A new Takagi-Sugeno fuzzy system approach for fuzzy state feedback controller design and its application to malware propagation on heterogeneous complex network

Nguyen Ngoc Quynh, Nguyen Phuong Dong, Nguyen Long Giang, Hoang Viet Long

***Abstract*— Nowadays, digital transformation has brought many great changes and is becoming an essential part of real life, however, it also goes along with a considerable likelihood of being targeted in cyberattack. Indeed, the more businesses embrace digital transformation or use online services, the more opportunities hackers have to expand their cyberattacks. Hence, there is an essential need on analyzing and predicting of cyberattack on network systems. For this aim, we propose to study a controlled fractional network-based SCIRS (Susceptible - Carrier - Infectious - Recovered - Susceptible) malware propagation model and its stabilization problem based on fractional interconnected Takagi-Sugeno fuzzy system. A fuzzy state feedback controller is proposed to asymptotically stabilize the unstable malware-free equilibrium of the proposed malware propagation model and then, we establish sufficient conditions in terms of linear matrix inequalities. The effectiveness of proposed approach is illustrated by a case study of SCIRS malware propagation model on heterogeneous complex network.**

***Tóm tắt*— Ngày nay, chuyển đổi số đã mang đến những thay đổi tích cực và đang trở thành một phần thiết yếu trong cuộc sống của chúng ta, tuy nhiên, quá trình chuyển đổi số cũng đặt ra những mối đe dọa lớn về nguy cơ gây mất an toàn thông tin đối với các doanh nghiệp. Thực tế, càng nhiều doanh nghiệp thực hiện chuyển đổi số hoặc sử dụng các dịch vụ trực tuyến thì các tin tặc càng có nhiều cơ hội để mở rộng phạm vi tấn công mạng. Vì vậy, việc phân tích và dự đoán các cuộc tấn công vào hệ thống mạng là rất cần thiết. Với mục đích này, nhóm tác giả đề xuất nghiên cứu mô hình lan truyền mã độc SCIRS (Susceptible - Carrier - Infectious - Recovered - Susceptible) dựa trên mạng phân thứ có điều khiển và bài toán ổn định hóa tương ứng dựa trên hệ mờ Takagi-Sugeno liên kết phân thứ. Bộ điều khiển phản hồi trạng thái mờ được đề xuất để ổn định hóa trạng thái cân bằng không có mã độc không ổn định của mô hình lan truyền mã độc đề xuất và sau đó, nhóm tác giả thiết lập các điều kiện đủ về bất đẳng thức ma trận tuyến tính. Tính hiệu quả của phương pháp đề xuất được minh họa bằng một nghiên cứu điển hình về mô hình lan truyền mã độc SCIRS trên mạng phức hợp không đồng nhất.**

Keywords*— *Fractional network-based model; SCIRS malware propagation model; interconnected Takagi-Sugeno fuzzy system; fuzzy state feedback control.

Từ khóa*— *Mô hình dựa trên mạng phân thứ; mô hình lan truyền mã độc SCIRS; hệ mờ Takagi-Sugeno liên kết; điều khiển phản hồi trạng thái mờ.

I. INTRODUCTION

Along with the rapid development of the Internet and information networks, the cyberattack by malicious objects such as viruses, worms or other malicious codes is one of the most dangerous threats to the security and integrity of information networks and to the contemporary informative society. Various approaches have been applied to analyze the characteristic properties of malware infection and then provide some better predictions on dynamics, evolution and epidemic peaks of malware propagation, see [8, 15, 16, 20] for therein. The approach based on compartmental mathematical modeling was firstly studied by Kermack and McKendrick in 1927 [8] with the use of a three-compartment mathematical model, namely SIR epidemic model, to

This manuscript is received on November 21, 2023. It is commented on November 26, 2023 and is accepted on October 16, 2023 by the first reviewer. It is commented on November 27, 2023 and is accepted on October 16, 2023 by the second reviewer.

investigate the dynamic of epidemic disease on the biological population. Then, this approach has been widely studied and has achieved a lot of applicable results in various disciplines of natural and social sciences. Since the fact that the spread of malware on complex networks has many similarities with the infection of diseases in biological populations, a lot of studies have used mathematical deterministic models to describe the spread of malware programs on some familiar complex networks such as the Internet, sensor networks or social networks, see [3, 16, 19, 20] for there in.

However, note that the heterogeneity is one of the most characteristic properties of many complex networks, that is, nodes in different positions may have un-similar roles on the network and hence, their influences on malware propagation are also different. Here, the concept "heterogeneous complex network'" refers to a network where the nodes have different characteristics or properties in terms of their connectivity patterns, degrees of importance, or functionality. It is a fact that malicious code will spread more rapidly if it starts from a higher degree node. Therefore, some recent studies have taken into consideration the heterogeneity of complex network for malware propagation mathematical modeling. For example, Hosseini and Zandvakili [5] studied the mechanism of rumor spreading on social networks based on a large-scale SEIRS-C model and fuzzy logic. In an other work, Huang et al. [6] proposed a network-based epidemic model consisting of four compartments with vaccination to describe the spread of an epidemic disease on biological population. Due to the fitting-data ability and advantages in better simulation of many physical systems [17], fractional calculus and fractional dynamical systems have been widely applied to modeling many physical systems, especially in epidemiological models such as [1, 7]. Recently, some control problems for epidemic models on complex networks have paid more attentions by many scientists and in facts, there have some noticeable results on optimal control problems and stabilization problems for malware propagation model, see [6, 12, 13, 21]. The main approach of theses works was based on the use of Pontryagin maximum principle to establish some sufficient conditions for an optimal pair $(\mathbf{x}^*, \mathbf{u}^*)$. However, the obtained conditions are often given in the form of a system consisting of state differential equations, co-state equation, stationary condition, transversality condition. This leads to a challenge for numerically solving these conditions and it is quite difficult to check that whether these conditions are feasible. In this work, we aim to study a stabilization problem for a network-based malware propagation model with fractional derivative based on a new type of Takagi-Sugeno fuzzy system and design a fuzzy state feedback control subjecting to this problem. The main contributions of this work are highlighted as follows:

- Establish a fractional network-based SCIRS malware propagation model with quarantine control $v(t)$, where the infection on complex network is caused by both Infectious (I) and Carrier (C) compartments. Then, we discuss some characteristic properties of the proposed malware propagation model.
- Introduce the stabilization problem for the unstable malware-free equilibrium of the proposed malware propagation model and establish the corresponding interconnected Takagi-Sugeno fuzzy system for this problem.
- Formulate the fuzzy state feedback control for the stabilization problem and determine the sufficient conditions under LMIs form.

