Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.049985

ARTICLE

SCIRD: Revealing Infection of Malicious Software in Edge Computing-Enabled IoT Networks

Jiehao Ye, Wen Cheng, Xiaolong Liu, Wenyi Zhu, Xuan’ang Wu and Shigen Shen*

School of Information Engineering, Huzhou University, Huzhou, 313000, China

*Corresponding Author: Shigen Shen. Email: shigens@zjhu.edu.cn

Received: 24 January 2024 Accepted: 08 April 2024 Published: 15 May 2024

ABSTRACT

The Internet of Things (IoT) has characteristics such as node mobility, node heterogeneity, link heterogeneity, and topology heterogeneity. In the face of the IoT characteristics and the explosive growth of IoT nodes, which brings about large-scale data processing requirements, edge computing architecture has become an emerging network architecture to support IoT applications due to its ability to provide powerful computing capabilities and good service functions. However, the defense mechanism of Edge Computing-enabled IoT Nodes (ECIoTNs) is still weak due to their limited resources, so that they are susceptible to malicious software spread, which can compromise data confidentiality and network service availability. Facing this situation, we put forward an epidemiology-based susceptible-curb-infectious-removed-dead (SCIRD) model. Then, we analyze the dynamics of ECIoTNs with different infection levels under different initial conditions to obtain the dynamic differential equations. Additionally, we establish the presence of equilibrium states in the SCIRD model. Furthermore, we conduct an analysis of the model’s stability and examine the conditions under which malicious software will either spread or disappear within Edge Computing-enabled IoT (ECIoT) networks. Lastly, we validate the efficacy and superiority of the SCIRD model through MATLAB simulations. These research findings offer a theoretical foundation for suppressing the propagation of malicious software in ECIoT networks. The experimental results indicate that the theoretical SCIRD model has instructive significance, deeply revealing the principles of malicious software propagation in ECIoT networks. This study solves a challenging security problem of ECIoT networks by determining the malicious software propagation threshold, which lays the foundation for building more secure and reliable ECIoT networks.

KEYWORDS

Edge computing; Internet of Things; malicious software; propagation model; heterogeneity

1 Introduction

Internet of Things (IoT) networks have experienced rapid development in areas such as smart cities, smart health, and smart transportation. Such networks have characteristics such as node mobility, node heterogeneity, link heterogeneity, and topology diversity [1]. Facing these characteristics and the large data processing demands brought by the explosive growth of IoT nodes, edge computing has become an emerging network architecture that provides powerful computing capabilities and good service functions to support IoT applications [2–4]. In this manner, Edge Computing-enabled IoT (ECIoT) architecture brings computation, storage, and analytic capabilities closer to the data source, enabling real-time decision-making and reducing the latency of data transmission to cloud-based systems [5]. However, ECIoT nodes (ECIoTNs) with distributed and interconnected nature involve security vulnerabilities [6] introduced by malicious software such as Trojans, spyware, viruses, worms, rootkits, etc. Each type of malicious software has certain characteristics and infiltrates the ECIoT through different methods [7]. Incidents of significant losses caused by the spread of malicious software are not uncommon in society [8]. In November 2022, a new type of ransomware attacked the Australian insurance giant Medibank, which affected the personal information of 9.7 million customers, involving multiple sectors such as healthcare institutions and government departments [9]. The attackers typically spread malicious software to victims' systems through email attachments or network vulnerabilities, and then demanded ransom to decrypt the infected files. The ransomware attack has caused significant financial losses and leads to data breaches and system paralysis. In the same year, the Bank of Zambia was hit by ransomware attacks, causing disruptions in some systems, threatening crucial financial data and impacting its normal operations and financial system stability, and resulting in certain negative effects on the country's economy. These two attacks resulted in many organizations facing the risks of data loss, business disruptions, and substantial financial losses [10].

Recent research shows that malicious software in ECIoT is capable of spreading itself and has become a major factor affecting ECIoT security [11]. Once malicious software exploits vulnerabilities in ECIoTNs and spreads widely in the ECIoT, it can eavesdrop on ECIoTNs data and even cause ECIoTNs to completely lose their functionality by depleting their energy sources [12,13]. This seriously affects the availability, confidentiality, and stability of ECIoT services. Therefore, it is urgent to study the infection behavior and influencing factors of malicious software in ECIoT and provide methods for analyzing the stability of the infection model of malicious software in ECIoT [14].

The goal of the current work is to explore the spread rule of malicious software within ECIoTNs and propose strategies to prevent and inhibit its spread. It also proposes a malicious software infection model that integrates the expected probability of malicious software infection behavior by extending epidemic theory [15]. Subsequently, we study the stability of this model and finally obtain results that can reveal the infection mechanism of malicious software in ECIoT. By integrating insights from previous research, this study makes an effort to provide a comprehensive analysis of malicious software spreading dynamics in ECIoT networks and offer valuable insights for designing effective security countermeasures.

Here are our contributions:

(1) An epidemiology-based Susceptible-Curb-Infectious-Removed-Dead (SCIRD) model is proposed, which studies the characteristics of malicious software propagation in ECIoT networks by considering node heterogeneity, link heterogeneity, and topology structure heterogeneity. The model extends the Markov chain to study the state transition of ECIoTNs.

(2) The differential equations of the SCIRD model are derived, which represent the proportion dynamics of different compartments, namely S, C, I, R, and D, in the SCIRD model at various extents.

(3) Equilibrium states in the SCIRD model are demonstrated. Therefore, the conditions to determine whether malicious software will spread or die out in ECIoT networks can be obtained to guide the security mechanism defending malicious software propagation.

The key contributions of this paper are as follows. The application of the proposed SCIRD model can help researchers gain a deeper understanding of the propagation mechanism of malicious software in ECIoT networks, including characteristics such as propagation speed, range, and pathways, which will provide a more systematic and comprehensive perspective for the analysis, prediction, and formulation of strategies to combat malicious software propagation. Such a model can facilitate a better understanding and control of malicious software propagation behavior, contributing to enhancing security alertness and preventive capabilities of ECIoT networks. Moreover, our model can be extended to one considering different types of network topologies such as random, small-world, and scale-free networks to study the dynamics and patterns of malicious software propagation in different network structures.

The remaining sections of this paper are structured as follows. In Section 2, we examine the current state of research and put forth several issues that need to be addressed regarding the propagation of malicious software in ECIoT networks. In Section 3, we build a state graph for ECIoTNs infected by malicious software, taking into consideration the distinctive characteristics of current malicious software propagation, and propose the SCIRD model. Section 4 is dedicated to demonstrating equilibrium states of the SCIRD model, calculating the fundamental reproduction number, and affirming the model stability. Moving forward, in Section 5, we propose an algorithm using Matlab, and conduct experiments to validate the stability of equilibrium points. Finally, in Section 6, we provide a summary of the paper. Fig. 1 shows the paper workflow providing sufficient visual aids to guide readers through the various phases and steps of the work.

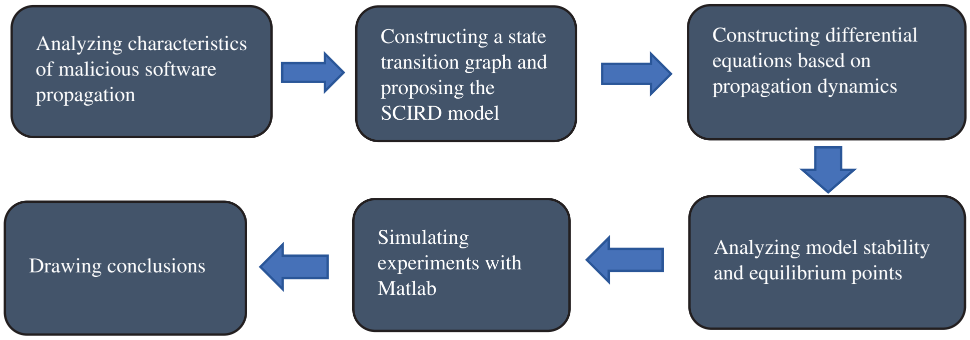
Analyzing characteristics of malicious software propagation
Constructing a state transition graph and proposing the SCIRD model
Constructing differential equations based on propagation dynamics
Analyzing model stability and equilibrium points
Simulating experiments with Matlab
Drawing conclusions

Figure 1: Paper workflow diagram

2 Related Work

The propagation of malicious software in the context of ECIoT bears certain similarity to infectious diseases to some extent [16]. Common epidemic models are classified based on the type of infectious diseases, such as the Susceptible-Infectious (SI) [17] and Susceptible-Infectious-Susceptible (SIS) [18] models. They can also be categorized based on the transmission mechanisms, including Partial Differential Equations (PDEs), Ordinary Differential Equations (ODEs), and network dynamics. For examples, the model STSIR (Social Internet of Things Susceptible-Infectious-Removed) was proposed to illustrate malicious software propagation among IoT nodes considering people behavior [19], however, the application of the model may require adjustments and validation in specific scenarios. By adding the state E (exposed), an SEIR (Susceptible-Exposed-Infectious-Removed) model was proposed to analyze the interval of logging, the number of friends in the list, and the influence of the malicious software's initial spreading rate [20], but the fixed immunity assumption in the SEIR model may not accurately describe factors in the propagation of malicious software.

Some researchers have studied the spread of malicious software from different perspectives. Guo et al. [21] put forward a method to represent the impact of different network structures on virus transmission using growth curves. Li et al. [22] began to study the impact model of information dissemination in mobile social networks from a multi-role perspective. Li et al. [23] used structural optimization to control information diffusion in social networks. Wang et al. [24] proposed a new data-driven approach, based on intuitive assumptions, to enhance the detection of zombie networks. They utilized honeypots to simulate zombie network attacks on medical devices and assets connected to the IoT with healthcare settings. In addition to the above models, others include models twin-SIR (twin Susceptible-Infectious-Removed) [25], SLBRS (Susceptible-Latent-Breaking-out-Recovered-Susceptible) [26], SEIRS-QV (Susceptible-Exposed-Infected-Recovered-Susceptible with Quarantine and Vaccination) [27], SEIQ-VS (Susceptible-Exposed-Infected-Quarantine with Vaccination-Susceptible) [28], and SIQR (Susceptible-Infected-Quarantine-Removed) [29]. Wherein, the twin-SIR model lacks of consideration for real-world factors such as changes of node behavior and network structure. The SLBRS model is indeed novel when proposed, but, due to considering multiple factors, its complexity increases, its interpretability decreases, and it requires higher requirements for actual data. Both the SEIRS-QV and SEIQ-VS models consider a wide range of influencing factors, but they both require accurate parameter estimation and extensive data support. The SIQR model neglects some complex propagation dynamics, such as latency and immune details.

These models all add certain states to the original classical SIR (Susceptible-Infectious-Removed) or SI model, while considering the communication radius and node distribution density. Besides, worm viruses are also highly contagious in the IoT, so people have proposed various propagation models based on compartmental populations [30], specifically designed for heterogeneous and hierarchical networks incorporating human behaviors. At the same time, the dynamics of worm propagation in complex networks have been extensively modeled and studied, and it has been confirmed that the network topology has a significant impact on the worm propagation in such networks [31,32]. The researchers also proposed a propagation model for the defense of PLC-PC (Programmable Logic Controller-Personal Computer) worms in industrial networks [33]. In the meanwhile, Yang et al. presented a new VEIQS (Vaccination-Exposed-Infected-Quarantine-Susceptible) worm propagation model [34]. But the model typically assumes that propagation is unobstructed and does not take into account the impact of defensive measures. Table 1 summarizes some representative papers on the propagation of malicious software, and compares with our work to provide a brief overview for better understanding in terms of the model name, main contributions, projecting point, and weakness.

