Analyzing the Influence of Users, Devices, and Search Engines on Viral Spread in the Social Internet of Things

Chenquan Gan[a,b], Hongming Chen[a], Yi Qian[a], Liang Tian[c], Qingyi Zhu[b], Deepak Kumar Jain[d,e], Vitomir Štruc[f,*]

[a]*School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[b]*School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[c]*School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[d]*Key Laboratory of Intelligent Control and Optimization for Industrial Equipment of Ministry of Education, Dalian University of Technology, Dalian, 116024, China*
[e]*Symbiosis Institute of Technology, Symbiosis International University, Pune 412115, India*
[f]*University of Ljubljana, Faculty of Electrical Engineering, Trzaska cesta 25, SI-1000 Ljubljana*

Abstract

The Social Internet of Things (SIoT) seamlessly integrates the Internet of Things (IoT) with social networks, intensifying the interconnections among objects, humans, and their interactions. While SIoT facilitates rapid information access and sharing through search engines, it also increases the risk of computer virus propagation. It is, therefore, critical to understand how viruses propagate in SIoT networks and which factors contribute the most to viral spread. While such understanding is of paramount importance, comprehensive studies on this topic are still limited in the literature. To address this gap, we study in this paper the long-term behavior of viral spread in SIoT, examining the roles of users, devices, and search engines. Specifically, we propose a novel dynamical virus propagation model that accounts for key factors, such as user awareness, device security levels, search engines, and external storage media. In comparison to competing solutions, the proposed model offers a unique perspective on viral spread in SIoT by focusing on multiple influential factors, their interactions, while also considering the inherent characteristics of the SIoT framework. A comprehensive theoretical analysis of the model is conducted to identify patterns and the key aspects of virus propagation in SIoT. To further validate the findings, a virus propagation algorithm is also designed, and multiple simulations including model comparisons are conducted on two real network datasets (Facebook and P2P), demonstrating the validity of the theoretical findings.

Keywords: Viral spread, Social Internet of Things, user awareness, device security level, search engine

1. Introduction

Social networks are defined as structures composed of individuals or organizations that are connected by various types of interdependencies, such as relationships, friendships, professional associations, or common interests

*Corresponding author
Email addresses: gcq2010cqu@163.com (Chenquan Gan), s230101008@stu.cqupt.edu.cn (Hongming Chen), s200131028@stu.cqupt.edu.cn (Yi Qian), besttianliang@gmail.com (Liang Tian), zhuqy@cqupt.edu.cn (Qingyi Zhu), deepak@cqupt.edu.cn (Deepak Kumar Jain), vitomir.struc@fe.uni-lj.si (Vitomir Štruc)

[1]. These connections are typically represented by nodes (individuals or entities) and edges (relationships or interactions) in a graph, where nodes correspond to users or members, and edges represent the relationships or connections between them [2]. Social networks can manifest in various forms, including online platforms (such as Facebook, Twitter, or LinkedIn) that facilitate digital interactions, or offline communities and groups where people interact face-to-face. The concept of a social network [3, 4] emphasizes the importance of relationships and the flow of information within a group or community.

With the rapid popularization of mobile smart devices, an increasing number of users rely on social networks for interaction, resulting in new characteristics, such as dynamic, complex, and massive data being exchanged among connected users and local structures being present within the social networks themselves [5, 6]. Given the characteristics of social networks, a new field called the Social Internet of Things (SIoT), which combines social networks with the Internet of Things (IoT), was proposed in [7]. SIoT heavily relies on the organization and relationships within social networks and utilizes connections between objects-and-objects, humans-and-objects, as well as humans-and-humans to facilitate services and applications for IoT [8, 9, 10, 11]. Unlike the Web of Things (WoT) [12], which combines IoT technology with internet technology, SIoT emphasizes user participation in IoT. By simulating social relationships between device owners, SIoT can facilitate device collaboration and interaction, enabling resource sharing and autonomous interaction between social networks and physical smart devices [13, 14]. This further brings about changes in various aspects of human life, such as smart homes [15], digital healthcare [16], Internet of Vehicles [17], and related application scenarios [18, 19].

With the continuous expansion of the scale and application scenarios of SIoT, it is progressively evolving into the primary platform for communication, information dissemination, and knowledge sharing [20, 21]. The advent of powerful search engines (SEs) further enhances SIoT's capability to deliver varied information customized to factors such as user interest and content relevance, thereby establishing a robust connection between users and devices within the SIoT framework. Although the widespread use of search engines accelerates the speed of information dissemination in SIoT, it also introduces a new avenue for the proliferation of computer viruses. Additionally, because it is critical to ensure the autonomy of devices in SIoT to facilitate sufficient interaction, this inadvertently creates an environment conducive to the outbreak and spread of computer viruses [22]. Since computer viruses are nowadays diverse, highly covert, intelligent, and have multiple ways of spreading, devising effective prevention measures is highly challenging. However, without such measures, the damages caused by viruses may outweigh the benefits brought about by SIoT [23].

Due to the long development cycle, substantial cost, and the lag in anti-virus research from a code-centric perspective, there has been great interest in studying the long-term behavior of computer virus propagation by drawing upon ideas from epidemic models [24, 25, 26]. Although previous research has proposed various computer virus propagation models and considered factors such as users [27] and devices [28, 29], the role of search engines has been largely overlooked so far. While a few studies did attempt to incorporate search engines into their analyses as well [30, 31], these efforts fell short in comprehensively accounting for the unique characteristics of SIoT networks, relying predominantly on conventional network structures. Addressing the intricacies of the network structure in SIoT necessitates considerations on how to leverage the relationships between individuals

and objects to accommodate changes induced by the substantial amount of network data [32, 33].

Different from existing studies on virus propagation, the role of search engines (as conduits for information dissemination) and their interaction with both users and devices has to date remained underexplored in the SIoT literature. While Wu *et al.* [34] analyzed SIoT virus transmissions by utilizing epidemiology theory and individual-group game theory, they did not focus specifically on the interplay between users, devices and search engines. Similarly, Zhang *et al.* [35] used a Markov chain based epidemic method to alleviate the spread of malicious software in SIoT and prevent malicious software from dominating the network, but did not put special emphasis on the interactions among search engines on the one hand and users and devices on the other. In this paper, we address this gap and present a study into virus propagation in SIoT that explores the impact of users, devices, and search engines on viral spread. Specifically, the paper aims to study three key research questions wihtin this area, including: (1) How users (and their security awareness), devices (and their security level), and search engines (that serve as an information dissemination medium) jointly influence the long-term propagation behavior of computer viruses in SIoT, (2) Which factors among the three are the most crucial for the virus propagation, and (3) How to effectively prevent and control the virus propagation by regulating these factors. To this end, we propose a novel model for virus propagation in SIoT and through the Lyapunov stability theorem, verify and prove the validity and long-term predictability of the proposed model. The main research contributions of this paper can be summarized into the following points:

1) We conduct a thorough examination of the virus propagation in SIoT, analyzing the process from the user, device, and search engine standpoints. To the best of our knowledge, this is the first study considering these three key factors when studying virus spread in SIoT.
2) We propose a novel dynamical virus spread model that captures the impact of user awareness, device security level, search engines, and external storage media on virus propagation in SIoT.
3) We design a virus propagation algorithm to demonstrate the feasibility of the model on two real-world network datasets (the Facebook and P2P datasets), including model comparisons.

2. Related work

To ensure a comprehensive and systematic review of the existing literature, we conducted a structured literature search, focusing on virus propagation models in the context of the Social Internet of Things (SIoT) and related network environments. This literature search covered major academic databases including IEEE Xplore, Web of Science, Scopus, and Google Scholar. The core search strings used were: virus propagation, malware propagation, epidemic models, social Internet of Things, device security, and search engines. We also examined the reference lists of key review articles and pioneering papers to identify other relevant studies. The inclusion criteria for the literature prioritized English peer-reviewed journal articles and conference papers published between 2010 and 2024 that provided theoretical models, empirical analyses, or simulation studies related to the influencing factors of virus propagation in network systems. The literature obtained through the above search strategy was subsequently categorized and analyzed from three perspectives: user modeling, device modeling, and network topology.

When studying the process of computer virus propagation in different scenarios, it is common to draw insights from epidemic models and incorporate real-world factors [36, 37, 38, 39, 40, 41]. To provide the necessary background for our work, we discuss in this section existing research on network virus propagation from the perspectives of users, devices, and network topology. The work covered in these sections represents representative/seminal methods on virus propagation (also in SIoT) and was identified through a literature search of prior works and study of key surveys in this area[36, 37, 38, 39, 40, 41].

Modeling Users. Users are commonly modeled as device owners/holders and are, therefore, inextricably linked to the infection of various devices with computer viruses. Han and Tan [42] proposed a time-delayed SIRS (susceptible-infected-recovered-susceptible) virus propagation model by studying the time delay between inducing users to click on viruses and devices being infected. The existence of this time delay was found to be partly related to user behavior. In [40], an evolutionary Poisson game framework was established to capture the stochastic, dynamic, and heterogeneous interaction behaviors among users. The work in [39] found that adding more relationships or increasing the number of objects owned by each user increased the propagation rate of malicious software by simulating its propagation process. Based on the fact that user behavior is commonly affected by the user's subjective consciousness, Sobhani and Keshavarz-Haddad considered the user's response to receiving malicious files and studied the viral spread process in the campus scene [43]. The work in [44] analyzed the impact of user awareness on communication behavior by studying individual states, both conscious and unconscious. A common insight from the reviewed work is that *user awareness* is a key factor that cannot be ignored when studying the impact of users on virus propagation. Nonetheless, research on user-oriented virus transmission often overlooks the fact that devices may also be infected at different infection rates or in different ways, something we account for in our proposed model.

Modeling Devices. When studying the impact of devices on virus propagation, Amador and Artalejo [45] considered the characteristic of immune computers sending warning signals to reduce virus transmission and established a random SIRS model to analyze the behavior and persistence of virus transmission. Regarding the way devices are infected, Gan and Yang [46] considered removable storage media and proposed a dynamical model that captures the virus transmission mechanisms. In addition, for anti-virus patches installed on the device, Yang et al. [47] designed a node-level malware propagation model to evaluate the impact of patch forwarding on computer virus propagation. The authors of [29] simulated the interaction between virus and patch transmission based on the dynamic competitive transmission process. It is evident that, while users do typically manipulate and interact with various devices, the influence of device-related factors on virus spread is significant and therefore needs to be included in meaningful virus propagation models.

