MINISTRY OF EDUCATION
AND TRAINING

VIETNAM ACADEMY OF
SCIENCE AND TECHNOLOGY

GRADUATE UNIVERSITY OF SCIENCE AND TECHNOLOGY

Nguyen Phuong Dong

ON THE STUDY OF SOME FUZZY FRACTIONAL MALWARE PROPAGATION MODELS AND APPLICATION IN WIRELESS SENSOR NETWORK

SUMMARY OF APPLIED MATHEMATICS DOCTORAL THESIS

Hanoi - 2023

The doctoral thesis has been completed at: Graduate University of Science and Technology - Vietnam Academy of Science and Technology

Supervisor 1: Assoc. Prof. Dr. Hoang Viet Long, Faculty of Information Technology, University of Technology-Logistic of Public Security

Supervisor 2: Assoc. Prof. Dr. Nguyen Long Giang, Institute of Information and Technology, Vietnam Academy of Science and Technology

Reviewer 1: Assoc. Prof. Dr. Nguyen Ngoc Anh

Reviewer 2: Assoc. Prof. Dr. Le Hoang Son

Reviewer 3: Assoc. Prof. Dr. Vu Trong Luong

The doctoral thesis shall be defended in front of the Thesis Committee at Academy Level at Graduate University of Science and Technology - Vietnam Academy of Science and Technology at ... ^{h} ... date ... month ... year 2023.

This thesis can be found at:

- The Library of Graduate University of Science and Technology
- The National Library of Vietnam

INTRODUCTION

1. The rational of the study

For the goal of understanding the characteristics and predicting the spread of malicious code on network systems and inspired by similarities with disease infections in biological populations, the research direction uses differential equation models to model and analyze the spread of malicious code on the network has recently received a lot of attentions. It is a fact that signal transmission processes on the network always depend significantly on the characteristics of environment, structure, and properties of the conducting materials. In addition, the propagation mechanism of malware programs is to take advantage of signal transmission between network nodes to replicate, spread and cause the spread of malicious code on the network. During a long history of development, fractional calculus and fractional dynamical systems described by fractional differential equations have been shown a great ability to model and fit data better than integer-order models. For example, V.D. Djordjevíc et al (2003), M. Di Paola et al (2011), N.H. Can et al (2020). Therefore, there are a number of recent studies that have applied fractional dynamic systems to establish epidemic models and predict the spread of malicious code on network systems such as J. Huo and H. Zhao (2016), J. Singh et al. (2018), J.R. Graef et al. (2020), Y. Chen et al. (2021), X. Fu and J. Wang (2022).

Traffic regulation systems, environmental and ecological monitoring, information systems or biological networks, etc. ... are often better described by heterogeneous complex network models. Recently, many researchers have used mathematical models based on complex network structures as an effective tool to study the mechanism of malware spread on the network, predicting the evolution and impact of such malware programs on network systems. In classic models, authors often ignore the factor of network-size and assume that all nodes in network are well-mixed and, therefore, the rate of contact causing infection are the same for whole network, i.e., roles of all nodes in the network are similar. This assumption makes our study simpler and easier to handle, but it is not reasonable when in reality, many types of complex networks such as the Internet, Facebook, Instagram, sensor networks and biological networks, etc., always have very large number of nodes, and the interaction capabilities of different nodes in the network are obviously not the same. Therefore, for more realistic descriptions and evaluations, we need to consider the heterogeneity in contact of complex networks when establishing mathematical models of malware propagation on the network. The research of R. Pastor-Satorras and A. Vespignani (2001) is known as a pioneering work for studying mathematical models of malware propagation on complex heterogeneous networks. In particular, this work proposes a network-based SIS malware propagation model and presents a detailed study of basic epidemiological characteristics and numerical solution results for the proposed model. With the motivation from this research, many studies on malware propagation models based on complex networks

were conducted and a lot of noticeable results were obtained such as C.H. Li et al. (2014), Y. Zan et al. (2014), S. Huang et al. (2017), H.F. Huo et al. (2019), C. Li and A.M. Yousef (2019), K. Li et al. (2019), S. Hosseini and A. Zandvakili (2022), etc.

On the other hand, lack of information about parameters and input data due to calculation errors, limitations of measuring equipment or complicated and unnecessary precise measurement and calculation is a problem often encountered in practice. In addition, because the environment of transmission processes always contains elements of uncertainty, we need to take into account quantities representing uncertainty when establishing models, solving and interpreting problems in natural environments. Since then, the research direction combining fuzzy set theory, fuzzy logic or fuzzy analysis in the study of modeling the processes of malware spread on the network appeared and had noticeable results. For example, the studies on malware propagation models described by differential equations with fuzzy parameters: E. Massad et al. (2008), P.K. Mondal et al (2015), S.K. Nandi et al (2018), S. Adak and S. Jana (2022). The novelty of these work is to consider the speed of spreading malicious code, the malicious code handling function contains fuzzy parameters and build the concepts of fuzzy expected value of infection compartment, fuzzy basic reproduction number. However, these documents only introduced a general malware propagation models with fuzzy parameters or initial conditions, detailed analytical properties and epidemiological characteristics of the proposed malware propagation models have not been properly developed and discussed. In particular, there are currently not many studies on malware propagation models that accept fuzzy-valued expression. Another research direction on malware propagation models has combined large-scale differential systems and fuzzy set theory - fuzzy logic as Zan et al. (2014), Hosseini and Zandvakili (2022). These studies used fuzzy-rule bases to establish the interaction mechanism between compartments and determine the model's parameters.

Motivated by aforesaid, PhD student realize the prospect of development of the research direction on modeling the spread of malware propagation on wireless sensor networks based on differential equations models. Additionally, in order to better describe malware propagation in the real-world scenario with uncertainties in parameters and data, malware propagation models with fuzzy parameters or fuzzy rule-based malware propagation models are also shown to be a topic of scientific and practical significance. Furthermore, through the overall research process, the PhD student also realized that because the wireless sensor network has a complex and heterogeneous network structure, there is a great potential of studying the malware propagation on wireless sensor networks based on the use of network-based differential systems, that combined with fuzzy set theory and fractional calculus. These research ideas were initially implemented in the doctoral thesis with the expectation of contributing to studies on modeling and qualitative properties of malware spreading processes on wireless sensor networks.

2. The aim, object and scope of the study

2.1. The aim of the study

The thesis studies some mathematical models describing the spread of malware programs on a complex heterogeneous networks (wireless sensor network). The three main goals of the thesis include:

- Propose some mathematical models describing the spread of malware programs on complex heterogeneous networks.
- Determine the threshold value for malware propagation $\mathfrak{R}_0$.
- Study some qualitative properties such as: the unique existence and positivity of solutions to the Cauchy problem for proposed malware propagation models, the existence of equilibrium points, asymptotic stability, bifurcation analysis and stabilization control problem.

2.2. The object and scope of the study

The thesis focuses on study some mathematical models describing the spread of malware programs on complex heterogeneous networks with the following objects and scope of research:

- Mathematical models of malware propagation on complex heterogeneous networks described by fractional differential systems with fuzzy parameters or established by fuzzy logic;
- Qualitative properties such as positivity, malware propagation threshold value, asymptotic stability and control problem for the proposed malware propagation models.

3. The research contents

The thesis research is aimed at the 3 classes of malware propagation models with the corresponding research contents as follows:
The model 1: Fuzzy fractional SIQR malware propagation model. For this model, the thesis establish the theoretical foundation of fractional calculus in the sense of Caputo Atangana−Baleanu for fuzzy-valued functions and studies the existence and representation of integral solutions of Cauchy problem to fuzzy fractional SIQR malware propagation model.
The model 2: Fractional network-based SE_1E_2IQR malware propagation model whose transmission function is determined by fuzzy logic. For this model, the thesis studies the existence and uniqueness of positive solution and asymptotic stability analysis.
The model 3: Controlled fractional network-based SIRS malware propagation model with saturated treatment function. For this model, the thesis studies the existence and uniqueness

of positive solution, asymptotic stability analysis and the stabilization problem for the proposed malware propagation model based on fractional interconnected Takagi-Sugeno fuzzy systems.

4. The research method

The doctoral thesis has combined the tools of fractional calculus, fuzzy analysis and fuzzy set theory, stability theory for fractional dynamical systems and techniques of matrix analysis and linear matrix inequality.

5. The obtained results

The thesis studies some qualitative properties of mathematical models describing the spread of malicious code on wireless sensor networks. The achieved results are as follows:

(i) Study a fractional SIQR malware propagation model with fuzzy data that uses the concepts of fuzzy fractional Caputo-Atangana-Baneanu derivative (Definition 2.1) and fuzzy fractional Riemann-Liouville Atangana-Baleanu integral (Definition 2.2), prove the existence and uniqueness of fuzzy integal solutions of the proposed malware propagation model (Theorem 2.3 and Theorem 2.4) and illustrate the obtained results by some numerical simulations.

(ii) Study a fractional network-based SE_1E_2IQR malware propagation model whose transmission function is determined by fuzzy-rule base and prove some qualitative properties of the proposed malware propagation model such as the positiveness of solution, evaluation of basic reproduction number $\mathfrak{R}_0$ (The formula (3.4), the sensitivity analysis of $\mathfrak{R}_0$ w.r.t. parameters, the local and global asymptotic stability of the malware-free equilibrium $\mathbf{P}_0$ (Theorem 3.3 and Theorem 3.4) and forward bifurcation analysis at $\mathfrak{R}_0 = 1$ (Theorem 3.5)

(iii) Study a controlled fractional network-based SIRS malware propagation model with saturated treatment function and its stabilization problem for the proposed malware propagation model based on fractional interconnected Takagi-Sugeno fuzzy system. The obtained results consists of the positiveness of solution, evaluation of basic reproduction number $\mathfrak{R}_0$ (The formula (4.3)), the sensitivity analysis of $\mathfrak{R}_0$ w.r.t. parameters, the local and global asymptotic stability of the malware-free equilibrium $\mathbf{P}_0$ (Theorem 4.3 and Theorem 4.4), backward bifurcation analysis at $\mathfrak{R}_0 = 1$ (Theorem 4.5) and some sufficient conditions in form LMIs for the stabilizability of the malware-free equilibrium $\mathbf{P}_0$ (Theorem 4.6).

6. The structure of the thesis

In addition to the Introduction, Conclusion and References sections, the thesis layout includes 4 chapters:

Chapter 1: This is a preparatory knowledge chapter that includes an overview of fractional derivative and integrals, qualitative theory of fractional differential equations, fuzzy set theory and analysis of fuzzy-valued functions, Takagi-Sugeno fuzzy system and scale-free network.

Chapter 2: This chapter studies the uncertain behavior of the fuzzy fractional SIQR malware propagation model that describes the spread of malware programs across sensor networks. For this aim, the thesis presents results on fractional derivatives and integrals in the Atangana-Baleanu sense and applies them in the investigation of Cauchy problem to fuzzy fractional SIQR malware propagation model that mathematically modelled by fuzzy fractional differential equations.