Notations: The following notation is used to denote an index set $\mathcal{I}_N := \{1, 2, \ldots, N\} \subset \mathbb{N}$. For a vector $\mathbf{x} \in \mathbb{R}^n$, we denote the k$^{\text{th}}$ - component by x_k and its transpose by $\mathbf{x}^\top$. The sets $\mathbb{S}_n$ and $\mathbb{S}_n^{++}$ denote for the sets of symmetric and positive definite symmetric matrices of order n, respectively. The set $\mathbb{R}_+^n$ consists of all vectors with non-negative components. The notations $\mathbf{0}$ and $\mathbf{1}$ stand for the zero matrix and unity matrix, respectively. For each $n \in \mathbb{N}$, denote $\mathbb{P}(i)$ by the probability that a node has the degree of i and $\langle N\rangle = \sum_{i=1}^{N} i\mathbb{P}(i)$ by the mean degree of the network.

II. THE FRACTIONAL INTERCONNECTED TAKAGI-SUGENO FUZZY SYSTEM

Many previous works have proved that Takagi-Sugeno (TS) fuzzy system is an efficient method for better simulating various classes of nonlinear dynamical systems [10, 11, 13, 18]. In this paper, we propose an extension of Takagi-Sugeno fuzzy system for a fractional network-based dynamical model which consists of N interconnected fractional differential subsystems with observer:

$$\begin{cases} \mathfrak{D}_{+}^{\alpha}\mathbf{x}_i(t) = \mathrm{F}\left(\mathbf{x}_i(t),\mathbf{u}_i(t)\right) + \sum_{j=1}^{N} \mathrm{F}_{ij}\left(\mathbf{x}_i(t),\mathbf{x}_j(t)\right) \\ \mathbf{y}_i(t) = \overline{\mathrm{F}}\left(\mathbf{x}_i(t)\right), \end{cases}$$

where $i \in \mathcal{I}_N$, the mappings F, $\overline{\mathrm{F}}$ and F_{ij} are the state function, connectivity function and observer function, respectively. Next, by using some appropriate methods such as identification, sector non-linearity or linearization [10], we can directly construct a generalized Takagi-Sugeno fuzzy system $\mathbf{S}$ composed of N fractional interconnected Takagi-Sugeno fuzzy system whose fuzzy rules are given in Figure 1. Where A_i^k, B_i^k, D_i^k are constructed matrices and Θ_{ij}^k is the connectivity matrix between the subsystem $\mathbf{S}_i$ and $\mathbf{S}_j$ in the i^th^ - rule. The index Δ_i is the number of fuzzy rules in the subsystem $\mathbf{S}_i$. For each $k \in \{1, 2, \ldots, \Delta_i\}$, some terms of the subsystem $\mathbf{S}_i$ can be explained as follows:

- $\mathbf{z}_i(t) = \begin{bmatrix} z_{i1}(t) & z_{i2}(t) & \cdots & z_{iq}(t) \end{bmatrix}^{\top}$ is a premise variable vector of the subsystem $\mathbf{S}_i$. Note that the premise variable vector $\mathbf{z}_i(t)$ is often chosen by $\mathbf{x}_i(t)$ or a function of $\mathbf{x}_i(t)$.

- For each $j = 1, 2, \ldots, p$, the set M_{ij}^k are antecedent fuzzy sets of the k^th^ - rule.

Finally, by combining all fuzzy rules of the i^th^ - subsystem, we receive:

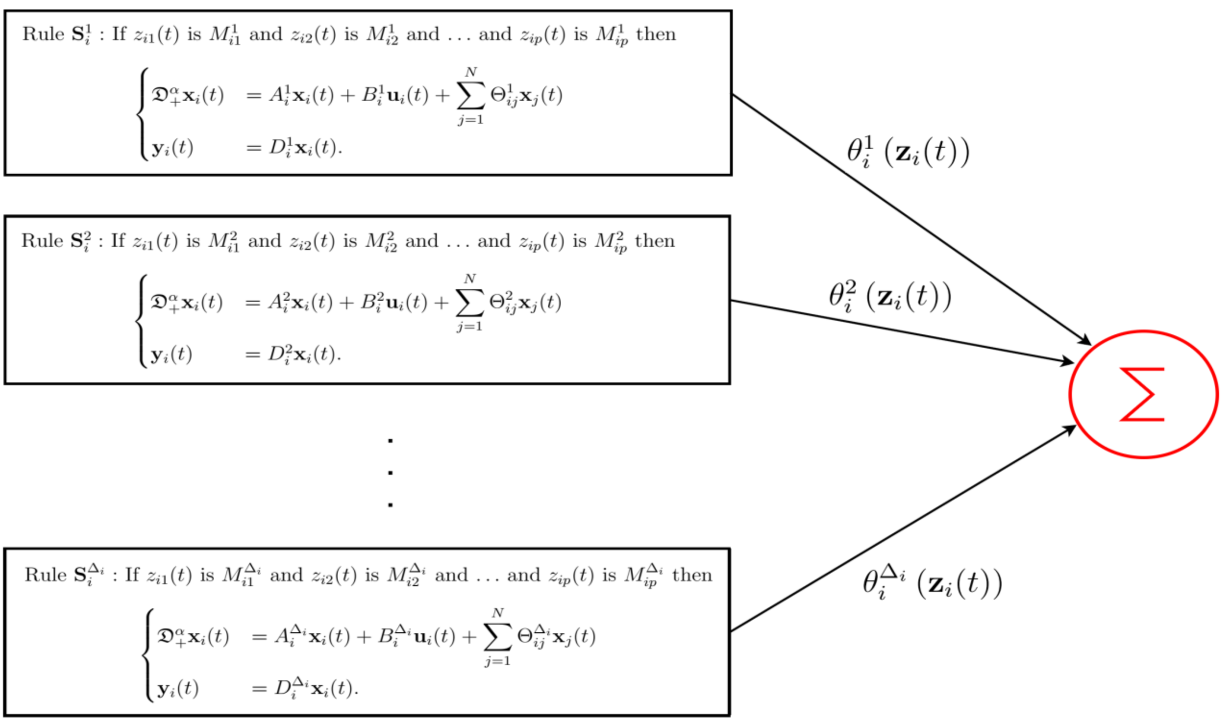

Figure 1. The fractional interconnected Takagi-Sugeno fuzzy system for the i^th^ - subsystem