Modeling the Network Topology. Another critical factor impacting viral spread is the network topology, as highlighted by multiple studies on this topic, e.g., [48, 49, 30, 31, 38]. Yang et al. [48] considered the heterogeneity of propagation networks, proposed a SIRS model based on heterogeneous nodes, and discussed in detail the dynamic properties of the developed model. Feng et al. [49] proposed an improved SIRS model to capture the dynamic process of virus propagation, taking into account communication radius and node distribution density. In SIoT, due to the widespread application of search engines, the initial structure of SIoT has gradually

Table 1: Comparison of related work

References	Main Contributions	Methods	Limitations	Relevance to this work
[38, 39, 40, 42, 44]	Subjective factors such as user behavior, awareness, and interaction patterns, which are the core variables influencing the spread of computer viruses, have enabled the transformation of virus spread research from being driven solely by technology to one that users and technology jointly drive. This change has led to a more user-centric approach in the study of virus spread.	By constructing mathematical models to quantify user factors, users are classified into different states. Through analyzing the probability of state transitions, the dynamic effects of user behaviors on virus transmission are revealed. Simulating the user network and the virus transmission process verifies the hypotheses.	High computational complexity and lack of real-time feedback make it difficult to adjust the virus detection strategy in time.	The users who inherit such tasks are the key influencing factors. By transforming the simple classification of users into one based on their level of awareness, this solution addresses the issues of coarse user stratification and disconnection from devices.
[29, 45, 46, 47]	This type of model establishes the core position of the device as a carrier of virus transmission. By analyzing its security characteristics and interactions with other devices, it reveals the crucial role of the device in restricting virus transmission and provides a theoretical basis for defense strategies based on device behavior.	By constructing differential equations or stochastic process models to describe the virus transmission dynamics at the device level, with device nodes as the basic units, focusing on the infection, recovery, and immunity processes of individual devices, and for the interaction between viruses and patches in the device network, using simulation analysis to examine the dynamic relationship between the two.	Ignoring the user's operation behaviors on the device, failing to cover the key transmission channels of SIoT, and not differentiating the security levels of the devices, results in the model being unable to accurately reflect the virus transmission mechanism in the real SIoT environment.	The model proposed in this paper draws on the idea that devices are the core carriers. It achieves this through device security classification, dynamic binding of users and devices, and the addition of new search engines as communication channels.
[30, 31, 38, 48, 49]	The network topology structure has a crucial impact on the spread of viruses. New transmission channels, such as search engines, have not only changed the characteristics of network connections but also accelerated the spread of viruses, driving the development of virus transmission models towards adapting to specific topological structures.	By quantitatively analyzing the network topology to study its impact on the rate and scope of virus transmission, and through simulation to verify the influence of the topology on the transmission, analyze the steady state and patterns of the transmission, and ensure the reliability of the conclusion.	The model fails to match the two-layer topology of SIoT society and the Internet of Things, fails to integrate multiple dimensions such as users and devices, and lacks a mechanism for the microscopic state transitions of nodes. As a result, it is difficult for this model to accurately depict the propagation dynamics of viruses in the real SIoT environment.	The model proposed in this paper utilizes the network topology structure to construct an architecture that conforms to the dual-layer topology of the SIoT society and the Internet of Things. It integrates multiple dimensions, such as users, devices, and topology, for interlinked modeling, significantly enhancing the accuracy and practical value of virus transmission analysis.

changed. In [30], a two-layer model for malware propagation has been proposed, which proves from a macro perspective that when search engines exist, the number of malware increases exponentially in the early stages, and the reciprocal of infection time follows a power-law distribution. Furthermore, different models [31, 38] have also shown that search engines can change the topology of the network and accelerate the dissemination of information. With the help of search engines, computer viruses have gained new ways of spreading. Although there is currently a small number of studies available in the open literature that explore the impact of search engines on virus transmission behavior, these studies do not comprehensively consider the role of users or devices

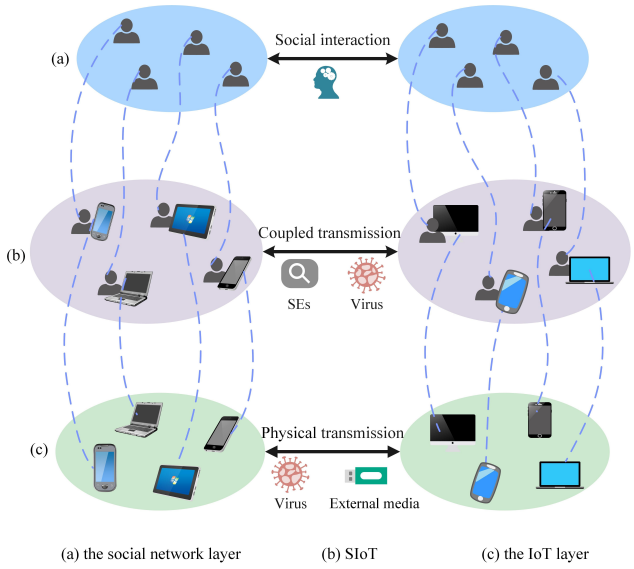

Figure 1: Overview of the network architecture considered in our work.

in the transmission process.

Comparative Analysis and Main Contributions. A high-level analysis of the literature discussed above is presented in Table 1. The table summarizes the main contributions, methods used and the key limitations of the surveyed prior work. More importantly, it also elaborates on the connection to the work presented in this paper and characteristics of the model proposed herein. As can be seen, our proposed model builts on the ideas presented in prior work, but extends them to mitigate key limitations, including the way users and devices are modeled, the utilization of a network topology that conforms with the dual-layer topology of SIoT and the modelling of search engines and their interactions with both users and devices. We aim to investigate the long-term behavior of viral spread in SIoT networks by modeling the impact of users, devices, and search engines, as well as their interdependence. To this end, we introduce a differential dynamic system [50] to model and analyze the dynamic behavior of virus transmission in SIoT and study the existence, uniqueness, and stability of the proposed system. We use the Hurwitz criterion [51] to determine the local asymptotic stability, which points to good convergence near the equilibrium of the system. Additionally, we adopt the geometric method in Lyapunov stability theory [52, 53] to prove that the system would eventually converge to the unique equilibrium under any initial conditions, providing a theoretical basis for virus prevention and control.

3. The proposed dynamical model

In this section, we present one of the main contributions of this work, i.e., a novel model for virus propagation in the Social Internet of Things (SIoT).

3.1. Background

For the virus propagation scenario, we consider a network topology, as presented in Fig. 1. Here, users come from (a) the *social network layer* that accounts for the social interactions between users (device owners). Within this layer, users can facilitate the diffusion of social attributes, such as awareness and relationships, through communication and interactive behaviors [54, 55]. (c) The *IoT layer* represents the device layer, responsible for the physical transmission between the various devices. When devices engage in physical transmission, they are often susceptible to computer virus attacks and may become infected with computer viruses. For example, when transferring information to an end-device from an external storage media, the targeted end-device will be infected if the external media is contaminated with a computer virus. In turn, this leads to the virus spreading to other devices. Additionally, there is user participation in the process of physical transmission, as the devices are manipulated by the device owners. Therefore, the diffusion of social attributes in (a) will affect users' control over their devices, thereby influencing the virus spreading in (c). The (b) *SIoT framework* consists of the social network layer in Figure (a) and the IoT layer, shown in Figure (c) [56], and, therefore, encompasses users (device owners) as well as devices, as shown in Figure 1 (b). In the context of SIoT, Search Engines (SEs) have emerged as the conduit for propagating information between the social network and IoT layers in (a) and (c), respectively. Users can retrieve the desired information from the SEs through a specific device, and SEs present a relevance ranking of the desired information. Furthermore, users can access the desired information through their devices, establishing new connections [57]. However, while SEs bring convenience, they also expose new security risks. The information content provided by the SEs through unverified URLs is in general unknown, and it is possible that such URLs point to network traps carrying computer viruses. Clicking on these links can lead to device infection and even a network-wide spread of the virus, where the propagation dynamics are impacted by the varying levels of device security among users. To better understand this process, we aim (in this paper) to analyze the virus propagation dynamics from the viewpoints of users and devices, with a specific focus on examining the impact of SEs.

3.2. Mathematical framework

State Description. As emphasized above, the SIoT framework consists of a social network and an IoT layer. Accordingly, the virus propagation process in SIoT is the process of viruses circulating between these two layers. Given the users' perspective, the personal attributes (such as behavior or awareness) generated by the interaction between users from the social network layer usually affect devices, thus affecting virus propagation. For example, users use external storage media to access devices, or users access different devices through SEs. When a device is infected with computer viruses because of the interaction with a SE, users become pivotal in assessing potential security risks. The user's subjective perception of these risks, termed *security awareness*, is therefore a crucial factor that needs to be considered in virus-propagation models. It needs to be noted that virus propagation often happens due to the lack of a comprehensive understanding of the information returned by SEs and insufficient response time. If users cannot promptly and accurately determine the presence of viruses in data provided by the SEs, the likelihood of transmission significantly rises. Consequently, users commonly

rely on background anti-virus software to assist in evaluating potential security risks. Considering variations in users' security awareness, their choice of anti-virus software also differs. Thus, we categorize users in the social network layer into the following two groups/states for our proposed model:

- **Weak-knowledge Users** (W): This group consists of users who know nothing or little about viruses or virus spread. Such users will commonly resort to free anti-virus software or trial-versions of paid anti-virus solutions.

- **Power Users** (P): This group features users with greater knowledge of viruses and virus propagation, typically with past experience of virus infections. Users from this group have considerable awareness of virus prevention and are willing to subscribe to paid anti-virus software.

Computer virus infections exclusively occur on the device side, spreading across various devices. As emphasized above, the variations in user security awareness result in different versions of anti-virus software installed, leading to diverse security levels among devices. Consequently, the susceptibility of a device to virus infections also varies significantly. Devices with elevated security levels can mitigate the spread of viruses within the network to some extent, and such security levels, therefore, need to be included in virus-propagation models. We classify devices in the IoT layer into the following two groups/states for the proposed model:

- **Low-security Devices**: Devices from this group have free anti-virus software installed and/or ensure only the most basic protection. The virus database updates are slow.

- **High-security Devices**: Devices from this group feature paid anti-virus software and a more comprehensive level of protection. The software is capable of updating to the latest virus database sufficiently frequently.

Additionally, device states need to be defined that reflect virus-infection status. For our model, we consider the following three high-level states for the devices in the IoT layer:

- **Susceptible**: This state corresponds to devices that do not carry computer viruses.

- **Infected**: This state represents devices that have been infected with a computer virus.

- **Recovered**: This state denotes devices that are immune to computer viruses.

Since infections occur on devices of different security levels, we model the state of each device in the IoT layer more comprehensively through one of the following three states:

- **A susceptible device with a low security level (S_L)**: This state accounts for devices installed with free anti-virus software that do not carry computer viruses.

- **An infected device with a low security level (I_L)**: This state corresponds to devices with free anti-virus software that are still infected by unknown computer viruses.

- **A recovered device with a high security level (R_H)**: This state defines devices with comprehensive protection due to the installation of paid anti-virus software.

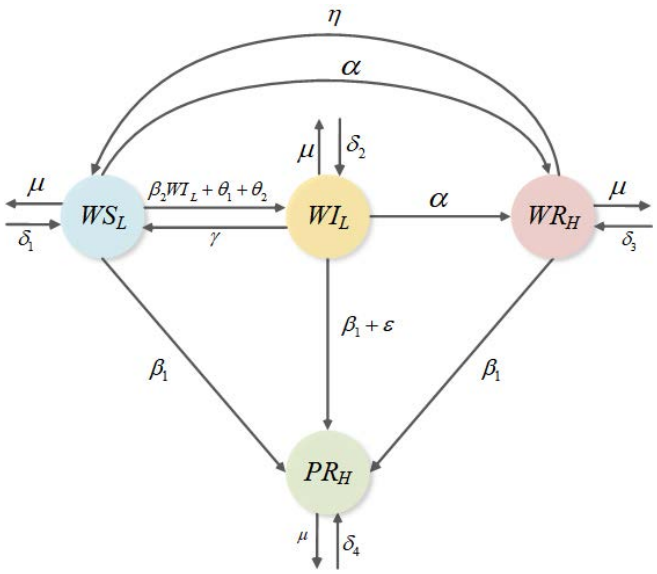

Figure 2: The state transfer diagram of the proposed viral propagation model.

When a device is equipped with a free version of antivirus software, its level of protection is limited to the most fundamental functions, and potentially outdated virus databases. Such devices will be easily infected by unknown computer viruses. Thus, a recovered device with a low security level (R_L) does not exist. Similarly, there is no susceptible or infected device with a high security level (S_H or I_H) and we, therefore, do not account for such devices in our model.

Virus propagation in SIoT refers to the spreading process between the social network and IoT layers, with the joint participation of users and devices. Any node in SIoT can be regarded as composed of users (device holders) and their corresponding devices and is, therefore, accounted for with one of the following four states in our model:

- WS_L **state**: This state describes a weak-knowledge user with susceptible devices with low security levels.
- WI_L **state**: This state defines a weak-knowledge user with infected devices with low-security levels.
- WR_H **state**: This state corresponds to a weak-knowledge user whose devices are recovered devices with high-security levels.
- PR_H **state**: This state denotes power users with recovered devices with high-security levels.

It is important to note that the PS_L (i.e., a state that corresponds to power users with susceptible devices with low-security levels) and PI_L states (i.e., a state that corresponds to power users with infected devices with low-security levels) do not exist and are not considered in our model.

Basic Assumptions and Definitions. To model the spread of computer viruses in SIoT, we consider users and their devices as nodes. Similarly, the communication between users and devices is modelled as edges between nodes. Given the state descriptions presented above, a node in SIoT in our model is always in one of four states: WS_L, WI_L, WR_H, PR_H. The nodes change states and affect each other in accordance with the following assumptions and corresponding definitions:

Table 2: Summary of the parameters of the proposed viral propagation model.

