alpha L(B,C,P)&=K[A-dB-dP-dC],\\D^\alpha L(B,C,P)&=-Kd[C+P].\end{aligned}$$

$D^\alpha L\le 0$ for $R_0<1$, implies that K_0 is the only invariant set of the system (7.12) for $D^\alpha L=0$. According to LaSalle Invariance Principle K_0 is globally asymptotically stable. This completes the proof. Additionally, if system is stable for $\alpha=1$, it will be stable for $\alpha<1$ as reported in [63].

7.5.4 Endemic Stability

To investigate the endemic equilibrium at point $K^* = (C^*, P^*)$, for $R_0 > 1$ and $C^* \geq 0$, we have to find the stability for $R_0 > 1$.

Theorem 5.3 Point K^* is locally asymptomatically stable for $R_0 > 1$.

Proof. Consider the function $f : R^2 \to R^2$ with components and Jacobian matrix for integer order model (7.10) as:

$$D^\alpha C = f_1(C^*, P^*) = \frac{\beta(N-P^*-C^*)C^*}{N} - \frac{\delta\beta P^* C^*}{N} - \gamma C^* - dC^*,$$
$$D^\alpha P = f_2(C^*, P^*) = \gamma C^* - \frac{\delta\beta P^* C^*}{N} - \xi P^* - dP^*.$$

The endemic equilibrium point $K^* = (C^*, P^*)$ and the Jacobian matrix at the endemic point is given below for $\alpha = 1$.

$$J(C^*, P^*) = \begin{bmatrix} \frac{\partial f_1}{\partial C^*} & \frac{\partial f_1}{\partial P^*} \\ \frac{\partial f_2}{\partial C^*} & \frac{\partial f_2}{\partial P^*} \end{bmatrix}.$$

$$J(K^*) = \begin{pmatrix} \beta - (\gamma + d) - \frac{\beta(P^*+2C^*)}{N} - \frac{\delta\beta P^*}{N} & -\frac{\beta C^*}{N} - \frac{\delta\beta C^*}{N} \\ \gamma - \frac{\delta\beta P^*}{N} & -\frac{\delta\beta C^*}{N} - \xi - d \end{pmatrix}. \tag{7.14}$$

Characteristic equation of (7.14) is

$$|\lambda I - J(K^*)| = \begin{vmatrix} \lambda - \beta + (\gamma + d) + \frac{\beta(P^*+2C^*)}{N} + \frac{\delta\beta P^*}{N} & \frac{\beta C^*}{N} + \frac{\delta\beta C^*}{N} \\ -\gamma + \frac{\delta\beta P^*}{N} & \lambda + \frac{\delta\beta C^*}{N} + \xi + d \end{vmatrix} = 0,$$

which simplifies as:

$$\lambda^2 + (b_{11} + b_{22})\lambda + (b_{11}b_{22} - b_{12}b_{21}) = 0, \tag{7.15}$$

where

$$b_{11} = -\beta + (\gamma + d) + \frac{\beta(P^*+2C^*)}{N} - \frac{\delta\beta P^*}{N},$$
$$b_{12} = \frac{\beta C^*}{N} + \frac{\delta\beta C^*}{N}, \quad b_{21} = \gamma - \frac{\delta\beta P^*}{N}, b_{22} = \frac{\delta\beta C^*}{N} + \xi + d_1.$$

To analyze the stability of system (7.8), we use Hurwitz criteria as reported in [143, 144].

For application of the Hurwitz criteria, let us consider the general characteristic

equation of a system:

$$b_0 s^n + b_1 s^{n-1} + b_2 s^{n-2} + b_3 s^{n-3} \cdots \; b_{n-1} s^1 + b_n = 0,$$

with n determinants in $n^t h$ order equation and the first two determinants, i.e., D_1 and D_2, of the said characteristic equation are as:

$$\begin{aligned} D_1 &= b_1, \\ D_2 &= \begin{vmatrix} b_1 & b_3 \\ b_0 & b_2 \end{vmatrix} = b_1 b_2 - b_3 b_0. \end{aligned}$$

Now equating the coefficient of general characteristics equation with (7.15), we have

$$\begin{aligned} b_0 &= 1, \\ b_1 &= b_{11} + b_{22}, \\ b_2 &= b_{11} b_{22} - b_{12} b_{21}, \end{aligned}$$

Determinants (D_1 and D_2) of the characteristic equation (7.15) are expressed using Hurwitz process as:

$$\begin{aligned} D_1 &= b_1 = b_{11} + b_{22}, \\ D_1 &= \left(-\beta + \gamma + d + \tfrac{\beta(P^* + 2C^*)}{N} - \tfrac{\delta\beta P^*}{N} \tfrac{\delta\beta C^*}{N} + \xi + d \right), \\ D_1 &= \beta \left[-1 + \tfrac{1}{R_0} + \tfrac{P^*}{N}(1 - \delta) + \tfrac{C^*}{N}(2 + \delta) + \tfrac{\xi + d}{\beta} \right], \end{aligned}$$

simplifying the above expression, we get

$$\begin{aligned} D_1 &= \beta \left[-1 + \tfrac{1}{R_0} - \tfrac{\frac{1}{R_0} + C^* - 1}{\delta - 1}(\delta - 1) + C^*(2 + \delta) + \tfrac{\xi + d}{\beta} \right], \\ D_1 &= \beta \left[-C^* + C^*(2 + \delta) + \tfrac{\xi + d}{\beta} \right], \\ D_1 &= \beta \left[C^*(1 + \delta) + \tfrac{\xi + d}{\beta} \right], \end{aligned}$$

where

$$C^* = \frac{\sqrt{b^2 - 4ac} - b}{2a}, P^* = \frac{\frac{1}{R_0} + C^* - 1}{\delta - 1},$$

and thus

$D_1 > 0$.

$$D_2 = b_1 b_2 - b_3 b_0,$$

$$D_2 = b_1 b_2 = (b_{11} + b_{22})(b_{11} b_{22} - b_{12} b_{21}),$$

$$D_2 = D_1 (b_{11} b_{22} - b_{12} b_{21}).$$

D_1 is positive,

$$D_2 = b_{11} b_{22} - b_{12} b_{21},$$

$$D_2 = \left(-\beta + (\gamma + d) + \tfrac{\beta(P^* + 2C^*)}{N} - \tfrac{\delta \beta P^*}{N}\right)\left(\tfrac{\delta \beta C^*}{N} + \xi + d\right) - \left(\tfrac{\beta C^*}{N} - \tfrac{\delta \beta C^*}{N}\right)\left(\gamma - \tfrac{\delta \beta P^*}{N}\right),$$

$$D_2 = -\tfrac{\gamma \beta C^*}{N} + \tfrac{\delta \beta^2 P^* C^*}{N^2} + \tfrac{\gamma \beta C^*}{N} + \tfrac{\delta^2 \beta^2 P^* C^*}{N^2} + \tfrac{(\gamma + d)\gamma \beta C^*}{N} + (\gamma + d)(\xi + d) + \tfrac{\delta \beta^2 C^* (P^* + 2C^*)}{N^2} + (\xi + d)\tfrac{\beta(P^* + 2C^*)}{N} - \tfrac{\delta \beta^2 C^*}{N} - \beta(\xi + d) - \tfrac{\delta^2 \beta^2 P^* C^*}{N^2} - \tfrac{\gamma \beta C^*}{N}(\xi + d).$$

Simplifying the above expression, we get

$$D_2 = -\tfrac{\gamma \beta C^*}{N} + \tfrac{\delta \beta^2 P^* C^*}{N^2} + \tfrac{d \delta \beta C^*}{N} + \tfrac{\delta \beta^2 P^* C^*}{N} + \tfrac{2\delta \beta^2 C^{*2}}{N} + (\xi + d)\tfrac{\beta 2 C^*}{N} - \tfrac{\delta \beta^2 C^*}{N} - \beta(\xi + d),$$

$$D_2 = \gamma + d \left[\begin{array}{l} -\tfrac{\gamma C^* R_0}{N} + \tfrac{\delta \beta P^* C^* R_0}{N^2} + \tfrac{d \delta C^* R_0}{N} + \delta \beta P^* C^* R_0 + \tfrac{2\delta \beta C^{*2} R_0}{N} \\ + R_0(\xi + d)\tfrac{\beta 2 C^*}{N} - \tfrac{\delta \beta R_0 C^*}{N} - R_0(\xi + d) \end{array} \right],$$

$$D_2 = \beta \left[\begin{array}{l} -\tfrac{\gamma C^*}{N} + \tfrac{\delta \beta P^* C^*}{N^2} + \tfrac{d \delta C^*}{N} + \tfrac{\delta \beta P^* C^*}{N} + \tfrac{2\delta \beta C^{*2}}{N} + (\xi + d)\tfrac{\beta 2 C^*}{N} \\ -\tfrac{\delta \beta C^*}{N} - (\xi + d) \end{array} \right],$$

$$D_2 = \beta \left[-\tfrac{\gamma C^*}{N} + \tfrac{\delta \beta P^* C^*}{N^2} + \tfrac{d \delta C^*}{N} + \tfrac{\delta \beta P^* C^*}{N} + (2C^* - 1)(\delta \beta C^* + \xi + d) \right],$$

$$D_2 = \beta \left[\tfrac{C^*(\delta \beta P^* - \gamma)}{N} + \tfrac{\delta \beta P^* C^*}{N^2} + \tfrac{d \delta C^*}{N} + (2C^* - 1)(\delta \beta C^* + \xi + d) \right].$$

For $R_0 > 1$, compromised nodes increases and the value of D_2 becomes positive, therefore $D_2 > 0$. Since D_1 and D_2 are positive, so all the Eigenvalues of the equation (7.15) are in the left half plane for $R_0 > 1$, so there exists an endemic equilibrium point K^* which is locally asymptotically stable. This completes the proof.

7.6 Simulation and Results

In this section, numerical simulations are performed for FO-BCP model to understand the propagation dynamics of bugged hardware and controlling strategy for the spread of malicious code in compromised nodes. Numerical simulations are made for the designed FO-BCP model given in equation (7.6) using scientific computer programming language MATLAB R2015b 64bit. Error diagrams of comparison of methods are shown in error plots:

$$\begin{aligned} D^{\alpha}B(t) &= f\left[B(t), C(t), P(t), t\right], \\ D^{\alpha}C(t) &= f\left[B(t), C(t), P(t), t\right], \\ D^{\alpha}P(t) &= f\left[B(t), C(t), P(t), t\right], \\ B(0) = B_0,\ C(0) &= C_0,\ P(0) = P_0. \end{aligned}$$

The recursive relation of GL based numerical solver is developed using the procedure given in section (7.2), to get

$$\begin{aligned} B(t_m) &= \left(A - \tfrac{\beta B(t_m)C(t_m)}{N} + \xi P(t_m) - dB(t_m)\right) h^{-\alpha} - \sum_{j=1}^{k} c_j^r B(t_{m-j}), \\ C(t_m) &= \left(\tfrac{\beta BC}{N} + \tfrac{\delta\beta PC}{N} - \gamma C - dC\right) h^{-\alpha} - \sum_{j=1}^{k} c_j^r C(t_{m-j}), \\ P(t_m) &= \left(\gamma C - \tfrac{\delta\beta PC}{N} - \xi P - dP\right) h^{-\alpha} - \sum_{j=1}^{k} c_j^r P(t_{m-j}). \end{aligned}$$

Numerical solutions for the designed FO-BCP model are calculated for six cases by varying the parameters as mentioned in Table 7.1. The dynamic behavior of the FO-BCP system with different fractional orders (FO) is studied using the GL based numerical solver. Results of GL method are compared with the well known Runge-Kutta (RK) method for integer order scenarios to validate the accuracy of the GL results for BCP model for $\alpha = 1$. The results of all six cases of the model given in equation (7.6) are calculated using GL method with step size $h = 0.001$ and $t \in [0,\ 70]$ (time t taken in months). Simulation results are plotted in figures 7.4 and 7.5 for cases 1-3 and 4-6 of the model in terms of Bugged B, Compromised C and Patched P nodes against time. Numerical solutions for $\alpha = 1$ are calculated using RK method for each case and result are provided in figures 7.4 and 7.5.

TABLE 7.1: Parameters variation in the simulation of the FO-BCP model.