Chapter 3: This chapter presents a study on fractional network-based SE_1E_2IQR malware propagation model whose transmission function is based on fuzzy rules. The obtained results includes establishing a malware propagation model whose transmission function is based on fuzzy rules, investigates the qualitative properties of the proposed model and presents some evaluations and simulation calculations.

Chapter 4: In this chapter, the thesis studies a controlled fractional network-based SIRS malware propagation model with a saturated treatment function. The obtained results are as follows: establishing a network-based malware propagation model, investigating some qualitative properties of the proposed model and its stabilization control problem based on fractional interconnected Takagi-Sugeno fuzzy system.

Chapter 1

PRELIMINARIES

This chapter presents some theoretical results and necessary lemmas for some next chapters, that are referred from Takagi and Sugeno (1985), Barabási and Albert (1999), Diethhelm (2010), Bede (2013), Atangana and Baleanu (2016). The structure of this chapter is as follows:

1.1. Some notes on fractional analysis

In this section, we recall some fundamental concepts and properties of fractional calculus and fractional differential systems.

1.2. Fuzzy sets and fuzzy analysis

This section presents some notes on fuzzy sets theory, fuzzy rule base and analysis of fuzzy-valued functions.

1.3. Takagi-Sugeno fuzzy system

In this section, we present the theoretical results on Takagi-Sugeno fuzzy systems and analytical method to construct Takagi-Sugeno fuzzy systems for nonlinear dynamical systems.

1.4. Interconnected fractional Takagi-Sugeno fuzzy system

This section introduces the structure of Takagi-Sugeno fuzzy systems for scale-free networks or large-scale networks, whose local models are governed fractional differential systems.

1.5. The scale-free network

This section presents a general discussion on Barabási-Albert scale-free network and energy-aware Barabási-Albert scale-free network to describe the structure of wireless sensor network.

Chapter 2

THE FRACTIONAL SIQR MALWARE PROPAGATION MODEL WITH FUZZY DATA

This chapter focuses on describing the uncertain behavior of malware propagation on wireless sensor networks based on the fuzzy fractional differential system model. The results of Chapter 2 are referenced from the publication [**P1**].

2.1. The formulation of fuzzy fractional SIQR malware propagation model

In this, the thesis use the fuzzy fractional differential system model consisting of 4 variable function (S-I-Q-R) corresponding to 4 compartments of malware propagation model to characterize the propagation of malware programs on wireless sensor networks with uncertainty. Denote $S(t)$, $I(t)$, $Q(t)$ and $R(t)$ by densities of susceptible, infectious, quarantined and recovered nodes in time t, respectively. Then, the malware propagation model that describes the spread of malicious objects is given in following diagram (see Figure 3.1).

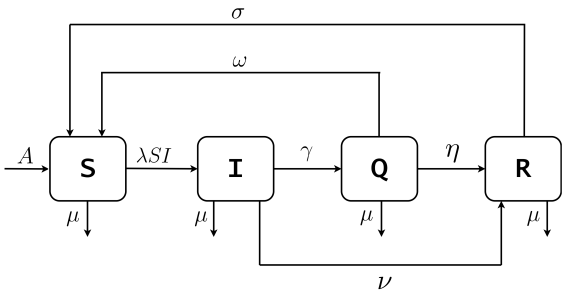

Figure 2.1: The flowchart of SIQR malware propagation model

In order to protect sensor networks against malicious attacks, we need to understand the epidemiological characteristics of the spread. In this chapter, the thesis approaches research on the mechanism of malware spread based on mathematical models. Specifically, the thesis assumes that every sensor node in compartments **(S)**, **(I)**, **(Q)** or **(R)** leaves the network with rate μ due to energy depletion. The uncertain dynamics of malware propagation on wireless sensor networks is described by the following system of differential equations:

$$\begin{cases} {}^{abc}\mathscr{D}_{+}^{\beta} S(t) &= A - \lambda S(t)I(t) + \omega Q(t) + \sigma R(t) - \mu S(t) \\ {}^{abc}\mathscr{D}_{+}^{\beta} I(t) &= \lambda S(t)I(t) - (\nu + \gamma + \mu)I(t) \\ {}^{abc}\mathscr{D}_{+}^{\beta} Q(t) &= \gamma I(t) - (\eta + \mu + \omega)Q(t) \\ {}^{abc}\mathscr{D}_{+}^{\beta} R(t) &= \nu I(t) + \eta Q(t) - (\sigma + \mu)R(t) \end{cases} \tag{2.1}$$

subject to the initial conditions $S(0)=S_0$, $I(0)=I_0$, $Q(0)=Q_0$, $R(0)=R_0$.

2.2. Caputo Atangana-Baleanu fractional derivative and Riemann-Liouville Atangana-Baleanu fractional integral for fuzzy-valued functions

Definition 2.1. Assume that $f(t)$ belongs to class $C^1([0,b],\mathscr{E})$. Then, the Caputo Atangana - Baleanu fractional derivative of order $\beta\in(0,1)$ of fuzzy-valued function $f(t)$ is

$$^{abc}\mathscr{D}_{+}^{\beta}f(t):=\frac{\Phi(\beta)}{1-\beta}\int_0^t\mathbb{E}_{\beta}\left[-\beta\frac{(t-\tau)^{\beta}}{1-\beta}\right]f'_{gH}(\tau)d\tau.$$

Proposition 2.1. *Assume that $f\in C^1([0,b],\mathscr{E})$ and its $\alpha-$cuts can be represented in parametric form $[f(t)]^{\alpha}=[f_{\alpha}^{-}(t),f_{\alpha}^{+}(t)]$ for each $t\in[0,b]$ and $\alpha\in[0,1]$. Then,*

(i) *If f is gH-differentiability in type 1 then* $\left[^{abc}\mathscr{D}_{+}^{\beta}f(t)\right]^{\alpha}=\left[^{abc}\mathrm{D}_{+}^{\beta}f_{\alpha}^{-}(t),{}^{abc}\mathrm{D}_{+}^{\beta}f_{\alpha}^{+}(t)\right].$

(ii) *If f is gH-differentiability in type 2 then* $\left[^{abc}\mathscr{D}_{+}^{\beta}f(t)\right]^{\alpha}=\left[^{abc}\mathrm{D}_{+}^{\beta}f_{\alpha}^{+}(t),{}^{abc}\mathrm{D}_{+}^{\beta}f_{\alpha}^{-}(t)\right].$

Definition 2.2. Assume that $f(t)$ belongs to class $L^1([0,b],\mathscr{E})$. Then, the Riemann−Liouville Atangana−Baleanu fractional integral of order $\beta\in(0,1]$ of fuzzy-valued function $f(t)$ is

$$^{ab}\mathcal{I}_{+}^{\beta}f(t):=\frac{1-\beta}{\Phi(\beta)}f(t)+\frac{\beta}{\Phi(\beta)\Gamma(\beta)}\int_0^t(t-\tau)^{\beta-1}f(\tau)d\tau=\frac{1-\beta}{\Phi(\beta)}f(t)+\frac{\beta}{\Phi(\beta)}\mathcal{I}_{+}^{\beta}f(t).$$

In addition, for each $\alpha\in[0,1]$, $\alpha-$cut of $^{ab}\mathcal{I}_{+}^{\beta}f(t)$ is given by

$$\left[^{ab}\mathcal{I}_{+}^{\beta}f(t)\right]^{\alpha}=\left[^{ab}\mathrm{I}_{+}^{\beta}f_{\alpha}^{-}(t),{}^{ab}\mathrm{I}_{+}^{\beta}f_{\alpha}^{+}(t)\right].$$

Remark 2.1. In some special cases of β, the Riemann−Liouville Atangana−Baleanu fractional integral is identified with well-known concept:

(i) If $\beta=0$ then the Riemann−Liouville Atangana−Baleanu fractional integral becomes

$$^{ab}\mathcal{I}_{+}^{0}f(t)=\frac{1-0}{\Phi(0)}f(t)+\frac{0}{\Phi(0)\Gamma(0)}\int_0^t(t-\tau)^{-1}f(\tau)d\tau=f(t).$$

(ii) If $\beta=1$ then the Riemann−Liouville Atangana−Baleanu fractional integral becomes

$$^{ab}\mathcal{I}_{+}^{1}f(t)=\frac{1-1}{\Phi(1)}f(t)+\frac{1}{\Phi(1)\Gamma(1)}\int_0^t(t-\tau)^{1-1}f(\tau)d\tau=\int_0^t f(\tau)d\tau.$$

Theorem 2.1. *Let $\beta\in(0,1)$ and $f:[0,T]\subset\mathbb{R}\to\mathscr{E}$ be gH-differentiability with no switching point in $[0,T]$. Then, If $\beta=0$ then the Riemann−Liouville Atangana−Baleanu fractional integral and Caputo Atangana−Baleanu fractional derivative of $f(t)$ satisfies*

$$^{ab}\mathcal{I}_{+}^{\beta}\left(^{abc}\mathscr{D}_{+}^{\beta}f(t)\right)=f(t)\ominus_{gH}f(0),\qquad t\in[0,T].$$

Proposition 2.2. *Let $f:[0,b]\subset\mathbb{R}\to\mathscr{E}$ belong to $C^1([0,b],\mathscr{E})$. Then, fuzzy Laplace transform of Caputo Atangana−Baleanu fractional derivative $^{abc}\mathscr{D}_{+}^{\beta}f(t)$ of the function $f(t)$ is given by*

$$\tilde{\mathscr{L}}\left\{^{abc}\mathscr{D}_{+}^{\beta}f(t)\right\}(s)=\begin{cases}\dfrac{\Phi(\beta)}{1-\beta}\dfrac{s^{\beta}\tilde{\mathscr{L}}\{f(t)\}(s)\ominus s^{\beta-1}f(0)}{s^{\beta}+\frac{\beta}{1-\beta}} & \text{if } f \text{ is gH-differentiability in type 1}\\ \dfrac{(-1)\Phi(\beta)}{1-\beta}\dfrac{s^{\beta-1}f(0)\ominus s^{\beta}\tilde{\mathscr{L}}\{f(t)\}(s)}{s^{\beta}+\frac{\beta}{1-\beta}} & \text{if } f \text{ is gH-differentiability in type 2.}\end{cases}$$

Proposition 2.3. *Assume that $f : [0,\infty) \to \mathscr{E}$ is continuous. Then, for each $t > 0$, we have*

$$\tilde{\mathscr{L}}\left\{\int_0^t \mathbb{E}_\beta\left[-\beta\frac{(t-\tau)^\beta}{1-\beta}\right] f(\tau)d\tau\right\}(s) = \frac{s^{\beta-1}}{s^\beta + \frac{\beta}{1-\beta}}\tilde{\mathscr{L}}\{f(t)\}(s).$$

2.3. The existence and uniqueness of fuzzy solutions to Cauchy problem for fuzzy fractional differential systems under gH-differentiability

In this section, the doctoral thesis studies the existence and uniqueness of fuzzy integral solutions to Cauchy problem for fuzzy fractional differential systems under gH-differentiability and Caputo Atangana−Baleanu fractional derivative:

$$\begin{cases} {}^{abc}\mathscr{D}_+^\beta x(t) &= \mathrm{F}\left(t, x(t)\right) \\ x(0) &= x_0, \end{cases} \tag{2.2}$$

where ${}^{abc}\mathscr{D}_+^\beta x(t)$ is the Caputo Atangana−Baleanu fractional derivative of $x(t)$, $t \in J = [0,T]$, $x_0 \in \mathscr{E}^n$ and $\mathrm{F} : [0,T] \times \mathscr{E}^n \to \mathscr{E}^n$ is a fuzzy vector-valued function satisfying the following hypotheses:

(HF1) The fuzzy vector-valued function $\mathrm{F}(\cdot,\xi) : [0,T] \to \mathscr{E}^n$ is strongly measurable for each $\xi \in \mathscr{E}^n$ and $\mathrm{F}(t,\cdot) : \mathscr{E}^n \to \mathscr{E}^n$ is continuous for a.e. $t \in [0,T]$;

(HF2) There exists a matrix M_0 such that $\mathbb{D}_n\left(\mathrm{F}(t,\xi), \hat{\mathbf{0}}\right) \leq \mathrm{M}_0\mathbb{D}_n(\xi, \hat{\mathbf{0}})$ for all $\xi \in \mathscr{E}^n$.