$$\begin{cases} \mathfrak{D}_{+}^{\alpha}\mathbf{x}_i(t) = \sum_{k=1}^{\Delta_i}\theta_i^k\left(\mathbf{z}_i(t)\right)\Big\{A_i^k\mathbf{x}_i(t) + B_i^k\mathbf{u}_i(t) \\ \qquad\qquad\qquad\qquad + \sum_{j=1}^{N}\Theta_{ij}^k\mathbf{x}_j(t)\Big\} \\ \mathbf{y}_i(t) = \sum_{k=1}^{\Delta_i}\theta_i^k\left(\mathbf{z}_i(t)\right)D_i^k\mathbf{x}_i(t), \end{cases}$$

where $\varphi_i^k\left(\mathbf{z}_i(t)\right) = \prod_{j=1}^{p} M_{ij}^k\left(z_{ij}(t)\right)$ and the normalized weight of the k^{th} - fuzzy rule is given by:

$$\theta_i^k\left(\mathbf{z}_i(t)\right) = \frac{\varphi_i^k\left(\mathbf{z}_i(t)\right)}{\sum_{k=1}^{\Delta_i}\varphi_i^k\left(\mathbf{z}_i(t)\right)}.$$

III. A NEW NETWORK-BASED MODEL FOR MALWARE PROPAGATION

A. The formulation of malware propagation model

In this work, we aim to characterize the spread of malicious objects on heterogeneous complex network by using a compartmental model with reinfection where the whole population of nodes is classified into four following compartments:

(S) Susceptible compartment consists of all nodes which are free of malicious codes but are vulnerable by malware programs.

(C) Carrier compartment consists of all nodes which are not damaged by malicious objects but can propagate malicious codes along with information transmitting process, i.e., they serve as spreading vector.

(I) Infectious compartment consists of all nodes which have been infected by malicious codes and are directly influenced by malware actions such as deplete node's energy, cause damage to node and can transmit malicious code to its neighbor nodes.

(R) Recovered compartment consists of all carrier and infectious nodes that are removed all malicious codes and they are regarded to be temporary immunity against malware attacks.

Recently, there have several works studied compartmental malware propagation models in information networks that divided the set of nodes spreading malicious codes into the set of infectious nodes, i.e., nodes are damaged by malicious codes, and the set of carrier nodes, i.e., nodes are just transmission vector. For example, see [3, 4]. These models, like many preceding classical malware propagation models, were constructed by using the well-mixed assumption of the network's nodes, that is, the rate of contact causing malware spread is assumed to be similar for all network's nodes.

However, it is a fact that the structures of many real-world complex networks are hierarchic and hence, the malware propagation on these networks is heterogeneous, that is, the higher degree a node has, the greater the malware infection rate and the ability to spread malicious code (if infected) to other nodes are. Consequently, this paper considers a malware propagation model on heterogeneous complex network by dividing the whole population into N groups and in each group, the nodes are assumed to have same epidemiological property and belong to one of four possible compartments: **(S) - (C) - (I) - (R)**. In addition, we assume that there is a rate η of reinfection of recovered nodes, that is the reason why our considered model is named by network-based SCIRS malware propagation model. Now, we denote by $S_i(t), C_i(t), I_i(t), R_i(t)$ and $N_i(t)$ by the density of susceptible nodes, carrier nodes, infectious nodes, recovered nodes and total population in the i^{th} – group.

The interactions between compartments of the proposed malware propagation model can be schematically described in Figure 2. We can see that the network has a rate A of a new node logging in and a rate d of an out-of energy node logging out. A susceptible node of degree i can become a carrier node and infectious node at the rate $\sigma_i(1-\beta)\Psi_1$ and $\sigma_i\beta\Psi_2$, respectively. Under the action of anti-malware programs, the malicious objects can be removed from the network and then, infected nodes including carrier and infectious node become recovered nodes with the rate of ω and ϖ.

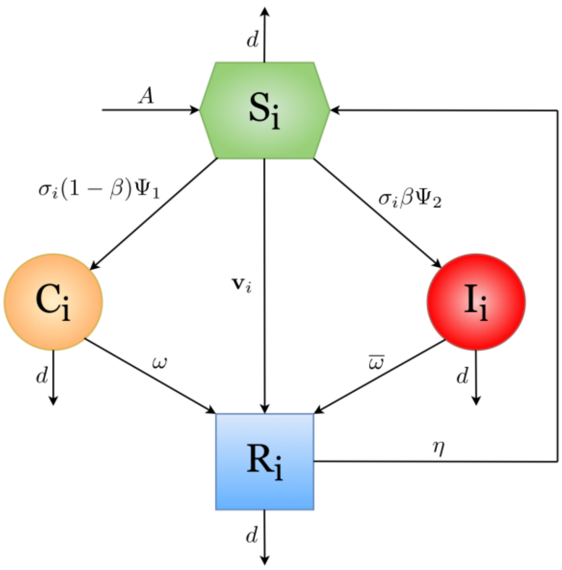

Figure 2. The flowchart of SCIRS malware propagation model in the i^{th} - group

However, the immunization is just temporary and a recovered node can be lose the immunity and back to the compartment **(S)** at a rate of η. Here, in order to ensure the balance in size and structure of the network, we assume that $A = d$. The proposed model's parameters endowed with their descriptions are given in Table 1.

TABLE 1. THE USED PARAMETERS

No	Para.	Description
1	A	The rate of a new node joining the network
2	d	The rate of an out-of-energy node logging out the network
3	β	The ratio of susceptible nodes targeted by malicious codes
4	σ_i	The degree-dependent transmission rate $\sigma_i = i\sigma$
5	ω	The antivirus rate of carrier nodes
6	ϖ	The antivirus rate of infectious nodes
7	η	The rate of a recovered node losing immunity
8	$\mathbf{v}_i(t)$	The degree-dependent quarantine control