Table 1: List some representative papers on the spread of malware on computers

Paper	Proposed model	Main contributions	Projecting point	Weakness
Lazfi et al. [17]	SI	Describing interactions between infectious and susceptible nodes	Classical model	Not considering the recovery and death states
Gómez-Corral et al. [18]	SIS	Dynamic description of an extended SI model	Classical model	Not considering the recovery and death states

(Continued)

Table 1 (continued)

Paper	Proposed model	Main contributions	Projecting point	Weakness
Wu et al. [19]	STSIR	Reasonable description of the propagation of malicious software	Improved and innovative model	Unable to fully consider security measures and the complexity of the actual network environment
Coronel et al. [20]	SEIR	Considering the impact of latency on the propagation of malicious software	Classical model	Difficulty in accurately modeling the complexity and heterogeneity of nodes
Yi et al. [25]	twin-SIR	Introducing a rumor clarification node with spreading ability	Improved and innovative model	Lack of consideration for real-world factors such as changes of node behavior and network structure
Tang et al. [26]	SLBRS	Considering the outbreak situation of malicious software	Improved and innovative model	Existing multiple factors that increase complexity and require high actual data
Hosseini et al. [27]	SEIRS-QV	Introducing immune attenuation and vaccine effectiveness	Improved and innovative model	Requiring accurate parameter estimation and extensive data support
Tran Le et al. [28]	SEIQ-VS	Providing the dynamics of infectious disease transmission	Improved and innovative model	Requiring accurate parameter estimation and extensive data support
Dong et al. [29]	SIQR	Considering the isolation state of nodes	Improved and innovative model	Neglecting complex propagation dynamics
This paper	SCIRD	Considering the heterogeneity of communication connectivity among ECIoTNs	Improved and innovative model	Special for ECIoTNs

However, the above research still fails to address some problems related to the spread of ECIoT malicious software. One problem is how to describe the actual situation where an ECIoTN becomes ineffectual due to energy depletion, physical degradation, or malicious software attacks. The other problem is how to ascertain the conditions under which malicious software will spread or disappear in wireless hardware. Herein, considering the heterogeneity of communication connectivity among ECIoTNs, we address the first problem by adding two states, namely, the dead state and the suppressed state, to the traditional SIR model. Furthermore, we address the second problem by studying the equilibrium point stability of our non-homogeneous model and mathematically verifying the correctness of our theoretic results.

3 Designing a State Diagram for ECIoT with Malicious Software Infection

Viewed in terms of the network's topology, we assume that the malicious software-infected ECIoT consists of M stationary ECIoTNs that are uniformly distributed across a two-dimensional region. Each ECIoTN is equipped with an omnidirectional antenna available for signal transmission. When an ECIoTN detects local data, it can forward this data to neighboring ECIoTNs located within its transmission range. These neighboring ECIoTNs then relay the data to their respective neighbors in an ongoing fashion.

Based on the characteristics of ECIoTNs, we develop a state diagram to represent the behavior of an ECIoTN within the malicious software-infected ECIoT. This can be analogized to an epidemiology-based model for malicious software propagation. In the state diagram, an ECIoTN is assigned to a single state that reflects its manner. We categorize an ECIoTN as state S if it exhibits its vulnerabilities but remains uninfected. When an ECIoTN is infected with malicious software but there exists security software that can contain the propagation of malicious software, it is classified as state C. When an ECIoTN becomes infected by malicious software and can transmit malicious software to neighboring nodes through data or control information, it transitions to state I. Upon applying security patches and achieving immunity to the current malicious software, an ECIoTN enters state R. An ECIoTN is assigned to state D when it becomes non-functional, either due to complete energy depletion or damage caused by malicious software. Thus, we extend the traditional SIR model to establish the SCIRD model, encompassing all the states of ECIoTNs within the malicious software-infected ECIoT.

As illustrated in Fig. 2, any ECIoTN within the network has the potential to undergo a state transition in reaction to external factors. This means that the current state of an ECIoTN can be altered due to external influences. When susceptible ECIoTNs become infected through the propagation of malicious software, not all nodes are necessarily affected, as a portion of nodes can successfully thwart the infection due to the presence of security software. This results in a transition of their state from S to C. However, security software is incapable of completely impeding the spread of malicious software. Furthermore, when infected ECIoTNs have the ability to transmit malicious software, their state transitions from S to I. Once a complete infection occurs, we employ patching of the security programs to treat the infected ECIoTNs, granting them immunity against known malicious software. This action leads to a state transition from I to R. Additionally, considering the mechanical nature of computers, any ECIoTN has the potential to transition to state D due to hardware malfunction or power depletion.

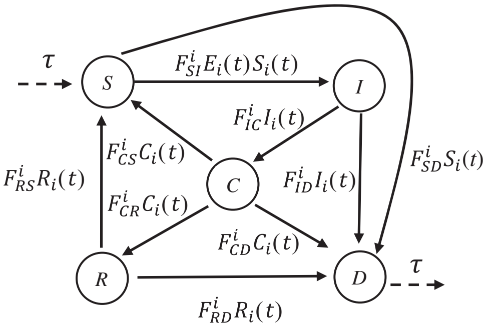

Figure 2: State diagram for an ECIoTN

We categorize the ECIoTNs based on their heterogeneous communication connectivity. Within the ECIoT, all ECIoTNs can be classified into L clusters, each characterized by the same degree of connectivity. For simplicity, we adopt a unified notation to represent both the cluster and its degree, where $i \in \{1, 2, \ldots, L\}$ is used to denote the degree of cluster i. To simplify the description, we use $S_i(t)$, $C_i(t)$, $I_i(t)$, $R_i(t)$, and $D_i(t)$ to represent the proportions of ECIoTNs in cluster i at time t that are in states S, C, I, R, and D, respectively. Clearly, we can derive alternative expressions for these quantities as

$$S_i(t) + C_i(t) + I_i(t) + R_i(t) + D_i(t) = 1, \tag{1}$$

$$I_i(0) = \alpha, 0 < \alpha < 1, \tag{2}$$

$$C_i(0) = R_i(t) = D_i(t) = 0, \tag{3}$$

$$S_i(0) = 1 - \alpha, \tag{4}$$

where α means the initial proportion of ECIoTNs assigned to cluster i in state I.

Let F^i_{fg} denote the feasibility of an ECIoTN in cluster $i \in \{1, 2, \ldots, L\}$ transforming its state from $f \in \{S, C, I, R, D\}$ to $g \in \{S, C, I, R, D\}$. At time t, an ECIoTN assigned to cluster $i \in \{1, 2, \ldots, L\}$ in state S meets one or more infectious ECIoTNs with feasibility $E_i(t)$:

$$E_i(t) = \frac{1}{\langle ad \rangle} \sum\nolimits_{i=1}^{L} \delta_i \vartheta_i I_i(t). \tag{5}$$

Here, $\langle ad \rangle$ represents the average degree of the ECIoTNs, δ_i represents the feasibility that an ECIoTN involves degree i, and ϑ_i represents the spread capability of an ECIoTN. These variables have the following conditions:

$$\sum\nolimits_{i=1}^{L} \delta_i = 1, \tag{6}$$

and

$$< ad >= \sum\nolimits_{i=1}^{L} i\delta_i. \tag{7}$$

Various equations for the spread capability that may be borrowed to ECIoTNs have been presented. Representative examples contain (1) $\vartheta_i = i$ [35]; (2) $\vartheta_i = AC$ [36], where AC is a fixed value; and (3) $\vartheta_i = \varphi i^r / (1 + \phi i^r)$ [37], with three variables: φ, r, and ϕ.

Up to this point, we have established the dynamics of all states. At time t, an ECIoTN assigned to cluster $i \in \{1, 2, \ldots, L\}$ in state C becomes I, R, and D at proportions $F^i_{CI}C_i(t)$, $F^i_{CR}C_i(t)$, and $F^i_{CD}C_i(t)$, respectively. An ECIoTN assigned to cluster $i \in \{1, 2, \ldots, L\}$ in state I becomes D at the proportion $F^i_{ID}I_i(t)$. An ECIoTN assigned to cluster $i \in \{1, 2, \ldots, L\}$ in state R becomes D at the proportion $F^i_{RD}R_i(t)$. Furthermore, certain malfunctioning ECIoTNs that are irreparable need to be substituted with new ones to ensure the proper functioning of the entire ECIoTN. This manner leads to increasing the proportion $\boldsymbol{\tau}$ to the proportion $S_i(t)$. As a result, we can achieve our SCIRD model characterizing the proportions of ECIoTNs assigned to cluster $i \in \{1, 2, \ldots, L\}$ in states S, C, I, R, D using differential equations, as follows:

$$\begin{cases} \dfrac{dS_i(t)}{dt} = \tau + F^i_{RS}R_i(t) + F^i_{CS}C_i(t) - F^i_{SI}E_i(t)S_i(t) - F^i_{SD}S_i(t) \\ S_i(0) = 1 - \alpha \end{cases}, \tag{8}$$

$$\begin{cases} \dfrac{dC_i(t)}{dt} = F^i_{IC}I_i(t) - F^i_{CS}C_i(t) - F^i_{CR}C_i(t) - F^i_{CD}C_i(t) \\ C_i(0) = 0 \end{cases}, \tag{9}$$

$$\begin{cases} \dfrac{dI_i(t)}{dt} = F^i_{SI}E_i(t)S_i(t) - F^i_{IC}I_i(t) - F^i_{ID}I_i(t) \\ I_i(0) = \alpha \end{cases}, \tag{10}$$

$$\begin{cases} \dfrac{dR_i(t)}{dt} = F^i_{CR}C_i(t) - F^i_{RS}R_i(t) - F^i_{RD}R_i(t) \\ R_i(0) = 0 \end{cases}, \tag{11}$$

$$\begin{cases} \dfrac{dD_i(t)}{dt} = F^i_{SD}S_i(t) + F^i_{ID}I_i(t) + F^i_{CR}C_i(t) + F^i_{RD}R_i(t) - \tau \\ D_i(0) = 0 \end{cases}, \tag{12}$$

satisfying equations

$$\begin{aligned} &\forall t, S_i(t), I_i(t), C_i(t), R_i(t), D_i(t) \geq 0, \\ &S_i(t) + C_i(t) + I_i(t) + R_i(t) + D_i(t) = 1, \\ &0 < \alpha < 1. \end{aligned} \tag{13}$$

4 Stability Analysis of the SCIRD Model for ECIoT with Malicious Software Infection

4.1 Steady States

Our main focus is to determine the steady states of our SCIRD model for ECIoT with malicious software infection, enabling us to identify the critical thresholds at which malicious software will either spread or die out within the ECIoTNs.

Theorem 1. There exist steady states in the SCIRD model including Eqs. (8)–(13) for ECIoT with malicious software infection.