(HF3) There exists a matrix M_1 such tha $\mathbb{D}_n\left(\mathrm{F}(t,\xi), \mathrm{F}(t,\overline{\xi})\right) \leq \mathrm{M}_1\mathbb{D}_n(\xi,\overline{\xi})$ for all ξ, $\overline{\xi} \in \mathscr{E}^n$.

Consider the space

$$C\left([0,T],\mathscr{E}^n\right) = \{\varphi : [0,T] \to \mathscr{E}^n : \varphi(t) \text{ is continuous on } [0,T]\}$$

endowed with the weighted metric $\mathcal{H}_\lambda(\varphi,\psi) = \sup_{[0,T]}\left\{\mathbb{D}_n(\varphi(t),\psi(t))e^{-\lambda t}\right\}$ with a large enough $\lambda > 0$. The space $\left(C\left([0,T],\mathscr{E}^n\right), \mathcal{H}_\lambda\right)$ is complete. Assume that all components of $x(t)$ have a sane type of gH-differentiability with no switching point on $J = [0,T]$. We consider the following theorem:

Theorem 2.2. *Assume that $x \in C\left([0,T],\mathscr{E}^n\right)$ satisfies Cauchy problem (2.2).*

(i) *If $x(t)$ is gH-differentiable in type 1 then it satisfies the following integral equation*

$$x(t) = x_0 + \frac{1-\beta}{\Phi(\beta)}\mathrm{F}(t,x(t)) + \frac{\beta}{\Gamma(\beta)\Phi(\beta)}\int_0^t (t-\tau)^{\beta-1}\mathrm{F}(\tau,x(\tau))d\tau. \tag{2.3}$$

(ii) *If $x(t)$ is gH-differentiable in type 2 then it satisfies the following integral equation*

$$x(t) = x_0 \ominus (-1)\left[\frac{1-\beta}{\Phi(\beta)}\mathrm{F}(t,x(t)) + \frac{\beta}{\Gamma(\beta)\Phi(\beta)}\int_0^t (t-\tau)^{\beta-1}\mathrm{F}(\tau,x(\tau))d\tau\right]. \tag{2.4}$$

Definition 2.3. Let $x : [0,T] \subset \mathbb{R} \to \mathscr{E}^n$ be continuous. Then, we have

(i) The function $x(t)$ is said to be fuzzy integral solution of type (i) of Cauchy problem (2.2) if it satisfies the integral equation (2.3).

(ii) The function $x(t)$ is said to be fuzzy integral solution of type (ii) of Cauchy problem (2.2) if it satisfies the integral equation (2.4).

Theorem 2.3. *If the hypotheses* ***(HF1)***, ***(HF2)***, ***(HF3)*** *are fulfilled and the spectral radii of matrices* $\frac{(1-\beta)}{\Phi(\beta)}\mathrm{M}_0$ *and* $\frac{(1-\beta)}{\Phi(\beta)}\mathrm{M}_1$ *are less than* 1 *then Cauchy problem (2.2) has a unique fuzzy integral solution of type (i) defined in* $[0,T]$.

For each $x \in C([0,T],\mathscr{E}^n)$, consider an operator $\mathscr{F}[x]$ given by

$$\mathscr{F}[x](t) = x_0 \ominus \left[\frac{(1-\beta)}{\Phi(\beta)}\mathrm{F}(t,x(t)) + \frac{\beta}{\Gamma(\beta)\Phi(\beta)}\int_0^t (t-\tau)^{\beta-1}\mathrm{F}(\tau,x(\tau))d\tau\right]. \tag{2.5}$$

Denote $\hat{C}\left([0,T],\mathscr{E}^n\right)$ by the space of fuzzy-valued functions $x \in C([0,T],\mathscr{E}^n)$ such that the equality (2.5) is true for each $t \in [0,T]$.

Theorem 2.4. *Assume that* $\hat{C}\left([0,T],\mathscr{E}^n\right) \neq \emptyset$, *the hypotheses* ***(HF1)***, ***(HF2)***, ***(HF3)*** *are fulfilled and the spectral radii of matrices* $\frac{(1-\beta)}{\Phi(\beta)}\mathrm{M}_0$ *and* $\frac{(1-\beta)}{\Phi(\beta)}\mathrm{M}_1$ *are less than* 1. *Then, Cauchy problem (2.2) has a unique fuzzy integral solution of type (ii) defined in* $[0,T]$.

Remark 2.2. We assume that all components of the solution vector $x(t)$ has the same gH-differentiable type and has no switching point on $J=[0,T]$. In general, if the components of $x(t) = \begin{pmatrix} x_1(t) & \cdots & x_n(t)\end{pmatrix}^\top$ has different types of gH-differentiability on J, the existence and uniqueness of fuzzy solution presented in Theorem 2.3 and Theorem 2.4 still holds.

2.4. Discussions

(a) The thesis simulates uncertain behavior of fuzzy solution of fuzzy fractional SIQR malware propagation model (2.1) with parameters

$$\begin{array}{llll} A = 0.2 & \mu = 0.2 & \lambda = 0.3 & \nu = 0.15 \\ \omega = 0.008 & \sigma = 0.01 & \gamma = 0.2 & \eta = 0.008 \end{array}$$

and fuzzy initial conditions $S_0 = (0.63, 0.64, 0.65)$, $I_0 = (0.23, 0.24, 0.25)$, $Q_0 = (0.09, 0.095, 0.1)$ and $R_0 = (0,0,0)$. Figure 2.2 presents the plot of numerical solution of fuzzy fractional SIQR malware propagation model with some different values of β. For these above parameters, we can calculate the threshold value $\mathfrak{R}_0 = 0.545 < 1$, that is, according to epidemiological theory, the malware-free equilibrium is asymptotically stable. In fact, from Figure 2.2, we can see that the infectious component $I(t)$ of the solution tends to approach 0 over time, meaning that malicious codes have can be removed from the network.

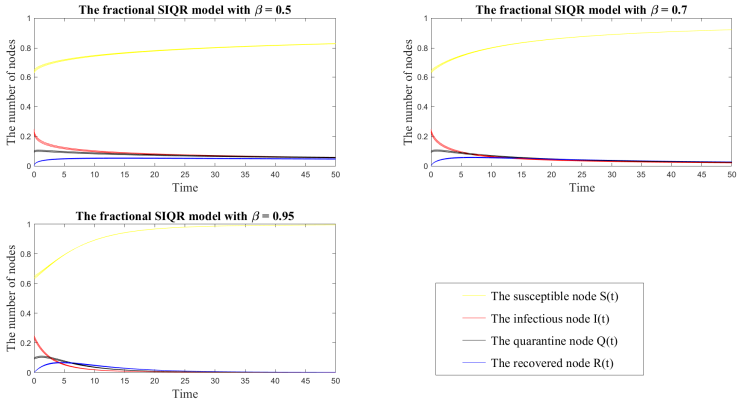

Figure 2.2: The plot of numerical solution of fuzzy fractional SIQR malware propagation model in Case (a)

(b) The thesis simulates uncertain behavior of fuzzy solution of fuzzy fractional SIQR malware propagation model (2.1) with parameters

$$A = 0.2 \qquad \mu = 0.2 \qquad \lambda = 0.9 \qquad \nu = 0.15$$
$$\omega = 0.008 \qquad \sigma = 0.01 \qquad \gamma = 0.2 \qquad \eta = 0.008$$

and fuzzy initial conditions $S_0 = (0.63, 0.64, 0.65)$, $I_0 = (0.23, 0.24, 0.25)$, $Q_0 = (0.09, 0.095, 0.1)$ and $R_0 = (0, 0, 0)$. Figure 2.3 presents the plot of numerical solution of fuzzy fractional SIQR malware propagation model with some different values of β. For these above parameters, we can calculate the threshold value $\mathfrak{R}_0 = 1.636 > 1$. This implies malware-free equilibrium is unstable and hence, the spread of malware programs will continue. Indeed, according to Figure 2.3, we can see that the behavior of the infectious state function $I(t)$ approaches a positive value (component I^* of the endemic equilibrium) as time increases.

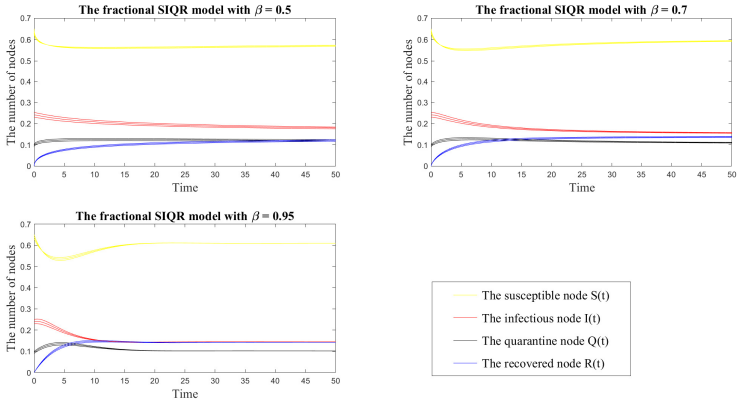

Figure 2.3: The plot of numerical solution of fuzzy fractional SIQR malware propagation model in Case (b)

Chapter 3

THE FRACTIONAL NETWORK-BASED SE_1E_2IQR MALWARE PROPAGATION MODEL WITH FUZZY-RULE BASED TRANSMISSION FUNCTION

In order to take into account the heterogeneity in contact of network's nodes and uncertainty factors in malware propagation, this chapter focuses on a fractional network-based SE_1E_2IQR malware propagation model with fuzzy-rule based transmission function, where the proposed network-based model introduces a quarantine compartment (Q) and exposed group include two compartments: E_1 (Type 1-Exposed compartment) and E_2 (Type 2-Exposed compartment). This chapter is written based on the publication **[P2]**.