Parameter	Meaning
$\delta_1, \delta_2, \delta_3, \delta_4$	The connection rate of nodes in WS_L, WI_L, WR_H, and PR_H states, respectively.
β_1	The probability that weak-knowledge users will be affected by powerful-aware users.
β_2	The probability of communication between devices, that is, the infection rate between devices.
θ_1, θ_2	The probability of device infection caused by users using search engines or external storage media.
γ	The probability of reinstalling the system on the devices.
ε	The probability is that weak-knowledge users become more aware of security.
α	The probability that a user selects a paid trial version of anti-virus software.
η	The probability of anti-virus software failure.
μ	The break probability of node connection in SIoT.

(D1) Nodes (i.e., users and devices) in our model may enter or disconnect from the SIoT. To capture this aspect, we define the connection rate per unit time of the nodes in WS_L, WI_L, WR_H, and PR_H states as $\delta_1, \delta_2, \delta_3, \delta_4$, respectively, and the disconnection probability per unit time of node connection in SIoT as μ.

(D2) Weak-knowledge users may be positively affected by Power Users. We model this characteristic through nodes in the WS_L or WI_L or WR_H state that can switch to the PR_H state with the probability per unit time β_1.

(D3) Due to the communication between devices, a susceptible device with a weak-knowledge user and a low security level may be infected by other infected devices. We capture this aspect by defining a probability per unit time β_2 according to which a node in the WS_L state switches to the WI_L state.

(D4) Due to users using search engines or external storage media, a susceptible device with a weak-knowledge user and a low security level may be infected by other infected devices. We model this transition with nodes in WS_L state that switch to the WI_L state with a probability per unit time θ_1 or θ_2.

(D5) Due to the installation and update of antivirus software, some devices may become recovered devices. In our model, this is captured by nodes in the WS_L or WI_L states that switch to the WR_H state with a probability per unit time α.

(D6) Due to reinstalling the system on the devices or anti-virus software failure, some devices may become susceptible. We again capture this aspect in our model with nodes in the WI_L or WR_L states that switch over to the WS_H state with probability per unit time γ or η.

(D7) Due to improvements in self-awareness, weak-knowledge users become more aware of security. We capture this final aspect with nodes in the WI_L state that switch to the PR_H state with a probability per unit time ε.

Based on the presented assumptions and probability definitions, we define the state transfer diagram of our model, as shown in Fig. 2. The meaning of the model parameters is summarized in Table 2.

Model Formulation. For the theoretical analysis presented in the following section, we utilize the following notation. For any time instance t, let $x(t), y(t), z(t)$ and $m(t)$ represent the number of nodes with an WS_L, WI_L, WR_H and PR_H state, respectively. Furthermore, let $N(t)$ represent the number of all nodes in

the model, so that $N(t) = x(t) + y(t) + z(t) + m(t)$. For brevity, $x(t), y(t), z(t), m(t)$ and $N(t)$ are hereafter abbreviated as x, y, z, m and N, respectively.

Based on the assumptions presented above and the state transfer diagram from Fig. 2, our final **virus propagation model** can be represented by the following state-transfer equations, i.e., as a differential dynamical system:

$$\begin{cases} \dfrac{dx}{dt} = \delta_1 + \gamma y + \eta z - \beta_2 xy \\ \qquad\quad - (\alpha + \theta_1 + \theta_2 + \beta_1 + \mu)\, x, \\ \dfrac{dy}{dt} = \delta_2 + \beta_2 xy + (\theta_1 + \theta_2)\, x \\ \qquad\quad - (\gamma + \alpha + \beta_1 + \varepsilon + \mu)\, y, \\ \dfrac{dz}{dt} = \delta_3 + \alpha y + \alpha x - (\eta + \beta_1 + \mu)\, z, \\ \dfrac{dm}{dt} = \delta_4 + \beta_1 x + (\beta_1 + \varepsilon)\, y + \beta_1 z - \mu m, \end{cases} \tag{1}$$

with initial condition $(x(0), y(0), z(0), m(0)) \in R_+^4$.

4. Model analysis

In the previous section, we established a virus propagation model oriented towards user awareness and device security levels. In this section, we now discuss its global dynamical behavior, i.e., the model's equilibrium and stability.

4.1. Basic definitions

To understand the analysis of the virus propagation model presented below, we first provide some basic definitions.

Dynamical system: This term is used to describe the dynamic process of the evolution of a system through time [50]. In this paper, the model defined in Eq. (1) corresponds to a differential dynamical system that can capture the dynamics of computer-virus propagation in the complex SIoT environment at any instance in time. Dynamical systems can be used to continuously capture and quantitatively analyze the time-varying behavior of virus propagation, and therefore serve as the (theoretical) basis for modeling the propagation mechanism of malicious software in the SIoT environment. Dynamical system are also useful for evaluating security strategies, and for implementing dynamic prevention and control.

Equilibrium: The equilibrium is critical to analyze the local and global behavior of dynamical systems [50]. In this study, we are interested in the final state of the computer viruses affected by SEs and other transmission mechanisms in the SIoT with respect to user behavior and device interaction. By systematically analyzing the stability of the equilibrium state of the model ((1)), we can determine both the final distribution of the viruses as well as asses the continuous transmission mechanisms of the virus in the SIoT environment. Thus, the analysis of the equilibrium of the proposed model provides a theoretical basis for understanding the infection dynamics under complex social-driven conditions.

Viral equilibrium: In general, a dynamical system may become stable over time, but the final number of certain (undesired) states is not necessarily zero [50]. Specifically, in the SIoT environment, when the propagation model defined in Eq. (1) reaches stability, the number of infected devices usually remains non-zero. This indicates that even when the system is in a stable state, computer viruses will still exist/persist and continue to spread in the SIoT environment. This aspect can be analyzed through the viral equilibrium.

System stability: This term describes the long-term behavior of the equilibrium of a dynamical system [50]. Therefore, conducting a stability analysis of the equilibrium state described by the model in Eq. (1) not only enables us to reveal the long-term behavioral of computer virus propagation in the Social Internet of Things (SIoT), but also allows for the quantitative prediction of the steady-state distribution scale and continuous propagation potential of the virus within the system. This analysis provides a crucial theoretical basis for assessing virus propagation risks, formulating dynamic isolation strategies, and optimizing the trust management mechanism in the network.

4.2. System simplification

Given the high dimensionality and complexity of the system in (1), it is essential to simplify it to facilitate the analysis. Noting that $N = x + y + z + m$, the system from Eq. (1) can be transformed into the following simplified form:

$$\begin{cases} \dfrac{dN}{dt} = \delta - \mu N, \\ \dfrac{dy}{dt} = \delta_2 + (\beta_2 y + \theta_1 + \theta_2)(N - y - z - m) \\ \qquad - (\gamma + \alpha + \beta_1 + \varepsilon + \mu) y, \\ \dfrac{dz}{dt} = \delta_3 + \alpha y + \alpha (N - y - z - m) \\ \qquad - (\eta + \beta_1 + \mu) z, \\ \dfrac{dm}{dt} = \delta_4 + \beta_1 (N - y - z - m) + (\beta_1 + \varepsilon) y \\ \qquad + \beta_1 z - \mu m, \end{cases} \tag{2}$$

where $\delta = \delta_1 + \delta_2 + \delta_3 + \delta_4$ and the initial conditions are $(N(0), y(0), z(0), m(0)) \in R_+^4$.

Given the first equation of the simplified system in (2), it is straightforward to see that $\lim_{t\to\infty} N = \delta/\mu$. According to [58], it is possible to define a limit system that is consistent with the dynamic characteristics of the system in (2), i.e.:

$$\begin{cases} \dfrac{dy}{dt} = \quad \delta_2 + (\beta_2 y + \theta_1 + \theta_2)(N^* - y - z - m) \\ \qquad\qquad -(\gamma + \alpha + \beta_1 + \varepsilon + \mu) y, \\ \dfrac{dz}{dt} = \quad \delta_3 + \alpha (N^* - z - m) - (\eta + \beta_1 + \mu) z, \\ \dfrac{dm}{dt} = \quad \delta_4 + \beta_1 N^* + \varepsilon y - (\beta_1 + \mu) m. \end{cases} \tag{3}$$

where $N^* = \delta/\mu$ and the initial condition are defined as $(y(0), z(0), m(0)) \in R_+^3$. According to the work [50],

the positively invariant region of the above system is

$$\begin{aligned}\Omega = \big\{ (y,z,m) \,|y \geq 0, z \geq 0, m \geq 0,\\ 0 \leq y+m+z \leq N^* \big\}.\end{aligned} \tag{4}$$

Based on the presented discussion, it is easy to see that the system from Eq. (3) is equivalent to our initial model from Eq. (1) in terms of dynamical behavior, allowing us to focus our following analyses on the more convenient system in (3).

4.3. Equilibrium

In this section, we discuss the existence and uniqueness of the equilibrium for the derived system from Eq. (3).

Theorem 1. *The unique (viral) equilibrium $E^* = (y^*, z^*, m^*)$ of system (3) is locally asymptotically stable, where*

$$\begin{aligned} y^* = \frac{l_2 + \sqrt{l_2^2 - 4l_1 l_3}}{-2l_1}, z^* = \frac{\delta_3 + \alpha\left(N^* - m^*\right)}{\alpha + \eta + \beta_1 + \mu}, m^* = \frac{\delta_4 + \beta_1 N^* + \varepsilon y^*}{\beta_1 + \mu},\\ l_1 = -\beta_2\left[\left(\beta_1 + \mu\right)\left(\alpha + \eta + \beta_1 + \mu + \varepsilon\right) + \varepsilon\eta\right] < 0,\\ l_2 = \beta_2\left[\left(\delta_1 + \delta_2\right)\left(\eta + \beta_1 + \mu\right) + \delta_3\eta\right] - \varepsilon\left(\theta_1 + \theta_2\right)\left(\eta + \beta_1 + \mu\right)\\ - \left(\beta_1 + \mu\right)\left(\alpha + \eta + \beta_1 + \mu + \varepsilon\right)\left(\theta_1 + \theta_2 + \gamma + \alpha + \beta_1 + \varepsilon + \mu\right),\\ l_3 = \delta_2\left(\beta_1 + \mu\right)\left(\alpha + \eta + \beta_1 + \mu\right) + \left(\theta_1 + \theta_2\right)\left[\left(\delta_1 + \delta_2\right)\left(\eta + \beta_1 + \mu\right) + \delta_3\eta\right] > 0. \end{aligned} \tag{5}$$

Proof : Assume $(\tilde{y}, \tilde{z}, \tilde{m})$ is an equilibrium of the system in (3). According to the definition of the equilibrium, substitute $(\tilde{y}, \tilde{z}, \tilde{m})$ into the system (3) we get

$$\begin{cases} \delta_2 + \left(\beta_2\tilde{y} + \theta_1 + \theta_2\right)\left(N^* - \tilde{y} - \tilde{z} - \tilde{m}\right)\\ \qquad - \left(\gamma + \alpha + \beta_1 + \varepsilon + \mu\right)\tilde{y} = 0,\\ \delta_3 + \alpha\left(N^* - \tilde{z} - \tilde{m}\right) - \left(\eta + \beta_1 + \mu\right)\tilde{z} = 0,\\ \delta_4 + \beta_1 N^* + \varepsilon\tilde{y} - \left(\beta_1 + \mu\right)\tilde{m} = 0. \end{cases} \tag{6}$$

By solving the second and third equations of the system (6), one can obtain $\tilde{z} = \dfrac{\delta_3 + \alpha\left(N^* - \tilde{m}\right)}{\alpha + \eta + \beta_1 + \mu}, \tilde{m} = \dfrac{\delta_4 + \beta_1 N^* + \varepsilon\tilde{y}}{\beta_1 + \mu}$. Then, substitute it into the first equation of the system (6) to get

$$-l_1\tilde{y}^2 - l_2\tilde{y} - l_3 = 0. \tag{7}$$

Since $\tilde{y}, \tilde{z}, \tilde{m} \geq 0$, Eq. (7) has a unique root $\tilde{y} = \dfrac{l_2 + \sqrt{l_2^2 - 4l_1 l_3}}{-2l_1}$. Therefore, $\tilde{y} = y^*, \tilde{z} = z^*, \tilde{m} = m^*$ and $E^* = (y^*, z^*, m^*)$ exist and are unique.