Proof. Once the SCIRD attains its steady states, the proportional changes in all state variables cease. This indicates that all differential Eqs. (8)–(12) equal to zero. Therefore we obtain

$$\begin{cases} \tau + F^i_{RS}R_i(t) + F^i_{CS}C_i(t) - F^i_{SI}E_i(t)S_i(t) - F^i_{SD}S_i(t) = 0 \\ F^i_{IC}I_i(t) - F^i_{CS}C_i(t) - F^i_{CR}C_i(t) - F^i_{CD}C_i(t) = 0 \\ F^i_{SI}E_i(t)S_i(t) - F^i_{IC}I_i(t) - F^i_{ID}I_i(t) = 0 \\ F^i_{CR}C_i(t) - F^i_{RS}R_i(t) - F^i_{RD}R_i(t) = 0 \\ F^i_{SD}S_i(t) + F^i_{ID}I_i(t) + F^i_{CR}C_i(t) + F^i_{RD}R_i(t) - \tau = 0 \end{cases} \tag{14}$$

At the same time, we can define two steady states: $\Gamma_1\left(S^1_i, C^1_i, I^1_i, R^1_i, D^1_i\right)$ and $\Gamma_2\left(S^2_i, C^2_i, I^2_i, R^2_i, D^2_i\right)$. Here,

$$S^1_i = \frac{\tau}{F^i_{SD}}, \tag{15}$$

$$C^1_i = 0, \tag{16}$$

$$I^1_i = 0, \tag{17}$$

$$R^1_i = 0, \tag{18}$$

$$D^1_i = 1 - \frac{\tau}{F^i_{SD}}, \tag{19}$$

$$S^2_i = \frac{F^i_{IC} + F^i_{ID}}{F^i_{SI}Z_i(t)}, \tag{20}$$

$$I^2_i = \frac{(F^i_{RS} + F^i_{RD})(F^i_{IC} + F^i_{CR} + F^i_{CD})(F^i_{SD}(F^i_{IC} + F^i_{ID}) - \tau F^i_{SI}Z_i}{[F^i_{SI}Z_i((F^i_{CS} + F^i_{CR} + F^i_{CD})(F^i_{RS} - (F^i_{RS} + F^i_{RD})(F^i_{IC} + F^i_{CR} + F^i_{CD})(F^i_{IC} + F^i_{ID})) + F^i_{RS}F^i_{CR}F^i_{ID} + (F^i_{RS} + F^i_{RD})F^i_{CS}F^i_{ID})]}, \tag{21}$$

$$C^2_i = \frac{F^i_{IC}}{F^i_{CS} + F^i_{CR} + F^i_{CD}} * I^2_i, \tag{22}$$

$$R^2_i = \frac{F^i_{CR}}{F^i_{RS} + F^i_{RD}} * \frac{F^i_{IC}}{F^i_{CS} + F^i_{CR} + F^i_{CD}} * I^2_i, \tag{23}$$

$$D^2_i = 1 - S^2_i - C^2_i - I^2_i - R^2_i, \tag{24}$$

where

$$Z_i = \frac{1}{\langle ad \rangle} \sum\nolimits_{i=1}^{L} \delta_i \vartheta_i. \tag{25}$$

This completes the proof.

According to epidemiological theory, steady state Γ_1 obtained from Theorem 1 is referred to the malicious software-free equilibrium, while Γ_2 is denoted as the endemic equilibrium. These equilibria serve as analytical tools to examine the dynamics of the SCIRD model of ECIoTNs exposed to malicious software infection. At steady state Γ_1, the value of the proportion I^1_i is zero, indicating the disappearance of malicious software. Conversely, when an ECIoT reaches Γ_2, the value of the proportion I^2_i is greater than zero, representing the spread of malicious software.

In summary, at steady state Γ_1, malicious software within the ECIoT would eventually vanish. However, if the ECIoT is in Γ_2, malicious software would continue to propagate, leading to a persistent infection ratio within the ECIoTNs, and eventually reaching a steady level of contagion. In the context of practical defense and control processes of malicious software in IoT networks, administrators should strive for the steady state Γ_1. The continuous patching of security programs by administrators helps suppress the spread of malicious software. Moreover, it is crucial to avoid the steady state Γ_2, which represents the proliferation of malicious software. As malicious software ultimately infects a proportion of ECIoTNs, it imposes significant damage on the usual functioning of ECIoT networks.

4.2 Fundamental Reproduction Number

In order to explore dynamical characteristics of the proposed SCIRD model, our current focus is on determining the fundamental reproduction number denoted by ω using the next-generation matrix method [38], which guides the steady state. This number serves as a measure to quantify the proportion of vulnerable ECIoTNs that are susceptible to the impact of malicious software throughout their lifecycle. Generally, when $\omega < 1$, there exists a steady state indicating the eventual disappearance of malicious software. In other words, within all susceptible ECIoTNs, each infectious ECIoTN fails to infect more than a single new individual. However, when $\omega > 1$, an endemic steady state persists, signifying the continuous existence of malicious software in the infected ECIoTNs, as each infectious ECIoTN infects more than one susceptible ECIoTN.

Subsequently, we proceed to calculate the fundamental reproduction number ω, utilizing the next-generation matrix technique. Let

$$[f_I] = \left[F_{SI}^{i} E_i(t) S_i(t)\right] \tag{26}$$

and

$$[v_I] = \left[F_{IC}^{i} I_i(t) + F_{ID}^{i} I_i(t)\right]. \tag{27}$$

We achieve

$$\mathbf{F} = \left[\frac{\partial f_I}{\partial I_i(t)}\right]_{\Gamma_1} = \left[F_{SI}^{i} S_i^{1} Z_i\right] \tag{28}$$

and

$$\mathbf{V} = \left[\frac{\partial v_I}{\partial I_i(t)}\right]_{\Gamma_1} = \left[F_{IC}^{i} + F_{ID}^{i}\right]. \tag{29}$$

Then, we can obtain the fundamental reproduction number ω as

$$\omega = \rho\left(\mathbf{FV}^{-1}\right) = \frac{F_{SI}^{i} \tau Z_i}{F_{SD}^{i}(F_{IC}^{i} + F_{ID}^{i})}. \tag{30}$$

4.3 Analysis of Equilibrium Point Stability

Now we will perform stability analysis on the equilibrium points in the model to investigate whether the model displays the characteristics of viral contagion. Assessing the stability of an equilibrium point involves determining whether the system's key conditions associated with that point lead trajectories to converge towards it over time, indicating stability. Conversely, if an equilibrium point is deemed unstable, the trajectories will diverge away from it as time progresses.

The SCIRD model, which includes Eqs. (8)–(13) for malicious software-infected ECIoTNs, can be simplified to a set of differential equations containing Eqs. (8)–(11). Besides, Eq. (12) can be replaced by $D_i(t) = 1 - S_i(t) - C_i(t) - I_i(t) - R_i(t)$ and can be neglected. Therefore, our focus will be on examining the stability characteristics of the SCIRD model, which encompasses Eqs. (8)–(11).

Theorem 2. If $\omega < 1$, steady equilibrium state $\Gamma_1\left(S_i^1, C_i^1, I_i^1, R_i^1, D_i^1\right)$ is locally stable in the long run, however, if $\omega > 1$, it is unstable.

Proof. In accordance with the stability theory for ordinary differential equations, we begin by calculating Jacobian matrix J [39] associated with the SCIRD model, which is represented by

$$\mathbf{J} = \begin{bmatrix} \frac{\partial \dot{S}_i(t)}{\partial S_i(t)} & \frac{\partial \dot{S}_i(t)}{\partial C_i(t)} & \frac{\partial \dot{S}_i(t)}{\partial I_i(t)} & \frac{\partial \dot{S}_i(t)}{\partial R_i(t)} \\ \frac{\partial \dot{C}_i(t)}{\partial S_i(t)} & \frac{\partial \dot{C}_i(t)}{\partial C_i(t)} & \frac{\partial \dot{C}_i(t)}{\partial I_i(t)} & \frac{\partial \dot{C}_i(t)}{\partial R_i(t)} \\ \frac{\partial \dot{I}_i(t)}{\partial S_i(t)} & \frac{\partial \dot{I}_i(t)}{\partial C_i(t)} & \frac{\partial \dot{I}_i(t)}{\partial I_i(t)} & \frac{\partial \dot{I}_i(t)}{\partial R_i(t)} \\ \frac{\partial \dot{R}_i(t)}{\partial S_i(t)} & \frac{\partial \dot{R}_i(t)}{\partial C_i(t)} & \frac{\partial \dot{R}_i(t)}{\partial I_i(t)} & \frac{\partial \dot{R}_i(t)}{\partial R_i(t)} \end{bmatrix} \tag{31}$$

$$= \begin{bmatrix} -F_{SI}^iE_i(t) - F_{SD}^i & F_{CS}^i & -F_{SI}^i(t)Z_iS_i(t) & F_{RS}^i \\ 0 & -(F_{CS}^i + F_{CR}^i + F_{CD}^i) & F_{IC}^i & 0 \\ F_{SI}^iE_i(t) & 0 & F_{SI}^iZ_iS_i(t) - F_{IC}^i - F_{ID}^i & 0 \\ 0 & F_{CR}^i & 0 & -F_{RS}^i - F_{RD}^i \end{bmatrix}.$$

Furthermore, we compute the Jacobian matrix at the equilibrium point representing the absence of malicious software $\Gamma_1\left(S_i^1, C_i^1, I_i^1, R_i^1, D_i^1\right)$ as

$$\mathbf{J}(\Gamma_1) = \begin{bmatrix} -F_{SD}^i & F_{CS}^i & -F_{SI}^iZ_iS_i^1 & F_{RS}^i \\ 0 & -(F_{CS}^i + F_{CR}^i + F_{CD}^i) & F_{IC}^i & 0 \\ 0 & 0 & F_{SI}^iZ_iS_i^1 - F_{ID}^i - F_{IC}^i & 0 \\ 0 & F_{CR}^i & 0 & -F_{RS}^i - F_{RD}^i \end{bmatrix}. \tag{32}$$

Let λ represent an eigenvalue and $\mathbf{H}$ denote the identity matrix. We can compute the eigenfunction of matrix $\mathbf{J}(\Gamma_1)$ using the following calculation:

$$|\lambda\mathbf{H} - \mathbf{J}(\Gamma_1)| = \begin{bmatrix} \lambda + F_{SD}^i & -F_{CS}^i & F_{SI}^iZ_iS_i^1 & -F_{RS}^i \\ 0 & \lambda + F_{CS}^i + F_{CR}^i + F_{CD}^i & -F_{IC}^i & 0 \\ 0 & 0 & \lambda - F_{SI}^iZ_iS_i^1 + F_{ID}^i + F_{IC}^i & 0 \\ 0 & -F_{CR}^i & 0 & \lambda + F_{RS}^i + F_{RD}^i \end{bmatrix}. \tag{33}$$

Therefore, we can obtain all the eigenvalues:

$$\lambda_1 = -F_{SD}^i, \tag{34}$$

$$\lambda_2 = -F_{CS}^i - F_{CR}^i - F_{CD}^i, \tag{35}$$

$$\lambda_3 = F_{SI}^iZ_iS_i^1 - F_{ID}^i - F_{IC}^i = (F_{ID}^i + F_{IC}^i)(\omega - 1), \tag{36}$$

$$\lambda_4 = -F_{RS}^i - F_{RD}^i. \tag{37}$$

From the above formula derivation, we can deduce that $\lambda_1 < 0$ and $\lambda_4 < 0$ only if $\omega < 1$. Thus, if $\omega < 1$, steady equilibrium state $\Gamma_1 \left(S_i^1, C_i^1, I_i^1, R_i^1, D_i^1\right)$ is locally asymptotically stable, however, if $\omega > 1$, it is unstable. At this point, we have completed the proof.