3.1. The model's formulation

In this section, the thesis regard a wireless sensor network as energy-aware Barabási-Albert free-scale network and describes the propagation mechanism of malicious code on the network based on mathematical modeling. We divide the total number of network nodes into n groups based on the number of links that a node in the group has per unit of time. Denote $S_k(t)$, $E_{1,k}(t)$, $E_{2,k}(t)$, $I_k(t)$, $Q_k(t)$ and $R_k(t)$ by the density of Susceptible nodes, Type 1-Exposed nodes, Type 2-Exposed nodes, Infectious, Quarantined and Recovered of degree k for each $k = 1, 2, \ldots, n$, respectively. The malware propagation on the network can be described in the following diagram:

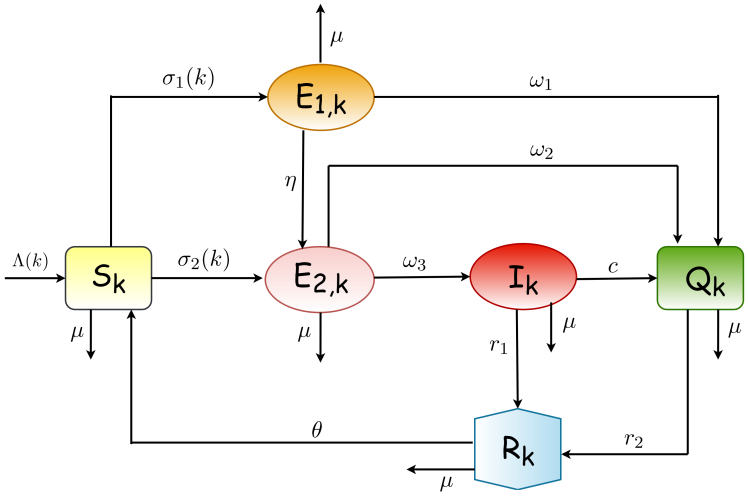

Figure 3.1: The flowchart of the network-based SE_1E_2IQR malware propagation model

It is a fact that the speed of information transmission on the network is directly affected by

uncertain factors such as geography or climate conditions. Therefore, the thesis proposes to use the linguistic variable q ($q \in \{\text{high, medium, low}\}$) to represent uncertain factors occurring when modeling the malware propagation model. In particular, the thesis assigns three linguistic variables "Low", "Medium", "High" with fuzzy values corresponding to fuzzy rules and uses a fuzzy inference system to derive these rules into the proposed malware propagation model in the form of propagating constant M_q. Indeed, consider three fuzzy numbers $A_1 = (0, 0, 0.3, 0.4)$, $A_2 = (0.3, 0.5, 0.7)$ and $A_3 = (0.6, 0.7, 1, 1)$ representing the terms "low", "medium", "high" and using two triangular fuzzy numbers $B_1 = (0, 0.3, 0.6)$ and $B_2 = (0.4, 0.7, 1.0)$ to determine whether output state belong to the Type 1-Exposed state or Type 2-Exposed state.

Let x represent the density of infectious node, y represent the node's state change rate, and z represent the output state of each rule. Now, the thesis proposes a MISO fuzzy system with 9 rules as follows:

Rule 1: If x is "LOW" and y is "LOW" then z belongs to E_1.

Rule 2: If x is "LOW" and y is "MEDIUM" then z belongs to E_1.

Rule 3: If x is "MEDIUM" and y is "LOW" then z belongs to E_1.

Rule 4: If x is "MEDIUM" and y is "MEDIUM" then z belongs to E_2.

Rule 5: If x is "LOW" and y is "HIGH" then z belongs to E_2.

Rule 6: If x is "MEDIUM" and y is "HIGH" then z belongs to E_2.

Rule 7: If x is "HIGH" and y is "LOW" then z belongs to E_2.

Rule 8: If x is "HIGH" and y is "MEDIUM" then z belongs to E_2.

Rule 9: If x is "HIGH" and y is "HIGH" then z belongs to E_2.

Based on the diagram in Figure 3.1, the thesis establish a mathematical model describing the spread of malware programs between six compartments (S), (E_1), (E_2) , (I), (Q) and (R) in wireless sensor network. In addition, with the goal of demonstrating the non-locality and memorability of the data diffusion process, the thesis use Caputo fractional derivative to establish a fractional large-scale differential equation model, called the fractional network-based SE_1E_2IQR malware propagation model. In particular, for each $k = \overline{1, n}$, we consider

$$\begin{cases} {}_0^C\mathfrak{D}_t^\beta S_k(t) &= \Lambda(k) - (\sigma_1(k) + \sigma_2(k))\, S_k(t)\Theta(t) - \mu S_k(t) + \theta R_k(t) \\ {}_0^C\mathfrak{D}_t^\beta E_{1,k}(t) &= \sigma_1(k) S_k(t)\Theta(t) - (\eta + \omega_1 + \mu)\, E_{1,k}(t) \\ {}_0^C\mathfrak{D}_t^\beta E_{2,k}(t) &= \sigma_2(k) S_k(t)\Theta(t) - (\mu + \omega_2 + \omega_3)\, E_{2,k}(t) + \eta E_{1,k}(t) \\ {}_0^C\mathfrak{D}_t^\beta I_k(t) &= \omega_3 E_{2,k}(t) - (\mu + c + r_1) I_k(t) \\ {}_0^C\mathfrak{D}_t^\beta Q_k(t) &= \omega_1 E_{1,k}(t) + \omega_2 E_{2,k}(t) + c I_k(t) - (r_2 + \mu) Q_k(t) \\ {}_0^C\mathfrak{D}_t^\beta R_k(t) &= r_1 I_k(t) + r_2 Q_k(t) - (\mu + \theta) R_k(t), \end{cases} \tag{3.1}$$

with initial condition

$$S_k(0) = S_k^0,\ E_{1,k}(0) = E_{1,k}^0,\ E_{2,k}(0) = E_{2,k}^0,\ I_k(0) = I_k^0,\ Q_k(0) = Q_k^0,\ R_k(0) = R_k^0, \tag{3.2}$$

where $\sigma_1(k), \sigma_2(k)$ are the degree-dependent transmission rates given by $\sigma_1(k) = \sigma_1 k$, $\sigma_2(k) = \sigma_2 k$, respectively. In addition, we assume that

$$N_k(t) = \frac{\Lambda(k)}{\mu}\mathbb{E}_\beta(-\mu t^\beta) + \frac{\Lambda(k)}{\mu}\left[1 - \mathbb{E}_{\beta,1}(-\mu t^\beta)\right] = \frac{\Lambda(k)}{\mu} := b_k.$$

The function $\Theta(t)$ represents the probability that a given link connects to an infectious node given by $\Theta(t) = \frac{M_q}{\langle k\rangle}\sum_{i=1}^{n}\frac{\nu(i)}{b_i}\mathbb{P}(i)I_i(t)$, where $\mathbb{P}(i)$ is the probability that a randomly chosen node has degree i, $\langle k\rangle = \sum_{i=1}^{n} i\mathbb{P}(i)$ represents the average degree of the network , $M_q \in [0,1]$ is the output parameter of the MISO system deduced from fuzzy rules for the linguistic variable q, the function $\nu(i) = i$ represents the number of average links that an infectious node of degree i will spread malware programs to other nodes.

3.2. The qualitative properties of the proposed malware propagation model

3.2.1. The existence of positively invariant set

Denote $\mathbf{x}^k(t) = \begin{pmatrix} E_{1,k}(t) & E_{2,k}(t) & I_k(t) & S_k(t) & Q_k(t) & R_k(t)\end{pmatrix}^\top$, $\mathbf{x}(t) = \begin{pmatrix}\mathbf{x}^1(t) & \cdots & \mathbf{x}^n(t)\end{pmatrix}^\top$

$$f(\mathbf{x}^k(t)) = \begin{pmatrix} f_1(\mathbf{x}^k(t)) \\ f_2(\mathbf{x}^k(t)) \\ f_3(\mathbf{x}^k(t)) \\ f_4(\mathbf{x}^k(t)) \\ f_5(\mathbf{x}^k(t)) \\ f_6(\mathbf{x}^k(t))\end{pmatrix} = \begin{pmatrix} \sigma_1(k)S_k(t)\Theta(t) - (\eta+\omega_1+\mu)\,E_{1,k}(t) \\ \sigma_2(k)S_k(t)\Theta(t) - (\mu+\omega_2+\omega_3)\,E_{2,k}(t) + \eta E_{1,k}(t) \\ \omega_3 E_{2,k}(t) - (\mu+c+r_1)I_k(t) \\ \Lambda(k) - (\sigma_1(k)+\sigma_2(k))\,S_k(t)\Theta(t) - \mu S_k(t) + \theta R_k(t) \\ \omega_1 E_{1,k}(t) + \omega_2 E_{2,k}(t) + cI_k(t) - (r_2+\mu)Q_k(t) \\ r_1 I_k(t) + r_2 Q_k(t) - (\mu+\theta)R_k(t)\end{pmatrix},$$

This section starts with a result on the existence and uniqueness of a non-negative solution and a positively invariant set for the fractional network-based SE_1E_2IQR malware propagation model. Firstly, we considers the following table:

Table 3.1: The table of parameters

Notation	**Value**	**Notation**	**Value**
b_k	$\frac{\Lambda(k)}{\mu}$	α_1	$\omega_1+\mu+\eta$
α_2	$\omega_2+\omega_3+\mu$	α_3	$r_2+\mu$
α_4	$\mu+\theta$	α_5	$r_1+c+\mu$
$\alpha_{6,k}$	$\eta\sigma_1(k)+\alpha_1\sigma_2(k)$	$\alpha_{7,k}$	$\alpha_2\alpha_5\sigma_1(k)\omega_1 + \alpha_5\alpha_{6,k}\omega_2 + c\alpha_3\alpha_{6,k}\omega_3$

Theorem 3.1. *Assume that*

$$S_k^0 > 0, \quad E_{1,k}^0 \geq 0, \quad E_{2,k}^0 \geq 0, \quad I_k^0 \geq 0, \quad Q_k^0 \geq 0, \quad R_k^0 \geq 0 \tag{3.3}$$

for all $k = \overline{1,n}$. *Then, the fractional network-based* SE_1E_2IQR *malware propagation model with initial condition* $\mathbf{x}(0)$ *satisfying (3.3) always admits a unique non-negative solution* $\mathbf{x}(t)$ *and*

the function $\Theta(t)$ is positive for all $t > 0$. Moreover, the set

$$\Sigma^+ = \left\{\mathbf{x}(t) \in \mathbb{R}_+^{6n} : S_k + E_{1,k} + E_{2,k} + I_k + Q_k + R_k = b_k,\ k = \overline{1,n}\right\}$$

is a positively invariant set for the proposed malware propagation model.