Parameter	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
A	1.665	1.665	1.665	1.665	1.665	2
β	0.01	0.0145	0.01	0.0145	0.0424	0.0412
δ	0.348	0.348	0.716	0.348	0.348	0.005
γ	0.084	0.084	0.084	0.005	0.274	0.72
ξ	0.126	0.126	0.126	0.005	0.005	0.005
d	0.05	0.05	0.05	0.05	0.05	0.05

The results of both techniques are overlapping consistently for $\alpha = 1$. In order to assess the precision of GL solutions, error analysis based on absolute difference of RK versus GL for $\alpha = 1$ is performed and results of absolute deviations are also presented in figures 7.4 and 7.5 for each case using semi-logarithmic scale. Error plots in figures 7.4 and 7.5 show good matching of GL based solver with an accuracy of up to four decimal places which exhibits the working accuracy of the proposed methodology.

Fractional dynamics of the model are difficult to analyze using RK and other analytical solvers, therefore GL based solver is exploited to study the fractional dynamic of the FO-BCP model. We use GL based numerical solvers for detail experimentation in order to analyze the behavior of FO-BCP model for variation of fractional order α in the system (7.6). The fractional analysis give us an opportunity to observe fast transients and super slow changes in the model dynamic. The effects of these changes may highlight certain hidden important facts. The solution of all six cases are determined for FO-BCP model by using GL based solver for different values of fractional orders α, i.e., $\alpha = [0.5, 0.75, 0.8, 0.85, 0.9, 0.95, 1]$, for input interval $t \in [0, 70]$ with step size $h = 0.001$. Results of the FO-BCP model in term of Bugged B, Compromised C and Patched P nodes are plotted in figures 7.6 and 7.7 for cases 1-3 and 4-6, respectively. The dynamics of FO-BCP model shows that fractional order α is a controlling parameter of the model beside other tunable quantities of the system (7.6). In case 1, figures 7.4 and 7.5 show that at start of the vulnerability, the leakage of data through the implanted hardware is covert and also exploitation of the hardware from hackers is limited. The number of Compromised nodes (figure 7.4e) are small in number and same trend is also observed in Patched nodes (due to new vulnerability, patches are unavailable). For time $t = 60$, $\alpha = [0.5, 0.75, 0.8, 0.85, 0.9, 0.95,$

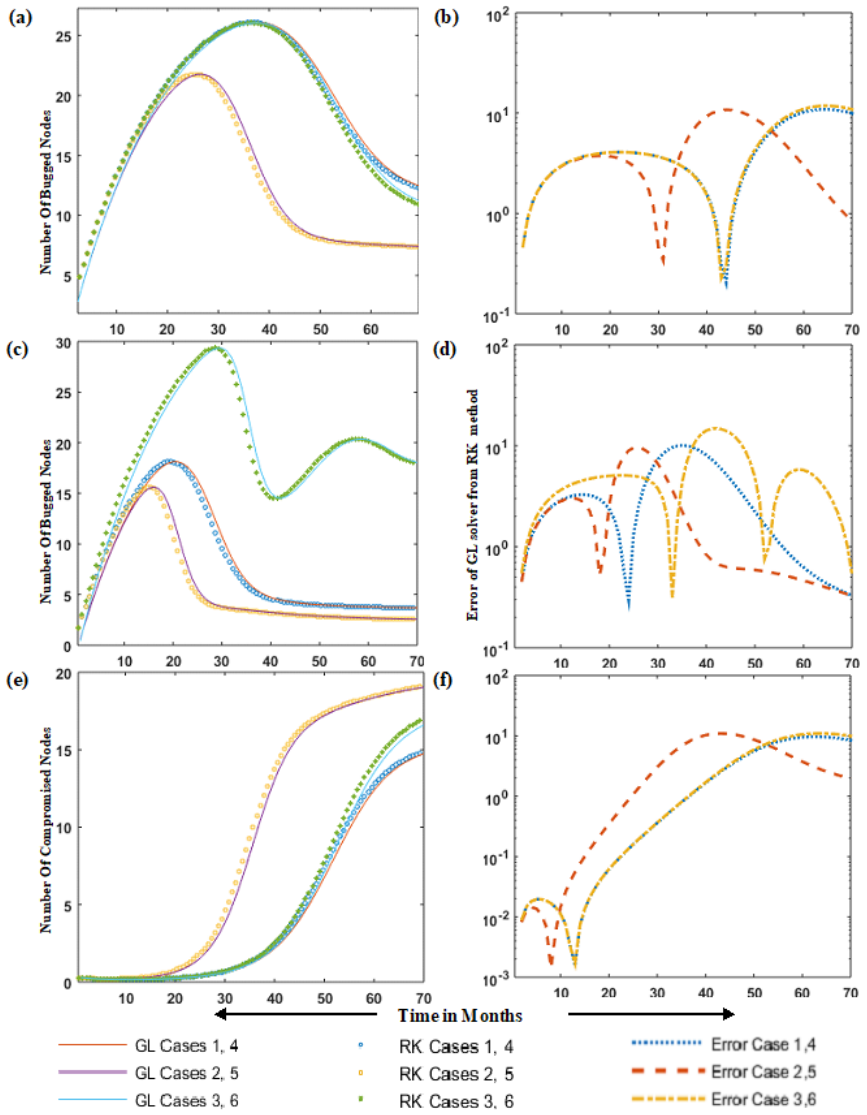


FIGURE 7.4: Comparison of solutions for GL solver with RK method in case of Bugged B hosts; (a) and (b) for cases 1 to 3, (c) and (d) for cases 4 to 6 and (e) to (f) for Compromised C nodes for case 1 to 3.

1], the number of Bugged nodes are 10.71, 20.96, 23.23, 25.23, 25.9, 22.02 and 14.83 respectively (Figure 7.6a). Changing the value of α in FO models describes a comprehensive range of scenarios which Bugged nodes can have in different network environments. Slight increase in the infectious contact rate β from 1% to 1.45% causes increase in the number of Compromised nodes as shown in figure 7.4e for case 2. In case 2 number of Compromised nodes are 15 in 42 months and in case 1 number of Compromised nodes are 2 in 42 months. However, in case 2 for $\alpha = 0.9$ the value of Compromised nodes are 2 in 42 months (figure 7.6e). In case 3, all parameter values of case 1 are retained except the value of

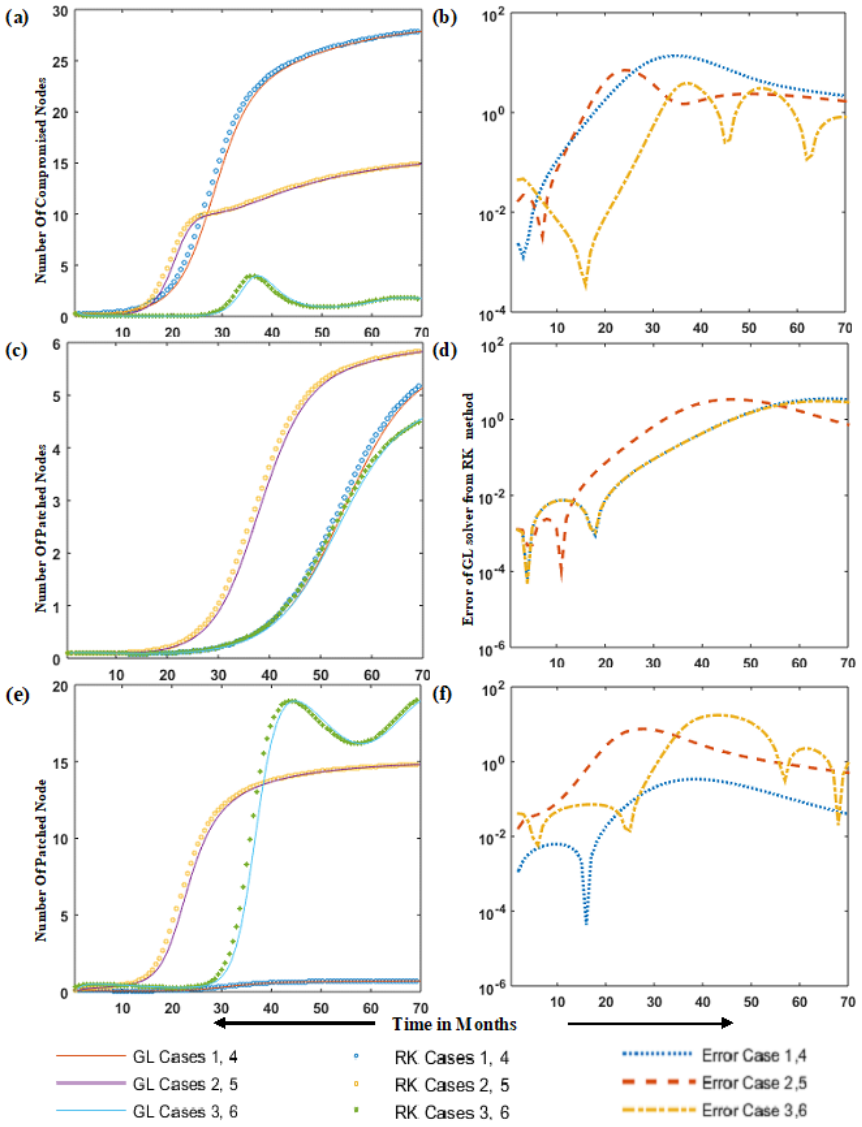


FIGURE 7.5: Comparison of solutions for GL solver with RK method in case of compromised hosts; (a) and (b) for cases 4 to 6, (c) and (d) for cases 1 to 3 for patched P hosts while (e) and (f) for cases 4 to 6.

δ which represents the loss of immunity. The value of δ in case 1 is 34.8% and increasing the value of δ in case 3, causes increase in the number of Compromised nodes (figure 7.4e) i.e., $t = 60.11$, $B = 13.92$, $C = 13.92$, $P = 3.85$. Case 4 figures 7.4c and 7.5c illustrates the behavior of the FO-BCP model by changing the parameter ξ that represents the inefficiency of patching and γ that represents the rate at which Compromised nodes becomes patched. Different aspects of attacking vectors (known vulnerability, insider attack or social engineering etc) on Compromised nodes can be described by varying the value of α as shown in figure 7.7b. Fractional order models can highlight minute details by tuning the value of

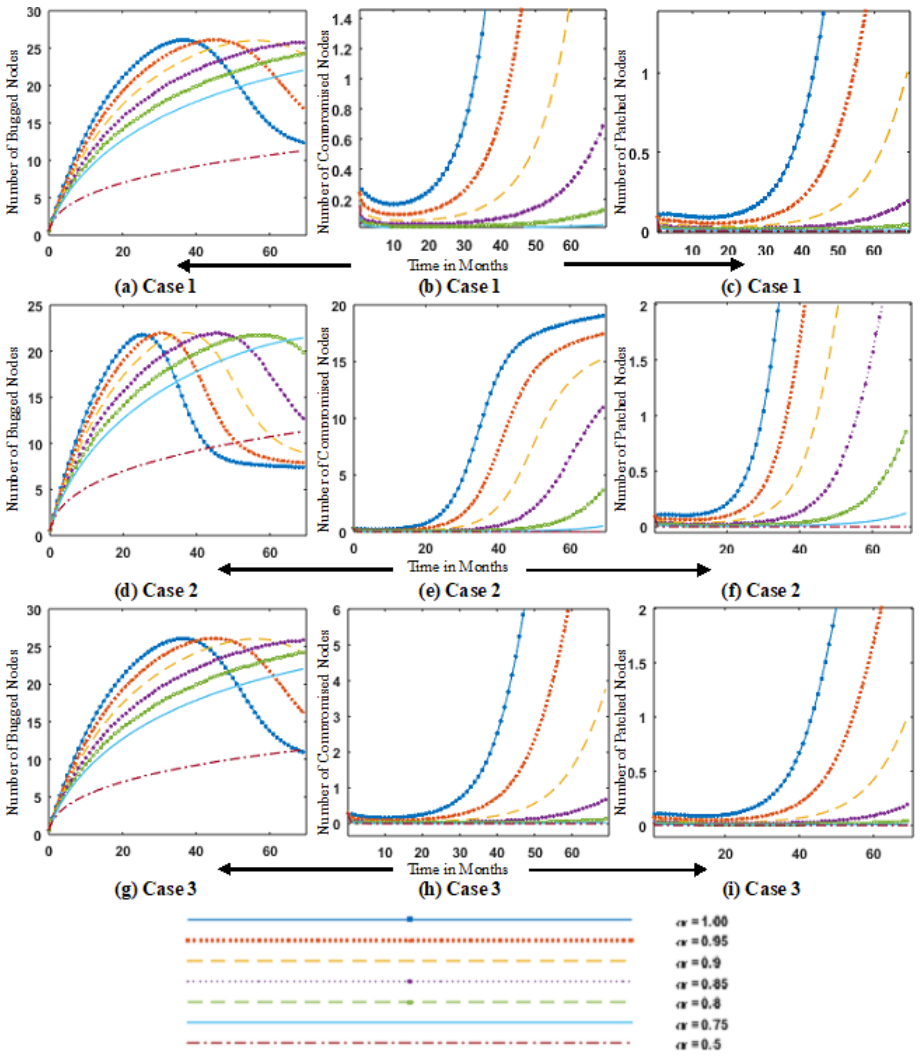


FIGURE 7.6: Dynamics of the bugged B, compromised C and patched P computers for cases 1 to 3 of FO-BCP model for 70-month time t by taking different fractional orders.