According to Theorem 2, when $\omega < 1$, the proportions of ECIoTN cluster $i \in \{1, 2, \ldots, L\}$ in state S, C, I, R, and D will evolve over time to approach S_i^1, 0, 0, 0, and D_i^1, respectively.

Theorem 3. If $\omega > 1$, steady equilibrium state $\Gamma_2 \left(S_i^2, C_i^2, I_i^2, R_i^2, D_i^2\right)$ is locally asymptotically stable.

Proof. We rescript C_i^2, I_i^2 and R_i^2 as

$$C_i^2 = \frac{\left(F_{RS}^i + F_{RD}^i\right)\left(F_{IC}^i + F_{CR}^i + F_{CD}^i\right)\left(F_{IC}^i + F_{ID}^i\right)F_{SD}^i}{\left[F_{SI}^i Z_i \left(\left(F_{CS}^i + F_{CR}^i + F_{CD}^i\right)\left(F_{RS}^i - \left(F_{RS}^i + F_{RD}^i\right)\left(F_{IC}^i + F_{CR}^i + F_{CD}^i\right)\left(F_{IC}^i + F_{ID}^i\right)\right) + F_{RS}^i F_{CR}^i F_{ID}^i + \left(F_{RS}^i + F_{RD}^i\right)F_{CS}^i F_{ID}^i\right)\right]} * \frac{F_{IC}^i}{F_{CS}^i + F_{CR}^i + F_{CD}^i} * (\omega - 1), \tag{38}$$

$$I_i^2 = \frac{\left(F_{RS}^i + F_{RD}^i\right)\left(F_{IC}^i + F_{CR}^i + F_{CD}^i\right)\left(F_{IC}^i + F_{ID}^i\right)F_{SD}^i}{\left[F_{SI}^i Z_i \left(\left(F_{CS}^i + F_{CR}^i + F_{CD}^i\right)\left(F_{RS}^i - \left(F_{RS}^i + F_{RD}^i\right)\left(F_{IC}^i + F_{CR}^i + F_{CD}^i\right)\left(F_{IC}^i + F_{ID}^i\right)\right) + F_{RS}^i F_{CR}^i F_{ID}^i + \left(F_{RS}^i + F_{RD}^i\right)F_{CS}^i F_{ID}^i\right)\right]} * (\omega - 1), \tag{39}$$

$$R_i^2 = \frac{\left(F_{RS}^i + F_{RD}^i\right)\left(F_{IC}^i + F_{CR}^i + F_{CD}^i\right)\left(F_{IC}^i + F_{ID}^i\right)F_{SD}^i}{\left[F_{SI}^i Z_i \left(\left(F_{CS}^i + F_{CR}^i + F_{CD}^i\right)\left(F_{RS}^i - \left(F_{RS}^i + F_{RD}^i\right)\left(F_{IC}^i + F_{CR}^i + F_{CD}^i\right)\left(F_{IC}^i + F_{ID}^i\right)\right) + F_{RS}^i F_{CR}^i F_{ID}^i + \left(F_{RS}^i + F_{RD}^i\right)F_{CS}^i F_{ID}^i\right)\right]} * \frac{F_{IC}^i}{F_{CS}^i + F_{CR}^i + F_{CD}^i} * \frac{F_{CR}^i}{F_{RS}^i + F_{RD}^i} * (\omega - 1). \tag{40}$$

As a matter of course, S_i^2, I_i^2 and R_i^2 are all greater than 0 when $\omega > 1$. This implies that if $\omega > 1$, a local equilibrium $\Gamma_2 \left(S_i^2, C_i^2, I_i^2, R_i^2, D_i^2\right)$ exists. Using Eq. (30), it can be concluded that the Jacobian matrix at the endemic equilibrium $\Gamma_2 \left(S_i^2, C_i^2, I_i^2, R_i^2, D_i^2\right)$ as

$$\mathbf{J}\left(\Gamma_2\right) = \begin{bmatrix} -F_{SI}^i Z_i I_i^2 - F_{SD}^i & F_{CS}^i & -F_{SI}^i(t) Z_i S_i^2 & F_{RS}^i \\ 0 & -\left(F_{CS}^i + F_{CR}^i + F_{CD}^i\right) & F_{IC}^i & 0 \\ F_{SI}^i Z_i I_i^2 & 0 & F_{SI}^i Z_i S_i^2 - F_{IC}^i - F_{ID}^i & 0 \\ 0 & F_{CR}^i & 0 & -F_{RS}^i - F_{RD}^i \end{bmatrix}. \tag{41}$$

It can be obtained in the same way that the eigenfunction of matrix $\mathbf{J}\left(\Gamma_2\right)$ as

$$
\begin{aligned}
|\lambda \mathbf{H} - \mathbf{J}\,(\Gamma_2)| &= \begin{bmatrix} \lambda + F^i_{SI} Z_i I_i^2 + F^i_{SD} & -F^i_{CS} & F^i_{SI} Z_i S_i^2 & -F^i_{RS} \\ 0 & \lambda + F^i_{CS} + F^i_{CR} + F^i_{CD} & -F^i_{IC} & 0 \\ -F^i_{SI} Z_i I_i^2 & 0 & \lambda - F^i_{SI} Z_i I_i^2 S_i^2 + F^i_{ID} + F^i_{IC} & 0 \\ 0 & -F^i_{CR} & 0 & \lambda + F^i_{RS} + F^i_{RD} \end{bmatrix} \\
&= \lambda^4 + \left(F^i_{SI} Z_i I_i^2 + F^i_{SD} + F^i_{CS} + F^i_{CR} + F^i_{CD} - F^i_{SI} Z_i I_i^2 S_i^2 + F^i_{ID} + F^i_{IC} + F^i_{RS} + F^i_{RD}\right) \lambda^3 \\
&\quad + [(F^i_{SI} Z_i I_i^2 + F^i_{SD})(F^i_{CS} + F^i_{CR} + F^i_{CD}) + (F^i_{SI} Z_i I_i^2 S_i^2 + F^i_{ID} + F^i_{IC})(F^i_{RS} + F^i_{RD}) + (F^i_{SI} Z_i I_i^2 + F^i_{SD}) \\
&\quad (-F^i_{SI} Z_i I_i^2 S_i^2 + F^i_{ID} + F^i_{IC}) + (F^i_{SI} Z_i I_i^2 + F^i_{SD})(F^i_{RS} + F^i_{RD}) + (F^i_{CS} + F^i_{CR} + F^i_{CD})(-F^i_{SI} Z_i I_i^2 S_i^2 + F^i_{ID} + F^i_{IC}) \\
&\quad + (F^i_{CS} + F^i_{CR} + F^i_{CD})(F^i_{RS} + F^i_{RD})]\lambda^2 + [(F^i_{SI} Z_i I_i^2 + F^i_{SD})(F^i_{CS} + F^i_{CR} + F^i_{CD})(-F^i_{SI} Z_i I_i^2 S_i^2 + F^i_{ID} + F^i_{IC}) \\
&\quad + (F^i_{SI} Z_i I_i^2 + F^i_{SD})(F^i_{CS} + F^i_{CR} + F^i_{CD})(F^i_{RS} + F^i_{RD}) + (F^i_{CS} + F^i_{CR} + F^i_{CD})(-F^i_{SI} Z_i I_i^2 S_i^2 + F^i_{ID} + F^i_{IC}) \\
&\quad (F^i_{RS} + F^i_{RD})]\lambda + (F^i_{SI} Z_i I_i^2 + F^i_{SD})(F^i_{CS} + F^i_{CR} + F^i_{CD})(F^i_{RS} + F^i_{RD})(-F^i_{SI} Z_i I_i^2 S_i^2 + F^i_{ID} + F^i_{IC}) \\
&\quad \triangleq \lambda^4 + b_3 \lambda^3 + b_2 \lambda^2 + b_1 \lambda + b_0.
\end{aligned} \tag{42}
$$

Clearly, it is infeasible to determine all the eigenvalues of matrix $\mathbf{J}\,(\Gamma_2)$ directly from Eq. (41). Thus, the spread of malicious software within a compromised ECIoTN will be ongoing, and the proportion of contagious ECIoTN nodes will ultimately stabilize. It is evident that we are supposed to strive to avert this scenario by regulating the values of ECIoTN purview.

Given a quartic polynomial expression, we can determine its positivity by inspecting the discriminant, denoted as Δ. Here we can obtain that

$$
\begin{aligned}
\Delta = b_3^2 - 4b_2 &= (F^i_{SI} Z_i I_i^2 + F^i_{SD} + F^i_{CS} + F^i_{CR} + F^i_{CD} - F^i_{SI} Z_i I_i^2 S_i^2 + F^i_{ID} + F^i_{IC} + F^i_{RS} + F^i_{RD})^2 \\
&\quad - 4[(F^i_{SI} Z_i I_i^2 + F^i_{SD})(F^i_{CS} + F^i_{CR} + F^i_{CD}) + (F^i_{SI} Z_i I_i^2 S_i^2 + F^i_{ID} + F^i_{IC})(F^i_{RS} + F^i_{RD}) + (F^i_{SI} Z_i I_i^2 + F^i_{SD}) \\
&\quad (-F^i_{SI} Z_i I_i^2 S_i^2 + F^i_{ID} + F^i_{IC}) + (F^i_{SI} Z_i I_i^2 + F^i_{SD})(F^i_{RS} + F^i_{RD}) + (F^i_{CS} + F^i_{CR} + F^i_{CD}) \\
&\quad (-F^i_{SI} Z_i I_i^2 S_i^2 + F^i_{ID} + F^i_{IC}) + (F^i_{CS} + F^i_{CR} + F^i_{CD})(F^i_{RS} + F^i_{RD})]
\end{aligned} \tag{43}
$$

Through simulation, we attain that the discriminant Δ is negative. This implies that the quadratic term has no real roots, resulting in no intersections between the curve and the x-axis. Thus, the function is either always positive or always negative, ensuring it is strictly positive. As the coefficient in front of λ^4 is 1, and based on the proof above, we can conclude that the entire polynomial is always greater than 0. Therefore, we have successfully completed the proof.

According to Theorem 3, when $\omega > 1$, the proportions of ECIoTN nodes $i \in \{1, 2, \ldots, L\}$ in states S, C, I, R, and D will evolve over time to approach S_i^2, C_i^2, I_i^2, R_i^2, and D_i^2, respectively. As a result, the propagation of malicious software within the infected ECIoTNs will be ongoing, and the ratio of infected ECIoTNs will ultimately reach a steady state. It is apparent that we should strive to prevent this scenario by manipulating the ECIoTN parameters' values.

5 Experiments

To confirm the SCIRD model for malicious software-infected ECIoTNs, we implemented the model using MATLAB R2022a. The computational algorithm, Algorithm 1, was utilized for this purpose.