3.2.2. The threshold value $\mathfrak{R}_0$ and equilibrium states

Equilibrium states are determined by the system of equations $f(\mathbf{x}^k(t)) = \overline{0}$. It is easy to see that in malware-free equilibrium state, since there is no malicious code spreading on the network, so $E_{1,k} = E_{2,k} = I_k = 0$ for all $k = overline1, n$. Therefore, the proposed malware propagation model has a unique malware-free equilibrium $\mathbf{P}_0$ given by $\mathbf{P}_0 = \underbrace{(0, 0, 0, b_1, 0, 0, \ldots, 0, 0, 0, b_n, 0, 0)}_{6n}$.

Next, using the next generation matrix method, the thesis determines a threshold value $\mathfrak{R}_0$. Indeed, the state change in the proposed malware propagation model has the following characteristics:

- There are only three compartments that cause malware propagation in the proposed malware propagation model, which are the compartments: (E_1), (E_2) and (I).
- The state change of nodes from infectious compartment to exposed compartments or between two exposed compartments is just regarded as the state change between infected nodes.

Then, we find out the threshold value $\mathfrak{R}_0$ as follows:

$$\mathfrak{R}_0 = \frac{M_q}{\langle k\rangle}\sum_{k=1}^{n}\frac{\omega_3\nu(k)\mathbb{P}(k)(\eta\sigma_1(k) + \alpha_1\sigma_2(k))}{\alpha_1\alpha_2\alpha_5} = \frac{\omega_3 M_q\langle\alpha_6\nu\rangle}{\alpha_1\alpha_2\alpha_5\langle k\rangle}, \tag{3.4}$$

where $\langle\alpha_6\nu\rangle = \sum_{k=1}^{n}\nu(k)\mathbb{P}(k)(\eta\sigma_1(k) + \alpha_1\sigma_2(k))$.

Next, we denote $A_k = M_q\nu(k)\mathbb{P}(k)\,\alpha_3\alpha_4\alpha_{6,k}\omega_3$, $\tilde{A}_2 = \alpha_1\alpha_2\alpha_3\alpha_4\alpha_5$ and

$$\tilde{A}_{1,k} = \omega_3\left(\alpha_3\alpha_4\alpha_{6,k} + r_1\alpha_3\alpha_{6,k}\right) + \left(\alpha_3\alpha_4\alpha_5\alpha_{6,k} + \alpha_4\alpha_{7,k} + \alpha_2\alpha_3\alpha_4\alpha_5\sigma_1(k) + r_2\alpha_{7,k}\right) = \omega_3\alpha_{8,k} + \alpha_{9,k}.$$

Theorem 3.2. *If $\mathfrak{R}_0 > 1$ then the proposed malware propagation model has a unique endemic equilibrium state $\mathbf{P}_* = (E_{1,1}^*, E_{2,1}^*, I_1^*, S_1^*, Q_1^*, R_1^*, \ldots, E_{1,n}^*, E_{2,n}^*, I_n^*, S_n^*, Q_n^*, R_n^*)$, given by*

$$S_k^* = \frac{\alpha_1\alpha_2\alpha_5}{\omega_3\alpha_{6,k}\Theta^*}I_k^*,\ \ E_{1,k}^* = \frac{\alpha_2\alpha_5\sigma_1(k)}{\omega_3\alpha_{6,k}}I_k^*,\ \ E_{2,k}^* = \frac{\alpha_5}{\omega_3}I_k^*,\ \ Q_k^* = \frac{\alpha_{7,k}}{\omega_3\alpha_3\alpha_{6,k}}I_k^*, \tag{3.5}$$

$$R_k^* = \frac{r_1\alpha_3\alpha_{6,k}\omega_3 + r_2\alpha_{7,k}}{\alpha_3\alpha_4\alpha_{6,k}\omega_3}I_k^*,\ \ \Theta^* = \frac{M_q}{\langle k\rangle}\sum_{i=1}^{n}\frac{\nu(i)}{b_i}\mathbb{P}(i)I_i^*,\ \ I_k^* = \frac{b_k\alpha_3\alpha_4\alpha_{6,k}\omega_3\Theta^*}{\left(\omega_3\alpha_{8,k} + \alpha_{9,k}\right)\Theta^* + \tilde{A}_2}.$$

3.2.3. The asymptotic behavior of malware-free equilibrium $\mathbf{P}_0$

In this section, the thesis discuss on the asymptotic behavior of malware-free equilibrium $\mathbf{P}_0$ of the proposed malware propagation model. Firstly, we present the relationship between

$\mathfrak{R}_0$ and asymptotic stability of malware-free equilibrium $\mathbf{P}_0$:

Theorem 3.3. *The following assertions hold*

(i) *If* $\mathfrak{R}_0 > 1$ *then malware-free equilibrium* $\mathbf{P}_0$ *is unstable.*

(ii) *If* $\mathfrak{R}_0 < 1$ *and* $\alpha_1\alpha_2 + \alpha_1\alpha_5 + \alpha_2\alpha_5 > \dfrac{\sigma_2 M_q \langle n^2 \rangle}{\langle n \rangle}$ *then malware-free equilibrium* $\mathbf{P}_0$ *is locally asymptotically stable.*

(iii) *If* $\mathfrak{R}_0 < 1$ *and* $\alpha_1\alpha_2 + \alpha_1\alpha_5 + \alpha_2\alpha_5 \leq \dfrac{\sigma_2 M_q \langle n^2 \rangle}{\langle n \rangle}$ *then the stability of malware-free equilibrium depends on parameters and fractional order* β.

Next, the thesis discuss on an important topic on the epidemiological theory related to the global asymptotic stability of malware-free equilibrium $\mathbf{P}_0$:

Theorem 3.4. *If the threshold value*

$$\tilde{\mathfrak{R}}_0 = \frac{\omega_3 M_q (\sigma_1 + \sigma_2) \langle n^2 \rangle}{\alpha_2 \alpha_5 \langle n \rangle} < 1$$

then malware-free equilibrium $\mathbf{P}_0$ *of the fractional network-based* SE_1E_2IQR *malware propagation model is globally asymptotically stable on* Σ^+.

Remark 3.1. Since $\alpha_1 = \eta + \mu + \omega_1 > \eta$ then $\frac{\omega_3(\sigma_1(k)+\sigma_2(k))}{\alpha_2\alpha_5} > \frac{\omega_3(\eta\sigma_1(k)+\alpha_1\sigma_2(k))}{\alpha_1\alpha_2\alpha_5}$, that is, $\tilde{\mathfrak{R}}_0 > \mathfrak{R}_0$. On the other hand, according to Theorem 3.4, since the equilibrium $\mathbf{P}_0$ is globally asymptotically stable if and only if $\tilde{\mathfrak{R}}_0 > 1$ then the condition $\mathfrak{R}_0 < 1$ is not sufficient for completely eliminating malicious objects on the network.

3.2.4. The bifurcation analysis

In this section, we discuss on the bifurcation phenomena that occurs at $\mathfrak{R}_0 = 1$.

Theorem 3.5. *The fractional network-based* SE_1E_2IQR *malware propagation model always exhibits forward bifurcation at* $\mathfrak{R}_0 = 1$ *for all values of parameters.*

Chapter 4

THE STABILIZATION PROBLEM FOR A CONTROLLED FRACTIONAL NETWORK-BASED SIRS MALWARE PROPAGATION MODEL

In this chapter, we establish a controlled fractional network-based SIRS malware propagation model with saturated treatment functions in order to describe the dynamics of malware propagation on wireless sensor network in case the number of infected nodes exceeds the network's ability to handle malware. The results of this chapter are based on the publications [**P3**] and [**P4**].

4.1. The model's formulation

In this chapter, the thesis proposes to use a fractional network-based SIRS malware propagation model to study the effects of malware spread on complex heterogeneous networks. Denote $S_k(t)$, $I_k(t)$ and $R_k(t)$ by the densities of susceptible, infectious and recovered nodes of degree k at time t, respectively. In addition, the thesis assumes that $N_k(t) = S_k(t) + I_k(t) + R_k(t)$ is the density of nodes with degree k at time t. The state transitions between three compartments are based on the following rules:

- Each node becomes dead node at a rate μ when it runs out of energy, and new nodes are added to the network at a rate Λ. The rate Λ and death rate μ are assumed to be equal to ensure balance and continuity of the network.
- A susceptible node of degree k that contacts with malicious code, will be transferred into Infectious state at the rate $\sigma_k\Theta(t)$, with σ_k being the transmission rate. On the other hand, a susceptible node can be moved to state (R) with a varying isolation rate $\mathbf{u}_k(t)$.
- The thesis considers the nonlinear treatment function in the form $\varphi(I_k) = \dfrac{rI_k}{1+\gamma\Theta}$, where r is recovered rate and γ is used to measure the impact of infectious nodes whose treatment process are delayed.
- Nodes in state (R) log off the network at a rate of μ due to run out of energy, and recovery nodes may lose their immunization and return to susceptible state at a rate ω.

Based on the advantages of non-integer derivatives in modeling non-local processes and in order to demonstrate the influence of memory in the process of malware propagation on the network, the thesis studies the spread of malicious code on wireless sensor networks with

fractional derivatives. In particular, the thesis considers a fractional network-based malware propagation model whose k^{th}-system is as follows:

$$\begin{cases} {}_0^C\mathfrak{D}_t^\beta S_k(t) &= \Lambda - \sigma_k\Theta(t)S_k(t) - (\mu + \mathbf{u}_k(t))\, S_k(t) + \omega R_k(t) \\ {}_0^C\mathfrak{D}_t^\beta I_k(t) &= \sigma_k\Theta(t)S_k(t) - \mu I_k(t) - \dfrac{rI_k(t)}{1+\gamma\Theta(t)} \\ {}_0^C\mathfrak{D}_t^\beta R_k(t) &= \mathbf{u}_k(t)S_k(t) + \dfrac{rI_k(t)}{1+\gamma\Theta(t)} - (\mu+\omega)R_k(t), \end{cases} \tag{4.1}$$

with the initial condition

$$S_k(0) = S_k^0 > 0, \qquad I_k(0) = I_k^0 \geq 0, \qquad R_k(0) = R_k^0 \geq 0. \tag{4.2}$$

The function $\Theta(t) = \frac{1}{\langle k\rangle}\sum_{k=1}^n \varphi(k)\mathbb{P}(k)I_k(t)$ is probability that a given link is connected to an infectious node, where $\mathbb{P}(k)$ is the probability that a randomly chosen node has degree k, $\varphi(k) = k$ is the transmission rate of a node of degree k and $\langle k\rangle = \sum_{k=1}^n k\mathbb{P}(k)$ is the average degree of the network.