Since fractional differential equations and its applications have proved their great ability in accurately modeling a lots of physical systems and non-local phenomena, this work proposes to use fractional derivative to describe the dynamics of proposed network-based malware propagation model. Finally, the interactions among four compartments of the i^{th} - group can be characterized by the following fractional differential system:

$$
\begin{cases}
\mathfrak{D}_+^\alpha S_i(t) = -\sigma_i\left[(1-\beta)\Psi_1(t) + \beta\Psi_2(t)\right]S_i(t) \\
\qquad\qquad + \eta R_i(t) - \left(\mathbf{v}_i(t) + d\right)S_i(t) + A \\
\mathfrak{D}_+^\alpha C_i(t) = \sigma_i(1-\beta)\Psi_1(t)S_i(t) - \left(\omega + d\right)C_i(t) \\
\mathfrak{D}_+^\alpha I_i(t) = \sigma_i\beta\Psi_2(t)S_i(t) - \left(\varpi + d\right)I_i(t) \\
\mathfrak{D}_+^\alpha R_i(t) = \omega C_i(t) + \varpi I_i(t) - (d+\eta)R_i(t) \\
\qquad\qquad + \mathbf{v}_i(t)S_i(t),
\end{cases}
$$

where the notation $\mathfrak{D}_+^\alpha(\cdot)$ is the well-known Caputo fractional derivative of the state functions (see Definition VI.1 in Appendix section) and all model's parameters are non-negative. The function $\mathbf{v}_i(t)$ is a time-dependent input control, which is known as the malware preventive treatment of susceptible nodes by using firewall or antivirus program. In addition, the functions $\Psi_1(t)$ and $\Psi_2(t)$ are probabilities that a given link is connected to a carrier node or an infectious node, respectively. Moreover, we have:

$$
\Psi_1(t) = \langle N\rangle^{-1}\sum_{i=1}^{N} i\mathbb{P}(i)C_i(t)
$$

$$
\Psi_2(t) = \langle N\rangle^{-1}\sum_{i=1}^{N} i\mathbb{P}(i)I_i(t).
$$

B. The analysis of malware propagation model

Based on the formulation of fractional network-based SCIRS malware propagation model, we present some its characteristic properties:

- We regard the input control as the rate of susceptible nodes that are protected against malware code's attack by firewall or antivirus software and hence, we denote by the admissible control set on $[0,T]$.

$$
\mathcal{V} = \left\{\mathbf{v} \in \left(L^1[0,T]\right)^n : 0 \le \mathbf{v}_i(t) \le 1, i \in \mathcal{I}_N\right\}
$$

- For each $\mathbf{v} \in \mathcal{V}$, the positively invariant set Σ_+ of the proposed malware propagation model is given by:

$$
\Sigma_+ = \left\{\mathbf{x}(t) \in \mathbb{R}_+^{4N} : N_i(t) \le 1, i \in \mathcal{I}_N\right\},
$$

where $\mathbf{x}(t)=\left\{\left(S_i,C_i,I_i,R_i\right)\right\}_{i=\overline{1,N}}$ is the state vector of the proposed model.

- Denote $\mathbf{a}_i=d+\eta+\mathbf{v}_i$. Then, for each $\mathbf{v}\in\mathcal{V}$, the proposed malware propagation model admits a unique malware-free equilibrium $\mathcal{E}_{0,\mathbf{v}}$ given by:

$$\mathcal{E}_{0,\mathbf{v}}=\left\{\left(\frac{d+\eta}{\mathbf{a}_i},0,0,\frac{\mathbf{v}_i}{\mathbf{a}_i}\right)\right\}_{i=\overline{1,N}}.$$

Especially, if $\mathbf{v}\equiv\mathbf{0}$ then the equilibrium $\mathcal{E}_{0,\mathbf{v}}$ becomes $\mathcal{E}_0=\underbrace{(1,0,0,0,\ldots,1,0,0,0)}_{4N}$.

- By next-generation matrix method, the basic reproduction number $\mathcal{R}_0$, given by:

$$\mathcal{R}_0=\frac{\sigma(d+\eta)\langle\mathbf{v}N\rangle}{\langle N\rangle}\max\left\{\frac{1-\beta}{\omega+d},\frac{\beta}{\overline{\omega}+d}\right\},$$

strongly depends on the input control $\mathbf{v}_i(t)$, in which $\langle\mathbf{v}N\rangle=\sum_{i=1}^{N}\frac{i^2\mathbb{P}(i)}{d+\eta+\mathbf{v}_i}$.

- If $\mathcal{R}_0<1$ then the malware-free equilibrium $\mathcal{E}_{0,\mathbf{v}}$ is globally asymptotically stable on Σ_+, that is, the malware propagation on the network will be extinguished.

IV. FUZZY STATE FEEDBACK CONTROL

Our goal is to establish a quarantine input control $\mathbf{v}(t)=\left[\mathbf{v}_1(t)\ \cdots\ \mathbf{v}_N(t)\right]^\top$ so as to steer the state vector $\mathbf{x}(t)$ of the fractional network-based SCIRS malware propagation model into the equilibrium state $\mathcal{E}_0$, which means that the unstable malware-free equilibrium is stabilized. Some control techniques were proposed to study various stabilization problems for malware propagation models such as [9, 10, 13, 22]. However, there have not had any work done on the stabilization of fractional network-based models. Thus, in order to dealing with the stabilization problem for the proposed network-based malware propagation model, we consider a fuzzy state feedback control of the form $\mathbf{v}_i(t)=L_i^k\mathbf{y}_i(t)$, where L_i^k are control gain matrices for each $i\in\mathcal{I}_N$. Now, we will establish an interconnected Takagi-Sugeno fuzzy model for the proposed malware propagation model. Since the rate A of newly joining nodes is equal to the rate d of logging-out nodes, we can use the substitution $S_i=1-(C_i+I_i+R_i)$ to reduce the complexity of computations. It should be noted that the state function $S_i(t)$ is positive and always receive a constant rate A of newly joining nodes, we can reasonably assume that $C_i+I_i+R_i\in[0.1;0.9]$. Hence, by denoting:

$$\mathbf{w}(t)=\left\{\left(C_i,I_i,R_i\right)\right\}_{i=\overline{1,N}},$$

we receive the following system:

$$\begin{aligned}\mathfrak{D}_+^{\alpha}\mathbf{w}_i(t)&=\begin{bmatrix}w_i^{11}&0&0\\0&w_i^{22}&0\\\omega&\overline{\omega}&-(d+\eta)\end{bmatrix}\mathbf{w}_i(t)\\&+\begin{bmatrix}0\\0\\S_i-1\end{bmatrix}\mathbf{v}_i(t)\\&+\sum_{\substack{j=1\\j\neq i}}^{N}\begin{bmatrix}w_{ij}^{11}&0&0\\0&w_{ij}^{22}&0\\0&0&0\end{bmatrix}\mathbf{w}_j(t),\end{aligned}\tag{1.1}$$