Remark 1. *This theorem indicates that in the SIoT environment, the virus propagation system has a unique virus equilibrium, meaning that the virus will not completely disappear but will persist in the network. It reveals that in SIoT, due to the heterogeneity of devices, the diversity of user behaviors, and the various transmission channels, such as search engines, the virus can persist. The virus cannot be completely eradicated. Therefore,*

the prevention and control strategies should focus on controlling the virus transmission at an acceptable low level rather than striving for complete elimination.

4.4. Equilibrium stability analysis

Theorem 1 suggests that the system in (3) has a unique (viral) equilibrium. This section now discusses the local and global stability of the equilibrium.

Lemma 1. *The value*

$$\begin{aligned} p_0 = \quad & -\beta_2 \left(N^* - 2y^* - z^* - m^*\right) \\ & + \left(\theta_1 + \theta_2 + \gamma + \alpha + \beta_1 + \varepsilon + \mu\right) \end{aligned}$$

is a positive number.

Proof : According to Theorem 1 and the first equation of the system in (6), $N^* - 2y^* - z^* - m^* = \dfrac{\left(\gamma + \alpha + \beta_1 + \varepsilon + \mu\right) y^* - \delta_2}{\beta_2 y^* + \theta_1 + \theta_2} - y^*$ *is obtained, so there is*

$$\begin{aligned} -p_0 &= \beta_2 \left[\frac{\left(\gamma + \alpha + \beta_1 + \varepsilon + \mu\right) y^* - \delta_2}{\beta_2 y^* + \theta_1 + \theta_2} - y^*\right] \\ &\quad -\left(\theta_1 + \theta_2 + \gamma + \alpha + \beta_1 + \varepsilon + \mu\right) \\ &= \frac{-\beta_2 \delta_2 - \left(\theta_1 + \theta_2\right)\left(\beta_2 y^* + \theta_1 + \theta_2 + \gamma + \alpha + \beta_1 + \varepsilon + \mu\right)}{\beta_2 y^* + \theta_1 + \theta_2} \\ &\quad -\beta_2 y^* < 0. \end{aligned}$$

That is, $p_0 > 0$.

Remark 2. *This theorem indicates that the system is locally stable near the equilibrium, meaning that minor disturbances will not cause drastic changes in the virus transmission behavior. This implies that local safety measures can effectively curb the spread of the virus, but global strategies are still necessary to address the risk of large-scale transmission.*

Theorem 2. *The unique (viral) equilibrium* E^* *of the system (3) is locally asymptotically stable.*

Proof : The Jacobian matrix of system (3) at E^* *is:*

$$J_{E^*} = \begin{pmatrix} -p_0 & -\left(\beta_2 y^* + \theta_1 + \theta_2\right) & -\left(\beta_2 y^* + \theta_1 + \theta_2\right) \\ 0 & -p_1 & -\alpha \\ \varepsilon & 0 & -p_2 \end{pmatrix}, \tag{8}$$

where

$$\begin{aligned} p_0 &= -\beta_2 \left(N^* - 2y^* - z^* - m^*\right) \\ &\quad + \left(\theta_1 + \theta_2 + \gamma + \alpha + \beta_1 + \varepsilon + \mu\right) > 0, \\ p_1 &= \alpha + \eta + \beta_1 + \mu > 0, \\ p_2 &= \beta_1 + \mu > 0. \end{aligned} \tag{9}$$

From Eq. (8), the corresponding characteristic equation is obtained as follows:

$$\begin{aligned}&\lambda^3+(p_0+p_1+p_2)\,\lambda^2\\&+[p_1p_2+p_0p_1+p_0p_2+\varepsilon\,(\beta_2y^*+\theta_1+\theta_2)]\,\lambda\\&+p_0p_1p_2+\varepsilon\,(\beta_2y^*+\theta_1+\theta_2)\,(p_1-\alpha)=0,\end{aligned}\tag{10}$$

then,

$$\begin{aligned}\Delta_1&=p_0+p_1+p_2>0,\\\Delta_2&=(p_0+p_1+p_2)\left[p_1p_2+p_0p_1+p_0p_2+\varepsilon\,(\beta_2y^*+\theta_1\right.\\&\quad\left.+\,\theta_2)\right]-p_0p_1p_2-\varepsilon\,(\beta_2y^*+\theta_1+\theta_2)\,(p_1-\alpha)\\&=(p_0+p_2)\left[p_1\,(p_0+p_1+p_2)+p_0p_2\right]\\&+\varepsilon\,(\beta_2y^*+\theta_1+\theta_2)\,(p_0+p_2+\alpha)>0.\end{aligned}$$

Similarly, one can get

$$\Delta_3=\left[p_0p_1p_2+\varepsilon\,(\beta_2y^*+\theta_1+\theta_2)\,(p_1-\alpha)\right]\Delta_2>0.$$

According to the Hurwitz criterion, all roots of the characteristic equation (10) have negative real parts. Hence, the equilibrium is locally asymptotically stable [50].

Next, a geometric method is used to analyze the global stability of the (viral) equilibrium E^* [53]. First, consider the differential equation

$$\dot{a}=f\,(a)\,,a\in\psi.\tag{11}$$

Let $a\,(t,a_0)$ be the solution of Eq. (11), whose initial value is $a\,(0,a_0)=a_0$. Additionally, consider the following two assumptions:

1) There is a compact absorbing set $\xi\subset\psi$;

2) a^* is the unique equilibrium of equation (11) in ψ.

Let $a\to\mathbf{Q}(a)$ be a $\begin{pmatrix}n\\2\end{pmatrix}\times\begin{pmatrix}n\\2\end{pmatrix}$ matrix function, when $a^*\in\psi$, $\mathbf{Q}\,(a)\in C^1$. Suppose $\mathbf{Q}^{-1}\,(a)$ exists and is continuous when $a\in\xi$, and ξ is a compact absorbing set in ψ. Let us define

$$q=\lim_{t\to\infty}\sup\sup_{a\in H}\frac{1}{t}\int_0^t\mu\,(\mathbf{B}\,(a\,(t,a_0)))dt,$$

where

$$\mathrm{B}=\mathbf{Q}_f\mathbf{Q}^{-1}+\mathbf{Q}\mathbf{J}^{[2]}\mathbf{Q}^{-1},$$

and $\mathbf{Q}_f$ is the directional derivative of $\mathbf{Q}(a)$ in its f direction, $\mu(\mathbf{B})$ is the Lozinskii measure of the matrix, $J=\dfrac{\partial f}{\partial a}$ is the Jacobian matrix, and $\mathbf{J}^{[2]}$ is the second compound matrix of $J=(J_{ij})$. In particular, when $n=3$,

there is

$$\mathbf{J}^{[2]} = \begin{pmatrix} J_{11}+J_{22} & J_{23} & -J_{13} \\ J_{32} & J_{11}+J_{33} & J_{12} \\ -J_{31} & J_{21} & J_{22}+J_{33} \end{pmatrix}.$$

Lemma 2. *If ψ is a simply connected region and assumptions 1) and 2) hold, then when $q<0$, the unique equilibrium a^* of Eq. (11) in ψ is globally asymptotically stable [53].*

Theorem 3. *The (viral) equilibrium E^* of the system in (3) is globally asymptotically stable.*

Proof : It is easy to see through Theorem 1 and Theorem 2 that assumptions 1) and 2) are valid, so only $q<0$ needs to be proven. Assume

$$\mathbf{Q}(y,z,m) = diag\left(\frac{y}{z}, 1, \frac{y}{z}\right),$$

and use $\mathbf{Q}_f$ to express the differential form of $\mathbf{Q}$ to (y,z,m), then there is

$$\mathbf{Q}_f\mathbf{Q}^{-1} = diag\left(\frac{\dot{y}}{y}-\frac{\dot{z}}{z}, 0, \frac{\dot{y}}{y}-\frac{\dot{z}}{z}\right).$$

Let $A(t) = (y(t), z(t), m(t))$ be the general solution of the system in (3), and the Jacobian matrix of system (2) at $A(t)$ is as follows:

$$\mathbf{J} = \begin{pmatrix} W_1-W_2 & W_3 & W_4 \\ 0 & -p_1 & -\alpha \\ \varepsilon & 0 & -p_2 \end{pmatrix}, \tag{12}$$

where $W_1 = \beta_2(N^*-2y-z-m)$, $W_2 = (\theta_1+\theta_2+\gamma+\alpha+\beta_1+\varepsilon+\mu)$, $W_3 = -(\beta_2 y+\theta_1+\theta_2)$, and $W_4 = -(\beta_2 y+\theta_1+\theta_2)$.

The second compound matrix of $\mathbf{J}$ is

$$\mathbf{J}^{[2]} = \begin{pmatrix} \mathbf{J}_{11}^{[2]} & -\alpha & \beta_2 y+\theta_1+\theta_2 \\ 0 & \mathbf{J}_{22}^{[2]} & -(\beta_2 y+\theta_1+\theta_2) \\ -\varepsilon & 0 & \mathbf{J}_{33}^{[2]} \end{pmatrix},$$

where

$$\begin{aligned} \mathbf{J}_{11}^{[2]} &= -(\theta_1+\theta_2+\gamma+2\alpha+2\beta_1+\varepsilon+2\mu+\eta) \\ &\quad +\beta_2(N^*-2y-z-m), \\ \mathbf{J}_{22}^{[2]} &= -(\theta_1+\theta_2+\gamma+\alpha+2\beta_1+\varepsilon+2\mu) \\ &\quad +\beta_2(N^*-2y-z-m), \\ \mathbf{J}_{33}^{[2]} &= -(\alpha+\eta+2\beta_1+2\mu). \end{aligned}$$

Furthermore, let $\mathbf{B}$ *be* $\mathbf{B}=\mathbf{Q}_f\mathbf{Q}^{-1}+\mathbf{Q}\mathbf{J}^{[2]}\mathbf{Q}^{-1}$*, then*

$$\mathbf{B}=\begin{pmatrix} \dfrac{\dot{y}}{y}-\dfrac{\dot{z}}{z}+\mathbf{J}_{11}^{[2]} & -\dfrac{y}{z}\alpha & \beta_2 y+\theta_1+\theta_2 \\ 0 & \mathbf{J}_{22}^{[2]} & -\dfrac{z}{y}\left(\beta_2 y+\theta_1+\theta_2\right) \\ -\varepsilon & 0 & \dfrac{\dot{y}}{y}-\dfrac{\dot{z}}{z}+\mathbf{J}_{33}^{[2]} \end{pmatrix}.$$

The Lozinskii measure for calculating matrix $\mathbf{B}$ *is*

$$\mu\left(\mathbf{B}\right)=\inf\left\{\begin{array}{l} c: D_+\left\|\mathbf{k}\right\|\leq c\left\|\mathbf{k}\right\| \\ \quad \text{is true for every solution of } \dot{\mathbf{k}}=\mathbf{B}\mathbf{k} \end{array}\right\},$$

where D_+ *represents the number of right floors. Here, the norm of* $\mathbf{k}=(k_1,k_2,k_3)\in\mathbb{R}^3$ *is defined as follows:*

$$\left\|\mathbf{k}\right\|=\sup\left\{\left\|k_1\right\|+\left\|k_3\right\|,\left\|k_2\right\|\right\}.$$

Next, estimate $D_+\left\|\mathbf{k}\right\|$ *in two cases.*

Case 1: *when* $\left\|k_2\right\|\geq\left\|k_1\right\|+\left\|k_3\right\|$*, there is* $\left\|\mathbf{k}\right\|=\left\|k_2\right\|$*, then*

$$\begin{aligned} &D_+\left\|k\right\|=\dot{k}_2 \\ &=\Big[\beta_2\left(N^*-2y-z-m\right)-\big(\theta_1+\theta_2+\gamma+\alpha \\ &+2\beta_1+\varepsilon+2\mu\big)\Big]\left\|k_2\right\|-\frac{z}{y}\left(\beta_2 y+\theta_1+\theta_2\right)\left\|k_3\right\| \\ &\leq\Big[\beta_2\left(N^*-y-z-m\right)-\big(\theta_1+\theta_2+\gamma+\alpha \\ &\quad+\beta_1+\varepsilon+2\mu\big)-\frac{z}{y}\left(\theta_1+\theta_2\right)\Big]\left\|k_2\right\|, \end{aligned}$$