4.2. The qualitative properties of the proposed malware propagation model

4.2.1. The existence of positively invariant set

For convenience of readers, we denote

$$\tilde{\mathbf{x}}_k(t) = \begin{pmatrix} S_k(t) & I_k(t) & R_k(t) \end{pmatrix}^\top, \qquad \tilde{\mathbf{x}}(t) = \begin{pmatrix} \tilde{\mathbf{x}}_1(t) & \tilde{\mathbf{x}}_2(t) & \cdots & \tilde{\mathbf{x}}_n(t) \end{pmatrix}^\top$$

$$\Sigma^+ = \left\{\tilde{\mathbf{x}}(t) \in \mathbb{R}_+^{3n} : S_k(t) + I_k(t) + R_k(t) = 1,\ k = \overline{1,n},\ t \geq 0\right\}$$

$$\mathrm{F}_k(t, \tilde{\mathbf{x}}(t), \mathbf{u}(t)) = \begin{pmatrix} \Lambda - \sigma_k\Theta(t)S_k(t) - (\mu + \mathbf{u}_k(t))\, S_k(t) + \omega R_k(t) \\ \sigma_k\Theta(t)S_k(t) - \mu I_k(t) - \dfrac{rI_k(t)}{1+\gamma\Theta(t)} \\ \mathbf{u}_k(t)S_k(t) + \dfrac{rI_k(t)}{1+\gamma\Theta(t)} - (\mu+\omega)R_k(t) \end{pmatrix}.$$

The input control $\mathbf{u}_k(t)$ is regarded as the rate of susceptible nodes protected by the firewall per unit time. Denote

$$\mathscr{U}_{ad} = \left\{\mathbf{u}(\cdot) \in \left(L^1[0,T]\right)^n : 0 \leq \mathbf{u}_k(t) \leq b,\ k = \overline{1,n}\right\} \quad (0 < b < 1),$$

is an admissible control set consisting of all Lebesgue measurable functions on $[0, T]$.

Theorem 4.1. *For each control input $\mathbf{u} \in \mathscr{U}_{ad}$, Cauchy problem for the controlled fractional network-based SIRS malware propagation model has a unique non-negative solution $\tilde{\mathbf{x}}(t)$. In particular, if $\tilde{\mathbf{x}}(0) \in \Sigma^+$ then for all $t > 0$, the solution $\tilde{\mathbf{x}}(t)$ belongs to the set Σ^+.*

4.2.2. The threshold value $\mathfrak{R}_0$ and equilibrium states

In order to find equilibrium states, the thesis solves a system of algebraic equations $\mathrm{F}_k(t, \tilde{\mathbf{x}}(t), \mathbf{u}(t)) = \overline{0}$. If the network is clear of malware programs, the proposed malware propagation model admits

a unique malware-free equilibrium $\mathbf{P}_0 = (S_1^0, I_1^0, R_1^0, \ldots, S_n^0, I_n^0, R_n^0)$ is given by

$$\mathbf{P}_0 = \underbrace{\left(\frac{\mu+\omega}{\mu+\omega+\mathbf{u}_1}, 0, \frac{\mathbf{u}_1}{\mu+\omega+\mathbf{u}_1}, \ldots, \frac{\mu+\omega}{\mu+\omega+\mathbf{u}_n}, 0, \frac{\mathbf{u}_n}{\mu+\omega+\mathbf{u}_n}\right)}_{3n},$$

while if there exist malware programs spreading on the network, then the proposed malware propagation model has at least one endemic equilibrium $\mathbf{P}_* = (S_1^*, I_1^*, R_1^*, \ldots, S_n^*, I_n^*, R_n^*)$ under some certain conditions related to the threshold value $\mathfrak{R}_0$.

According to the next generation matrix method, the threshold value $\mathfrak{R}_0$ is given by

$$\mathfrak{R}_0 = \frac{\sigma(\mu+\omega)}{(\mu+r)\langle k\rangle}\sum_{k=1}^{n}\frac{k^2\mathbb{P}(k)}{(\mu+\omega+\mathbf{u}_k)} = \frac{\sigma(\mu+\omega)\langle k^2\mathbf{u}\rangle}{(\mu+r)\langle k\rangle}, \tag{4.3}$$

where $\langle k^2 u\rangle = \sum_{k=1}^{n}\frac{k^2\mathbb{P}(k)}{(\mu+\omega+\mathbf{u}_k)}$.

Theorem 4.2. *If $\mathfrak{R}_0 > 1$ then the fractional network-based SIRS malware propagation model has at least one endemic equilibrium $\mathbf{P}_* = (S_1^*, I_1^*, R_1^*, \ldots, S_n^*, I_n^*, R_n^*)$ defined by*

$$S_k^* = \frac{1}{\sigma_k\Theta^*}\left(\mu + \frac{r}{1+\gamma\Theta^*}\right)I_k^*, \quad R_k^* = \frac{1}{\mu+\omega}\left[\frac{r}{1+\gamma\Theta^*} + \frac{\mathbf{u}_k}{\sigma_k\Theta^*}\left(\mu+\frac{r}{1+\gamma\Theta^*}\right)\right]I_k^*,$$
$$I_k^* = \frac{\sigma_k\Theta^*}{\left\{\mu + \frac{r}{1+\gamma\Theta^*} + \sigma_k\Theta^* + \frac{\sigma_k\Theta^*}{\mu+\omega}\left[\frac{r}{1+\gamma\Theta^*} + \frac{\mathbf{u}_k}{\sigma_k\Theta^*}\left(\mu+\frac{r}{1+\gamma\Theta^*}\right)\right]\right\}}.$$

4.2.3. The asymptotic behavior of malware-free equilibrium $\mathbf{P}_0$

Theorem 4.3. *The following assertions are fulfilled*

(i) *If $\mathfrak{R}_0 > 1$ then malware-free equilibrium $\mathbf{P}_0$ is unstable.*

(ii) *If $\mathfrak{R}_0 < 1$ malware-free equilibrium $\mathbf{P}_0$ is locally asymptotically stable.*

Theorem 4.4. *Denote $\tilde{\mathfrak{R}}_0 = \frac{\sigma(\mu+\omega)\langle k^2\mathbf{u}\rangle}{\mu\langle k\rangle}$. Then, if the threshold value $\tilde{\mathfrak{R}}_0 < 1$ then malware-free equilibrium $\mathbf{P}_0$ is globally asymptotically stable.*

Remark 4.1. It is easy to see that $\mathfrak{R}_0 < \tilde{\mathfrak{R}}_0$, that is, the condition $\mathfrak{R}_0 < 1$ is not enough to ensure the global attraction of the equilibrium state $\mathbf{P}_0$ and in this case, we cannot eliminate malware attacks unless the value of $\mathfrak{R}_0$ decreases such that $\mathfrak{R}_0 < \tilde{\mathfrak{R}}_0 < 1$.

4.2.4. The backward bifurcation

Next, the thesis will establish a sufficient condition such that the backward bifurcation phenomena occurs at $\mathfrak{R}_0 = 1$.

Theorem 4.5. *The fractional network-based SIRS malware propagation model exhibits the backward bifurcation at $\mathfrak{R}_0 = 1$ if*

$$\gamma > \frac{(\mu+r)\langle k^3 a\rangle\langle k\rangle}{r\langle k^2 u\rangle}\left(1+\frac{r}{\mu+\omega}\right),$$

where $\langle k^3 a\rangle = \frac{1}{\langle k\rangle}\sum_{k=1}^{n}\frac{k^3\mathbb{P}(k)}{\mu+\omega+\mathbf{u}_k}$.

4.3. The stabilization problem for the controlled fractional network-based SIRS malware propagation model

The thesis considers a scenario when $\mathfrak{R}_0 > 1$, that is, the equilibrium state $\mathbf{P}_0$ is unstable, and establish a quarantine control function $\mathbf{u}(t)$ to stabilize this equilibrium state, that is, it transfers the state function of the proposed malware propagation model to the state $\tilde{\mathbf{P}}_0 = \underbrace{(1,0,0,1,0,0,\ldots,1,0,0)}_{3n}$. Denote

$$\tilde{\mathbf{e}}(t) = \tilde{\mathbf{x}}(t) - \tilde{\mathbf{P}}_0 = \underbrace{(S_1 - 1, I_1, R_1, S_2 - 1, I_2, R_2, \ldots, S_n - 1, I_n, R_n)}_{3n}.$$

Then, the considered stabilization problem is equivalent to a control problem that stabilizes the vector $\mathbf{e}(t)$ to $\overline{0}$. Next, the thesis will use the fractional interconnected Takagi-Sugeno fuzzy system to establish the control function $\mathbf{u}(t)$. Since $\Lambda = \mu$, that is, $N_i(t)$ is constant, by substituting $S_i = 1 - I_i - R_i$, we only need to consider the dynamics in terms of I_i and R_i. On the other hand, since $S_i(t) > 0$ and is bounded above by 1 and the i^{th}-group receives a new node at a rate Λ, it can be assumed that $S_i(t) \in [0.1, 0.9]$ for all $t > 0$ and entails $I_i(t) + R_i(t) \in [0.1, 0.9]$. Then, the considered nonlinear system can be rewritten as follows:

$${}_0^C\mathfrak{D}_t^\beta \mathbf{e}_i(t) = \begin{pmatrix} -\mu - \frac{r}{1+\gamma\Theta(t)} + \frac{\sigma_i i\mathbb{P}(i)(S_i(t)-1)}{\langle k\rangle} & 0 \\ \frac{r}{1+\gamma\Theta(t)} & -(\mu+\omega) \end{pmatrix} \mathbf{e}_i(t) + \begin{pmatrix} 0 \\ S_i(t) - 1 \end{pmatrix} \mathbf{u}_i(t) + \sum_{\substack{j=1 \\ j\neq i}}^{n} \begin{pmatrix} \frac{\sigma_i(S_i(t)-1)}{\langle k\rangle} j\mathbb{P}(j) & 0 \\ 0 & 0 \end{pmatrix} \mathbf{e}_j(t). \tag{4.4}$$

Denote $\mathbf{z}_i(t) = \begin{pmatrix} z_{i1}(t) & z_{i2}(t) & \cdots & z_{iq}(t) \end{pmatrix}^\top$ is the antecedent variables vector. The thesis establishes a fractional interconnected Takagi-Sugeno fuzzy system for the nonlinear systems (4.4) with the following fuzzy rules:

Rule $\mathbf{E}_i^p$: If z_{i1} is F_{i1}^p and z_{i2} is F_{i2}^p and $\cdots$ and z_{iq} is F_{iq}^p then

$${}_0^C\mathfrak{D}_t^\beta \mathbf{e}_i(t) = A_i^p \mathbf{e}_i(t) + B_i^p \mathbf{u}_i(t) + \sum_{\substack{j=1 \\ j\neq i}}^{n} \alpha_{ij}^p \mathbf{e}_j(t),$$

where A_i^p, B_i^p and α_{ij}^p are real matrices for all $i = \overline{1,n}$ and $p = \overline{1,r_i}$. The nonlinear system (4.4) can be expressed by the following fractional differential system:

$${}_0^C\mathfrak{D}_t^\beta \mathbf{e}_i(t) = \sum_{p=1}^{r_i} w_i^p\left(\mathbf{z}_i(t)\right) \left\{ A_i^p \mathbf{e}_i(t) + B_i^p \mathbf{u}_i(t) + \sum_{\substack{j=1 \\ j\neq i}}^{n} \alpha_{ij}^p \mathbf{e}_j(t) \right\} \qquad \left(i = \overline{1,n}\right), \tag{4.5}$$

where $w_i^p\left(\mathbf{z}_i(t)\right)$ is a membership function indicating the activation degree of the p^{th}-local model of the subsystem $\mathbf{E}_i$. Therefore, the fractional interconnected Takagi-Sugeno fuzzy system for

the proposed malware propagation model is given by:

$$
{}_0^C\mathfrak{D}_t^{\beta}\mathbf{e}(t) = \begin{pmatrix} \displaystyle\sum_{p=1}^{r_1} w_1^p\left(\mathbf{z}_1(t)\right)\left\{A_1^p\mathbf{e}_1(t) + B_1^p\mathbf{u}_1(t) + \sum_{\substack{j=1\\ j\neq i}}^{n}\alpha_{1j}^p\mathbf{e}_j(t)\right\} \\ \vdots \\ \displaystyle\sum_{p=1}^{r_n} w_n^p\left(\mathbf{z}_n(t)\right)\left\{A_n^p\mathbf{e}_n(t) + B_n^p\mathbf{u}_n(t) + \sum_{\substack{j=1\\ j\neq i}}^{n}\alpha_{nj}^p\mathbf{e}_j(t)\right\} \end{pmatrix}. \tag{4.6}
$$

The p^{th}-fuzzy rule of input control function in the subsystem $\mathbf{E}_i$ can be considered as follows:

Rule $\mathbf{E}_i^p$: If z_{i1} is F_{i1}^p and z_{i2} is F_{i2}^p and $\cdots$ and z_{iq} is F_{iq}^p then $\mathbf{u}_i(t) = K_i^p\mathbf{x}_i(t)$.

The state-feedback control $\mathbf{u}_i(t)$ for the subsystem $\mathbf{E}_i$ is $\mathbf{u}_i(t) = \displaystyle\sum_{p=1}^{r_i} w_i^p\left(\mathbf{z}_i(t)\right)K_i^p\mathbf{x}_i(t)\ \left(i = \overline{1,n}\right)$.

Denote $\mathbf{u}(t) = \begin{pmatrix}\mathbf{u}_1(t) & \ldots & \mathbf{u}_n(t)\end{pmatrix}^{\top}$ by the state-feedback control vector for the proposed malware propagation model. Next, the thesis establishes sufficient conditions to stabilize the unstable equilibrium state:

Theorem 4.6. *Assume that there exist some matrices* $\mathrm{P}_i \in \mathbf{S}_{++}^n$, $\mathrm{Q}_i \succ 0$, $\mathrm{U}_i^{pm}, \mathrm{U}_{ij}^{pm} \in \mathbf{S}^n$ *and* K_i^p *satisfies the following inequalities:*

$$
\mathrm{Q}_i^{pm} \preceq \mathrm{U}_i^{pm} \tag{LMI.1}
$$

$$
\left(\alpha_{ij}^p\right)^{\top}\mathrm{P}_i + \mathrm{P}_i\alpha_{ij}^p + \left(\alpha_{ji}^m\right)^{\top}\mathrm{P}_j + \mathrm{P}_j\alpha_{ji}^m \preceq 2\mathrm{U}_{ij}^{pm} \tag{LMI.2}
$$

$$
\mathbb{U} = \begin{pmatrix} \mathrm{U}_1 & \mathrm{U}_{12} & \cdots & \mathrm{U}_{1n} \\ \mathrm{U}_{12}^{\top} & \mathrm{U}_2 & \cdots & \mathrm{U}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{U}_{1n}^{\top} & \mathrm{U}_{2n}^{\top} & \cdots & \mathrm{U}_n \end{pmatrix} \prec 0, \tag{LMI.3}
$$

where for each $i, j = \overline{1,n}$, *the matrices* U_i *and* U_{ij} $(i \neq j)$ *are given by*

$$
\mathrm{U}_i = \begin{pmatrix} \mathrm{U}_i^{11} & \mathrm{U}_i^{12} & \cdots & \mathrm{U}_i^{1r_i} \\ (\mathrm{U}_i^{12})^{\top} & \mathrm{U}_i^{22} & \cdots & \mathrm{U}_i^{2r_i} \\ \vdots & \vdots & \ddots & \vdots \\ (\mathrm{U}_i^{1r_i})^{\top} & (\mathrm{U}_i^{2r_i})^{\top} & \cdots & \mathrm{U}_i^{r_ir_i} \end{pmatrix}, \qquad \mathrm{U}_{ij} = \begin{pmatrix} \mathrm{U}_{ij}^{11} & \mathrm{U}_{ij}^{12} & \cdots & \mathrm{U}_{ij}^{1r_j} \\ \mathrm{U}_{ij}^{21} & \mathrm{U}_{ij}^{22} & \cdots & \mathrm{U}_{ij}^{2r_j} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{U}_{ij}^{r_i1} & \mathrm{U}_{ij}^{r_i2} & \cdots & \mathrm{U}_{ij}^{r_ir_j} \end{pmatrix}.
$$

Then, the fractional interconnected Takagi-Sugeno fuzzy system (4.6) is stabilized under the fuzzy state-feedback control $\mathbf{u}(t)$, *where*

$$
\mathrm{Q}_i^{pm} = \left(\mathrm{G}_i^{pm}\right)^{\top}\mathrm{P}_i + \mathrm{P}_i\mathrm{G}_i^{pm} \qquad \textit{và} \qquad \mathrm{G}_i^{pm} = A_i^p + B_i^pK_i^m.
$$

Remark 4.2. In order to apply MatLab program to solve the system of LMIs in Theorem 4.6, the thesis will apply Schur's complement theorem to transform the linear matrix inequalities (LMI.1), (LMI.2) and (LMI.3) into linear matrix inequalities in a more convenient form. For this aim, the thesis carry out the following transformations:

$$\mathrm{C}_i = \mathrm{P}_i^{-1}, \qquad K_i^p = \mathrm{W}_i^p \mathrm{C}_i^{-1}, \qquad \tilde{\mathrm{U}}_i^{pm} = \mathrm{C}_i \mathrm{U}_i^{pm} \mathrm{C}_i, \qquad \tilde{\mathrm{U}}_{ij}^{pm} = \mathrm{C}_i \mathrm{U}_{ij}^{pm} \mathrm{C}_j + \mathrm{C}_j \mathrm{U}_{ij}^{pm} \mathrm{C}_i$$

and $\tilde{\mathrm{Q}}_i^{pm} = \mathrm{C}_i \left\{ \left(\mathrm{G}_i^{pm}\right)^\top \mathrm{P}_i + \mathrm{P}_i \mathrm{G}_i^{pm} \right\} \mathrm{C}_i = \mathrm{C}_i \left(A_i^p\right)^\top + A_i^p \mathrm{C}_i + B_i^p \mathrm{W}_i^m + \left(\mathrm{W}_i^m\right)^\top \left(B_i^p\right)^\top$. By multiplying the left and right sides of the matrices U_i, U_{ij} with $\mathrm{diag}\underbrace{[\mathrm{C}_i, \ldots, \mathrm{C}_i]}_{n}$, we obtain

$$\tilde{\mathrm{U}}_i = \begin{pmatrix} \tilde{\mathrm{U}}_i^{11} & \tilde{\mathrm{U}}_i^{12} & \cdots & \tilde{\mathrm{U}}_i^{1r_i} \\ (\tilde{\mathrm{U}}_i^{12})^\top & \tilde{\mathrm{U}}_i^{22} & \cdots & \tilde{\mathrm{U}}_i^{2r_i} \\ \vdots & \vdots & \ddots & \vdots \\ (\tilde{\mathrm{U}}_i^{1r_i})^\top & (\tilde{\mathrm{U}}_i^{2r_i})^\top & \cdots & \tilde{\mathrm{U}}_i^{r_i r_i} \end{pmatrix}, \qquad \tilde{\mathrm{U}}_{ij} = \begin{pmatrix} \tilde{\mathrm{U}}_{ij}^{11} & \tilde{\mathrm{U}}_{ij}^{12} & \cdots & \tilde{\mathrm{U}}_{ij}^{1r_j} \\ \tilde{\mathrm{U}}_{ij}^{21} & \tilde{\mathrm{U}}_{ij}^{22} & \cdots & \tilde{\mathrm{U}}_{ij}^{2r_j} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{\mathrm{U}}_{ij}^{r_i 1} & \tilde{\mathrm{U}}_{ij}^{r_i 2} & \cdots & \tilde{\mathrm{U}}_{ij}^{r_i r_j} \end{pmatrix}.$$

Therefore, we can rewrite the system of LMIs in Theorem 4.6 as follows:

$$\tilde{\mathrm{Q}}_i^{pm} \preceq \tilde{\mathrm{U}}_i^{pm} \tag{LMI.4}$$

$$\left(\alpha_{ij}^p\right)^\top \mathrm{C}_i + \mathrm{C}_i \alpha_{ij}^p + \left(\alpha_{ji}^m\right)^\top \mathrm{C}_j + \mathrm{C}_j \alpha_{ji}^m \preceq 2\tilde{\mathrm{U}}_{ij}^{pm} \tag{LMI.5}$$

$$\tilde{\mathbb{U}} = \begin{pmatrix} \tilde{\mathrm{U}}_1 & \tilde{\mathrm{U}}_{12} & \cdots & \tilde{\mathrm{U}}_{1n} \\ \tilde{\mathrm{U}}_{12}^\top & \tilde{\mathrm{U}}_2 & \cdots & \tilde{\mathrm{U}}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{\mathrm{U}}_{1n}^\top & \tilde{\mathrm{U}}_{2n}^\top & \cdots & \tilde{\mathrm{U}}_n \end{pmatrix} \prec 0. \tag{LMI.6}$$