where the entries of matrices are given by:

$$w_i^{11}=-(\omega+d)+\frac{\sigma_i(1-\beta)i\mathbb{P}(i)(S_i-1)}{\langle N\rangle}$$

$$w_i^{22}=-(\overline{\omega}+d)+\frac{\sigma_i\beta i\mathbb{P}(i)(S_i-1)}{\langle N\rangle}$$

$$w_{ij}^{11}=\frac{\sigma_i(1-\beta)j\mathbb{P}(j)(S_i-1)}{\langle N\rangle}$$

$$w_{ij}^{22}=\frac{\sigma_i\beta j\mathbb{P}(j)(S_i-1)}{\langle N\rangle}.$$

Next, we choose the premise variable $\mathbf{z}_i(t)$ by non-constant term $S_i\in[0.1;0.9]$ in the system (1.1) with corresponding weighting functions:

$$\nu_{i1}^{1}\left(\mathbf{z}_i(t)\right)=\frac{1-\mathbf{z}_i(t)}{0.8},\ \nu_{i2}^{1}\left(\mathbf{z}_i(t)\right)=\frac{\mathbf{z}_i(t)-0.2}{0.8}.$$

Thus, the premise variable $\mathbf{z}_i(t)$ is rewritten as:

$$\mathbf{z}_i(t)=0.1\nu_{i1}^{1}\left(\mathbf{z}_i(t)\right)+0.9\nu_{i2}^{1}\left(\mathbf{z}_i(t)\right).$$

Now, let $M_{i,1}$ and $M_{i,2}$ be two antecedent fuzzy sets subjecting to two above weighting functions $\nu_{i1}^{1}\left(\mathbf{z}_i(t)\right)$ and $\nu_{i2}^{1}\left(\mathbf{z}_i(t)\right)$, respectively (Figure 3). Denote $\theta_i^k\left(\mathbf{z}_i(t)\right)=\dfrac{\nu_{ik}(\mathbf{z}_i(t))}{\sum_{k=1}^{2}\nu_{ik}(\mathbf{z}_i(t))}$.

Next, we give the appropriate fuzzy rules: Rule $\mathbf{S}_i^k$: If $\mathbf{z}_i(t)$ is $M_{i,k}$ then

$$\begin{cases}\mathfrak{D}_+^{\alpha}\mathbf{w}_i(t)=A_i^k\mathbf{w}_i(t)+B_i^k\mathbf{v}_i(t)+\sum\limits_{\substack{j=1\\ j\neq i}}^{N}\Theta_{ij}^k\mathbf{w}_j(t)\\ \mathbf{y}_i=D_i^k\mathbf{w}_i(t),\end{cases}$$

and the controller for Rule $\mathbf{S}_i^k$ is:

$$\mathbf{v}_i(t)=L_i^k\mathbf{w}_i(t)$$

for each $k=1,2$, where A_i^k, B_i^k, D_i^k and Θ_{ij}^k are constant matrices, that will be specified later. Then, the fractional interconnected Takagi-Sugeno fuzzy system for the subsystem $\mathbf{S}_i$ is given by:

$$\mathfrak{D}_+^{\alpha}\mathbf{w}_i(t)=\sum_{k=1}^{2}\theta_i^k\left(\mathbf{z}_i(t)\right)\Big\{A_i^k\mathbf{w}_i(t)+B_i^k\mathbf{v}_i(t)+\sum_{\substack{j=1\\ j\neq i}}^{N}\Theta_{ij}^k\mathbf{w}_j(t)\Big\}, \tag{1.2}$$

and the static fuzzy state feedback controller $\mathbf{v}_i(t)$ is given by:

$$\mathbf{v}_i=\sum_{k=1}^{2}\theta_i^k\left(\mathbf{z}_i(t)\right)L_i^k\mathbf{w}_i(t). \tag{1.3}$$

For simplicity in representation, we use θ_i^k instead of $\theta_i^k\left(\mathbf{z}_i(t)\right)$. By substituting the control (1.3) into the system (1.2), we directly obtain:

$$\begin{aligned}\mathfrak{D}_+^{\alpha}\mathbf{w}_i(t)=&\sum_{k=1}^{2}\left(\theta_i^k\right)^2\mathrm{W}_i^{kk}\mathbf{w}_i(t)\\&+\sum_{k=1}^{2}\sum_{j=1}^{N}\theta_i^k\Theta_{ij}^k\mathbf{w}_j(t)\\&+\sum_{k=1}^{2}w_i^p w_i^2\left(\mathrm{W}_i^{k2}+\mathrm{W}_i^{2k}\right)\mathbf{w}_i(t),\end{aligned} \tag{1.4}$$

where $W_i^{kp}=A_i^k+B_i^kL_i^p$ for $k=1,2$ and $i\in\mathcal{I}_N$. Next, by using the quadratic Lyapunov function