α as shown in figure 7.7. Reducing the value of ξ and γ reduces the number of Bugged nodes and increases the number of Compromised nodes respectively.

In figures 7.8a - 7.8i, the dynamics of FO-BCP model are analyzed by plotting the model simulations. Figure 7.8a shows that the number of Compromised nodes at $t = 0$ is approximately zero and does not start increasing until Bugged nodes reach at a certain threshold level. Change in the value of parameter β for cases 1 and 2 are shown in figure 7.8d. The sub-figure 7.8h for case 6 highlight the fact that Compromised nodes are only present when a certain number of Bugged nodes are available in the network.

Additional observations of fractional order system shows that change of α, will not

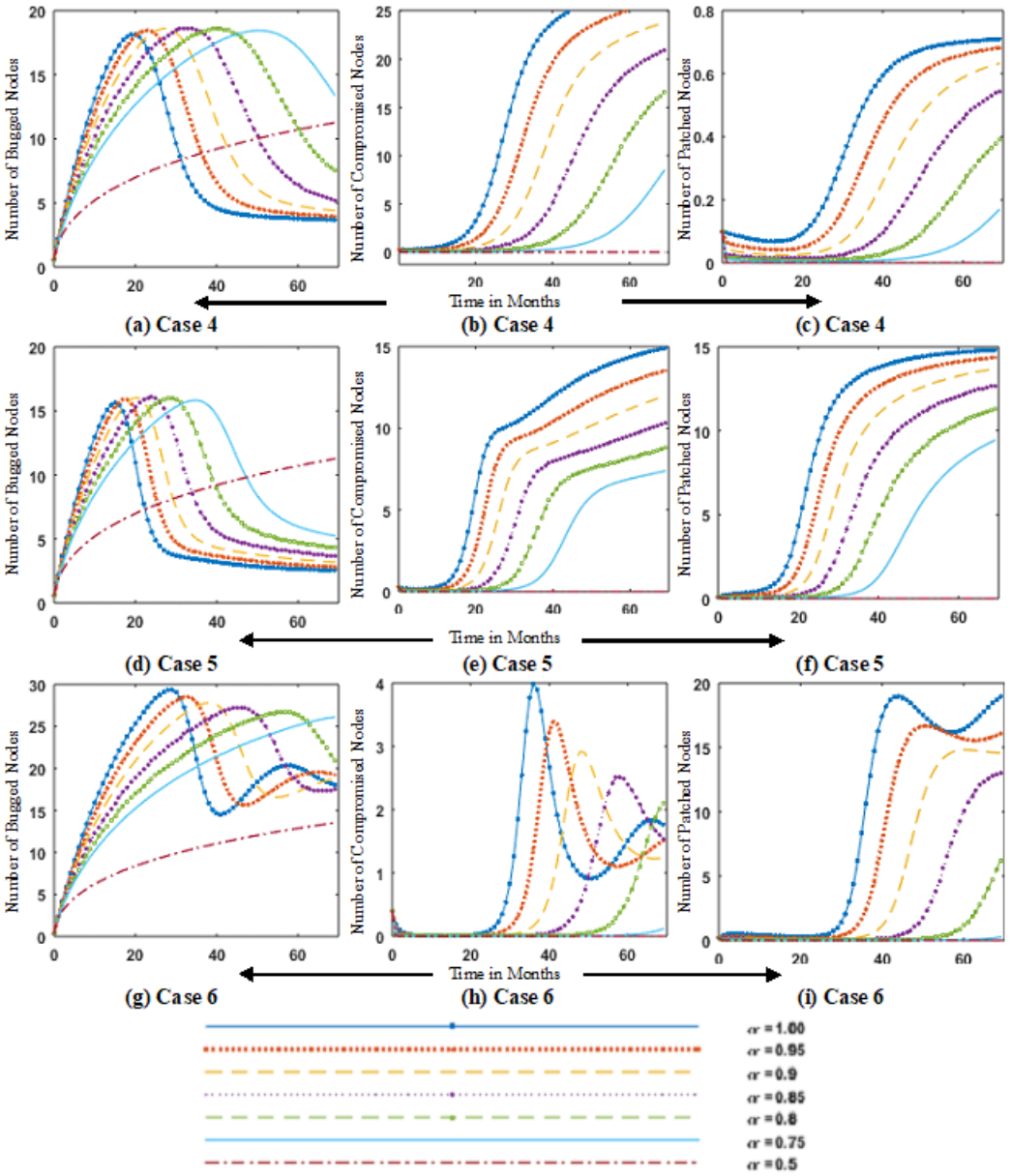


FIGURE 7.7: Dynamics of the bugged B, compromised C and patched P computers for cases 4 to 6 of FO-BCP Model for 70-month time t by taking different fractional orders.

only change the velocity of the system but also change the movement toward equilibrium point. Fast initial response is observed at $\alpha = 0.8$ with slow convergence at $\alpha = 0.1$. Fractional models have the capacity to control the convergence speed of the solution. To address the challenges of hardware implants, a novel BCP epidemic model is designed to investigate the spread of malicious code through implanted hardware bugs. The designed model is new, so a reference model for comparative analysis is not available in this case.

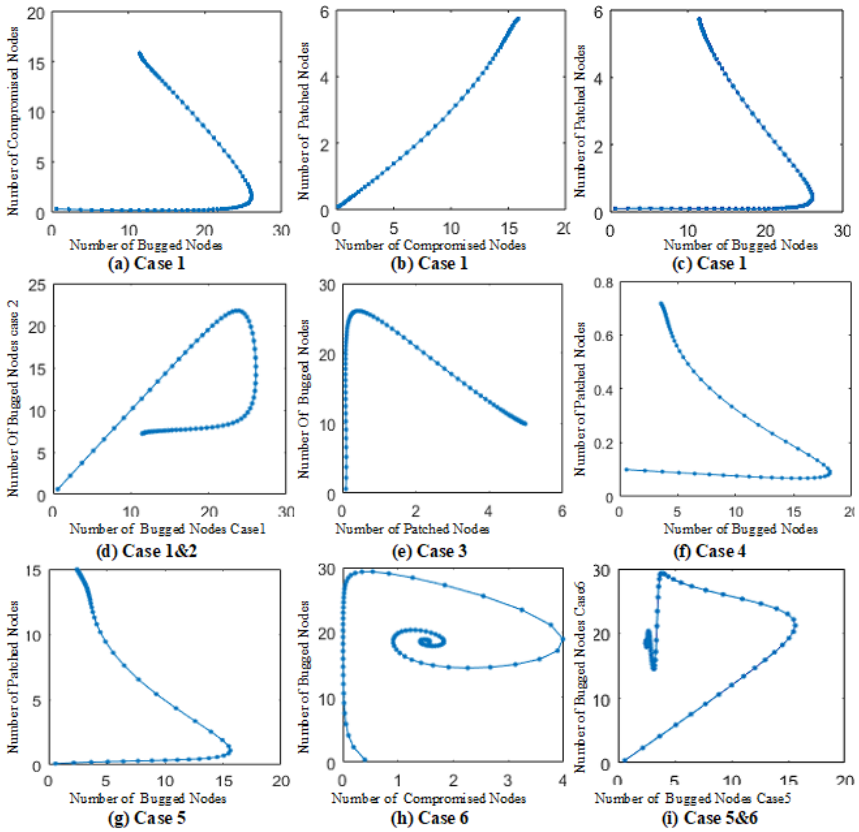


FIGURE 7.8: Dynamics of the bugged B, compromised C and patched P computers for cases 1 to 6 of FO-BCP model.

7.7 Chapter Summary

An FO-BCP based mathematical model is at least as stable as integer order model. Fractional derivative order α control the reachability of the solution toward its steady state point effectively. Fractional order model can handle the different responses, fast transient behavior and super slow evolutions with long memory characteristics. Conversion process of classical model into a fractional order model is very complex and the choice of order of differentiation α is very delicate. Theoretical analysis of FO-BCP mathematical model are carried out for disease free and endemic stability based on basic of reproduction number R_0 for an integer order value of α.

Chapter 8

Conclusion and Future Work

The landscape of malware has grown in parallel with the growth of software and technology. Adapting new strategy in design, discovering new platforms and techniques in industry present lucrative opportunity for attackers. The game of exploitation between vendors and malware authors has no sign of stopping. Due to the importance of the problem, spreading behavior of computer virus in critical networks with eradication and control scenarios are analyzed in this thesis in term of mathematical modeling. Rapid spread of computer virus and delay in the update of antivirus signature database, the role of quarantine and immunity gained importance. Model results are simulated for different scenarios by changing the initial conditions and parameter values. The change of initial conditions and parameters means the change of environment, which also includes the operating system. The change of parameter values also describe the behavior of the operating system for a given virus. Antivirus applications or operating system patch/update mechanisms may also be studied by appropriately adjusting the values of these parameters.

The values of parameters in each model are chosen based on the information available in literature, virus spread statistics, hiding ability, damages rate, limitation used in the model and the boundaries set in the theoretical analysis of the model. Parameters are changed to see the effect on the spread dynamics of the virus and see how the rate of change of different classes takes place. Different parameter

settings give rise to different cases that describe virus spread in various environments. Boundary conditions of the model have been derived from the theoretical analysis of the mathematical model based on basic reproduction number R_0.

Different viruses have different spread and hiding characteristics. Based on the nature of viruses and their spread, different time scales are used. Stuxnet has the ability to hide itself for months from being exposed, while some other viruses have ability to spread in minutes or seconds.

A $MSEQIR$ epidemic model is designed to analyzed the transmission of viruses in computer network in the presence of immunity and quarantine class. The propagation of virus in this model are both horizontal and vertical. We assume that system has temporary immunity and infected nodes will stay in the latent period before they become infectious. The virus free equilibrium of the model is asymptotically stable for $R_0 < 1$ and unstable for $R_0 > 1$. This model depicts the real situation of the system in the presence of immunity and quarantine. It is observed that quarantine and immunity play an important role in the situation where virus signature and patch update are difficult, especially in remote locations, bandwidth or resource limited systems. Due to the availability of two recovery mechanisms immunity and quarantine, recovery of infectious nodes are very high and crashing of nodes due to infection are low. The proposed model can effectively utilized for zero day attacks and preparation of pre-emptive antivirus software. The inclusion of quarantine class reduces the chances of the system to become endemic.

Stuxnet is an advance persistent threat (APT) type cyber attack, uses unusual methods to attack resources with an intend to access the critical information while remains undetected and require special arrangement for control and eradication. APT type attack typical establishes different connection points of compromise to target the victim and ensure that cyber attack can continue in failure of any one point. Attacker removed the evidence of APT occurrence without removing the re-entry path and can easily regain the control of the target system. A $\mathrm{SIPU_SU_I}$ dynamic epidemic model is designed for modeling transmission of Stuxnet virus in

an isolated critical network through removable storage media. If the infection contact rate $\beta_2 = 0$ for an $SIPU_SU_I$ model, it reduces to an SIR model. The $SIPU_SU_I$ model captures the spreading characteristics of a sophisticated digital virus such as the Stuxnet. Mathematical analysis shows that the dynamics of this model is determined through the basic reproduction number R_0. Disease free equilibrium of the model is globally asymptotically stable for $R_0 < 1$ and asymptotic endemic stability is also shown for $R_0 > 1$. The spread control of infectious disease is consistently achieved by retaining the basic reproduction number less than one. Removable storage media and infectious contact rate play an important role in the the extent of virus spread. Control strategies are also devised to minimize the devastation of virus infection. Numerical study is performed with state of the art differential equation solvers for validation of the model on available data for Stuxnet virus as well as number of scenarios for removable storage media. Numerical results are found consistently in good agreement with standard solutions and reported statistics.