Example 4.1. Consider a wireless sensor network with Barabási-Albert free-scale network structure for $n = 2$ and parameters are given by $\Lambda = \mu = 0.14, \omega = 0.1, \sigma = 0.8, r = 0.6, \gamma = 2$. Then, we can calculate $\langle k \rangle = \sum_{k=1}^n k\mathbb{P}(k) = \frac{10}{9}, \langle k^2 \rangle = \sum_{k=1}^n k^2\mathbb{P}(k) = \frac{4}{3}$ and $\mathfrak{R}_0 = 1.8018 > 1$. By choosing the terms $z_{i1} = S_i(t)$ and $z_{i2} = \frac{r}{1+\gamma\Theta(t)}$ in the system (4.4) as a premise variable, the thesis establishes a fractional interconnected Takagi-Sugeno fuzzy system corresponding to the proposed malware propagation model with weight functions $\eta_{i0}^1(z_{i1}) = \frac{1-z_{i1}}{0.8}, \eta_{i1}^1(z_{i1}) = \frac{z_{i1}-0.2}{0.8}$ for variables z_{i1} and $\eta_{i0}^2(z_{i2}) = \frac{5(1-z_{i2})}{2}, \eta_{i1}^2(z_{i2}) = \frac{5z_{i2}-3}{2}$ for variable z_{i2}. Denote $\mathbf{z}_i(t) = \begin{pmatrix} z_{i1}(t) & z_{i2}(t) \end{pmatrix}^\top$ and the corresponding fuzzy sets with weight functions by F_{ik}^χ for each $i = 1, 2$, $k = 0, 1$ and $\chi = 1, 2$. Now, we obtain the following fuzzy rules:

Rule $\mathbf{E}_i^1$: If z_{i1} is F_{i0}^1 and z_{i2} is F_{i0}^2 then ${}_0^C\mathfrak{D}_t^\beta \mathbf{e}_i(t) = A_i^1 \mathbf{e}_i(t) + B_i^1 \mathbf{u}_i(t) + \sum_{\substack{j=1 \\ j\neq i}}^2 \alpha_{ij}^1 \mathbf{e}_j(t)$,

Rule $\mathbf{E}_i^2$: If z_{i1} is F_{i0}^1 and z_{i2} is F_{i1}^2 then ${}_0^C\mathfrak{D}_t^\beta \mathbf{e}_i(t) = A_i^2 \mathbf{e}_i(t) + B_i^2 \mathbf{u}_i(t) + \sum_{\substack{j=1 \\ j\neq i}}^2 \alpha_{ij}^2 \mathbf{e}_j(t)$,

Rule $\mathbf{E}_i^3$: If z_{i1} is F_{i1}^1 and z_{i2} is F_{i0}^2 then ${}_0^C\mathfrak{D}_t^\beta \mathbf{e}_i(t) = A_i^3 \mathbf{e}_i(t) + B_i^3 \mathbf{u}_i(t) + \sum_{\substack{j=1 \\ j\neq i}}^2 \alpha_{ij}^3 \mathbf{e}_j(t)$,

Rule $\mathbf{E}_i^4$: If z_{i1} is F_{i1}^1 and z_{i2} is F_{i1}^2 then ${}_0^C\mathfrak{D}_t^\beta \mathbf{e}_i(t) = A_i^4 \mathbf{e}_i(t) + B_i^4 \mathbf{u}_i(t) + \sum_{\substack{j=1 \\ j\neq i}}^2 \alpha_{ij}^4 \mathbf{e}_j(t)$,

where for all $i, j = 1, 2$ and $p = \overline{1, 4}$, the matrices A_i^p, B_i^p và α_{ij}^p are given by

$$A_1^1 = \begin{pmatrix} -0.916 & 0 \\ 0.2 & -0.24 \end{pmatrix}, A_1^2 = \begin{pmatrix} -1.316 & 0 \\ 0.6 & -0.24 \end{pmatrix}, A_1^3 = \begin{pmatrix} -0.404 & 0 \\ 0.2 & -0.24 \end{pmatrix}, A_1^4 = \begin{pmatrix} -0.804 & 0 \\ 0.6 & -0.24 \end{pmatrix},$$
$$A_2^1 = \begin{pmatrix} -0.628 & 0 \\ 0.2 & -0.24 \end{pmatrix}, A_2^2 = \begin{pmatrix} -1.028 & 0 \\ 0.6 & -0.24 \end{pmatrix}, A_2^3 = \begin{pmatrix} -0.372 & 0 \\ 0.2 & -0.24 \end{pmatrix}, A_2^4 = \begin{pmatrix} -0.772 & 0 \\ 0.6 & -0.24 \end{pmatrix},$$
$$B_1^1 = B_1^2 = B_2^1 = B_2^2 = \begin{pmatrix} 0 \\ -0.9 \end{pmatrix}, B_1^3 = B_1^4 = B_2^3 = B_2^4 = \begin{pmatrix} 0 \\ -0.1 \end{pmatrix},$$
$$\alpha_{12}^1 = \alpha_{12}^2 = \begin{pmatrix} -0.144 & 0 \\ 0 & 0 \end{pmatrix}, \alpha_{12}^3 = \alpha_{12}^4 = \begin{pmatrix} -0.016 & 0 \\ 0 & 0 \end{pmatrix}, \alpha_{21}^1 = \alpha_{21}^2 = \begin{pmatrix} -1.152 & 0 \\ 0 & 0 \end{pmatrix}, \alpha_{21}^3 = \alpha_{21}^4 = \begin{pmatrix} -0.128 & 0 \\ 0 & 0 \end{pmatrix}.$$

Then, the fractional interconnected Takagi-Sugeno fuzzy system (4.5) can be rewritten as follows:

$$ {}_0^C\mathfrak{D}_t^\beta \mathbf{e}_i(t) = \sum_{p=1}^{4} w_i^p\left(\mathbf{z}_i(t)\right) \left\{ A_i^p \mathbf{e}_i(t) + B_i^p \mathbf{u}_i(t) + \sum_{\substack{j=1 \\ j\neq i}}^{2} \alpha_{ij}^p \mathbf{e}_j(t) \right\},$$

where $i = 1, 2$ and $w_i^p\left(\mathbf{z}_i(t)\right) = \varphi_i^p\left(\mathbf{z}_i(t)\right) \left[\sum_{p=1}^{4} \varphi_i^p\left(\mathbf{z}_i(t)\right)\right]^{-1}$, $\varphi_i^p\left(\mathbf{z}_i(t)\right) = \eta_{ik}^1 \eta_{ij}^2$. By using `lmi` MatLab toolbox for (LMI.4), (LMI.5) and (LMI.6), we obtain [1]:

$$\mathrm{C}_1 = \begin{pmatrix} 21.8174 & 1.3860 \\ 1.3860 & 92.7029 \end{pmatrix}, \mathrm{C}_2 = \begin{pmatrix} 18.5841 & 1.0680 \\ 1.0680 & 91.7758 \end{pmatrix}, \mathrm{P}_1 = \begin{pmatrix} 0.0459 & -0.0007 \\ -0.0007 & 0.0108 \end{pmatrix}, \mathrm{P}_2 = \begin{pmatrix} 0.0538 & -0.0006 \\ -0.0006 & 0.0109 \end{pmatrix},$$
$$K_1^1 = \begin{pmatrix} 0.1067 & 0.2151 \end{pmatrix}, \quad K_1^2 = \begin{pmatrix} 0.2983 & 0.0581 \end{pmatrix}, \quad K_1^3 = \begin{pmatrix} 0.3112 & -0.0300 \end{pmatrix}, \quad K_1^4 = \begin{pmatrix} 0.3358 & -0.0330 \end{pmatrix}$$
$$K_2^1 = \begin{pmatrix} 0.0605 & 0.2203 \end{pmatrix}, \quad K_2^2 = \begin{pmatrix} 0.2944 & 0.0617 \end{pmatrix}, \quad K_2^3 = \begin{pmatrix} 0.3172 & -0.0280 \end{pmatrix}, \quad K_2^4 = \begin{pmatrix} 0.3598 & -0.0315 \end{pmatrix}.$$

Therefore, the malware-free equilibrium of the proposed network-based malware propagation model is stabilizable.

[1] MATLAB code can be downloaded from the URL link: https://github.com/DongNP16/TS-fuzzy-system.git

GENERAL CONCLUSIONS

1. The obtained results

The doctoral thesis studies the mathematical modeling of malware propagation on complex networks based on differential models and fuzzy set theory. The obtained results of the doctoral thesis are as follows:

(i) Establish a fractional SIQR malware propagation model with fuzzy data, propose some new concepts of fuzzy Caputo-Atangana-Baneanu fractional derivative (Definition 2.1) and fuzzy Riemann-Liouville Atangana-Baleanu fractional integral (Definition 2.2), prove the existence and uniqueness of fuzzy integral solution of the proposed model (Theorem 2.3 and Theorem 2.4) and carry out some numerical simulations.

(ii) Establish a fractional network-based SE_1E_2IQR malware propagation model whose transmission function is constructed by fuzzy-rule base and prove some qualitative properties of this model such as the positiveness, threshold value $\mathfrak{R}_0$ (The formula (3.4), the asymptotic stability of malware-free equilibrium $\mathbf{P}_0$ (Theorem 3.3 and Theorem 3.4) and the forward bifurcation at $\mathfrak{R}_0 = 1$ (Theorem 3.5).

(iii) Establish a controlled fractional network-based SIRS malware propagation model with saturated treatment function and its stabilization problem based on fractional interconnected Takagi-Sugeno fuzzy systems. The obtained results are as follows: the positiveness of solutions, the threshold value $\mathfrak{R}_0$ (The formula (4.3)), the asymptotic stability (Theorem 4.3 and Theorem 4.4), the backward bifurcation at $\mathfrak{R}_0 = 1$ (Theorem 4.5) and some sufficient conditions in form of linear matrix inequalities for the stabilization (Theorem 4.6) of malware-free equilibrium $\mathbf{P}_0$.

2. Some future research

- Study more details on the epidemiological properties of malware propagation models containing uncertainty based on linear correlated fuzzy number approach, fuzzy in granular form or Z-numbers.
- Study the observable problem and guaranteed cost control problem for network-based malware propagation models based on the approach of fractional interconnected Takagi-Sugeno fuzzy systems that contains time-delay or disturbance.

LIST OF PUBLICATIONS

P1. N.P. Dong, H.V. Long, N.L. Giang, 2022, The fuzzy fractional SIQR model of computer virus propagation in wireless sensor network using Caputo Atangana–Baleanu derivatives, *Fuzzy Sets and Systems*, 429, pp. 28-59. **(SCIE-Q1)**

P2. N.P. Dong, H.V. Long, N.T.K. Son, 2022, The dynamical behaviors of fractional-order SE_1E_2IQR epidemic model for malware propagation on Wireless Sensor Network, *Communications in Nonlinear Science and Numerical Simulation*, 111, 106428. **(SCIE-Q1)**

P3. N.P. Dong, H.V. Long, N.T.K. Son, 2023, The analysis of a fractional network-based epidemic model with saturated treatment function and fuzzy transmission, *Iranian Journal of Fuzzy Systems*, 20(1), pp. 1-18. **(SCIE-Q2)**

P4. N.P. Dong, N.L. Giang, H.V. Long, 2023, Interconnected Takagi-Sugeno intelligent system and fractional SIRS epidemic model for stabilization of Wireless Sensor Networks. **(submitted)**