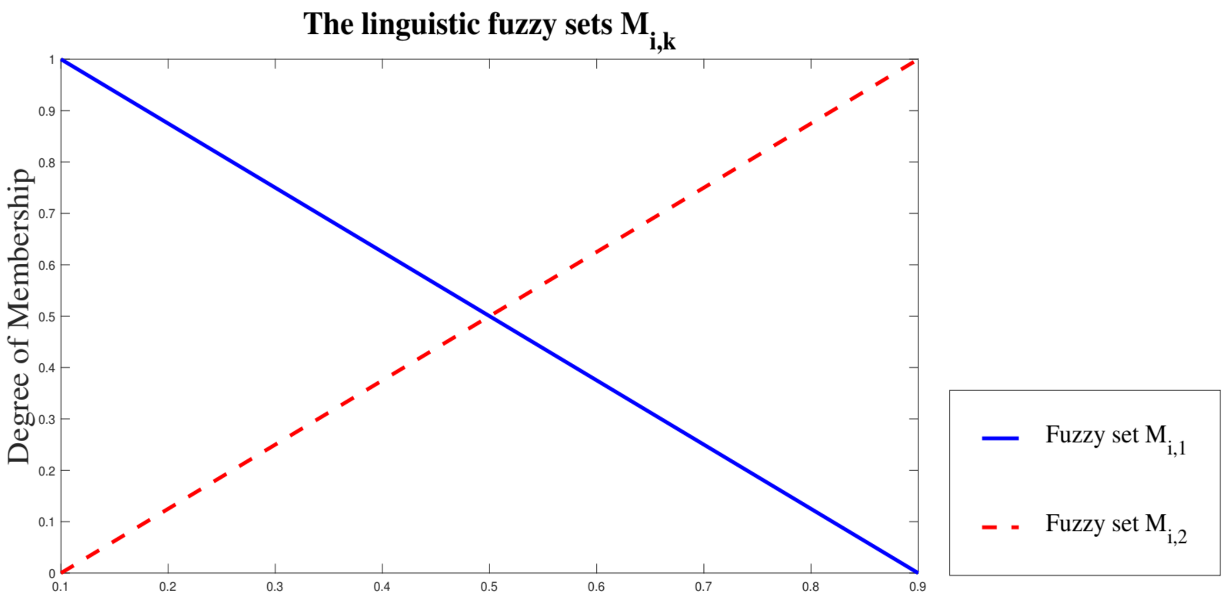

Figure 3. The membership functions of antecedent fuzzy sets

$\mathrm{L}\big(\mathbf{w}(t)\big)=\sum_{j=1}^{N}\mathrm{L}_i\big(\mathbf{w}(t)\big)=\sum_{j=1}^{N}\mathbf{w}_i^{\top}(t)\mathrm{Q}_i\mathbf{w}_i(t)$ and Lemma VI.1, we can establish some sufficient conditions for the proposed stabilization problem in linear matrix inequality form:

$$\begin{aligned}
&\mathrm{Q}_i \in \mathbb{S}^N_{++}\\
&\mathrm{H}_i^{kp}, \mathrm{H}_{ij}^{kp} \in \mathbb{S}^N\\
&\mathbf{0} < (W_i^{kp})^{\top}\mathrm{Q}_i + \mathrm{Q}_i W_i^{kp} \le \mathrm{H}_i^{kp}\\
&\left(\Theta_{ij}^{k}\right)^{\top}\mathrm{Q}_i + \mathrm{Q}_i\Theta_{ij}^{k} + \left(\Theta_{ji}^{p}\right)^{\top}\mathrm{Q}_j\\
&\qquad\qquad + \mathrm{Q}_j\Theta_{ji}^{p} \le 2\mathrm{H}_{ij}^{kp}\\
&\mathbb{H} = \begin{bmatrix} \mathrm{H}_1 & \cdots & \mathrm{H}_{1N}\\ \vdots & \ddots & \vdots\\ \mathrm{H}_{1N}^{\top} & \cdots & \mathrm{H}_N \end{bmatrix} < 0,
\end{aligned} \tag{1.5}$$

in which for each $k, p \in \{1,2\}$, entries of the matrix $\mathbb{H}$ is given by:

$$\mathrm{H}_i = \begin{bmatrix} \mathrm{H}_i^{11} & \mathrm{H}_i^{12}\\ (\mathrm{H}_i^{12})^{\top} & \mathrm{H}_i^{22} \end{bmatrix}, \mathrm{H}_{ij} = \begin{bmatrix} \mathrm{H}_{ij}^{11} & \mathrm{H}_{ij}^{12}\\ \mathrm{H}_{ij}^{21} & \mathrm{H}_{ij}^{22} \end{bmatrix}.$$

Remark IV.1. In order to solve the system of linear matrix inequalities (1.5), we use the variable changing $\mathrm{P}_i = \mathrm{Q}_i^{-1}$ and carry out some transformations based on Schur complement theorem (see Property 3.2 in [10]) to construct an equivalent LMIs system that is solvable by lmi solver toolbox in MATLAB.

V. ILLUSTRATING EXAMPLE

In the following, we illustrate the obtained theoretic result by considering the malware propagation on a heterogeneous complex network with maximum number of contact $N = 2$ and consider the model's parameters as:

$$A = d = 0.05, \quad \beta = 0.6, \quad \sigma = 0.8,$$
$$\omega = 0.2, \quad \bar{\varpi} = 0.4, \quad \eta = 0.01.$$

In addition, by direct computations, we obtain:

$$\langle N\rangle = \frac{10}{9}, \qquad \langle N^2\rangle = \frac{4}{3}.$$

Then, for each $i, j \in \mathcal{I}_N$ and $k \in \{1,2\}$, the matrices A_i^k, B_i^k and Θ_{ij}^k are given by:

$$A_1^1 = \begin{bmatrix} -0.4804 & 0 & 0\\ 0 & -0.7956 & 0\\ 0.2 & 0.4 & -0.06 \end{bmatrix}; B_1^1 = \begin{bmatrix} 0\\ 0\\ -0.9 \end{bmatrix}$$

$$A_1^2 = \begin{bmatrix} -0.2756 & 0 & 0\\ 0 & -0.4884 & 0\\ 0.2 & 0.4 & -0.06 \end{bmatrix}; B_1^1 = \begin{bmatrix} 0\\ 0\\ -0.1 \end{bmatrix}$$

$$A_2^1 = \begin{bmatrix} -0.3652 & 0 & 0\\ 0 & -0.6228 & 0\\ 0.2 & 0.4 & -0.06 \end{bmatrix}; B_1^1 = \begin{bmatrix} 0\\ 0\\ -0.9 \end{bmatrix}$$

$$A_2^2 = \begin{bmatrix} -0.2628 & 0 & 0\\ 0 & -0.4692 & 0\\ 0.2 & 0.4 & -0.06 \end{bmatrix}; B_1^1 = \begin{bmatrix} 0\\ 0\\ -0.1 \end{bmatrix}$$

$$\Theta_{12}^1 = \begin{bmatrix} -0.0576 & 0 & 0\\ 0 & -0.0864 & 0\\ 0 & 0 & 0 \end{bmatrix}$$

$$\Theta_{12}^2 = \begin{bmatrix} -0.0064 & 0 & 0\\ 0 & -0.0096 & 0\\ 0 & 0 & 0 \end{bmatrix}$$

$$\Theta_{21}^1 = \begin{bmatrix} -0.4608 & 0 & 0\\ 0 & -0.6912 & 0\\ 0 & 0 & 0 \end{bmatrix}$$

$$\Theta_{21}^2 = \begin{bmatrix} -0.0512 & 0 & 0\\ 0 & -0.0768 & 0\\ 0 & 0 & 0 \end{bmatrix}$$