From the first equation of system (3), one can get

$$\begin{aligned} D_+\left\|\mathbf{k}\right\|\leq\Big[&\frac{\dot{y}}{y}-\frac{\delta_2+\left(\theta_1+\theta_2\right)\left(N^*-m\right)}{y} \\ &-\mu\Big]\left\|\mathbf{k}\right\|\leq\left(\frac{\dot{y}}{y}-\mu\right)\left\|\mathbf{k}\right\|. \end{aligned}$$

Case 2: *when* $\|k_2\| < \|k_1\| + \|k_3\|$, *there is* $\|\mathbf{k}\| = \|k_1\| + \|k_3\|$, *then*

$$\begin{aligned}
&D_+ \|\mathbf{k}\| = \dot{k}_1 + \dot{k}_3 \\
&= \left[\frac{\dot{y}}{y} - \frac{\dot{z}}{z} + \beta_2 (N^* - 2y - z - m) - (\theta_1 + \theta_2\right. \\
&\left.+\gamma + 2\alpha + 2\beta_1 + \varepsilon + 2\mu + \eta) - \varepsilon\right] \|k_1\| \\
&-\frac{y}{z}\alpha \|k_2\| + \left[\frac{\dot{y}}{y} - \frac{\dot{z}}{z} - (\alpha + \eta + 2\beta_1 + 2\mu) + \beta_2 y\right. \\
&\left.+\theta_1 + \theta_2\right] \|k_3\| \\
&\leq \left[\frac{2\dot{y}}{y} - \left(\frac{\dot{z}}{z} + \alpha + \eta + \beta_1 + 2\mu\right)\right] (\|k_1\| + \|k_3\|) \\
&\leq \left[\frac{2\dot{y}}{y} - \frac{\delta_3 + \alpha (N^* - m)}{z} - \mu\right] \|\mathbf{k}\| \\
&\leq \left(\frac{2\dot{y}}{y} - \mu\right) \|\mathbf{k}\| .
\end{aligned}$$

Combining the above two cases,

$$D_+ \|\mathbf{k}\| \leq \left(\frac{2\dot{y}}{y} - \mu\right) \|\mathbf{k}\|$$

can be obtained, so

$$\mu (\mathbf{B}) \leq \frac{2\dot{y}}{y} - \mu.$$

For the solution $A(t) = (y(t), z(t), m(t))$ *of the system in (3) satisfying* $(y(0), z(0), m(0)) \in \xi$ *(*ξ *is the compact absorbing set in* Ω*), there must be*

$$\frac{1}{t}\int_0^t \mu (B) dt \leq \frac{1}{t}\int_0^t \left(\frac{2\dot{y}}{y} - \mu\right) dt = \frac{1}{t} \ln \frac{y(t)}{y(0)} - \mu,$$

thereby

$$q \leq -\mu < -\frac{\mu}{2} < 0.$$

Therefore, the unique equilibrium E^* *of the system (3) is globally asymptotically stable.*

Remark 3. *Global stability indicates that, regardless of the initial state of the system, the virus transmission process will eventually converge to a unique equilibrium. In the long term, the scale of virus spread is mainly determined by system parameters such as user awareness level and device security performance, and is independent of the initial infection size. Therefore, enhancing users' educational level, promoting high-security devices, and restricting malicious links in search engines can effectively control the final spread range of viruses.*

5. Simulations

In this section, we empirically evaluate the proposed virus propagation model. First, we examine numerical simulation based on differential equations. Next, we conduct a real network simulation using a virus propagation

Table 3: Summary of the main characteristics of the selected datasets.

Dataset	Number of nodes	Number of edges
Facebook dataset	4039	88234
Peer-to-Peer (P2P) dataset	62586	147892

algorithm in SIoT (see Algorithm 1) on both the Facebook and P2P datasets. Finally, we provide detailed information on settings, datasets, stability verification experiments, and parameter analysis.

5.1. Settings and datasets

All simulations in this paper are conducted using PyCharm (Python 3.8.0). The datasets, the virus propagation algorithm, and simulation methods are described below.

Datasets. We use the Facebook dataset and P2P dataset to simulate real networks for the evaluation of the proposed model. The two datasets are sourced from the Stanford University Network Analysis Platform (SNAP) [59], and are summarized in Table 3. The Facebook dataset[1] serves as a prominent example of social networks, frequently utilized for examining the transmission of information and interactions among users within social networks, aligning well with the SIoT environment. As for the Peer-to-Peer (P2P) dataset[2], it represents a distributed network that operates on shared interconnections. The nodes in the network are symmetrical, and each node can provide access to resources and data.

Since the number of nodes and connecting edges in the dataset is pre-determined, we set the parameters defining the probability of nodes entering and disconnecting from SIoT in our model (i.e., δ and μ) to 0 to eliminate simulation error as much as possible. It should be noted that when there are too many nodes in the dataset, computer viruses will spread very fast in the SIoT. Thus, to make the initial evolution more apparent, the relevant parameters will be set to smaller values in the following scenarios.

Virus propagation algorithm. Since there is no evolutionary state of nodes in the network constructed from real network datasets, it is crucial to design corresponding state evolution rules for all nodes to ensure the parameters in the real network are consistent with those of the model's dynamical system. Hence, to enable the proposed model to accurately simulate the propagation process of computer viruses on the dataset, we design an evolutionary algorithm for virus propagation in SIoT (shown in Algorithm 1) to guide the evolution of the dataset. The source code of the model experiment will be made public on GitHub after review[3]. The core idea of the algorithm is as follows: first, nodes in the dataset are randomly assigned different states. Next, each element in each state node array is accessed, and so is the corresponding edge, where nodes represent users, and the connecting edges represent the relationships between two users. Based on this algorithm, the Facebook dataset and P2P dataset can build real networks, which are consistent with the state evolution and system parameters of the proposed virus propagation model. The constructed network is an undirected graph with no connection

[1] http://snap.stanford.edu/data/egonets-Facebook.html

[2] http://snap.stanford.edu/data/p2p-Gnutella31.html

[3] https://github.com/siyu-625/Analyzing-the-Influence-of-Users-Devices-and-Search-Engines-on-Viral-Spread-in-SIoT.git

Algorithm 1: The virus propagation algorithm in SIoT

Input: Initialize the network $G = (v, e)$ with the given dataset.

Output: The number of nodes in each state.

Randomly allocate the initial number of nodes in different states.
Set the number of iterations to t.
for $t = 1$ *to* j *with the step of 1* **do**
  if *the node* i *is susceptible (such as* WS_L *in system (1)) at time* t *and does not leave the network at time* $t + 1$, **then**
    traverses its neighbor nodes, under the influence of the infected nodes, SEs, or external storage media, the node i becomes WI_L with probability β_2, θ_1 or θ_2
    else i becomes WR_H (or PR_H) with probability α (or β_1) or its state does not unchanged
  if *the node* i *is infected (such as* WI_L *in system (1)) at time* t *and does not leave the network at time* $t + 1$, **then**
    i becomes WS_L, WR_H or PR_H with probability γ, α or $\beta_1 + \varepsilon$
    else its state does not unchanged
  if *the node* i *is* WR_H *at time* t *and does not leave the network at time* $t + 1$, **then**
    i becomes WS_L or PR_H with probability η or β_1
    else its state does not unchanged
  if *the node* i *is* PR_H *at time* t *and does not leave the network at time* $t + 1$, **then**
    the state of i does not unchanged
  end
end
Count the number of nodes in each state and return the result.

Table 4: System parameters in Scenario 1.

Parameter	β_1	β_2	θ_1	θ_2	γ	ε	α	η
Value	0.012	0.0001	0.08	0.01	0.08	0.01	0.1	0.25

weights on the edges. Assuming that the network constructed has b nodes and d connecting edges, the edges in the algorithm will be traversed twice, a total of $2d$ times, and the total number of traversals is $b + 2d$ times. Therefore, the time complexity of the algorithm is $O(b + 2d)$.

Simulation methods. Two different simulation methods are used to evaluate the model, i.e.:

($O1$) Numerical simulation: In this setting, we employ the differential equations of the model with the corresponding initial conditions and system parameters, and directly conduct numerical evolutions. This method only simulates the ideal situation of the evolution process of the dynamical model.

($O2$) Real network simulation: In this setting, the real-world dataset defines the network structure according to Algorithm 1 that conforms to the network evolution rules. Simulations with the differential equations on the constructed real-world network are then utilized to investigate the evolution of the dynamic model. This method relies on real-world datasets, which makes the conclusions drawn from these simulations stronger.

To better distinguish the results of the two simulation methods, let $WS_L(t), WI_L(t), WR_H(t)$, and $PR_H(t)$ represent the simulation curves obtained through method ($O1$). Let $WS_{Le}(t), WI_{Le}(t), WR_{He}(t)$, and $PR_{He}(t)$

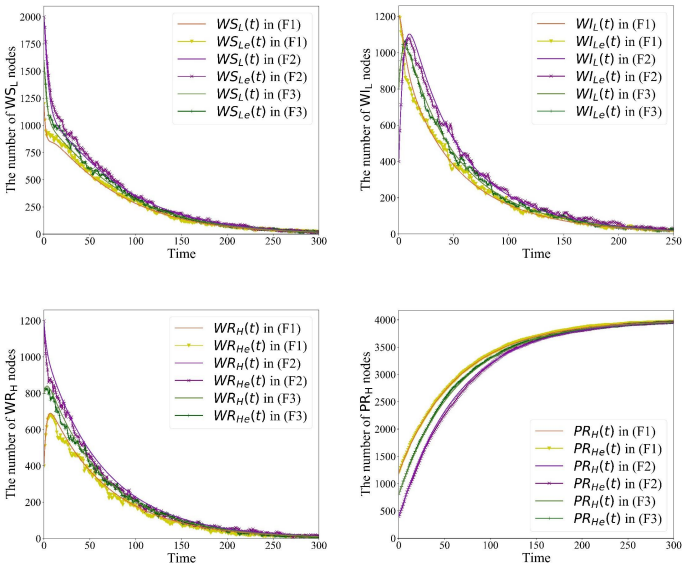

Figure 3: The evolution of the system (1) under Scenario 1 conditions.

denote the simulation curves obtained through method ($O2$). For different examples, the specific system parameters of the model are given in the following scenarios, but it is important to note that certain parameter values have been hypothetically selected because real-world data is unavailable.

5.2. Stability verification

Stability analyses are essential for predicting the scale of computer virus propagation in SIoT. Considering the system in (1) and Theorem 3, it is straightforward to see that the stability of the proposed model may depend on both the initial conditions and the system parameters. Consequently, we verify the model's stability through two approaches: (i) using the same system parameters for simulations with different initial conditions (see Scenarios 1 and 2), and (ii) using the same initial condition for simulations with different system parameters (see Scenarios 3 and 4).

Scenario 1. *When analyzing the Facebook dataset, the system in (1) with the parameters listed in Table 4 is taken into consideration, with the three groups of initial conditions provided below.*

$$(F1)\ \ (WS_L(0), WI_L(0), WR_H(0), PR_H(0)) = (1198, 1198, 401, 1198).$$

$$(F2)\ \ (WS_L(0), WI_L(0), WR_H(0), PR_H(0)) = (1997, 400, 1198, 400).$$

$$(F3)\ \ (WS_L(0), WI_L(0), WR_H(0), PR_H(0)) = (1598, 799, 799, 799).$$

Scenario 2. *When analyzing the P2P dataset, system (1) is considered with the parameters provided in Table 5, while the initial conditions are varied.*

$$(U1)\ \ (WS_L(0), WI_L(0), WR_H(0), PR_H(0)) = (18775, 18775, 6261, 18775).$$

$$(U2)\ \ (WS_L(0), WI_L(0), WR_H(0), PR_H(0)) = (31293, 6258, 18775, 6258).$$

$$(U3)\ \ (WS_L(0), WI_L(0), WR_H(0), PR_H(0)) = (25035, 12517, 12517, 12517).$$

Table 5: System parameters in Scenario 2.