Algorithm 1: The computational algorithm for verifying the SCIRD model

```
Inputs: $N, \alpha, \tau, F^i_{RS}, F^i_{SI}, F^i_{SD}, F^i_{SC}, F^i_{CI}, F^i_{ID}, F^i_{CR}, F^i_{RD}$
Initialize malicious software-infected ECIoTNs parameters containing $N, \alpha, \tau, F^i_{RS}, F^i_{SI}, F^i_{SD}, F^i_{SC}, F^i_{CI}, F^i_{ID}, F^i_{CR}$, and $F^i_{RD}$;
$S_i \leftarrow 1 - \alpha$; $C_i \leftarrow 0$; $I_i \leftarrow a$; $R_i \leftarrow 0$; $D_i \leftarrow 0$;
$t \leftarrow 0$; $\Delta t \leftarrow 1$;
$\kappa \leftarrow 200$;   //$\kappa$ represents the range
DO WHILE $t <= \kappa$
    $S_i(t + \Delta t) \leftarrow \tau + F^i_{RS}R_i(t) + F^i_{CS}C_i(t) - F^i_{SI}E_i(t)S_i(t) - F^i_{SD}S_i(t)$;
    $C_i(t + \Delta t) \leftarrow F^i_{IC}I_i(t) - F^i_{CS}C_i(t) - F^i_{CR}C_i(t) - F^i_{CD}C_i(t)$;
    $I_i(t + \Delta t) \leftarrow F^i_{SI}E_i(t)S_i(t) - F^i_{IC}I_i(t) - F^i_{ID}I_i(t)$;
    $R_i(t + \Delta t) \leftarrow F^i_{CR}C_i(t) - F^i_{RS}R_i(t) - F^i_{RD}R_i(t)$;
    $D_i(t + \Delta t) \leftarrow F^i_{SD}S_i(t) + F^i_{ID}I_i(t) + F^i_{CR}C_i(t) + F^i_{RD}R_i(t) - \tau$;
    $t \leftarrow t + 1$;
ENDDO
RETURN arrays $S_i, C_i, I_i, R_i, D_i$;
```

In the simulation program of MATLAB, the ECIoT network consists of 1500 static ECIoTNs. The interval Δt is 1d. We establish the ECIoTN topology and determine the values of the remaining parameters by consulting other research. In this case, we set the range of degrees to be between 2 and 20, with an average value of 4. Additionally, the infection rate is set as a function of the degree, denoted as $F^i_{SI} = \xi i$, and $\xi = 0.01$.

5.1 Assessing Stability of the Equilibrium State in the Absence of Malicious Software

In this part, we verify the correctness of Theorem 2 by setting various infection capacities.

5.1.1 Equal Infectivity

Here, the infection capacity ϑ_i is configured as $\vartheta_i = \varphi i^r / (1 + \phi i^r)$, where $\varphi = 5$, $r = 0.5$, and $\phi = 1$ [40]. Therefore, we calculate the mean value of $F^i_{SI} Z_i$ as $\sim$0.1727. The remaining values are adjusted as follows: $\tau = 0.025$, $F^i_{RS} = 0.008$, $F^i_{SD} = 0.13$, $F^i_{ID} = 0.05$, $F^i_{CR} = 0.26$, $F^i_{IC} = 0.12$, $F^i_{RD} = F^i_{SD} = F^i_{CD}$, and $F^i_{RS} = F^i_{CS}$. Based on the calculations, we obtain the $\omega \approx 0.1954 < 1$. With the conditions of Theorem 2 fulfilled, we can proceed to verify its correctness using Algorithm 1.

Fig. 3 describes the changing tendency of susceptible ECIoTNs under the circumstance of Theorem 2 for $\alpha = 0.05, \alpha = 0.15$, and $\alpha = 0.2$. In Fig. 2, the trajectory of the proportion of ECIoNs in the susceptible state, $S_i(t)$, exhibits different trends for various values of α, specifically, 0.8, 0.85, and 0.95. After $\sim$20d, all three curves decline rapidly and eventually stabilize at approximately 20% reduction. In other words, $S_i(t)$ approaches a stable point, denoted as $\Gamma_1 \left(S^1_i, C^1_i, I^1_i, R^1_i, D^1_i\right)$, with an S^1_i value of 0.2.

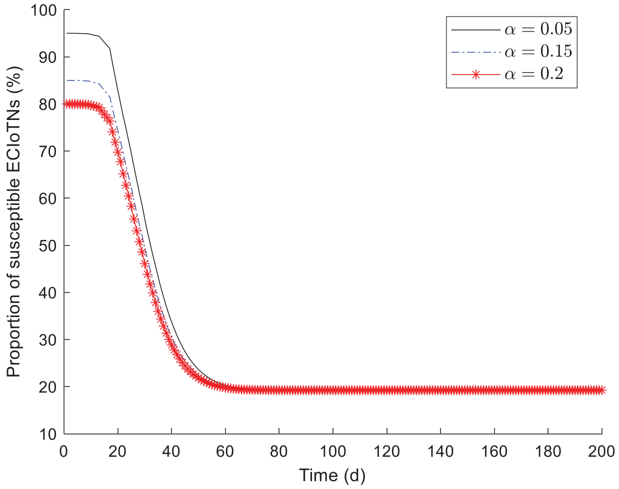

Figure 3: Changing tendency of susceptible ECIoTNs under the circumstance of Theorem 2 for $\alpha = 0.05, \alpha = 0.15$, and $\alpha = 0.2$

Figs. 4–7 depict the changing tendency of curb, infectious, removed, and dead ECIoTNs under the circumstance of Theorem 2 for $\alpha = 0.05, \alpha = 0.15$, and $\alpha = 0.2$. The changing trends of the proportions of ECIoTNs in states C, I, R, and D, denoted as $C_i(t)$, $I_i(t)$, $R_i(t)$, and $D_i(t)$, respectively, remain consistent across different values of α. In Fig. 4, the proportion of curb ECIoTNs exhibits minor changes in the first ~15d, followed by a gradual increase to 17%, 37%, and 48% in subsequent periods. Afterwards, it gradually decreases and eventually approaches 5%. This is consistent with the value of $C_i(t)$ in the stable point $\Gamma_1\left(S_i^1, C_i^1, I_i^1, R_i^1, D_i^1\right)$. In Fig. 5, its changing trend is similar to Fig. 3. It remains constant for the first ~20d and then gradually decreases, eventually approaching zero. This is consistent with the value of $I_i(t)$ in the stable point $\Gamma_1\left(S_i^1, C_i^1, I_i^1, R_i^1, D_i^1\right)$. In Fig. 6, the proportion of removed ECIoTNs exhibits minor changes in the first ~20d, followed by a gradual increase to 13%, 25%, and 32% in subsequent periods. Afterwards, it gradually decreases and eventually approaches 5%. This is consistent with the value of $R_i(t)$ in the stable point $\Gamma_1\left(S_i^1, C_i^1, I_i^1, R_i^1, D_i^1\right)$. In Fig. 7, the proportion of dead ECIoTNs exhibits minor changes in the first ~15d, and then it gradually increases and approaches 80%. This is consistent with the value of $D_i(t)$ in the stable point $\Gamma_1\left(S_i^1, C_i^1, I_i^1, R_i^1, D_i^1\right)$.

5.1.2 Diverse Infectivity

Apart from the infectivity factor $\vartheta_i = \varphi i^r/(1 + \phi i^r)$ in Section 5.1.1, we come up with different infection capacities: $\vartheta_i = i$ and $\vartheta_i = AC$, where AC is a fixed value. When keeping the values of other parameters unchanged, for $\vartheta_i = i$, we obtain $F_{SI}^i Z_i \approx 0.25$ and $\omega \approx 0.2828$, and for $\vartheta_i = AC = 2$, we obtain $F_{SI}^i Z_i \approx 0.1$ and $\omega \approx 0.1131$. Clearly, both of the fundamental reproduction numbers are less than 1, demonstrating their compliance with the conditions outlined in Theorem 2.

In Figs. 8–12, while there are variations in the peak values of the curves, the proportions of susceptible, curb, removed, and dead ECIoTNs ultimately converge to S_i^1, C_i^1, R_i^1, and D_i^1, respectively. Furthermore, $I_i^1 \rightarrow 0$ irrespective of the diverse infection capabilities, it can be observed that the malicious software within the ECIoTNs becomes extinct after ~70 d.

By conducting experiments under the equal infection capacity as well as diverse infection capacity, we have successfully validated Theorem 2. These experiments offer compelling evidence that the malicious software residing in infected ECIoTNs will ultimately be eliminated.

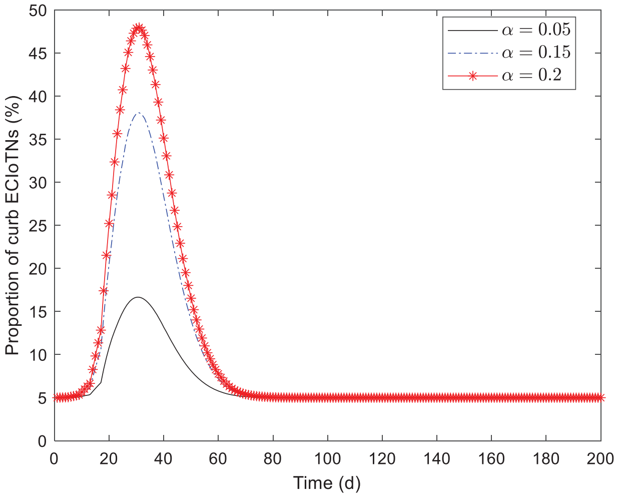

Figure 4: Changing tendency of curb ECIoTNs under the circumstance of Theorem 2 for $\alpha = 0.05$, $\alpha = 0.15$, and $\alpha = 0.2$

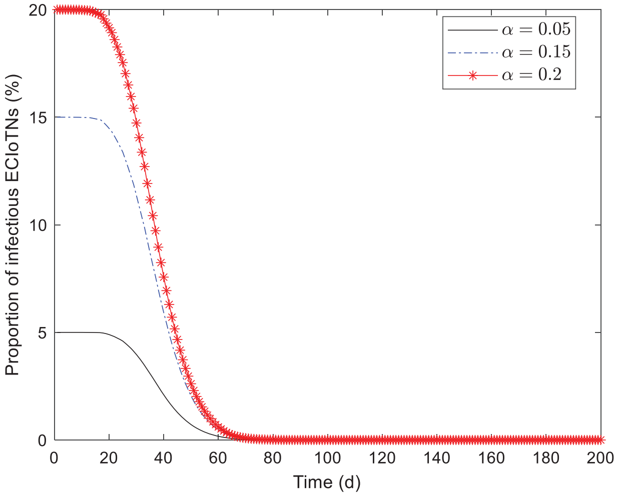

Figure 5: Changing tendency of infectious ECIoTNs under the circumstance of Theorem 2 for $\alpha = 0.05, \alpha = 0.15$, and $\alpha = 0.2$

When the conditions for Theorem 2 are satisfied, although malicious software infects a large number of ECIoTNs from the beginning, it is crucial to strive for the stable conditions of an equilibrium without malicious software. This phenomenon can be attributed to the stability of the system, which guarantees that the infected ECIoTNs will be cleared of malicious software, even in the presence of new outbreaks.

5.2 *Confirming Stability of Endemic Equilibrium*

In this case, we will employ a similar approach as in Section 5.1 to confirm the validity of Theorem 3, utilizing two distinct scenarios: equal infectivity and diverse infectivity.