Finally, by using the *lmi* toolbox in MATLAB for the system of LMIs (1.5), we need to solve 34 linear matrix inequalities and receive the following results. The positive definite matrices Q_i:

$$\mathrm{Q}_1 = \begin{bmatrix} 0.0258 & -0.0058 & -0.0124\\ -0.0058 & 0.0359 & -0.0186\\ -0.0124 & -0.0186 & -0.0285 \end{bmatrix}$$

$$\mathrm{Q}_2 = \begin{bmatrix} 0.0350 & 0.0013 & 0.0009\\ 0.0013 & 0.0532 & 0.0019\\ 0.0009 & 0.0019 & 0.0181 \end{bmatrix}.$$

The gain matrices L_i^k :

$$L_1^1 = \begin{bmatrix} 0.0178 & 0.3647 & -1.1440 \end{bmatrix}^\top$$
$$L_1^2 = \begin{bmatrix} 0.3077 & 1.1925 & -1.8409 \end{bmatrix}^\top$$
$$L_2^1 = \begin{bmatrix} 0.2572 & 0.5720 & 0.3957 \end{bmatrix}^\top$$
$$L_2^2 = \begin{bmatrix} 0.6549 & 1.4274 & 0.4712 \end{bmatrix}^\top.$$

VI. APPENDIX

In this section, we briefly recall from [2, 14] some auxiliary results used throughout this paper:

Definition VI.1 ([2]). Let $\alpha \in (0,1]$. The Caputo fractional derivative of order α of a function $f \in C^1(0,T)$ is defined by:

$$\mathfrak{D}_+^\alpha f(t) = \frac{1}{\Gamma(1-\alpha)} \int_0^t (t-s)^{-\alpha} f'(s) ds.$$

Consider a Cauchy problem for the following fractional differential system:

$$\mathfrak{D}_+^\alpha \mathbf{x}(t) = A\mathbf{x}(t) + f(\mathbf{x}(t)), \qquad t > 0 \quad (1.6)$$

subjecting to the initial condition $\mathbf{x}(0) = \mathbf{x}_0$, where A is a matrix of order n and $f : \mathbb{R}^n \to \mathbb{R}^n$ is a continuously differentiable function satisfying $f(\mathbf{0}) = \mathbf{0}$.

Definition VI.2 ([2]). The trivial solution $\mathbf{x} \equiv \mathbf{0}$ of the equation (1.6) is said to be *asymptotically stable* if it is *stable* and *attractive*, i.e., there exists a $\gamma > 0$ such that $\lim_{t\to\infty} \|\varphi(t, \mathbf{x}_0)\| = 0$ whenever $\| \mathbf{x}_0 \| < \gamma$.

Lemma VI.1 ([14]). Let $\mathbf{x}(t) \in \mathbb{R}^n$ be a continuously differentiable function and $\mathrm{P} \in \mathbb{S}_n^{++}$. Then, for each $t > 0$, the following inequality holds.

$$\frac{1}{2}\mathfrak{D}_+^\alpha \left(\mathbf{x}^\top(t) \mathrm{P} \mathbf{x}(t) \right) \le \mathbf{x}^\top(t) \mathrm{P} \mathfrak{D}_+^\alpha \mathbf{x}(t).$$

VII. CONCLUSIONS

In this paper, we suggest a new Takagi-Sugeno fuzzy system approach for a stabilization problem of a controlled fractional SCIRS malware propagation model on heterogeneous complex network with fuzzy state-feedback controller, which is one of the applicable models for malware spread prediction and epidemic controlling. The novelty of the proposed malware propagation model is the use of network-based construction in order to take into account the heterogeneity of complex network and considering the malware spreading class consisting of two compartments: Infectious (be damaged by malware code) and Carrier (be just transmission vector). The main result is obtained by using a quadratic Lyapunov function and gives some sufficient conditions in LMIs form to ensure the state-feedback stabilization of the proposed interconnected Takakgi-Sugeno fuzzy system. Finally, some numerical computations are done to illustrate the effectiveness of theoretic results.

ACKNOWNLEDGMENT

This work was supported by the Ministry of Education and Training of Vietnam via grant number B.2023-SP2-03. Nguyen Phuong Dong was funded by Vingroup JSC and supported by the PhD Scholarship Programme of Vingroup Innovation Foundation (VINIF), Institute of Big Data, code VINIF.2022.TS.022.

REFERENCES

[1] Y. Chen, F. Liu, Q. Yu & T. Li, “Review of fractional epidemic models”, Appl. Math. Model., 97 (2021), pp. 281-307.

[2] K. Diethelm, “The analysis of fractional differential equations. An application-oriented exposition using differential operators of Caputo type”, Lecture Notes in Mathematics, Vol. 2004, Springer-Verlag, Berlin, 2010.

[3] J.D. Hernández Guillén and A. Martín del Rey, “Modeling malware propagation using a carrier compartment”, Commun. Nonlinear Sci. Numer. Simulat., 56 (2018), pp. 217–226.

[4] J.D. Hernández Guillén and A. Martín del Rey, “A mathematical model for malware spread on WSNs with population dynamics”, Physica A, 545 (2020), pp. 123609.

[5] S. Hosseini and A. Zandvakili, “The SEIRS-C model of information diffusion based on rumour spreading with fuzzy logic in social networks”, Inter. J. Comput. Math., 99 (9) (2022), pp. 1918-1940.

[6] S. Huang, F. Chen and L. Chen, “Global dynamics of a network-based SIQRS epidemic model with demographics and vaccination”, Commun. Nonlinear Sci. Numer. Simulat., 43 (2017), pp. 296-310.

[7] J. Huo and H. Zhao, “Dynamical analysis of a fractional SIR model with birth and death on heterogeneous complex networks”, Phys. A, 448 (2016), pp. 41-56.

[8] W.O. Kermack and A.G. McKendrick, “A contribution to the mathematical theory of epidemics”, Proc. Roy. Soc. London, 115 (1927), pp. 700-721.

[9] H.J. Lee, “Robust static output-feedback vaccination policy design for an uncertain SIR epidemic model with disturbances: Positive Takagi–Sugeno model approach”, Biomed. Signal Process. Control, 72 (2022), Part A, pp. 103273.

[10] Z. Lendek, T. Guerra, R. Babuska and B. De Schutter, “Stability Analysis and Nonlinear Observer Design Using Takagi-Sugeno Fuzzy Models”, in Studies in Fuzziness and Soft Computing, Springer, vol. 262, 2010.