Parameter	β_1	β_2	θ_1	θ_2	γ	ε	α	η
Value	0.8×10^{-4}	0.5×10^{-5}	0.06	0.042	0.15	0.1	0.14	0.28

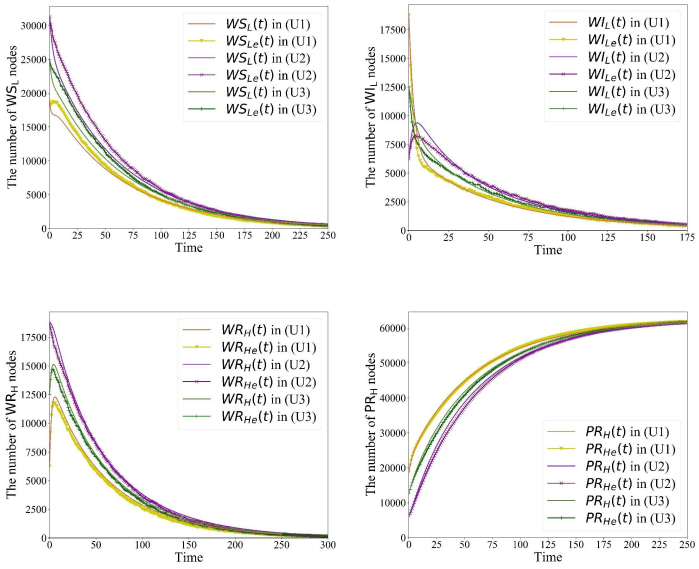

Figure 4: The evolution of the system (1) under Scenario 2 conditions.

In Scenarios 1 and 2, we use fixed system parameters and change the initial conditions. Specifically, we assume various numbers of nodes in different states and observe the viral spread as predicted by our model. The evolution of the system in (1) under the conditions outlined in Scenarios 1 and 2 is illustrated in Figs. 3 and 4 respectively. (i) These two figures show that, irrespective of the initial conditions, the model's equilibrium remains consistent, indicating the independence of computer virus propagation in SIoT from initial conditions. Controlling virus spread through these initial conditions is not feasible. (ii) It is notable that the curves in the real network depict oscillatory behavior, closely aligning with the trend of the numerical simulation curves, suggesting the applicability of the proposed model to real networks. (iii) Upon reaching a stable state, it is evident that the number of WI_L nodes is non-zero, signifying the persistent existence of computer viruses, in line with Theorem 3.

Scenario 3. *For the Facebook dataset, the system from (1) is examined with the parameters presented in Table 6. The specific initial condition considered equals* $(WS_L(0), WI_L(0), WR_H(0), PR_H(0)) = (1598, 799, 799, 799)$.

Scenario 4. *For the P2P dataset, the system in (1) is considered with the parameters in Table 7. The initial condition for the analysis is set to* $(WS_L(0), WI_L(0), WR_H(0), PR_H(0)) = (25035, 12517, 12517, 12517)$.

In Scenarios 3 and 4, we maintain fixed initial conditions and vary the system parameters. Specifically, we consider diverse parameter values to observe the spread of the virus as predicted by our model. The evolution of the system (1) under the conditions outlined in Scenarios 3 and 4 is shown in Figs. 5 and 6, respectively. (i) The

Table 6: System parameters in Scenario 3.

Parameter	β_1	β_2	θ_1	θ_2	γ	ε	α	η
Value1 (V1)	0.001	0.7×10^{-4}	0.02	0.01	0.01	0.015	0.12	0.33
Value2 (V2)	0.002	0.8×10^{-4}	0.02	0.015	0.015	0.03	0.1	0.32
Value3 (V3)	0.002	0.8×10^{-4}	0.025	0.01	0.01	0.02	0.1	0.3

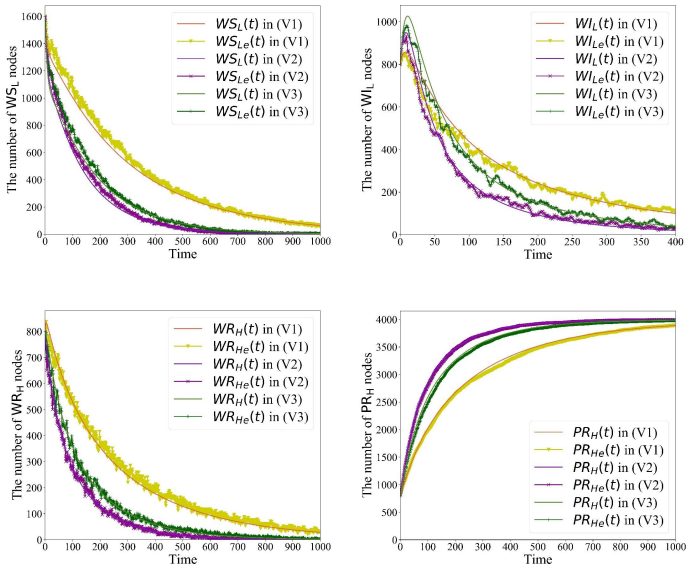

Figure 5: The evolution of the system (1) under Scenario 3 conditions.

figures illustrate that when the number of nodes in the initial state remains constant while the system parameters differ, distinct evolution trends are observed in the number of nodes within each state. This observation underlines the significant impact of system parameters on computer virus spread, suggesting that controlling virus spread can be achieved by adjusting these parameters. (ii) Although the system parameters differ, the numerical simulation and network simulation curves exhibit similar trends and eventually stabilize, thereby corroborating the conclusion of Theorem 3. (iii) An examination of the number of PR_H nodes under (V2) and (V3) reveals that, despite their marginal final-number variation, the recovery speed under (V2) is faster for the same initial number. Similarly, comparing the number of PR_H nodes under (V1) and (V2) or (V1) and (V3) shows that, with an identical number of nodes, the recovery speed under (V1) is the slowest, resulting in fewer final nodes in comparison to (V2) or (V3). This demonstrates that system parameters directly influence the speed and extent of infection.

5.3. Parameter analysis

Due to the obsrvation that system parameters have an impact on the spread of computer viruses, here we specifically discuss the main parameters, such as user awareness (see Scenario 5), device security level (see Scenario 6), and the transmission ways of SEs and external storage media (see Scenario 7).

Table 7: System parameters in Scenario 4.

Parameter	β_1	β_2	θ_1	θ_2	γ	ε	α	η
Value1 (V1)	0.6×10^{-4}	0.2×10^{-5}	0.06	0.042	0.05	0.006	0.14	0.08
Value2 (V2)	0.6×10^{-4}	0.2×10^{-5}	0.068	0.038	0.04	0.007	0.12	0.08
Value3 (V3)	0.8×10^{-4}	0.1×10^{-5}	0.06	0.052	0.042	0.007	0.1	0.1

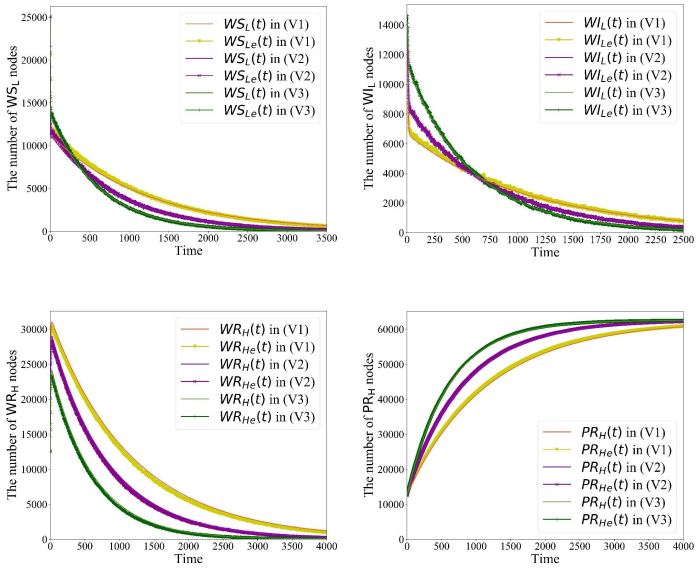

Figure 6: The evolution of the system (1) under Scenario 4 conditions.

Table 8: System parameters on the Facebook dataset in Scenario 5.

Parameter	β_2	θ_1	θ_2	γ	α	η
Value	0.1×10^{-4}	0.003	0.002	0.001	0.008	0.001

Table 9: System parameters on the P2P dataset in Scenario 5.

Parameter	β_2	θ_1	θ_2	γ	α	η
Value	0.1×10^{-6}	0.005	0.004	0.001	0.01	0.001

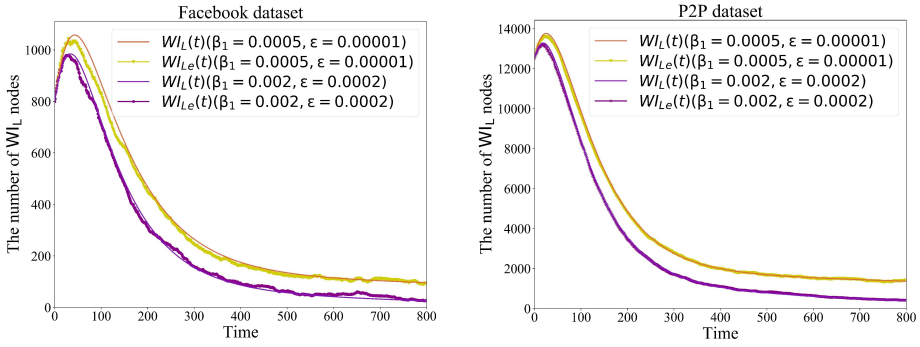

Figure 7: The impact of user awareness on virus propagation in Scenario 5.

Scenario 5. *When analyzing the model on the Facebook dataset, the system in (1) is considered with the param-*

Table 10: System parameters on the Facebook dataset in Scenario 6.

Parameter	β_1	β_2	θ_1	θ_2	γ	ε	η
Value	0.0003	0.0001	0.005	0.004	0.001	0.0001	0.001

Table 11: System parameters on the P2P dataset in Scenario 6.

Parameter	β_1	β_2	θ_1	θ_2	γ	ε	η
Value	0.0005	0.1×10^{-6}	0.005	0.004	0.001	0.0001	0.001

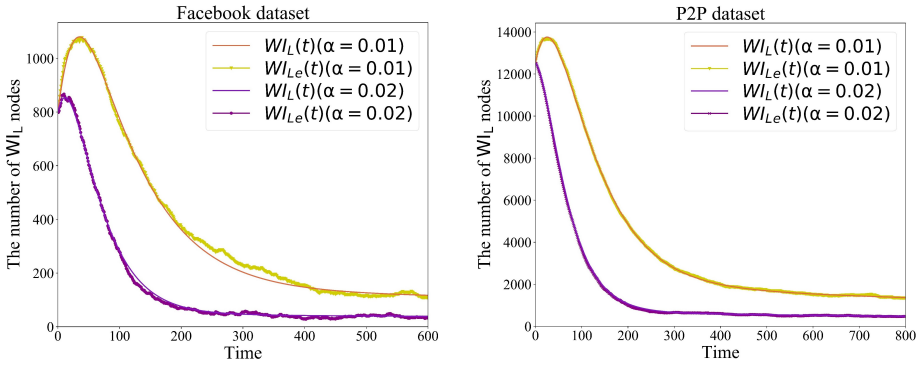

Figure 8: Impact of device security level on virus propagation in Scenario 6.

eters in Table 8, and the initial condition $(WS_L(0), WI_L(0), WR_H(0), PR_H(0)) = (1598, 799, 799, 799)$. *Similarly, on the P2P dataset, the system from (1) is examined with the parameters given in Table 9, and the initial condition* $(WS_L(0), WI_L(0), WR_H(0), PR_H(0)) = (25035, 12517, 12517, 12517)$.