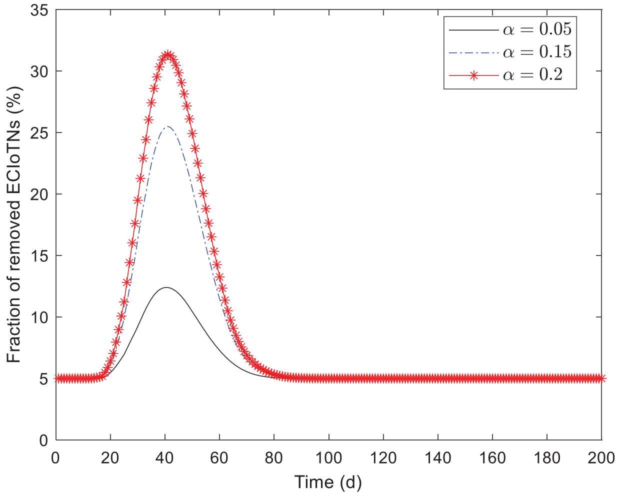

Figure 6: Changing tendency of removed ECIoTNs under the circumstance of Theorem 2 for $\alpha = 0.05, \alpha = 0.15$, and $\alpha = 0.2$

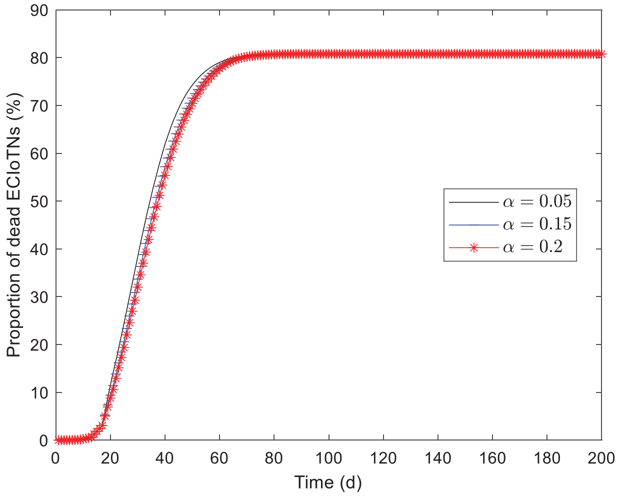

Figure 7: Changing tendency of dead ECIoTNs under the circumstance of Theorem 2 for $\alpha = 0.05, \alpha = 0.15$, and $\alpha = 0.2$

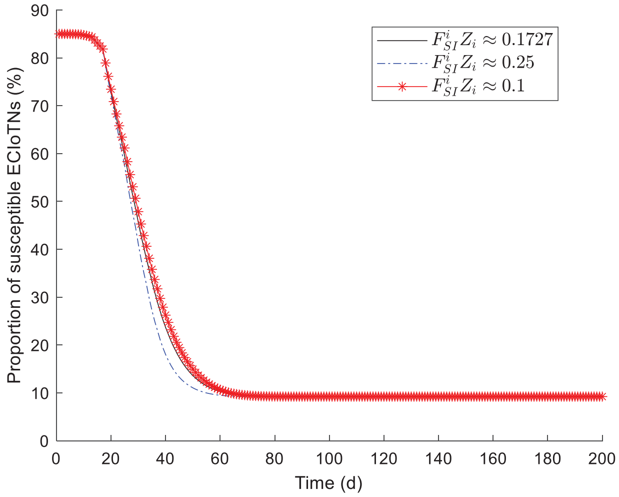

Figure 8: Changing tendency of susceptible ECIoTNs under the circumstance of Theorem 2 with diverse infection capabilities

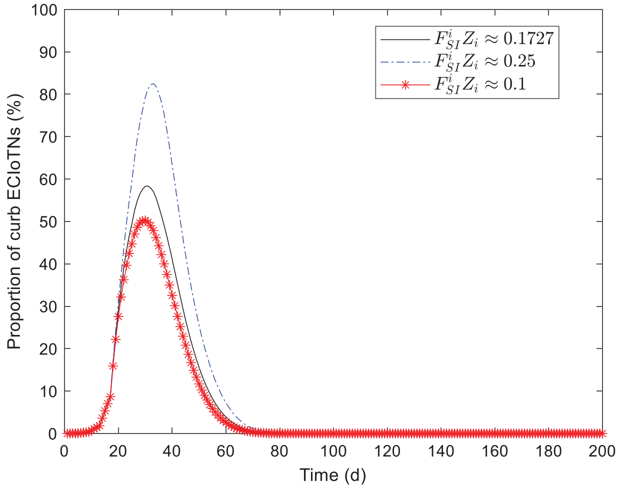

Figure 9: Changing tendency of curb ECIoTNs under the circumstance of Theorem 2 with diverse infection capabilities

5.2.1 Equal Infectivity

During the verification process, all values except $\varphi = 10$ [41] are set to be the same as those in Section 5.1. In this case, we can obtain $F^i_{SI}Z_i$ as ∼0.3454. At the same time, we set $\tau = 0.05$, $F^i_{SD} = 0.02$, $F^i_{ID} = 0.15$, and $F^i_{RS} = 0.01$. At this point, $\omega \approx 3.1981 > 1$, which satisfies the experimental data requirements of Theorem 3.

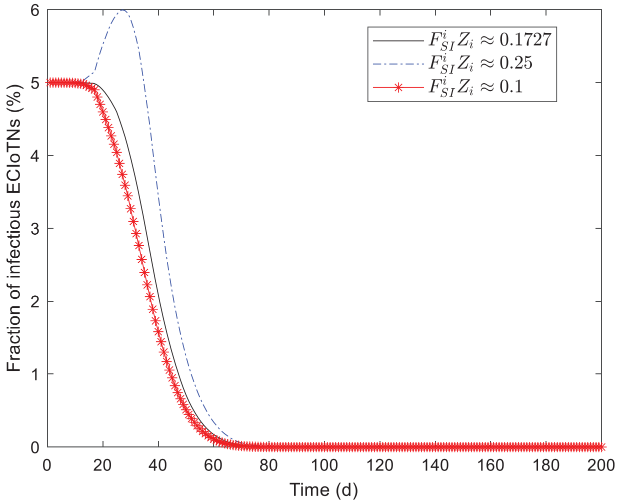

Figure 10: Changing tendency of infectious ECIoTNs under the circumstance of Theorem 2 with diverse infection capabilities

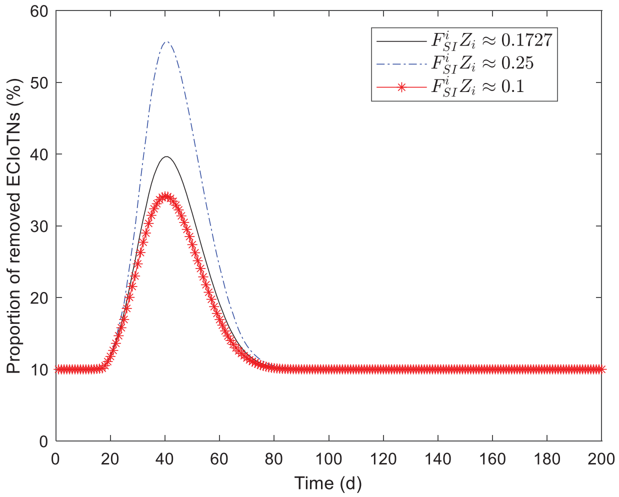

Figure 11: Changing tendency of removed ECIoTNs under the circumstance of Theorem 2 with diverse infection capabilities

Figs. 13–17 depict the the changing tendency of susceptible, curb, infectious, removed and dead ECIoTNs under the circumstance of Theorem 3 for $\alpha = 0.05, \alpha = 0.15$, and $\alpha = 0.2$. In Fig. 13, the changing tendency of the proportion of ECIoTNs in state S, denoted as $S_i(t)$, varies under different values of α. When α is 0.05, $S_i(t)$ decreases slowly, reaching around 93% before gradually increasing and approaching 100% to stabilize. On the other hand, when α is 0.15 and 0.2, $S_i(t)$ decreases to their respective minimum values of approximately 82% and 76% before slowly increasing towards 100% and stabilizing in its vicinity. In other words, $S_i(t)$ ultimately converges to the S_i^2 value of 1 in the stable point $\mathit{\Gamma}_2\left(S_i^2, C_i^2, I_i^2, R_i^2, D_i^2\right)$.

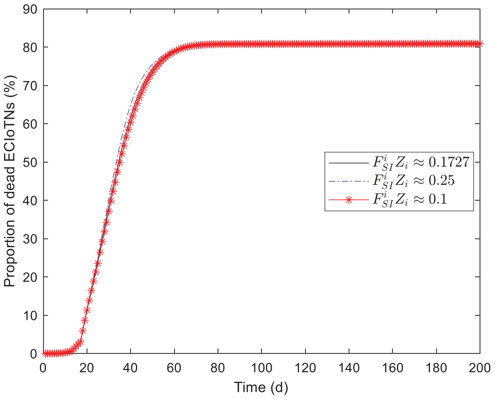

Figure 12: Changing tendency of dead ECIoTNs under the circumstance of Theorem 2 with diverse infection capabilities

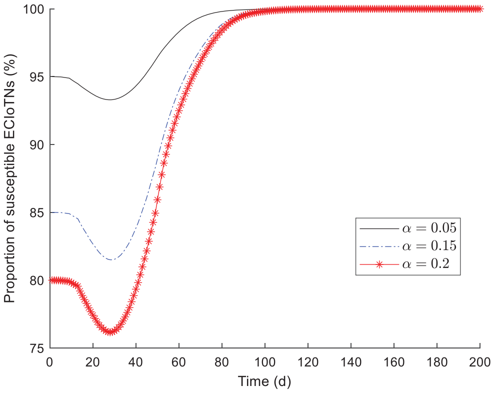

Figure 13: Changing tendency of susceptible ECIoTNs under the circumstance of Theorem 3 or $\alpha = 0.05, \alpha = 0.15$, and $\alpha = 0.2$

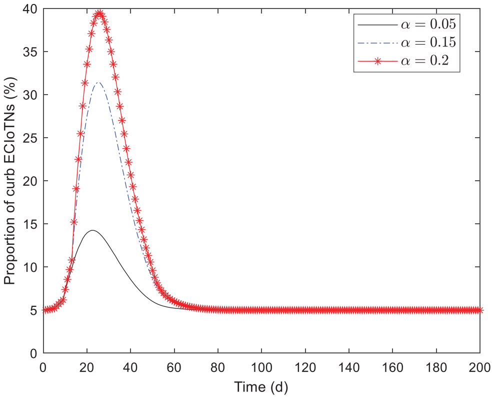

Figure 14: Changing tendency of curb ECIoTNs under the circumstance of Theorem 3 for or $\alpha = 0.05, \alpha = 0.15$, and $\alpha = 0.2$

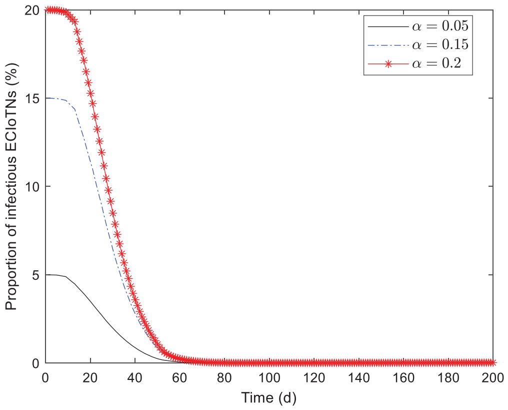

Figure 15: Changing tendency of infectious ECIoTNs under the circumstance of Theorem 3 or $\alpha = 0.05, \alpha = 0.15$, and $\alpha = 0.2$

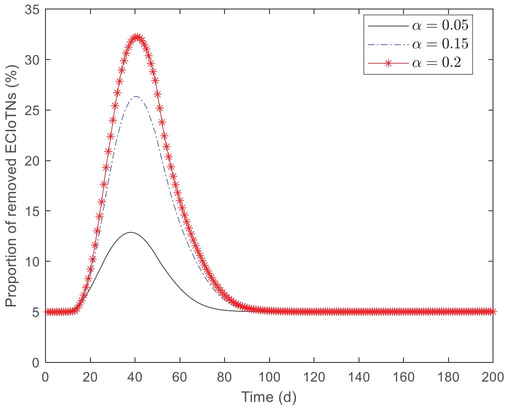

Figure 16: Changing tendency of removed ECIoTNs under the circumstance of Theorem 3 for $\alpha = 0.05, \alpha = 0.15$, and $\alpha = 0.2$