A detailed analysis of novel fractional order Stuxnet virus model is presented with richer dynamics for the transmission of virus spread in an isolated critical network through removable storage media. The fractional order Stuxnet virus based mathematical model is found at least as stable as integer order model. The value of fractional order α of proposed fractional model control the solution reachability toward steady state point more effectively. Additionally, the fractional order system of Stuxnet virus model can tackle the different responses viably, including super slow evolutions and very fast transients, these responses are found in system having long memory characteristics. Tacking the value of $\alpha = 0.98$ may adjust the number of damaged hosts to 1500 in case 1 which matches the number of damaged caused by Stuxnet virus. The process of transformation of classical model in to a fractional model is very sensitive to the value of order of differentiation α and can be converted to a simple SIR model if we choose the values of infectious contact rate $\beta_2 = 0$. Theoretical analysis of the model capture the Stuxnet virus spreading characteristics and is determined by mathematical derivation of the basic reproduction number R_0 for integer order scenarios. Disease

free and endemic equilibrium points of the model is globally asymptotically stable for $R_0 < 1$ and $R_0 > 1$, respectively.

The computing world depends on underlying hardware. Harnessing the strength of hardware with minor additions which create backdoors in the system and provide unlimited access to attacker. Hacking hardware through implant of malicious chip has changed the security aspects of hardware. According to security experts this sort of compromise is a God mode' exploit. Bugged hardware has created several challenges for security experts. It can even sometimes bypass very sophisticated security arrangements. Due to the importance of the issue, a BCP epidemic model is designed to investigate the spread of malicious code through implanted tiny hardware. Theoretical analysis of the model is carried out through basic reproduction number R_0 for disease free and endemic equilibrium points. Global stability of the model is proved using Lyapunov functions for disease free equilibrium point. It is observed that controlling the infectious contact rate β will control the number of compromised nodes while also controlling the number of bugged nodes and the number of compromised nodes.

A fractional order BCP model is designed to analyze the detailed spread characteristics of the malicious code in compromised hardware which are hidden in integer models. An FO-BCP based mathematical model is at least as stable as integer order model. Fractional derivative order α controls the reachability of the solution toward its steady state point. Fractional order models can handle the different responses, very fast transient behavior and super slow evolutions with long memory characteristics. Fractional order models provide an extra control parameter α. Conversion process of classical model into a fractional order model is very complex and the choice of order of differentiation α is very delicate. Theoretical analysis of FO-BCP mathematical model are carried out for disease free and endemic equilibrium points based on basic reproduction number R_0 for an integer order value of α. Global stability of the model is proved using Lyapunov functions for disease free equilibrium point. Fast initial response is observed at $\alpha = 0.8$ with super slow convergence at $\alpha = 0.1$. Fractional models have the capacity to control the convergence speed of the solution.

Limitations or assumptions that were used during the simulation of these models include: Equal scanning probability of all hosts, $1/2^{32}$ in case of IPv4 scheme without biased scanning of any subnets, unlimited availability of network bandwidth and connectivity, no consideration of heterogeneity of computer networks (in reality heterogeneous networks exist). In addition we also assume that all infected nodes have a probability of infecting all susceptible nodes with the same infection rate, with no consideration of firewall or protection, we further assume a fixed removal rate of nodes from all classes, the population to be homogeneous and well mixed, and no latency (exposure to infection causes immediate infection).

8.1 Future Work

Inability of virus detection approaches doesn't means that we should give up protecting our computers from malware. We have to redefine our problems and approaches, and with the ambition for solutions that work well in impossibilities. The challenge is to redefine the malicious behavior of program from benign behavior. Mathematical modeling help us in redefining and simulation of these behaviors.

1. The proposed model can be effectively utilized for zero day attacks and preparation of pre-emptive antivirus software. The inclusion of quarantine class reduces the chances of the system to become endemic.
2. Anomaly based detection systems using differential equation models boundary may be defined to monitor the processes on a host machine for any abnormal activity.
3. In future, one may explore in the application of designed model of stuxnet virus on actual dataset for device vectors and general malware specimens of SCADA enviroment. Additionally, it looks promising to investigate in design and analysis a mathematical model for the Stuxnet virus in case of real-world networks that exhibit more sophisticated topologies including scale-free and small-world.
4. The validity of the BCP model may be verified using bugged hardware. The spread of malware on BCP model may be explored on actual bugged devices

for real virus dataset, so that how an implanted hardware espionage device could interact with the host system.

5. In future, one may exploit the competency of stochastic numerical computing paradigm based on fractional evolutionary and swarming optimization mechanisms for superior dynamical analysis of the models arises in the studies of $MSEQIR$ epidemic model, $\mathrm{SIPU_SU_I}$ dynamic epidemic model designed for transmission of Stuxnet virus, Fractional stuxnet virus model and Intel Management Engine ME vulnerability as well as tiny hardware implants.
6. Design of time delay based differential equation models of the above work may provide more closeness of the claimed results because infected system require a time delay to become infectious.
7. Stochastic versions of the proposed models may provide more accurate results due to probabilistic nature of the virus infection and host connectivity with network.
8. Training of artificial intelligence (AI) based antivirus virus solutions using the boundaries of mathematical models instead of real virus data which is very difficult to gather and train the system.
9. In future, one may explore the utilization of these virus models for different operating system under different environments.

Bibliography

[1] P. Morgner, S. Pfennig, D. Salzner, and Z. Benenson, "Malicious iot implants: Tampering with serial communication over the internet," in *International Symposium on Research in Attacks, Intrusions, and Defenses*. Springer, 2018, pp. 535–555.

[2] H. W. Hethcote, "The mathematics of infectious diseases," *SIAM review*, vol. 42, no. 4, pp. 599–653, 2000.

[3] Z. Masood, K. Majeed, R. Samar, and M. A. Z. Raja, "Design of epidemic computer virus model with effect of quarantine in the presence of immunity," *Fundamenta Informaticae*, vol. 161, no. 3, pp. 249–273, 2018.

[4] J. Aycock, *Computer viruses and malware*. Springer Science & Business Media, 2006, vol. 22.

[5] G. Serazzi and S. Zanero, "Computer virus propagation models," in *Performance Tools and Applications to Networked Systems*. Springer, 2004, pp. 26–50.

[6] J. Ren and Y. Xu, "A compartmental model for computer virus propagation with kill signals," *Physica A: Statistical Mechanics and its Applications*, vol. 486, pp. 446–454, 2017.

[7] L.-X. Yang, M. Draief, and X. Yang, "The optimal dynamic immunization under a controlled heterogeneous node-based sirs model," *Physica A: Statistical Mechanics and its Applications*, vol. 450, pp. 403–415, 2016.

[8] J. Ren, Y. Xu, and J. Liu, "Investigation of dynamics of a virus–antivirus model in complex network," *Physica A: Statistical Mechanics and its Applications*, vol. 421, pp. 533–540, 2015.

[9] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *IEEE communications surveys & tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[10] R. Axelrod and R. Iliev, "Timing of cyber conflict," *Proceedings of the National Academy of Sciences*, vol. 111, no. 4, pp. 1298–1303, 2014.

[11] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & security*, vol. 72, pp. 212–233, 2018.

[12] E. Van der Walt, J. H. Eloff, and J. Grobler, "Cyber-security: Identity deception detection on social media platforms," *Computers & Security*, vol. 78, pp. 76–89, 2018.

[13] F. Ullah, M. Edwards, R. Ramdhany, R. Chitchyan, M. A. Babar, and A. Rashid, "Data exfiltration: A review of external attack vectors and countermeasures," *Journal of Network and Computer Applications*, vol. 101, pp. 18–54, 2018.

[14] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," *Computers & Security*, vol. 68, pp. 81–97, 2017.

[15] S. S. Hassan, S. D. Bibon, M. S. Hossain, and M. Atiquzzaman, "Security threats in bluetooth technology," *Computers & Security*, vol. 74, pp. 308–322, 2018.

[16] S. Kim and H. Lee, "Software systems at risk: An empirical study of cloned vulnerabilities in practice," *Computers & Security*, vol. 77, pp. 720–736, 2018.

[17] L. Ablon and A. Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. RAND Corporation, 2017.

[18] K. Haldar and B. K. Mishra, "Mathematical model on vulnerability characterization and its impact on network epidemics," *International Journal of System Assurance Engineering and Management*, vol. 8, no. 2, pp. 378–392, 2017.

[19] L. Ablon, M. Libicki, and A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, ser. EBL-Schweitzer. RAND Corporation, 2014.

[20] G. Hoglund and G. McGraw, *Exploiting Software: How To Break Code, Access Date 15 Dec 2018*. Pearson Education, 2004. [Online]. Available: https://books.google.com.pk/books?id=YtiwuELN-RYC

[21] T. Rid and P. McBurney, "Cyber-weapons," *the RUSI Journal*, vol. 157, no. 1, pp. 6–13, 2012.

[22] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[23] M. Finifter, D. Akhawe, and D. Wagner, "An empirical study of vulnerability rewards programs." in *USENIX Security Symposium*, 2013, pp. 273–288.

[24] B. Kesler, "The vulnerability of nuclear facilities to cyber attack; strategic insights: Spring 2010, access date 15 dec 2018," *Strategic Insights, Spring 2011*, 2011. [Online]. Available: https://core.ac.uk/download/pdf/36718376.pdf

[25] D. E. Sanger and T. Shanker, "Nsa devises radio pathway into computers," *The New York Times*, vol. 1, no. 15, p. 2014, 2014.

[26] J. Robertson and M. Riley, "The big hack: how china used a tiny chip to infiltrate us companies," *Bloomberg Businessweek*, vol. 4, 2018.

[27] E. Bozdag, "Therac-25 and the security of the computer controlled equipment, access date 15 dec 2019," *Ethics of Science and Technology (WM0314IN)*, 2009. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.96.369&rep=rep1&type=pdf

[28] M. Hoekstra, R. Lal, P. Pappachan, V. Phegade, and J. Del Cuvillo, "Using innovative instructions to create trustworthy software solutions." *HASP@ ISCA*, vol. 11, 2013.

[29] P. Stewin and I. Bystrov, "Understanding dma malware," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, vol. 6. Springer, 2012, pp. 21–41.

[30] X. Ruan, *Platform Embedded Security Technology Revealed: Safeguarding the Future of Computing with Intel Embedded Security and Management Engine*, ser. Expert's voice in computer security. Apress, 2014.

[31] M. Ermolov and M. Goryachy, "How to hack a turned-off computer, or running unsigned code in intel management engine, access date 15 dec 2018," *Black Hat Europe*, 2017. [Online]. Available: https://www.blackhat.com/docs/eu-17/materials/eu-17-Goryachy-How-To-Hack-A-Turned-Off-Computer-Or-Running-Unsigned-Code-In-Intel-Management-Engine.pdf

[32] P. Stewin, "A primitive for revealing stealthy peripheral-based attacks on the computing platform's main memory," in *International Workshop on Recent Advances in Intrusion Detection*. Springer, 2013, pp. 1–20.

[33] I. Skochinsky, "Intel me secrets, access date 15 nov 2018," *Code Blue*, 2014. [Online]. Available: http://recon.cx/2014/slides/Recon%202014%20Skochinsky.pdf

[34] G. Averlant, B. Morgan, E. Alata, V. Nicomette, and M. Kaâniche, "An abstraction model and a comparative analysis of intel and arm hardware isolation mechanisms," in *Dependable Computing (PRDC), 2017 IEEE 22nd Pacific Rim International Symposium on*. IEEE, 2017, pp. 245–254.

[35] C. Domas, "Hardware backdoors in x86 cpus, access date 15 dec 2018," 2018. [Online]. Available: https://i.blackhat.com/us-18/Thu-August-9/us-18-Domas-God-Mode-Unlocked-Hardware-Backdoors-In-x86-CPUs-wp.pdf,

[36] A. Ogolyuk, A. Sheglov, and K. Sheglov, "Uefi bios and intel management engine attack vectors and vulnerabilities," in *Proceedings of the XXth Conference of Open Innovations Association FRUCT*, vol. 776, no. 20. Directory of Open Access Journals, 2017, pp. 657–662.

[37] X. Wang, W. Ni, K. Zheng, R. P. Liu, and X. Niu, "Virus propagation modeling and convergence analysis in large-scale networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 10, pp. 2241–2254, 2016.

[38] A. Alhumaidan and J. Steggles, "Modelling and analysing qualitative biological models using rewriting logic," *Fundamenta Informaticae*, vol. 153, no. 1-2, pp. 1–28, 2017.

[39] B. K. Mishra and S. K. Pandey, "Dynamic model of worm propagation in computer network," *Applied mathematical modelling*, vol. 38, no. 7-8, pp. 2173–2179, 2014.

[40] X. Xiao, P. Fu, C. Dou, Q. Li, G. Hu, and S. Xia, "Design and analysis of seiqr worm propagation model in mobile internet," *Communications in nonlinear science and numerical simulation*, vol. 43, pp. 341–350, 2017.