In Scenario 5, we use fixed initial conditions and system parameters except for β_1 and ε. Specifically, we consider diverse β_1 and ε values to observe the spread of the virus as predicted by our model. Fig. 7 portrays the evolution of WI_L nodes affected by user awareness on the Facebook dataset and P2P dataset. It can be seen from Fig. 2 and Table 2 that β_1 and ε represent the probability of users changing from low-security awareness to high-security awareness. The numerical changes of these two parameters provide a way to analyze the propagation effect only from the user's perspective. β_1 and ε the larger, the smaller the number of WI_L nodes. This illustrates that user awareness does play a role in the process of virus transmission between nodes. Infected nodes with low-security awareness can hardly infect nodes with high-security awareness. On the contrary, nodes with high-security awareness will also affect nodes with low-security awareness. Accordingly, by informing users of the harm of computer viruses, the number of users with high-security awareness will be increased, thereby affecting the low-security awareness users with whom they contact, and improving the security awareness of the entire user layer. If more users are sensitive to computer viruses in the network (i.e., users with high-security awareness), the possibility of the device being attacked by viruses will also be reduced.

Scenario 6. *When analyzing the Facebook dataset, the system from (1) is considered with the parameters given in Table 10. The initial condition for the dataset is set to* $(WS_L(0), WI_L(0), WR_H(0), PR_H(0)) = (1598, 799, 799, 799)$. *Similarly, for the P2P dataset, the system from (1) is considered with the parameters from Table 11 and the following initial condition* $(WS_L(0), WI_L(0), WR_H(0), PR_H(0)) = (25035, 12517, 12517, 12517)$.

Table 12: System parameters on the Facebook dataset in Scenario 7.

Parameter	β_1	β_2	γ	ε	α	η
Value	0.0003	0.0001	0.16	0.0003	0.018	0.022

Table 13: System parameters on the P2P dataset in Scenario 7.

Parameter	β_1	β_2	γ	ε	α	η
Value	0.2×10^{-4}	0.1×10^{-5}	0.05	0.0002	0.012	0.02

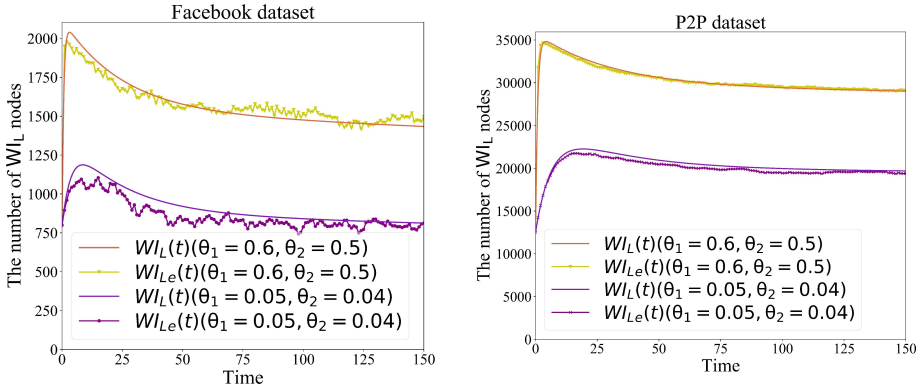

Figure 9: The impact of SEs and external storage media in Scenario 7.

In Scenario 6, we use fixed initial conditions and system parameters except for α. Specifically, we consider diverse α values to observe the spread of the virus as predicted by our model. Fig. 8 depicts the evolution of WI_L nodes affected by device security level on the Facebook dataset and P2P dataset, respectively. It can be seen from Fig. 2 and Table 2 that α only means that the user's security awareness has not changed, but the probability of choosing to try the paid anti-virus software. Parameter α can indicate that the propagation effect is only observed from the perspective of the device when the user perspective is the same. The simulation found that the value of α, the greater, the faster the number of infected nodes decreases and the smaller the final infection range after stabilization. Obviously, from the perspective of the device, improving the security level of the device can hinder the virus to a certain extent. Consequently, selecting devices with high-security performance or installing paid anti-virus software can effectively control the possibility of SIoT devices being infected.

Scenario 7. *For the analysis on the Facebook dataset, the system in (1) is considered with the parameters in Table 12. The specific initial condition is set to* $(WS_L(0), WI_L(0), WR_H(0), PR_H(0)) = (1598, 799, 799, 799)$. *For the P2P data, the parameters in Table 13 and the following initial condition* $(WS_L(0), WI_L(0), WR_H(0), PR_H(0)) = (25035, 12517, 12517, 12517)$ *are used.*

In Scenario 7, we use fixed initial conditions and system parameters except for θ_1 and θ_2. Specifically, we consider diverse θ_1 and θ_2 values to observe the spread of the virus as predicted by our model. Fig. 9 represents the evolution process of WI_L nodes affected by SEs and external storage media propagation in Scenario 7 on the Facebook dataset and P2P dataset, respectively. In SIoT, compared with external storage media, SEs will have faster propagation speed and a wider range. Accordingly, on behalf of SEs and external storage media θ_1

and θ_2 parameters, set to $\theta_1 > \theta_2$. With the growth of θ_1 and θ_2, the number of WI_L nodes also boosts, that is, the range of propagation radiation is wider. It can be seen that in reality, the transmission modes through SEs and external storage media greatly increase the probability of computer virus transmission and reduce network security. Through this scenario, it can also be found that the strategy of controlling the mode of transmission can effectively and significantly curb the virus. Inspired by this, the micro researchers of computer virus propagation can also quickly spread the updated security patch to the device side in this way after developing the patch of the new virus, so as to intervene at the beginning of the computer virus outbreak, control the source to control the propagation scale and reduce the harm.

5.4. Model comparison

To further verify the effectiveness of the proposed model, we chose a traditional model [49] and the latest model [22] for comparison and analyze the model's behavior from three aspects: (*i*) the ability of the model to describe and control the spread range of the virus, (*ii*) the number of infected nodes after the model reached a stable level after evolution, and (*iii*) the prediction of computer virus spread in real networks.

According to the model definition and description in the comparison model, we know that there are four states of nodes in the latest model: the S_H state with high user security awareness and no virus infection on the device; the S_L state with low user security awareness and no virus infection on the device; the I_1 state with virus infection on the device; and the R_1 state with virus recovery and immunity on the device. In the traditional model, there are three states of nodes: the device is not infected with the virus state S, the device is infected with the virus state I_2, and the device is recovered and immune to the virus state R_2. To compare the fairness of the experiment, we must ensure that the comparison Angle is the same, so we need to construct the correlation between the three models.

Referring to the dynamic model in Section 3 and the above node description, we find certain rules in defining node states. It can be considered that the node states of the three models infected with computer viruses are the same state, and the node states of the three models immune to computer viruses are the same state. The node states of the proposed model and the latest model are divided into low-security awareness node states and high-security awareness node states according to user security awareness, which can be considered the same state as the corresponding node states. The traditional model does not discuss user security awareness, so it is considered that the non-infected state is the accumulation of the two states in the proposed model. Through the above analysis, the node relationships of the three models can be summarized as follows:

$$\begin{cases} S_L = WS_L, \\ S_H = WR_H, \\ S = WS_L + WR_H, \\ I_1 = I_2 = WI_L, \\ R_1 = R_2 = PR_H. \end{cases} \tag{13}$$

Scenario 8. *We refer to table 4 system parameters and initial condition F_2 experiments in Scenario 1, according to equation 13, the initial condition $(S(0), I_2(0), R_2(0)) = (2395, 400, 400)$ of the traditional model and the initial condition $(S_L(0), S_H(0), I_1(0), R_1(0)) = (1997, 400, 1998, 400)$ of the latest model are obtained. We take β_2 (0.01, 0.001, 0.0001) successively in table 4, from Fig. 2 and Table 4, we know that the probability of an uninfected node becoming an infected node is the rate of infection; The remaining system parameters of the two comparison models are set according to equation 13, and the system parameter values of the corresponding node state transformation mode of the proposed model are the same.*

In Scenario 8, experiments were conducted according to the above conditions, and the experimental results were obtained as shown in Fig. 10. Under different infection rates, we found that the number of infected nodes in the traditional model and the latest model was greater than that in the proposed model most of the time, which indicates that the proposed model has better control over the spread of the computer virus and can reduce the spread of the computer virus according to the model method. In addition, after the proposed model reaches stability, the number of infected nodes is less. This is because the high-security awareness of users and the high-security level of devices proposed by the proposed model can eventually reduce the spread of computer viruses, and only a small part of computer viruses can continue to spread in the network.

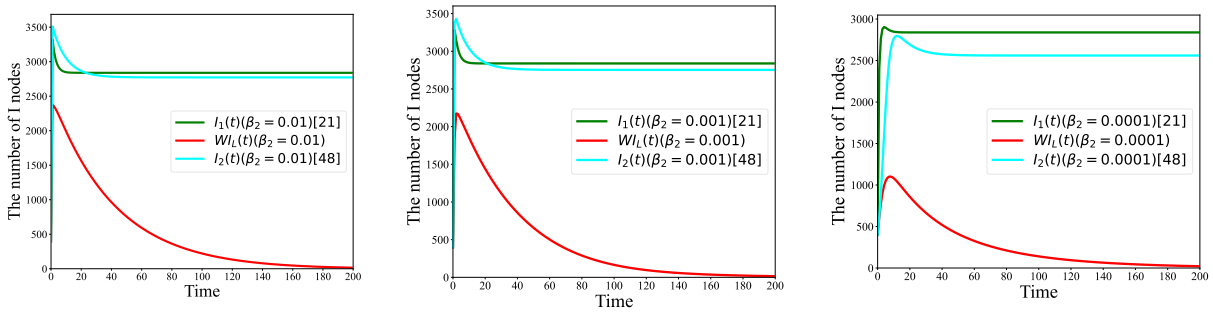

Figure 10: Visual comparisons of original models.

According to the algorithm 1 designed by us, the parameters and initial conditions of the above experimental system are the same, and the real network simulation and differential equation numerical simulation of the three models are respectively established in the Facebook real network dataset. The experimental results are shown in Fig. 11, which reflects the evolution process of the number of infected nodes. We found that the evolution trend of infected nodes in the real network simulation of the three models was consistent with that of the differential numerical simulation. However, careful comparison showed that the proposed model was more accurate in predicting the evolution process of infection in the real network, and the computer propagation and the evolution of infected nodes in the real network could be inferred through the numerical simulation. In other words, we can effectively control computer viruses according to their evolution trend through numerical simulation to avoid the large-scale spread of computer viruses and cause losses. The above experiments show that compared with the comparison model, the proposed model is more effective and reliable, more accurate in predicting the spread of

computer viruses in real networks, and provides a new method to contain computer viruses.

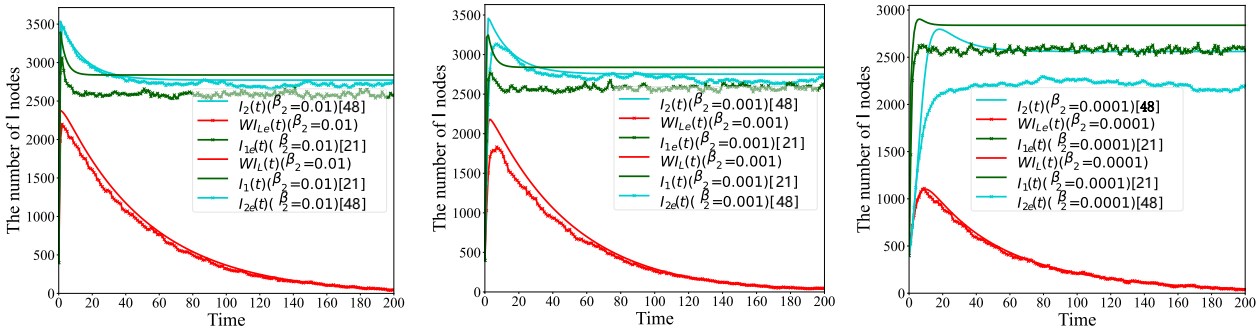

Figure 11: Evolution prediction of the number of infected nodes in Facebook network under different infection rates.