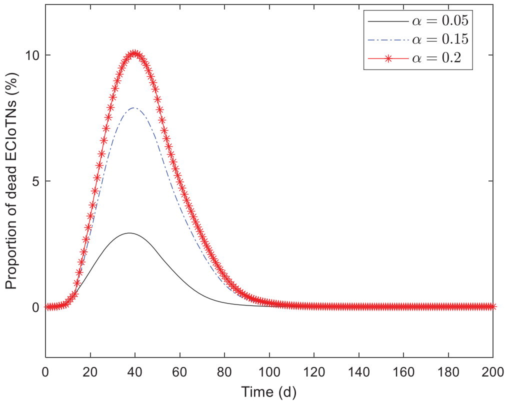

Figure 17: Changing tendency of dead ECIoTNs under the circumstance of Theorem 3 for $\alpha = 0.05, \alpha = 0.15$, and $\alpha = 0.2$

In Fig. 14, the proportion of curb ECIoTNs exhibits minor changes in the first $\sim$10d, followed by a gradual increase to 14%, 32%, and 40% in subsequent periods. Afterwards, it gradually decreases and eventually approaches 5%. This is consistent with the value of $C_i(t)$ in the stable point $\Gamma_2\left(S_i^2, C_i^2, I_i^2, R_i^2, D_i^2\right)$. In Fig. 15, the proportion of infectious ECIoTNs remains constant for the first $\sim$10d and then gradually decreases, eventually approaching zero. This is consistent with the value of $I_i(t)$ in the stable point $\Gamma_2\left(S_i^2, C_i^2, I_i^2, R_i^2, D_i^2\right)$. In Fig. 16, the proportion of removed ECIoTNs exhibits minor changes in the first $\sim$15d, followed by a gradual increase to 13%, 26%, and 33% in subsequent periods. Afterwards, it gradually decreases and eventually approaches 5%. This is consistent with the value of $R_i(t)$ in the stable point $\Gamma_2\left(S_i^2, C_i^2, I_i^2, R_i^2, D_i^2\right)$. In Fig. 17, the proportion of dead ECIoTNs exhibits minor changes in the first $\sim$10d, followed by a gradual increase to 3%, 8%, and 10% in subsequent periods. Afterwards, it gradually decreases and eventually approaches 0%. This is consistent with the value of $R_i(t)$ in the stable point $\Gamma_2\left(S_i^2, C_i^2, I_i^2, R_i^2, D_i^2\right)$.

According to the simulation results, we obtain the conclusion that no matter what proportions of infected ECIoTN there are, the ECIoTN cluster $i \in \{1, 2, \ldots, L\}$ in states S, C, I, R, and D would eventually stabilize.

5.2.2 Diverse Infectivity

In this section, using the identical parameter values as those provided in Section 5.1.2, for $\vartheta_i = i$, we can obtain $F_{SI}^i Z_i = 0.25$ and $\omega \approx 2.3148$, and for $\vartheta_i = AC = 2$, we obtain $F_{SI}^i Z_i \approx 0.5$ and $\omega \approx 4.6296$. At this point, the conditions of Theorem 3 are satisfied.

As depicted in Figs. 18–22, while there are variations in the peak values of the curves, the proportions of susceptible, curb, removed, and dead ECIoTNs ultimately converge to S_i^2, C_i^2, R_i^2, and D_i^2, respectively. In Fig. 20, when $F_{SI}^i Z_i \approx 0.5$, after the changing tendency of infectious ECIoTN stabilizes, it converges to 8%, and its convergence value is positive, which indicates that the malicious software in ECIoTNs continues to spread.

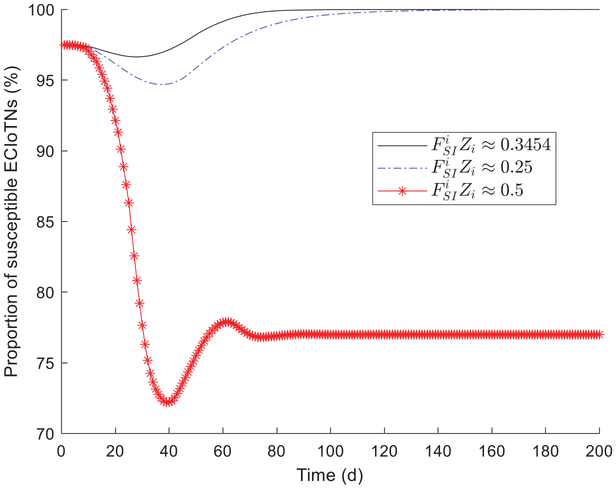

Figure 18: Changing tendency of susceptible ECIoTNs under the circumstance of Theorem 3 with diverse infection capabilities

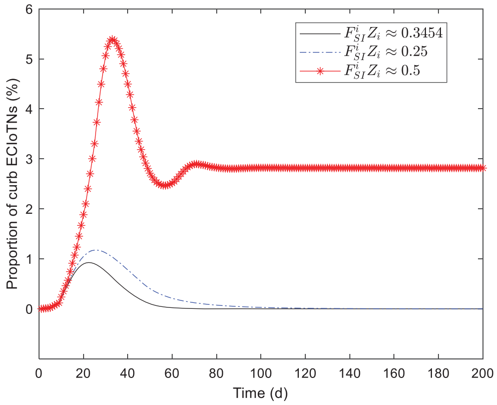

Figure 19: Changing tendency of curb ECIoTNs under the circumstance of Theorem 3 with diverse infection capabilities

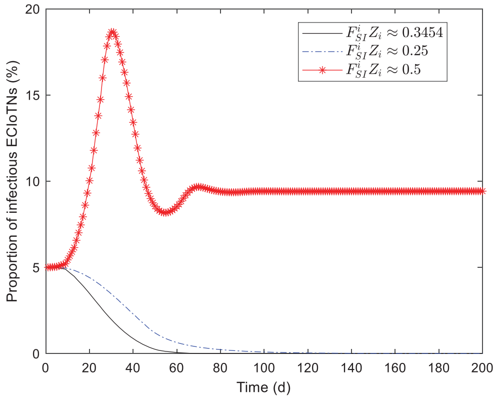

Figure 20: Changing tendency of infectious ECIoTNs under the circumstance of Theorem 3 with diverse infection capabilities

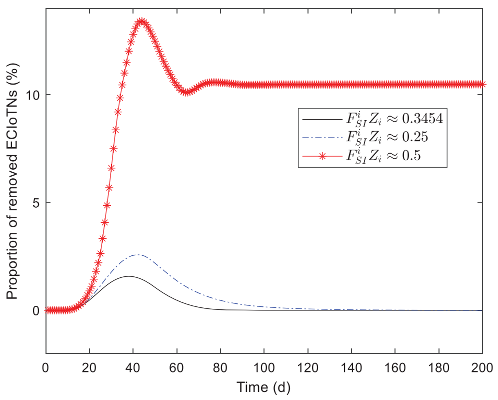

Figure 21: Changing tendency of removed ECIoTNs under the circumstance of Theorem 3 with diverse infection capabilities

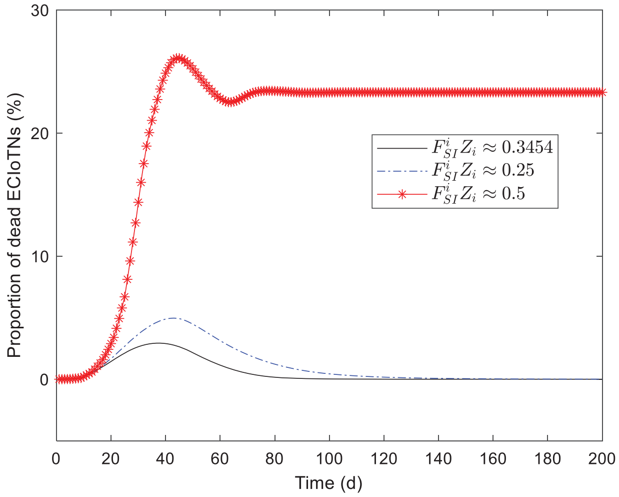

Figure 22: Changing tendency of dead ECIoTNs under the circumstance of Theorem 3 with diverse infection capabilities

In the end, we have successfully verified that Theorem 3 possesses both homogeneous and heterogeneous infection capabilities. The results of simulation experiments indicate that when the conditions of Theorem 3 are met, the infected ECIoTNs will eventually stabilize at a consistent level. As a result, during the defense process of ECIoT, it is of utmost importance to prevent the fulfillment of the stability conditions of the local equilibrium., as these conditions greatly enhance the potential for malicious software propagation.

6 Conclusion

Drawing inspiration from epidemiology, we have proposed an SCIRD model that takes into account the heterogeneous nature of the ECIoTN ecosystem and the varying connectivity of ECIoTN communication. By formulating a system of differential equations, we have described the dynamics of different states and degrees of high-speed rail fractions. Based on computational and experimental analysis, we have successfully demonstrated the existence of two equilibrium points within the SCIRD model. One represents a state without any malicious software, where malicious software eventually dissipates within ECIoTNs, while the other represents a localized equilibrium where malicious software persists and continues to propagate. Using the next generation matrix approach, we have calculated the fundamental reproduction number that governs the stability of these equilibrium points. Through computations and simulation experiments, we have verified that by controlling ECIoTN parameters, we can achieve stable conditions for a malicious software-free equilibrium and prevent the occurrence of localized equilibria. In our future work, we will focus on further optimizing the IoT security model by integrating the SCIRD infectious disease model to better reflect security issues in actual systems. We may consider incorporating more factors and variables, such as user behavior, interactions between IoT devices, to enhance the accuracy and applicability of the model, and provide guidance for the security management of real systems. Besides, future research can focus on developing new security mechanisms and technologies to enhance the security of IoT systems. This includes technological innovations in areas such as security authentication, encrypted communication, and intrusion detection and response, to address the constantly evolving security threats.

Acknowledgement: The authors would like to express their gratitude for the valuable feedback and suggestions provided by all the anonymous reviewers and the editorial team.

Funding Statement: This work was supported in part by National Undergraduate Innovation and Entrepreneurship Training Program under Grant No. 202310347039, Zhejiang Provincial Natural Science Foundation of China under Grant No. LZ22F020002, and Huzhou Science and Technology Planning Foundation under Grant No. 2023GZ04.

Author Contributions: Study conception and design: J. Ye, S. Shen; Data collection: W. Cheng, W. Zhu; Analysis and interpretation of results: J. Ye, X. Liu; Draft manuscript preparation: J. Ye, X. Wu, S. Shen. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data available on request from the authors.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] W. Lin *et al.*, "A deep neural collaborative filtering based service recommendation method with multi-source data for smart cloud-edge collaboration applications," *Tsinghua Sci. Technol.*, vol. 29, no. 3, pp. 897–910, 2024. doi: 10.26599/TST.2023.9010050.

[2] G. Wu, X. Chen, Z. Gao, H. Zhang, S. Yu, and S. Shen, "Privacy-preserving offloading scheme in multi-access mobile edge computing based on MADRL," *J. Parallel Distr. Comput.*, vol. 183, pp. 104775, 2024. doi: 10.1016/j.jpdc.2023.104775.