[41] W. O. Kermack and A. G. McKendrick, "Contributions to the mathematical theory of epidemics. ii.—the problem of endemicity," *Proc. R. Soc. Lond. A*, vol. 138, no. 834, pp. 55–83, 1932.

[42] R. Srivastava, L. You, J. Summers, and J. Yin, "Stochastic vs. deterministic modeling of intracellular viral kinetics," *Journal of theoretical biology*, vol. 218, no. 3, pp. 309–321, 2002.

[43] H. Hethcote, M. Zhien, and L. Shengbing, "Effects of quarantine in six endemic models for infectious diseases," *Mathematical Biosciences*, vol. 180, no. 1-2, pp. 141–160, 2002.

[44] P. W. Nelson and A. S. Perelson, "Mathematical analysis of delay differential equation models of hiv-1 infection," *Mathematical biosciences*, vol. 179, no. 1, pp. 73–94, 2002.

[45] R. M. Jafelice, L. C. de Barros, R. C. Bassanezi, and F. Gomide, "Fuzzy modeling in symptomatic hiv virus infected population," *Bulletin of Mathematical Biology*, vol. 66, no. 6, pp. 1597–1620, 2004.

[46] E. Braverman and S. Saker, "Periodic solutions and global attractivity of a discrete delay host macroparasite model," *Journal of Difference Equations and Applications*, vol. 16, no. 7, pp. 789–806, 2010.

[47] C.-H. Zhang, X.-P. Yan, and G.-H. Cui, "Hopf bifurcations in a predator–prey system with a discrete delay and a distributed delay," *Nonlinear Analysis: Real World Applications*, vol. 11, no. 5, pp. 4141–4153, 2010.

[48] S. Busenberg and K. Cooke, *Vertically transmitted diseases: models and dynamics*. Springer Science & Business Media, 2012, vol. 23.

[49] J. Amador, "The seiqs stochastic epidemic model with external source of infection," *Applied Mathematical Modelling*, vol. 40, no. 19-20, pp. 8352–8365, 2016.

[50] E. Braverman and A. Rodkina, "Stochastic difference equations with the allee effect," *arXiv preprint arXiv:1606.01928*, vol. 21, no. 3, pp. 109–121, 2016.

[51] L. Berezansky and E. Braverman, "Boundedness and persistence of delay differential equations with mixed nonlinearity," *Applied Mathematics and Computation*, vol. 279, pp. 154–169, 2016.

[52] H. A. M. Malik, A. W. Mahesar, F. Abid, A. Waqas, and M. R. Wahiddin, "Two-mode network modeling and analysis of dengue epidemic behavior in gombak, malaysia," *Applied Mathematical Modelling*, vol. 43, pp. 207–220, 2017.

[53] Y. Cai, K. Wang, and W. Wang, "Global transmission dynamics of a zika virus model," *Applied Mathematics Letters*, vol. 92, pp. 190–195, 2019.

[54] M. T. S. Pont, A. C. Castillo, H. M. Mora, and J. Szymanski, "Modelling the malware propagation in mobile computer devices," *Computers & Security*, vol. 79, pp. 80–93, 2018.

[55] B. K. Mishra and N. Jha, "Seiqrs model for the transmission of malicious objects in computer network," *Applied Mathematical Modelling*, vol. 34, no. 3, pp. 710–715, 2010.

[56] B. K. Mishra and S. K. Pandey, "Dynamic model of worms with vertical transmission in computer network," *Applied Mathematics and Computation*, vol. 217, no. 21, pp. 8438–8446, 2011.

[57] B. K. Mishra and S. K. Pandey, "Fuzzy epidemic model for the transmission of worms in computer network," *Nonlinear Analysis: Real World Applications*, vol. 11, no. 5, pp. 4335–4341, 2010.

[58] K. Haldar and B. K. Mishra, "A mathematical model for a distributed attack on targeted resources in a computer network," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 9, pp. 3149–3160, 2014.

[59] X. Wang, Z. He, X. Zhao, C. Lin, Y. Pan, and Z. Cai, "Reaction-diffusion modeling of malware propagation in mobile wireless sensor networks," *Science China Information Sciences*, vol. 56, no. 9, pp. 1–18, 2013.

[60] L.-X. Yang, X. Yang, and Y. Wu, "The impact of patch forwarding on the prevalence of computer virus: a theoretical assessment approach," *Applied Mathematical Modelling*, vol. 43, pp. 110–125, 2017.

[61] T. Dong, A. Wang, and X. Liao, "Impact of discontinuous antivirus strategy in a computer virus model with the point to group," *Applied Mathematical Modelling*, vol. 40, no. 4, pp. 3400–3409, 2016.

[62] T. Zhang, L.-X. Yang, X. Yang, Y. Wu, and Y. Y. Tang, "Dynamic malware containment under an epidemic model with alert," *Physica A: Statistical Mechanics and its Applications*, vol. 470, pp. 249–260, 2017.

[63] I. Petras, "Stability of fractional-order systems with rational orders," *arXiv preprint arXiv:0811.4102*, vol. 18, no. 5, pp. 291–301, 2008.

[64] E. Ahmed, A. El-Sayed, and H. A. El-Saka, "Equilibrium points, stability and numerical solutions of fractional-order predator–prey and rabies models," *Journal of Mathematical Analysis and Applications*, vol. 325, no. 1, pp. 542–553, 2007.

[65] J. Singh, D. Kumar, Z. Hammouch, and A. Atangana, "A fractional epidemiological model for computer viruses pertaining to a new fractional derivative," *Applied Mathematics and Computation*, vol. 316, pp. 504–515, 2018.

[66] M. A. Ansari, D. Arora, and S. P. Ansari, "Chaos control and synchronization of fractional order delay-varying computer virus propagation model," *Mathematical methods in the applied sciences*, vol. 39, no. 5, pp. 1197–1205, 2016.

[67] C. Pinto and J. Tenreiro Machado, "Fractional dynamics of computer virus propagation," *Mathematical Problems in Engineering*, vol. 2014, 2014.

[68] D. Baleanu, J. Machado, and A. Luo, *Fractional Dynamics and Control*, ser. SpringerLink : Bücher. Springer New York, 2011.

[69] N. ÖZalp and E. Demirci, "A fractional order seir model with vertical transmission," *Mathematical and Computer Modelling*, vol. 54, no. 1-2, pp. 1–6, 2011.

[70] J. Tenreiro Machado, M. F. Silva, R. S. Barbosa, I. S. Jesus, C. M. Reis, M. G. Marcos, and A. F. Galhano, "Some applications of fractional calculus in engineering," *Mathematical Problems in Engineering*, vol. 2010, 2010.

[71] J. Sabatier, O. P. Agrawal, and J. T. Machado, *Advances in fractional calculus*. Springer, 2007, vol. 4, no. 9.

[72] I. Podlubny, *Fractional differential equations: an introduction to fractional derivatives, fractional differential equations, to methods of their solution and some of their applications*. Elsevier, 1998, vol. 198.

[73] J. T. Machado, A. M. Galhano, and J. J. Trujillo, "On development of fractional calculus during the last fifty years," *Scientometrics*, vol. 98, no. 1, pp. 577–582, 2014.

[74] I. Petráš, "A note on the fractional-order chua's system," *Chaos, Solitons & Fractals*, vol. 38, no. 1, pp. 140–147, 2008.

[75] I. Petrás, "Fractional derivatives, fractional integrals, and fractional differential equations in matlab," in *Engineering education and research using MATLAB*. InTech, 2011.

[76] R. Scherer, S. Kalla, L. Boyadjiev, and B. Al-Saqabi, "Numerical treatment of fractional heat equations," *Applied Numerical Mathematics*, vol. 58, no. 8, pp. 1212–1223, 2008.

[77] Y. Wang, Z. Jin, Z. Yang, Z.-K. Zhang, T. Zhou, and G.-Q. Sun, "Global analysis of an sis model with an infective vector on complex networks," *Nonlinear Analysis: Real World Applications*, vol. 13, no. 2, pp. 543–557, 2012.

[78] F. Wang, Y. Zhang, C. Wang, J. Ma, and S. Moon, "Stability analysis of a seiqv epidemic model for rapid spreading worms," *Computers & Security*, vol. 29, no. 4, pp. 410–418, 2010.

[79] C. C. Zou, D. Towsley, and W. Gong, "On the performance of internet worm scanning strategies," *Performance Evaluation*, vol. 63, no. 7, pp. 700–723, 2006.

[80] L.-X. Yang and X. Yang, "The spread of computer viruses under the influence of removable storage devices," *Applied Mathematics and Computation*, vol. 219, no. 8, pp. 3914–3922, 2012.

[81] L.-X. Yang and X. Yang, "A new epidemic model of computer viruses," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 6, pp. 1935–1944, 2014.

[82] L.-X. Yang and X. Yang, "The effect of network topology on the spread of computer viruses: a modelling study," *International Journal of Computer Mathematics*, vol. 94, no. 8, pp. 1591–1608, 2017.

[83] L.-X. Yang, P. Li, Y. Zhang, X. Yang, Y. Xiang, and W. Zhou, "Effective repair strategy against advanced persistent threat: A differential game approach," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1713–1728, 2018.

[84] L. Yang, P. Li, X. Yang, and Y. Y. Tang, "A risk management approach to defending against the advanced persistent threat," *IEEE Transactions on Dependable and Secure Computing*, vol. 6, no. 2, pp. 1–10, 2018.

[85] E. Dilipraj, "Accessing the inaccessible," *system*, vol. 9, p. 2003, 2000.

[86] M. Guri, M. Monitz, and Y. Elovici, "Usbee: air-gap covert-channel via electromagnetic emission from usb," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016, pp. 264–268.

[87] C. J. Cohen, K. A. Scott, M. J. Huber, S. C. Rowe, and F. Morelli, "Behavior recognition architecture for surveillance applications," in *Applied Imagery Pattern Recognition Workshop, 2008. AIPR'08. 37th IEEE*. IEEE, 2008, pp. 1–8.

[88] T. Zhang, X. Wang, Z. Li, F. Guo, Y. Ma, and W. Chen, "A survey of network anomaly visualization," *Science China Information Sciences*, vol. 60, no. 12, p. 121101, 2017.

[89] C. Li and X. Liao, "The impact of hybrid quarantine strategies and delay factor on viral prevalence in computer networks," *Mathematical Modelling of Natural Phenomena*, vol. 11, no. 4, pp. 105–119, 2016.

[90] J. Nikolich-Žugich, "Ageing and life-long maintenance of t-cell subsets in the face of latent persistent infections," *Nature Reviews Immunology*, vol. 8, no. 7, p. 512, 2008.

[91] S. R. Subramanya and N. Lakshminarasimhan, "Computer viruses," *IEEE potentials*, vol. 20, no. 4, pp. 16–19, 2001.

[92] W. J. Freeman *et al.*, *Mass action in the nervous system*. Citeseer, 1975, vol. 2004.

[93] A. A. Berryman, "The orgins and evolution of predator-prey theory," *Ecology*, vol. 73, no. 5, pp. 1530–1535, 1992.

[94] *Necessary Conditions for an Extremum*, ser. Chapman & Hall/CRC Pure and Applied Mathematics. Taylor & Francis, 1971.

[95] S. Barnett, "A new formulation of the liénard–chipart stability criterion," in *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 70, no. 2. Cambridge University Press, 1971, pp. 269–274.

[96] L. Bilge and T. Dumitras, "Before we knew it: an empirical study of zero-day attacks in the real world," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 833–844.

[97] Z. Masood, R. Samar, and M. A. Z. Raja, "Design of a mathematical model for the stuxnet virus in a network of critical control infrastructure," *Computers & Security*, vol. 87, p. 101565, 2019.

[98] A. LaSota, "The present and potential future of mac hardware implants," 2019.

[99] A. L. Lloyd and R. M. May, "How viruses spread among computers and people," *Science*, vol. 292, no. 5520, pp. 1316–1317, 2001.

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

[101] A. L. Lloyd and R. M. May, "How viruses spread among computers and people," *Science*, vol. 292, no. 5520, pp. 1316–1317, 2001.

[102] J. Ren, Y. Xu, and J. Liu, "Investigation of dynamics of a virus–antivirus model in complex network," *Physica A: Statistical Mechanics and its Applications*, vol. 421, pp. 533–540, 2015.

[103] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *IEEE communications surveys & tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[104] X. Wang, W. Ni, K. Zheng, R. P. Liu, and X. Niu, "Virus propagation modeling and convergence analysis in large-scale networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 10, pp. 2241–2254, 2016.