[11] Y. Li and J. Li, “Stability analysis of fractional order systems based on T-S fuzzy model with the fractional order $\alpha : 0 < \alpha < 1$”, Nonlinear Dyn., 78 (2014), pp 2909–2919.

[12] K. Li, G. Zhu, Z. Ma and L. Chen, “Dynamic stability of an SIQS epidemic network and its optimal control”, Commun. Nonlinear Sci. Numer. Simulat., 66 (2019), pp. 84-95.

[13] W.W. Lin, W.J. Wang and S.H. Yang, “A novel stabilization criterion for large-scale T-S fuzzy systems”, IEEE Trans. Syst. Man Cybern. B. Cybern., 37 (4) (2007), pp. 1074-9.

[14] M.A. Duarte-Mermoud, N. Aguila-Camacho, J.A. Gallegos and R. Castro-Linares, “Using general quadratic Lyapunov functions to prove Lyapunov uniform stability for fractional order systems”, Commun. Nonlinear Sci. Numer. Simulat., 22 (1–3) (2015), pp. 650-659.

[15] B.K. Mishra and D.K. Saini, “SEIRS epidemic model with delay for transmission of malicious objects in computer network”, Appl. Math. Comput., 188 (2) (2007), pp. 1476-1482.

[16] B.K. Mishra and N. Keshri, “Mathematical model on the transmission of worms in wireless sensor network”, Appl. Math. Model., 37 (6) (2013), pp. 4103-4111.

[17] M. Di Paola, A. Pirrotta and A. Valenza, “Visco-elastic behavior through fractional calculus: An easier method for best fitting experimental results”, Mech. Mater., 43 (12) (2011), pp. 799-806.

[18] T. Takagi and M. Sugeno, “Fuzzy identification of systems and its applications to modeling and control”, IEEE Trans. Syst., Man, Cybern., 15 (1) (1985), pp. 116–132.

[19] H. M. Tuan and P.H. Thu, “Extrapolated nonstandard numerical schemes for solving an epidemiological model for computer viruses”, Journal of Science and Technology on Information Security, 3 (17) (2023), pp. 17-25.

[20] T.A. Tuan, N.N. Cuong, N. V. Anh and H.V. Long, “Proposing the application of a deep learning model to detect the malicious IP address of botnet in the computer network”, Journal of Science and Technology on Information Security, 3 (17) (2023), pp. 43-52.

[21] L.X. Yang, M. Draief and X. Yang, “The optimal dynamic immunization under a controlled heterogeneous node-based SIRS model”, Phys. A, 450 (2016), pp. 403-415.

[22] X. Zhang, Z. Cheng and Q. Liu, “A fuzzy logic approach to optimal control of nonlinear time-delay systems}, Fifth World Congress on Intelligent Control and Automation (IEEE Cat. No.04EX788), (1) (2004), pp. 902-906.

ABOUT THE AUTHORS

Nguyen Ngoc Quynh

Workplace: University of Engineering and Technology, Vietnam National University, Hanoi.

Email: nguyenngocquynh1997@vnu.edu.vn

Education: She received her BSc, MSc in Information Technology and Information Systems; She is a PhD student in Computer Science at Graduate University of Science and Technology (VAST) now.

Recent research interests: Information security; Imagine processing.

Cơ quan làm việc: Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội.

Email: nguyenngocquynh1997@vnu.edu.vn

Quá trình đào tạo: Nhận bằng Cử nhân, Thạc sĩ Công nghệ thông tin và Hệ thống thông tin; Hiện đang là nghiên cứu sinh ngành Khoa học máy tính tại Trường Đại học Khoa học và Công nghệ Hà Nội.

Hướng nghiên cứu hiện nay: Bảo mật thông tin; Xử lý hình ảnh.

Nguyen Phuong Dong

Workplace: Faculty of Mathematics, Hanoi Pedagogical University 2.

Email: nguyenphuongdong@hpu2.edu.vn

Education: He received his BSc, MSc in Mathematics Analysis from Hanoi National University of Education and is PhD student in Applied Mathematics at Graduate University of Science and Technology (VAST) now.

Recent research interests: Applied athematics; Fuzzy mathematics.

Cơ quan làm việc: Khoa Toán, Trường Đại học Sư phạm Hà Nội 2.

Email: nguyenphuongdong@hpu2.edu.vn

Quá trình đào tạo: Nhận bằng Cử nhân, Thạc sĩ Phân tích Toán học tại Trường Đại học Sư phạm Hà Nội; Hiện đang là nghiên cứu sinh Toán Ứng dụng tại Trường Đại học Khoa học và Công nghệ Hà Nội.

HƯớng nghiên cứu hiện nay: Ứng dụng toán học; Toán học mờ.

Nguyen Long Giang

Workplace: Institute of Information Technology, Vietnam Academy of Science and Technology.

Email: nlgiang@ioit.ac.vn

Education: He received his BSc, MSc in Information Technology from University of Engineering and Technology (VNU), PhD. degree in Mathematical assurance for computers and computational systems at Graduate University of Science and Technology in 2012.

Recent research interests: Data science; Soft computing.

Cơ quan làm việc: Viện Công nghệ thông tin, Viện Hàn lâm Khoa học và Công nghệ Việt Nam.

Email: nlgiang@ioit.ac.vn

Quá trình đào tạo: Nhận bằng Cử nhân, Thạc sĩ Công nghệ thông tin tại Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội; Tiến sĩ ngành Đảm bảo toán học cho máy tính và hệ thống tính toán tại Đại học Bách khoa Hà Nội vào năm 2012.

Hướng nghiên cứu hiện nay: Khoa học dữ liệu; Tính toán mềm.

Hoang Viet Long

Workplace: Faculty of Information Technology, University of Technology-Logistics of Public Security.

Email: longhv08@gmail.com

Education: He received his BSc, MSc in Mathematical Statistics from Hanoi National University of Education; PhD degree in Computer Science at Hanoi University of Science and Technology in 2011.

Recent research interests: Computer science; Machine learning.

Cơ quan làm việc: Khoa Công nghệ thông tin, Trường Đại học Kỹ thuật - Hậu cầu Công an nhân dân.

Email: longhv08@gmail.com

Quá trình đào tạo: Nhận bằng Cử nhân và Thạc sĩ Thống kê toán học tại Đại học Sư phạm Hà Nội; Tiến sĩ Khoa học máy tính tại Đại học Bách Khoa Hà Nội vào năm 2011.

Hướng nghiên cứu hiện nay: Khoa học máy tính; Học máy.