[3] Y. Shen, S. Shen, Q. Li, H. Zhou, Z. Wu and Y. Qu, "Evolutionary privacy-preserving learning strategies for edge-based IoT data sharing schemes," *Digit. Commun. Netw.*, vol. 9, no. 4, pp. 906–919, 2023. doi: 10.1016/j.dcan.2022.05.004.

[4] J. Ai, Z. Guo, and H. Chen, "Thwarting worm spread in heterogeneous networks with diverse variant placement," *IEEE Commun. Lett.*, vol. 22, no. 7, pp. 1346–1349, 2018. doi: 10.1109/LCOMM.2018.2820072.

[5] G. Wu, Z. Xu, H. Zhang, S. Shen, and S. Yu, "Multi-agent DRL for joint completion delay and energy consumption with queuing theory in MEC-based IIoT," *J. Parallel Distr. Comput.*, vol. 176, pp. 80–94, 2023. doi: 10.1016/j.jpdc.2023.02.008.

[6] V. A. Memos, K. E. Psannis, and Z. Lv, "A secure network model against bot attacks in edge-enabled industrial Internet of Things," *IEEE Trans. Ind. Inform.*, vol. 18, no. 11, pp. 7998–8006, 2022. doi: 10.1109/TII.2022.3162837.

[7] M. S. Arif, A. Raza, W. Shatanawi, M. Rafiq, and M. Bibi, "A stochastic numerical analysis for computer virus model with vertical transmission over the Internet," *Comput. Mater. Contin.*, vol. 61, no. 3, pp. 1025–1043, 2019. doi: 10.32604/cmc.2019.08405.

[8] R. M. Carnier, Y. Li, Y. Fujimoto, and J. Shikata, "Exact Markov chain of random propagation of malware with network-level mitigation," *IEEE Internet Things J.*, vol. 10, no. 12, pp. 10933–10947, 2023. doi: 10.1109/JIOT.2023.3240421.

[9] T. Wang, H. Li, C. Xia, H. Zhang, and P. Zhang, "From the dialectical perspective: Modeling and exploiting of hybrid worm propagation," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 1610–1624, 2023. doi: 10.1109/TIFS.2023.3246765.

[10] H. Ahn, J. Choi, and Y. H. Kim, "A mathematical modeling of Stuxnet-style autonomous vehicle malware," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 1, pp. 673–683, 2023. doi: 10.1109/TITS.2022.3213771.

[11] S. Shen, L. Xie, Y. Zhang, G. Wu, H. Zhang and S. Yu, "Joint differential game and double deep Q-networks for suppressing malware spread in Industrial Internet of Things," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 5302–5315, 2023. doi: 10.1109/TIFS.2023.3307956.

[12] M. Al-Fawa'Reh, J. Abu-Khalaf, P. Szewczyk, and J. J. Kang, "MalBoT-DRL: Malware botnet detection using deep reinforcement learning in IoT networks," *IEEE Internet Things J.*, vol. 11, no. 6, pp. 9610–9629, 2024. doi: 10.1109/JIOT.2023.3324053.

[13] G. Wu, H. Wang, H. Zhang, Y. Zhao, S. Yu and S. Shen, "Computation offloading method using stochastic games for software-defined-network-based multiagent mobile edge computing," *IEEE Internet Things J.*, vol. 10, no. 20, pp. 17620–17634, 2023. doi: 10.1109/JIOT.2023.3277541.

[14] S. Shen, C. Cai, Z. Li, Y. Shen, G. Wu, and S. Yu, "Deep Q-network-based heuristic intrusion detection against edge-based SIoT zero-day attacks," *Appl. Soft Comput.*, vol. 150, pp. 111080, 2024. doi: 10.1016/j.asoc.2023.111080.

[15] M. N. Aman, U. Javaid, and B. Sikdar, "IoT-Proctor: A secure and lightweight device patching framework for mitigating malware spread in IoT networks," *IEEE Syst. J.*, vol. 16, no. 3, pp. 3468–3479, 2022. doi: 10.1109/JSYST.2021.3070404.

[16] J. Chen, S. Sun, C. Xia, D. Shi, and G. Chen, "Modeling and analyzing malware propagation over wireless networks based on hypergraphs," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 6, pp. 3767–3778, 2023. doi: 10.1109/TNSE.2023.3273184.

[17] S. Lazfi, S. Lamzabi, A. Rachadi, and H. Ez-Zahraouy, "The impact of neighboring infection on the computer virus spread in packets on scale-free networks," *Int. J. Mod. Phys. B*, vol. 31, no. 30, pp. 1750228, 2017. doi: 10.1142/S0217979217502289.

[18] A. Gómez-Corral, F. Palacios-Rodríguez, and M. T. Rodríguez-Bernal, "On the exact reproduction number in SIS epidemic models with vertical transmission," *Comput. Appl. Math.*, vol. 42, pp. 291, 2023. doi: 10.1007/s40314-023-02424-5.

[19] G. Wu, L. Xie, H. Zhang, J. Wang, S. Shen and S. Yu, "STSIR: An individual-group game-based model for disclosing virus spread in Social Internet of Things," *J. Netw. Comput. Appl.*, vol. 214, pp. 103608, 2023. doi: 10.1016/j.jnca.2023.103608.

[20] A. Coronel, F. Huancas, I. Hess, E. Lozada, and F. Novoa-Muñoz, "Analysis of a SEIR-KS mathematical model for computer virus propagation in a periodic environment," *Mathematics*, vol. 8, no. 5, pp. 761, 2020. doi: 10.3390/math8050761.

[21] H. Guo, H. K. Cheng, and K. Kelley, "Impact of network structure on malware propagation: A growth curve perspective," *J. Manag. Inf. Syst.*, vol. 33, no. 1, pp. 296–325, 2016. doi: 10.1080/07421222.2016.1172440.

[22] J. Li, F. Li, W. Wang, and J. Zhai, "An information dissemination influence model for mobile social network under multi-role view," *Int. J. Uncertain. Fuzz. Knowl.-Based Syst.*, vol. 29, no. 1, pp. 1–15, 2021. doi: 10.1142/S021848852150001X.

[23] S. Li, B. Wang, S. Qian, Y. Sun, X. Yun and Y. Zhou, "Influence maximization for emergency information diffusion in social internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8768–8782, 2022. doi: 10.1109/TVT.2022.3146260.

[24] H. Wang, H. He, W. Zhang, W. Liu, P. Liu and A. Javadpour, "Using honeypots to model botnet attacks on the internet of medical things," *Comput. Electr. Eng.*, vol. 102, pp. 108212, 2022. doi: 10.1016/j.compeleceng.2022.108212.

[25] J. Yi, P. Liu, Z. Wang, and W. Liu, "Research on twin-SIR rumor spreading model in online social network," *J. Intell. Fuzz. Syst.*, vol. 40, no. 4, pp. 5863–5874, 2021. doi: 10.3233/JIFS-189426.

[26] W. Tang, Y. Liu, Y. Chen, Y. Yang, and X. Niu, "SLBRS: Network virus propagation model based on safety entropy," *Appl. Soft Comput.*, vol. 97, pp. 106784, 2020. doi: 10.1016/j.asoc.2020.106784.

[27] S. Hosseini and M. A. Azgomi, "The dynamics of an SEIRS-QV malware propagation model in heterogeneous networks," *Physica A: Stat. Mech. App.*, vol. 512, pp. 803–817, 2018. doi: 10.1016/j.physa.2018.08.081.

[28] D. Tran Le, T. T. Tran, K. Q. Dang, R. Alkanhel, and A. Muthanna, "Malware spreading model for routers in Wi-Fi networks," *IEEE Access*, vol. 10, pp. 61873–61891, 2022. doi: 10.1109/ACCESS.2022.3182243.

[29] N. P. Dong, H. V. Long, and N. L. Giang, “The fuzzy fractional SIQR model of computer virus propagation in wireless sensor network using Caputo Atangana-Baleanu derivatives,” *Fuzzy Sets Syst.*, vol. 429, pp. 28–59, 2022. doi: 10.1016/j.fss.2021.04.012.

[30] T. Wang, C. Xia, X. Li, and Y. Xiang, “Epidemic heterogeneity and hierarchy: A study of wireless hybrid worm propagation,” *IEEE Trans. Mob. Comput.*, vol. 21, no. 5, pp. 1639–1656, 2022. doi: 10.1109/TMC.2020.3026342.

[31] J. Dou, G. Xie, Z. Tian, L. Cui, and S. Yu, “Modeling and analyzing the spatial-temporal propagation of malware in mobile wearable IoT networks,” *IEEE Internet Things J.*, vol. 11, no. 2, pp. 2438–2452, 2024. doi: 10.1109/JIOT.2023.3295016.

[32] C. Gan, Y. Qian, A. Liu, and Q. Zhu, “Search-driven virus spreading on Social Internet of Things: A dynamical perspective,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 114, pp. 106624, 2022. doi: 10.1016/j.cnsns.2022.106624.

[33] Y. Yao, C. Sheng, Q. Fu, H. Liu, and D. Wang, “A propagation model with defensive measures for PLC-PC worms in industrial networks,” *Appl. Math. Model.*, vol. 69, pp. 696–713, 2019. doi: 10.1016/j.apm.2019.01.014.

[34] F. Yang, Z. Zhang, and A. Zeb, “Hopf bifurcation of a VEIQS worm propagation model in mobile networks with two delays,” *Alex. Eng. J.*, vol. 60, no. 6, pp. 5105–5114, 2021. doi: 10.1016/j.aej.2021.03.055.

[35] K. Wang, Y. Gong, and F. Hu, “SIS epidemic propagation on scale-free hypernetwork,” *Appl. Sci.*, vol. 12, no. 21, pp. 10934, 2022. doi: 10.3390/app122110934.

[36] Y. Xie and Z. Wang, “Transmission dynamics, global stability and control strategies of a modified SIS epidemic model on complex networks with an infective medium,” *Math. Comput. Simul.*, vol. 188, pp. 23–34, 2021. doi: 10.1016/j.matcom.2021.03.029.

[37] X. Liu, D. He, and C. Liu, “Information diffusion nonlinear dynamics modeling and evolution analysis in online social network based on emergency events,” *IEEE Trans. Comput. Soc. Syst.*, vol. 6, no. 1, pp. 8–19, 2019. doi: 10.1109/TCSS.2018.2885127.

[38] E. Zhang, G. Wang, Y. Feng, and R. Ma, “Mathematical analysis and design of PMTD strategies for an SIRO model of OS virus propagation,” *Comput. Commun.*, vol. 192, pp. 332–342, 2022. doi: 10.1016/j.comcom.2022.06.006.

[39] D. Bartl, M. Fabian, and J. Kolář, “Clarke Jacobians, Bouligand Jacobians, and compact connected sets of matrices,” *J. Math. Anal. Appl.*, vol. 516, no. 1, pp. 126491, 2022. doi: 10.1016/j.jmaa.2022.126491.

[40] S. Özgür and M. Orman, “Application of deep learning technique in next generation sequence experiments,” *J. Big Data*, vol. 10, pp. 160, 2023. doi: 10.1186/s40537-023-00838-w.

[41] C. Li, C. Tsai, and S. Yang, “Analysis of epidemic spreading of an SIRS model in complex heterogeneous networks,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 4, pp. 1042–1054, 2014. doi: 10.1016/j.cnsns.2013.08.033.