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

[106] L.-X. Yang, X. Yang, Q. Zhu, and L. Wen, "A computer virus model with graded cure rates," *Nonlinear Analysis: Real World Applications*, vol. 14, no. 1, pp. 414–422, 2013.

[107] L.-X. Yang, M. Draief, and X. Yang, "The optimal dynamic immunization under a controlled heterogeneous node-based sirs model," *Physica A: Statistical Mechanics and its Applications*, vol. 450, pp. 403–415, 2016.

[108] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *IEEE communications surveys & tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[109] L. Holder, D. Cook, J. Coble, and M. Mukherjee, "Graph-based relational learning with application to security," *Fundamenta Informaticae*, vol. 66, no. 1-2, pp. 83–101, 2005.

[110] M. Meisel, V. Pappas, and L. Zhang, "A taxonomy of biologically inspired research in computer networking," *Computer Networks*, vol. 54, no. 6, pp. 901–916, 2010.

[111] Y. S. Rao, A. K. Rauta, H. Saini, and T. C. Panda, "Mathematical model for cyber attack in computer network," *International Journal of Business Data Communications and Networking (IJBDCN)*, vol. 13, no. 1, pp. 58–65, 2017.

[112] B. K. Mishra and S. K. Pandey, "Effect of anti-virus software on infectious nodes in computer network: a mathematical model," *Physics Letters A*, vol. 376, no. 35, pp. 2389–2393, 2012.

[113] T. Dong, X. Liao, and H. Li, "Stability and hopf bifurcation in a computer virus model with multistate antivirus," in *Abstract and Applied Analysis*, vol. 2012. Hindawi, 2012.

[114] Y. Zhang, Y. Li, and L. Chen, "Biologically inspired model for computer virus detection," in *System of Systems Engineering (SoSE), 2012 7th International Conference on*, 2012, pp. 66–69.

[115] L. Bilge and T. Dumitras, "Before we knew it: an empirical study of zero-day attacks in the real world," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 833–844.

[116] B. Jakubczyk, *Perspectives in Control Theory: Proceedings of the Sielpia Conference, Sielpia, Poland, September 19–24, 1988*, ser. Progress in Systems and Control Theory. Birkhäuser Boston, 2013.

[117] B. Porter, *Stability criteria for linear dynamical systems*. Academic Press, 1968.

[118] M. Rohde, K. Aal, K. Misaki, D. Randall, A. Weibert, and V. Wulf, "Out of syria: Mobile media in use at the time of civil war," *International Journal of Human-Computer Interaction*, vol. 32, no. 7, pp. 515–531, 2016.

[119] C. Bronk and E. Tikk-Ringas, "The cyber attack on saudi aramco," *Survival*, vol. 55, no. 2, pp. 81–96, 2013.

[120] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[121] D. Albright, P. Brannan, and C. Walrond, "Stuxnet malware and natanz: Update of isis december 22, 2010 report," *Institute for Science and International Security*, vol. 15, pp. 739 883–3, 2011.

[122] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, no. 6, p. 29, 2011.

[123] Y. Wang, S. Wen, Y. Xiang, and W. Zhou, "Modeling the propagation of worms in networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 942–960, 2014.

[124] Q. K. A. Mirza, I. Awan, and M. Younas, "Cloudintell: An intelligent malware detection system," *Future Generation Computer Systems*, vol. 86, pp. 1042–1053, 2018.

[125] G. Li, Z. Peng, and L. Song, "Modeling and analyzing the spread of flash disk worms via multiple subnets," *Discrete Dynamics in Nature and Society*, vol. 2015, 2015.

[126] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on scada systems," in *2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing*. IEEE, 2011, pp. 380–388.

[127] M. Li, C. Fu, X.-Y. Liu, J. Yang, T. Zhu, and L. Han, "Evolutionary virus immune strategy for temporal networks based on community vitality," *Future Generation Computer Systems*, vol. 74, pp. 276–290, 2017.

[128] V. Capasso and G. Serio, "A generalization of the kermack-mckendrick deterministic epidemic model," *Mathematical Biosciences*, vol. 42, no. 1-2, pp. 43–61, 1978.

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

[130] C. Zhang, Y. Zhao, Y. Wu, and S. Deng, "A stochastic dynamic model of computer viruses," *Discrete Dynamics in Nature and Society*, vol. 2012, 2012.

[131] T. Chen, X.-s. Zhang, and Y. Wu, "Fpm: Four-factors propagation model for passive p2p worms," *Future Generation Computer Systems*, vol. 36, pp. 133–141, 2014.

[132] J. R. C. Piqueira and V. O. Araujo, "A modified epidemiological model for computer viruses," *Applied Mathematics and Computation*, vol. 213, no. 2, pp. 355–360, 2009.

[133] K. L. Calvert, M. B. Doar, and E. W. Zegura, "Modeling internet topology," *IEEE Communications magazine*, vol. 35, no. 6, pp. 160–163, 1997.

[134] K. Miller and B. Ross, *An Introduction to the Fractional Calculus and Fractional Differential Equations*. Wiley, 1993.

[135] H. J. Haubold, A. M. Mathai, and R. K. Saxena, "Mittag-leffler functions and their applications," *Journal of Applied Mathematics*, vol. 2011, 2011.

[136] I. Podlubny, "The laplace transform method for linear differential equations of the fractional order," *arXiv preprint funct-an/9710005*, 1997.

[137] D. Cafagna, "Fractional calculus: A mathematical tool from the past for present engineers [past and present]," *IEEE Industrial Electronics Magazine*, vol. 1, no. 2, pp. 35–40, 2007.

[138] R. Langner, "To kill a centrifuge: A technical analysis of what stuxnet's creators tried to achieve, access date 15 dec 2018," *The Langner Group*, 2013. [Online]. Available: https://www.langner.com/to-kill-a-centrifuge/

[139] C. Wueest, "Targeted attacks against the energy sector, access date 15 dec 2018," *Symantec Security Response, Mountain View, CA*, 2014. [Online]. Available: https://bluekarmasecurity.net/wp-content/uploads/2014/09/Symantec_Targeted-Attacks-Against-the-Energy-Sector_whitepaper.pdf

[140] H. R. Thieme, "Asymptotically autonomous differential equations in the plane," *The Rocky Mountain Journal of Mathematics*, pp. 351–380, 1994.

[141] L. Markus, "Ii. asymptotically autonomous differential systems," *Contributions to the Theory of Nonlinear Oscillations (AM-36)*, vol. 3, p. 17, 2016.

[142] P. Van den Driessche and J. Watmough, "Reproduction numbers and subthreshold endemic equilibria for compartmental models of disease transmission," *Mathematical biosciences*, vol. 180, no. 1-2, pp. 29–48, 2002.

[143] J. J. Gil, A. Avello, A. Rubio, and J. Florez, "Stability analysis of a 1 dof haptic interface using the routh-hurwitz criterion," *IEEE transactions on control systems technology*, vol. 12, no. 4, pp. 583–588, 2004.

[144] J. Rohn, "Positive definiteness and stability of interval matrices," *SIAM Journal on Matrix Analysis and Applications*, vol. 15, no. 1, pp. 175–184, 1994.

[145] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, no. 6, p. 29, 2011.

[146] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[147] M. Abdel-Basset, G. Manogaran, D. El-Shahat, and S. Mirjalili, "A hybrid whale optimization algorithm based on local search strategy for the permutation flow shop scheduling problem," *Future Generation Computer Systems*, vol. 85, pp. 129–145, 2018.

[148] S. S. Chaharborj, S. Chaharborj, and Y. Mahmoudi, "Study of fractional order integro-differential equations by using chebyshev neural network," *J. Math. Stat*, vol. 13, no. 1, pp. 1–13, 2017.

[149] M. A. Z. Raja, A. Mehmood, A. ur Rehman, A. Khan, and A. Zameer, "Bio-inspired computational heuristics for sisko fluid flow and heat transfer models," *Applied Soft Computing*, vol. 71, pp. 622–648, 2018.

[150] M. A. Z. Raja, Z. Shah, M. A. Manzar, I. Ahmad, M. Awais, and D. Baleanu, "A new stochastic computing paradigm for nonlinear painlevé ii systems in applications of random matrix theory," *The European Physical Journal Plus*, vol. 133, no. 7, p. 254, 2018.

[151] I. Ahmad, S. Ahmad, M. Awais, S. U. I. Ahmad, and M. A. Z. Raja, "Neuro-evolutionary computing paradigm for painlevé equation-ii in nonlinear optics," *The European Physical Journal Plus*, vol. 133, no. 5, p. 184, 2018.

[152] Y. Liu, W. Wei, and R. Zhang, "Desrp: An efficient differential evolution algorithm for stochastic demand-oriented resource placement in heterogeneous clouds," *Future Generation Computer Systems*, vol. 88, pp. 234–242, 2018.

[153] S. Akbar, F. Zaman, M. Asif, A. U. Rehman, and M. A. Z. Raja, "Novel application of fo-dpso for 2-d parameter estimation of electromagnetic plane waves," *Neural Computing and Applications*, vol. 31, no. 8, pp. 3681–3690, 2019.

[154] E. S. Pires, J. T. Machado, P. de Moura Oliveira, J. B. Cunha, and L. Mendes, "Particle swarm optimization with fractional-order velocity," *Nonlinear Dynamics*, vol. 61, no. 1-2, pp. 295–301, 2010.

[155] S. Kiranyaz, J. Pulkkinen, and M. Gabbouj, "Multi-dimensional particle swarm optimization in dynamic environments," *Expert Systems with Applications*, vol. 38, no. 3, pp. 2212–2223, 2011.

[156] M. A. Z. Raja, R. Samar, M. A. Manzar, and S. M. Shah, "Design of unsupervised fractional neural network model optimized with interior point algorithm for solving bagley–torvik equation," *Mathematics and Computers in Simulation*, vol. 132, pp. 139–158, 2017.

[157] S. Lodhi, M. A. Manzar, and M. A. Z. Raja, "Fractional neural network models for nonlinear riccati systems," *Neural Computing and Applications*, pp. 1–20, 2017.

[158] F. B. Ozsoydan and A. Baykasoglu, "A swarm intelligence-based algorithm for the set-union knapsack problem," *Future Generation Computer Systems*, vol. 93, pp. 560–569, 2019.

[159] J. Nocetti, "The cybersecurity dilemma: hacking, trust, and fear between nations,," pp. 1259–1260, 09 2017.

[160] B. Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford University Press, 2016.

[161] C. Park, M. Keil, and J. W. Kim, "The effect of it failure impact and personal morality on it project reporting behavior," *IEEE Transactions on Engineering Management*, vol. 56, no. 1, pp. 45–60, 2009.

[162] X. Fan and Y. Xiang, "Modeling the propagation of peer-to-peer worms," *Future generation computer systems*, vol. 26, no. 8, pp. 1433–1443, 2010.

[163] X. Zhang, G. Neglia, J. Kurose, and D. Towsley, "Performance modeling of epidemic routing," *Computer Networks*, vol. 51, no. 10, pp. 2867–2891, 2007.

[164] D. Barash and C. Webel, *Peace and Conflict Studies*. SAGE Publications, 2017.

[165] D. Barash and C. Webel, *Peace and Conflict Studies*. SAGE Publications, 2013.

[166] R. AlTawy and A. M. Youssef, "Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices," *IEEE Access*, vol. 4, pp. 959–979, 2016.

[167] C. Wilson, "Cyber threats to critical information infrastructure," in *Cyberterrorism*. Springer, 2014, pp. 123–136.

[168] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware trojan attacks: threat analysis and countermeasures," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1229–1247, 2014.

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

[170] B. K. Mishra and S. K. Pandey, "Dynamic model of worm propagation in computer network," *Applied mathematical modelling*, vol. 38, no. 7-8, pp. 2173–2179, 2014.

[171] B. K. Mishra and N. Jha, "Seiqrs model for the transmission of malicious objects in computer network," *Applied Mathematical Modelling*, vol. 34, no. 3, pp. 710–715, 2010.

[172] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *science*, vol. 286, no. 5439, pp. 509–512, 1999.

[173] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things(IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[174] C. C. Zou, D. Towsley, and W. Gong, "Modeling and simulation study of the propagation and defense of internet e-mail worms," *IEEE Transactions on dependable and secure computing*, vol. 4, no. 2, pp. 105–118, 2007.

[175] S. Das and I. Pan, *Fractional Order Signal Processing: Introductory Concepts and Applications*, ser. SpringerBriefs in Applied Sciences and Technology. Springer Berlin Heidelberg, 2011.

[176] I. Petráš, "A note on the fractional-order chua's system," *Chaos, Solitons & Fractals*, vol. 38, no. 1, pp. 140–147, 2008.

[177] K. Oldham and J. Spanier, *The fractional calculus theory and applications of differentiation and integration to arbitrary order*. Elsevier, 1974, vol. 111.

[178] A. A. A. Kilbas, H. M. Srivastava, and J. J. Trujillo, *Theory and applications of fractional differential equations*. Elsevier Science Limited, 2006, vol. 204.

[179] B. K. Mishra and R. Goswami, "Probabilistic e-epidemic model on computer worms," in *Informatics, Electronics & Vision (ICIEV), 2012 International Conference on*. IEEE, 2012, pp. 1091–1096.

[180] J. Tenreiro Machado, M. F. Silva, R. S. Barbosa, I. S. Jesus, C. M. Reis, M. G. Marcos, and A. F. Galhano, "Some applications of fractional calculus in engineering," *Mathematical Problems in Engineering*, vol. 2010, 2010.

[181] P. Van den Driessche and J. Watmough, "Further notes on the basic reproduction number," in *Mathematical epidemiology*. Springer, 2008, pp. 159–178.

[182] Y. Li, Y. Chen, and I. Podlubny, "Mittag–leffler stability of fractional order nonlinear dynamic systems," *Automatica*, vol. 45, no. 8, pp. 1965–1969, 2009.

[183] I. Petras, "Stability of fractional-order systems with rational orders," *arXiv preprint arXiv:0811.4102*, vol. 5, no. 9, pp. 195–208, 2008.

[184] J. J. Gil, A. Avello, A. Rubio, and J. Florez, "Stability analysis of a 1 dof haptic interface using the routh-hurwitz criterion," *IEEE transactions on control systems technology*, vol. 12, no. 4, pp. 583–588, 2004.

[185] J. Rohn, "Positive definiteness and stability of interval matrices," *SIAM Journal on Matrix Analysis and Applications*, vol. 15, no. 1, pp. 175–184, 1994.

[186] M. A. Z. Raja, A. Mehmood, A. ur Rehman, A. Khan, and A. Zameer, "Bio-inspired computational heuristics for sisko fluid flow and heat transfer models," *Applied Soft Computing*, vol. 71, pp. 622–648, 2018.

[187] M. A. Z. Raja, Z. Shah, M. A. Manzar, I. Ahmad, M. Awais, and D. Baleanu, "A new stochastic computing paradigm for nonlinear painlevé ii systems in applications of random matrix theory," *The European Physical Journal Plus*, vol. 133, no. 7, p. 254, 2018.

[188] I. Ahmad, S. Ahmad, M. Awais, S. U. I. Ahmad, and M. A. Z. Raja, "Neuro-evolutionary computing paradigm for painlevé equation-ii in nonlinear optics," *The European Physical Journal Plus*, vol. 133, no. 5, p. 184, 2018.

[189] Y. Liu, W. Wei, and R. Zhang, "Desrp: An efficient differential evolution algorithm for stochastic demand-oriented resource placement in heterogeneous clouds," *Future Generation Computer Systems*, vol. 88, pp. 234–242, 2018.

[190] S. Akbar, F. Zaman, M. Asif, A. U. Rehman, and M. A. Z. Raja, "Novel application of fo-dpso for 2-d parameter estimation of electromagnetic plane waves," *Neural Computing and Applications*, vol. 31, no. 8, pp. 3681–3690, 2019.

[191] F. Rao, P. S. Mandal, and Y. Kang, "Complicated endemics of an sirs model with a generalized incidence under preventive vaccination and treatment controls," *Applied Mathematical Modelling*, vol. 67, pp. 38–61, 2019.

[192] D. P. Lizarralde-Bejarano, S. Arboleda-Sánchez, and M. E. Puerta-Yepes, "Understanding epidemics from mathematical models: Details of the 2010 dengue epidemic in bello (antioquia, colombia)," *Applied Mathematical Modelling*, vol. 43, pp. 566–578, 2017.

[193] Q. Wu and T. Hadzibeganovic, "Pair quenched mean-field approach to epidemic spreading in multiplex networks," *Applied Mathematical Modelling*, vol. 60, pp. 244–254, 2018.

[194] M. D. Ortigueira and J. T. Machado, "What is a fractional derivative?" *Journal of computational Physics*, vol. 293, pp. 4–13, 2015.

[195] M. A. Z. Raja, R. Samar, E. S. Alaidarous, and E. Shivanian, "Bio-inspired computing platform for reliable solution of bratu-type equations arising in the modeling of electrically conducting solids," *Applied Mathematical Modelling*, vol. 40, no. 11-12, pp. 5964–5977, 2016.

[196] M. A. Z. Raja, M. A. Manzar, and R. Samar, "An efficient computational intelligence approach for solving fractional order riccati equations using ann

and sqp," *Applied Mathematical Modelling*, vol. 39, no. 10-11, pp. 3075–3093, 2015.

[197] J. Escalante-Martínez, J. Gómez-Aguilar, C. Calderón-Ramón, A. Aguilar-Meléndez, and P. Padilla-Longoria, "Synchronized bioluminescence behavior of a set of fireflies involving fractional operators of liouville–caputo type," *International Journal of Biomathematics*, vol. 11, no. 03, p. 1850041, 2018.

[198] M. Zeller, "Myth or reality—does the aurora vulnerability pose a risk to my generator?" in *2011 64th Annual Conference for Protective Relay Engineers*. IEEE, 2011, pp. 130–136.

[199] S. Cowely and M. Williams, "Slammer worm slaps net down, but not out, access date 15 dec 2017," *IDG News*, 2003. [Online]. Available: https://www.computerworld.com/article/2580601/update--slammer-worm-slugs-internet--slows-web-traffic.html

[200] N. Nissim, R. Yahalom, and Y. Elovici, "Usb-based attacks," *Computers & Security*, vol. 70, pp. 675–688, 2017.

[201] L.-P. Song, Z. Jin, G.-Q. Sun, J. Zhang, and X. Han, "Influence of removable devices on computer worms: dynamic analysis and control strategies," *Computers & Mathematics with Applications*, vol. 61, no. 7, pp. 1823–1829, 2011.

[202] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for scada systems," *Computers & security*, vol. 56, pp. 1–27, 2016.

[203] S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting scada cyber security: A survey of techniques," *Computers & Security*, vol. 70, pp. 436–454, 2017.

[204] J. Ren and Y. Xu, "A compartmental model to explore the interplay between virus epidemics and honeynet potency," *Applied Mathematical Modelling*, vol. 59, pp. 86–99, 2018.

[205] I. Ahn, H.-C. Oh, and J. Park, "Investigation of the c-seira model for controlling malicious code infection in computer networks," *Applied Mathematical Modelling*, vol. 39, no. 14, pp. 4121–4133, 2015.

[206] J. Graham, R. Olson, and R. Howard, *Cyber Security Essentials*. CRC Press, 2016.

[207] K. Zetter, "How digital detectives deciphered stuxnet, the most menacing malware in history," *Wired Magazine*, vol. 11, pp. 1–8, 2011.

[208] T. Alves, R. Das, A. Werth, and T. Morris, "Virtualization of scada testbeds for cybersecurity research: A modular approach," *Computers & Security*, vol. 77, pp. 531–546, 2018.

[209] M. T. Signes-Pont, A. Cortés-Castillo, H. Mora-Mora, and J. Szymanski, "Modelling the malware propagation in mobile computer devices," *Computers & Security*, vol. 79, pp. 80–93, 2018.

[210] E. Schmidt and J. Cohen, *The New Digital Age: Reshaping the Future of People, Nations and Business*. John Murray Press, 2013.

[211] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society*. IEEE, 2011, pp. 4490–4494.

[212] M. Kang and H. Saiedian, "Usbwall: A novel security mechanism to protect against maliciously reprogrammed usb devices," *Information Security Journal: A Global Perspective*, vol. 26, no. 4, pp. 166–185, 2017.

[213] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, 2nd ed. Syngress Publishing, 2014.

[214] T. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[215] J. H. Jones, "Notes on r0, access date 15 dec 2017," *Califonia: Department of Anthropological Sciences*, 2007. [Online]. Available: https://web.stanford.edu/~jhj1/teachingdocs/Jones-on-R0.pdf

[216] E. A. Barbashin, *Introduction to the Theory of Stability*. Wolters-Noordhoff Groningen, 1970, vol. 970.

[217] J. La Salle and S. Lefschetz, "Stability theory by liapunov's direct method," 1961.

[218] J. Salle and S. Lefschetz, *Stability by Liapunov's Direct Method with Applications by Joseph L Salle and Solomon Lefschetz*, ser. ISSN. Elsevier Science, 2012.

[219] A. Matrosov, E. Rodionov, D. Harley, and J. Malcho, "Stuxnet under the microscope, access date 1 dec 2018," *ESET LLC (September 2010)*, 2010. [Online]. Available: http://ca-apac.com/image/ITR%201.pdf

[220] W. J. Broad, J. Markoff, and D. E. Sanger, "Israeli test on worm called crucial in iran nuclear delay," *New York Times*, vol. 15, p. 2011, 2011.

[221] P. Mueller and B. Yadegari, "The stuxnet worm, access date 15 dec 2017," *Département des sciences de linformatique, Université de lArizona. Recuperado de*, 2012. [Online]. Available: https://www2.cs.arizona.edu/collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf

[222] P. Shakarian, J. Shakarian, and A. Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Elsevier Science, 2013.

[223] W. J. Broad, J. Markoff, and D. E. Sanger, "Israeli test on worm called crucial in iran nuclear delay," *New York Times*, vol. 15, p. 2011, 2011.

[224] P. Shahrear, A. K. Chakraborty, M. A. Islam, and U. Habiba, "Analysis of computer virus propagation based on compartmental model," *Applied and Computational Mathematics*, vol. 7, no. 1-2, pp. 12–21, 2018.

[225] N. H. Khanh, "Dynamical analysis and approximate iterative solutions of an antidotal computer virus model," *International Journal of Applied and Computational Mathematics*, vol. 3, no. 1, pp. 829–841, 2017.

[226] V. P. Latha, F. A. Rihan, R. Rakkiyappan, and G. Velmurugan, "A fractional-order model for ebola virus infection with delayed immune response on heterogeneous complex networks," *Journal of Computational and Applied Mathematics*, vol. 339, pp. 134–146, 2018.

[227] C. M. Pinto and A. R. Carvalho, "A latency fractional order model for hiv dynamics," *Journal of Computational and Applied Mathematics*, vol. 312, pp. 240–256, 2017.

[228] J. V. d. C. Sousa, M. N. dos Santos, L. Magna, and E. C. de Oliveira, "Validation of a fractional model for erythrocyte sedimentation rate," *Computational and Applied Mathematics*, vol. 37, no. 5, pp. 6903–6919, 2018.

[229] J. Singh, D. Kumar, and D. Baleanu, "On the analysis of chemical kinetics system pertaining to a fractional derivative with mittag-leffler type kernel," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 27, no. 10, p. 103113, 2017.

[230] J. Singh, D. Kumar, and D. Baleanu, "On the analysis of fractional diabetes model with exponential law," *Advances in Difference Equations*, vol. 2018, no. 1, p. 231, 2018.

[231] J. Singh, D. Kumar, M. Al Qurashi, and D. Baleanu, "A new fractional model for giving up smoking dynamics," *Advances in Difference Equations*, vol. 2017, no. 1, p. 88, 2017.

[232] J. M. Heffernan, R. J. Smith, and L. M. Wahl, "Perspectives on the basic reproductive ratio," *Journal of the Royal Society Interface*, vol. 2, no. 4, pp. 281–293, 2005.

[233] S. Lenhart and J. T. Workman, *Optimal control applied to biological models*. Chapman and Hall/CRC, 2007, vol. 2.

[234] U. Ledzewicz and H. Schättler, "On optimal singular controls for a general sir-model with vaccination and treatment," *Discrete and continuous dynamical systems*, vol. 2, pp. 981–990, 2011.

[235] O. A. Arqub and M. Al-Smadi, "Atangana–baleanu fractional approach to the solutions of bagley–torvik and painlevé equations in hilbert space," *Chaos, Solitons & Fractals*, vol. 117, pp. 161–167, 2018.

[236] O. A. Arqub and B. Maayah, "Numerical solutions of integrodifferential equations of fredholm operator type in the sense of the atangana–baleanu fractional operator," *Chaos, Solitons & Fractals*, vol. 117, pp. 117–124, 2018.

[237] O. Abu Arqub, "Application of residual power series method for the solution of time-fractional schrödinger equations in one-dimensional space," *Fundamenta Informaticae*, vol. 166, no. 2, pp. 87–110, 2019.

[238] O. Abu Arqub, "Numerical algorithm for the solutions of fractional order systems of dirichlet function types with comparative analysis," *Fundamenta Informaticae*, vol. 166, no. 2, pp. 111–137, 2019.

[239] O. A. Arqub, "Numerical solutions of systems of first-order, two-point bvps based on the reproducing kernel algorithm," *Calcolo*, vol. 55, no. 3, p. 31, 2018.

Appendix A

In this section, the proof of D_3 and D_5 are verified numerically for $R_0 > 1$. Let us consider the general characteristics equation of the system as:

$$a_0 s^n + a_1 s^{n-1} + a_2 s^{n-2} + a_3 s^{n-3} \cdots \ a_{n-1} s^1 + a_n = 0$$

The characteristics equation (3.25) is given as

$\lambda^6 + \lambda^5(A + B + C + D + F + E) + \lambda^4(AB + AC + AD + AF + EA +$
$BC + BD + BF + EB + CD + CF + EC + d\delta + DF + ED + EF - G\xi) +$
$\lambda^3(ABC + ABD + ABF + EAB + ACD + ACF + EAC + ADF + EAD +$
$\mathrm{e}AF - AG\xi + BCD + BCF + \mathrm{e}BC + Bd\delta + BDF + EBD + EBF + Cd\delta +$
$CDF + ECD + ECF - CG\xi + \mathrm{e}d\delta + d\delta D + EDF - EG\xi) +$
$\lambda^2(ABCD + ABCF + EABC + ABDF + EABD + \mathrm{E}ABF + ACDF +$
$EACD + EACF - ACG\xi + EADF - EAG\xi + BCd\delta + BCDF + EBCD +$
$EBCF + EBd\delta + Bd\delta D + EBDF + ECd\delta + Cd\delta D + ECDF - ECG\xi +$
$Ed\delta D - d\delta G\xi - F\eta\xi\Upsilon - F\eta\rho\varphi) + \lambda(ABCDF + EABCD + EABCF +$
$EABDF + EACDF - EACG\xi - AF\eta\xi\Upsilon - AF\eta\rho\varphi + EBCd\delta + BCd\delta D +$
$EBCDF + EBd\delta D + ECd\delta D - Cd\delta G\xi - CF\eta\xi\Upsilon - Ed\delta G\xi - DF\eta\rho\varphi -$
$\delta F\xi\sigma\Upsilon - \delta F\rho\sigma\varphi) + EABCDF - ACF\eta\xi\Upsilon - ADF\eta\rho\varphi + EBCd\delta D -$
$ECd\delta G\xi - C\delta F\xi\sigma\Upsilon - \delta DF\rho\sigma\varphi = 0.$

$a_0 = 1,$

$a_1 = A + B + C + D + E + F,$

$a_2 = AB + AC + BC + AD + BD + CD + AE + BE + CE + DE + AF +$
$BF + CF + DF + EF + d\delta - G\xi,$

$$a_3 = ABC + ABD + ACD + BCD + ABE + ACE + BCE + ADE + BD\text{e}$$
$$+CDE + ABF + ACF + BCF + ADF + BDF + CDF + AEF + BEF$$
$$+CEF + DEF + Bd\delta + Cd\delta + dD\delta + dE\delta - AG\xi - CG\xi - EG\xi,$$
$$a_4 = ABCD + ABCE + ABDE + ACDE + BCDE + ABCF + ABDF$$
$$+ACDF + BCDF + ABEF + ACEF + BCEF + ADEF + BDEF$$
$$+CDEF + BCd\delta + BdD\delta + CdD\delta + BdE\delta + CdE\delta + dDE\delta$$
$$- ACG\xi - AEG\xi - CEG\xi - dG\delta\xi - F\eta\xi\Upsilon - F\eta\rho\varphi,$$
$$a_5 = ABCDE + ABCDF + ABCEF + ABDEF + ACDEF + BCDEF$$
$$+BCdD\delta + BCdE\delta + BdDE\delta + CdDE\delta - AC\text{e}G\xi - CdG\delta\xi$$
$$-dEG\delta\xi - AF\eta\xi\Upsilon - CF\eta\xi\Upsilon - F\delta\xi\sigma\Upsilon - AF\eta\rho\varphi - DF\eta\rho\varphi - F\delta\rho\sigma\varphi,$$
$$a_6 = ABCDEF + BCdDE\delta - CdEG\delta\xi - ACF\eta\xi\Upsilon - CF\delta\xi\sigma\Upsilon - ADF\eta\rho\varphi - DF\delta\rho\sigma\varphi.$$

By equating the coefficients, we have

We choose the parameter values so that $R_0 = \frac{\beta\xi}{(d+\gamma)(d+\xi+\varphi)} \geq 1$ and for one set of these values we have

$R_0 = \frac{0.9*10}{(0.5+0.01)(0.5+10+0.1)} \geq 1$

then the parameter values are calculated as:

$A = 1,\ B = 10.6,\ C = 0.6,\ D = 0.51,\ E = 1.1,\ F = 1.35,\ G = 0.53,\ \delta = 0.5,$

$b = 0.12,\ \varphi = 0.1,\ \xi = 10,\ \Upsilon = 0.01,\ \rho = 0.1,\ \sigma = 0.001,\ \eta = 0.6,\ \beta = 0.9.$

Using these numeric values, characteristic equation of the Jacobean matrix (3.25) at endemic equilibrium point D^* is given as:

$4.76 + 27.50\lambda + 64.66\lambda^2 + 78.91\lambda^3 + 51.16\lambda^4 + 15.15\lambda^5 + \lambda^6,$

$$\{\lambda_1 \to -11.16\},\quad \{\lambda_2 \to -1.09\},\quad \{\lambda_3 \to -0.79\},\quad \{\lambda_4 \to -0.75 - 0.50\text{i}\},$$
$$\{\lambda_5 \to -0.75 + 0.50\text{i}\},\quad \{\lambda_6 \to -0.60\}.$$

which shows that all coefficients have positive values, so all eigenvalues are in left half plane, the value of $D_3 = 41108$ and $D_5 = 3.3107$ which are also positive.

Appendix B

Derivation of endemic equilibrium points

$$P^{'} = \gamma C - \frac{\delta\beta PC}{N} - \xi P - dP.$$

At steady state $P^{'} = 0$,

$$\gamma C - \tfrac{\delta\beta PC}{N} - \xi P - dP = 0,$$
$$\gamma C - \tfrac{\delta\beta CP^*}{N} - \xi P^* - dP^* = 0,$$

$$P^* = \tfrac{\frac{1}{R_0}+C^*-1}{\delta-1},$$
$$\gamma C - \tfrac{\delta\beta C\frac{\frac{1}{R_0}+C^*-1}{\delta-1}}{N} - \xi\tfrac{\frac{1}{R_0}+C^*-1}{\delta-1} - d\tfrac{\frac{1}{R_0}+C^*-1}{\delta-1} = 0,$$

$$\gamma C - \frac{\delta\beta C}{R_0(\delta-1)} + \frac{\delta\beta C}{\delta-1} - \frac{\delta\beta C^2}{\delta-1} - \frac{\xi}{R_0(\delta-1)} +$$
$$\frac{\xi}{\delta-1} - \frac{\xi C}{\delta-1} - \frac{d}{R_0(\delta-1)} + \frac{d}{\delta-1} - \frac{dC}{\delta-1} = 0,$$
$$-C^2\frac{\delta\beta}{\delta-1} + C\left[\gamma - \frac{\delta\beta}{R_0(\delta-1)} + \frac{\delta\beta}{\delta-1} - \frac{\xi}{\delta-1} - \frac{d}{\delta-1}\right]$$
$$+\left[\frac{d}{\delta-1} - \frac{d}{R_0(\delta-1)} + \frac{\xi}{\delta-1} - \frac{\xi}{R_0(\delta-1)}\right] = 0,$$
$$C^2\frac{\delta\beta}{\delta-1} + C\left[-\gamma + \frac{\delta\beta}{R_0(\delta-1)} - \frac{\delta\beta}{\delta-1} + \frac{\xi}{\delta-1} + \frac{d}{\delta-1}\right]$$
$$+\left[\frac{d}{R_0(\delta-1)} - \frac{d}{\delta-1} + \frac{\xi}{R_0(\delta-1)} - \frac{\xi}{\delta-1}\right] = 0,$$

multiplying $(\delta-1)$ to LHS

$$C^2\delta\beta + C\left[-\gamma(\delta-1) + \frac{\delta\beta}{R_0} - \delta\beta + \xi + d\right] + \left[\frac{d}{R_0} - d + \frac{\xi}{R_0} - \xi\right] = 0,$$

$$C^* = \frac{\sqrt{b^2 - 4ac} - b}{2a}.$$

Where

$$a = \delta\beta,\ b = \frac{\delta\beta}{R_0} - \delta\beta + \xi + d - \gamma(\delta - 1), c = \frac{d}{R_0} - d + \frac{\xi}{R_0} - \xi$$

and after simplifying the c, we know that for R_0 ¿ 1 c is negative

$$\begin{aligned} c &= d(\tfrac{1}{R_0} - 1) + \xi(\tfrac{1}{R_0} - 1), \\ c &= (\tfrac{1}{R_0} - 1)(d + \xi). \end{aligned}$$

Simplifying the equation for P^*,

$$\begin{aligned} &\tfrac{\beta(N-P-C)C}{N} + \tfrac{\delta\beta PC}{N} - \gamma C - dC = 0, \\ &C(\gamma + d)\left[\tfrac{\beta(N-P-C)C}{N(\gamma+d)} + \tfrac{\delta\beta PC}{N(\gamma+d)} - 1\right] = 0, \\ &C(\gamma + d)\left[\tfrac{\beta}{(\gamma+d)} - \tfrac{\beta P}{N(\gamma+d)} - \tfrac{\beta C}{N(\gamma+d)} + \tfrac{\delta\beta P}{N(\gamma+d)} - 1\right] = 0, \\ &C(\gamma + d)\left[R_0 - \tfrac{R_0 P}{N}(1 - \delta) - \tfrac{R_0 C}{N} - 1\right] = 0, \\ &C(\gamma + d)R_0\left[1 - \tfrac{P}{N}(1 - \delta) - \tfrac{C}{N} - \tfrac{1}{R_0}\right] = 0, \\ &P(1 - \delta) = 1 - C - \tfrac{1}{R_0}, \\ &P^* = \tfrac{\frac{1}{R_0} + C^* - 1}{\delta - 1}. \end{aligned}$$

Appendix C

An appendix section is introduced to narrate the necessary description of basic reproduction number R_0 on the basis of next generation matrix.

The basic reproduction number R_0 is most important quantity in the study of epidemiology modeling and its control strategies. The quantity is defined as a new causes of infection due to a single infected individuals in susceptible populations. There are several methods to calculate R_0 for more then one infectious class [232] and in some time it may cumbersome to calculate more states, however next generation method provides an easy solution. In next generation method R_0 is defined as spectral radius of the next generation operator and classes are categorized in two compartments infected and non-infected. The value of R_0 using next generation can be obtained by calculating the value of V and F matrix, where V is a matrix for the rate of individuals transfer from compartment and F is a matrix of appearance of new infection in the compartment.

Model IPU_I has two infected classes, to get R_0, we use only two classes IU_I from system of equation 4.5. Linearizing the system, we obtain

$$\begin{bmatrix} \frac{dI}{dt} \\ \frac{dU_I}{dt} \end{bmatrix} = (F - V) \begin{bmatrix} I \\ U_I, \end{bmatrix}$$

$$F = \begin{pmatrix} \frac{\beta_1}{2^{32}} & \beta_2 \\ \frac{\beta_2 U^*}{N^*} & 0 \end{pmatrix} \qquad V = \begin{pmatrix} \rho + r_1 & 0 \\ 0 & r_2 \end{pmatrix}.$$

Basic reproduction number R_0 is the dominant eigenvalue of FV^{-1}, that is

$$FV^{-1} = \begin{pmatrix} \frac{\beta_1}{2^{32}(\rho+r_1)} & \frac{\beta_2}{r_2} \\ \frac{\beta_2 U^*}{N^*(\rho+r_1)} & 0 \end{pmatrix},$$

and R_0 with next generation matrix is

$$R_0 = \frac{\beta_1}{2^{32}(\rho+r_1)} + \sqrt{\left(\frac{\beta_1}{2^{32}(\rho+r_1)}\right)^2 + \frac{4{\beta_2}^2 U^*}{N^*(\rho+r_1)r_2}}.$$