Scenario 9. *We refer to table 5 system parameters and initial condition U_2 experiments in Scenario 2, according to equation 13, the initial condition $(S(0), I_2(0), R_2(0)) = (50068, 6258, 6258)$ of the traditional model and the initial condition $(S_L(0), S_H(0), I_1(0), R_1(0)) = (31293, 6258, 18775, 6258)$ of the latest model are obtained. We take β_2 (0.0005, 0.00005, 0.000005) successively in table 4, other Settings are basically the same as in Scenario 8.*

In Scenario 9, the experimental results obtained through the experiment are shown in Fig. 12, similar to scenario 7, the same conclusion can be reached, the proposed model control propagation range is smaller; After the proposed model reaches stability, the number of infected nodes is less. Different system parameters and initial conditions have little influence on the effectiveness of the model, which is superior to the comparison model. According to the designed algorithm 1 and the same system parameters and initial conditions as the

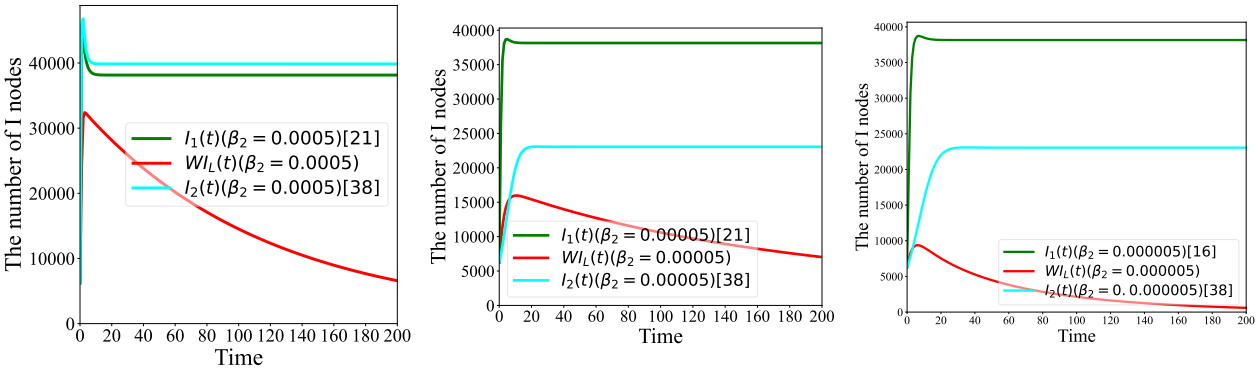

Figure 12: Evolution of the number of infected nodes under different infection rates.

previous experiments, the real network simulation and differential equation numerical simulation of the three models are respectively established in the P2P real network data set, and the experimental results are shown in Fig. 13. It can be found that the trend of corresponding curves on P2P data sets is also very similar, which fully confirms the applicability of the proposed model in real networks.

Simulation summary. The simulation/validation results presented above suggest that the proposed virus transmission model has excellent applicability - both in theory and in empirical research. The model incorporates multi-dimensional states of user security awareness and device security levels, which more accurately reflect

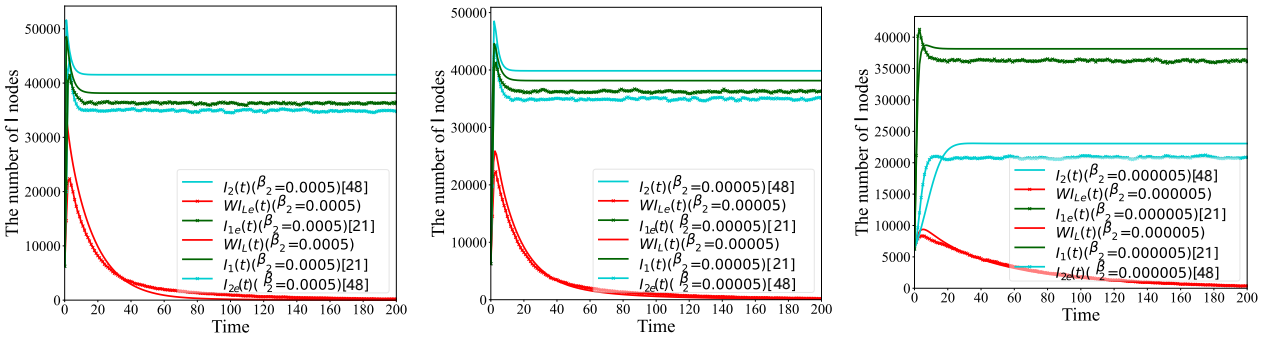

Figure 13: Evolution prediction of the number of infected nodes in P2P networks under different infection rates.

the complex mechanisms of virus transmission in the SIoT environment compared to competing studies. The stability analysis experiments show that the system has a unique global asymptotically stable equilibrium, which is consistent with the actual network simulation results, indicating that the model has good predictive capabilities. The parameter analysis experiments further reveal that the improvement of user security awareness, the enhancement of device security levels, and the control of transmission routes (such as search engines) are effective strategies to curb virus transmission. In the comparative analysis experiments, the traditional model, due to not considering these factors, has overly optimistic prediction results, while the proposed model significantly improves the accuracy of depicting real transmission behaviors by refining the states and parameter settings. Moreover, the designed virus transmission algorithm successfully combines the dynamical system model with the actual network structure, providing a reference for the study of virus transmission in the SIoT environment.

6. Discussion

Based on the simulation experiments in the previous section and the theoretical analysis in the earlier part of this paper, this section now elaborates on the three core research questions raised in the introduction: how user (security awareness), device (security level), and search engine (information dissemination medium) jointly affect the long-term virus transmission behavior in the SIoT; which of these factors is the most critical; and how to effectively control the virus transmission by regulating these factors. The simulation results show that these three types of factors are coupled with each other and jointly determine the dynamic process and final scale of virus transmission. The improvement of user security awareness (parameters β_1, ϵ) can significantly reduce the number of infected nodes; the increase of device security level (parameter α) can accelerate the disappearance of infection and narrow the transmission range; while the search engine (parameter θ_1) has been confirmed to be the key channel with the fastest transmission speed and the widest influence range. The theoretical analysis further indicates that the system will converge to a unique virus equilibrium point under any initial state, confirming the inevitability of the virus's persistent existence in the SIoT, and also suggesting that long-term prevention and control should focus on the continuous adjustment of the above parameters rather than relying on changes in the initial state.

This study reveals the dynamic coupling mechanism of various factors through multi-scenario simulations: Search engines, due to their extensive connectivity and efficient information distribution capabilities, become the

primary driving force for virus propagation, with their influence far exceeding that of traditional device-to-device communication or external storage media (θ_2). Notably, search engines not only accelerate the initial spread of viruses but also significantly expand the scope of propagation by altering the network topology. Although the improvement of user security awareness and device security levels cannot completely eliminate viruses, they can effectively reduce the scale and speed of propagation, serving as the foundation for long-term prevention and control. Particularly, the parameter sensitivity analysis indicates that when user security awareness (β_1) and device security levels (ϵ) are enhanced in tandem, the system converges to the equilibrium point at a significantly faster rate, and the final infection scale can be significantly reduced. The proposed virus propagation model demonstrates good predictive consistency and stability on both Facebook and P2P real network datasets, verifying its applicability in actual SIoT environments. Compared with existing models, this model more accurately characterizes the macroscopic dynamics of virus propagation by introducing a ternary coupling mechanism of users, devices, and search engines. Model comparison experiments show that this model reduces the prediction error of infection peaks compared to traditional models and effectively improves the fitting degree of propagation trends. These findings provide a theoretical basis for formulating targeted prevention and control strategies, suggesting the establishment of a search engine security certification mechanism, promoting the popularization of high-security-level devices, and conducting user cybersecurity education, among other multi-dimensional measures, to build a hierarchical defense system.

7. Conclusion

This study proposed a dynamic model for virus propagation in the SIoT environment. Through theoretical analysis and experimental verification, the model demonstrated excellent performance in revealing the propagation mechanism, predicting long-term trends, and evaluating the effectiveness of prevention and control strategies. Compared to previous studies, the model introduced three key dimensions: user awareness, device security level, and search engines, which better aligns with the characteristics of SIoT. We showed that the proposed model can capture more complex propagation dynamics and explain phenomena that single-factor models cannot. Through rigorous mathematical derivations, the existence, uniqueness, and global asymptotic stability of the virus equilibrium were proven, providing a theoretical basis for predicting the final scale of virus propagation and formulating long-term control strategies. Search engines were explicitly modeled as key communication channels in the proposed model. Both theory and experiments show that, compared to traditional pathways such as device-to-device communication or external storage media, search engines have faster transmission speed and a wider influence range. This discovery provides important insights for SIoT security practices and points to a new direction that requires enhanced monitoring and defense.

Although the model has several advantages, it also has certain limitations. The model was verified on two real network datasets, Facebook and P2P, which are representative of real-world networks, but validation on further SIoT network structures is required to further validate the model's generalization capabilities. Additionally, the modeling of search engines and external storage media is still relatively macroscopic and does not consider micro mechanisms such as ranking algorithms and user click behaviors. These factors may affect the actual transmission

efficiency of the virus. Moreover, artificial intelligence methods can be introduced to achieve real-time perception and adaptive adjustment of the propagation situation, thereby further improving the model's prediction accuracy and practical protection value. Further exploration of integrating game theory frameworks could be conducted to analyze the strategic interaction behavior of attackers and defenders in the virus propagation process and establish a dynamic strategy optimization model based on payoff matrices and evolutionary games. This approach provides a more confrontational and adaptive theoretical basis and solution for SIoT security protection. Through these cross-method and multidisciplinary explorations, the prediction accuracy, decision intelligence, and practical protection value of the model in complex environments could be further improved in future research.

Acknowledgements

The authors are grateful to the anonymous reviewers and the editor for their valuable comments and suggestions. This work was supported by the Guangxi Key Research and Development Program (No. AB24010317) and the Slovenian ARRS research program P2-0250.

References

[1] D. Camacho, Ángel Panizo-LLedot, G. Bello-Orgaz, A. Gonzalez-Pardo, E. Cambria, The four dimensions of social network analysis: An overview of research methods, applications, and software tools, Information Fusion 63 (2020) 88–120.

[2] C. Wilson, A. Sala, K. P. Puttaswamy, B. Y. Zhao, Beyond social graphs: User interactions in online social networks and their implications, ACM Transactions on the Web (TWEB) 6 (2012) 1–31.

[3] X. Hu, X. Xiong, Y. Wu, M. Shi, P. Wei, C. Ma, A hybrid clustered sfla-pso algorithm for optimizing the timely and real-time rumor refutations in online social networks, Expert Systems with Applications 212 (2023) 118638.

[4] C. Gan, W. Yang, Q. Zhu, M. Li, D. K. Jain, V. Štruc, D.-W. Huang, Hybrid rumor debunking in online social networks: A differential game approach, IEEE Transactions on Systems, Man, and Cybernetics: Systems (2025).

[5] K. A. Frank, R. Xu, Causal Inference for Social Network Analysis, in: The Oxford Handbook of Social Networks, Oxford Univ. Press, 2021.

[6] S. Peng, G. Wang, D. Xie, Social influence analysis in social networking big data: Opportunities and challenges, IEEE Network 31 (2017) 11–17.

[7] L. Atzori, A. Iera, G. Morabito, M. Nitti, The social internet of things (siot)-when social networks meet the internet of things: Concept, architecture and network characterization, Computer Networks (2012).

[8] C. Boudagdigue, A. Benslimane, A. Kobbane, J. Liu, Trust management in industrial internet of things, IEEE Transactions on Information Forensics and Security 15 (2020) 3667–3682.

[9] P. Dong, J. Ge, X. Wang, S. Guo, Collaborative edge computing for social internet of things: Applications, solutions, and challenges, IEEE Transactions on Computational Social Systems 9 (2021).

[10] H. Bangui, B. Buhnova, D. Kusnirakova, D. Halasz, Trust management in social internet of things across domains, Internet of Things 23 (2023) 100833.

[11] K. C. Chung, P. J. B. Tan, Understanding the dynamics of social interaction in siot: Human-machine engagement, Internet of Things 28 (2024) 101337.

[12] D. Guinard, V. Trifa, Towards the Web of Things: Web Mashups for Embedded Devices, Integration The Vlsi Journal, 2009.

[13] S. Rajendran, R. Jebakumar, Object recommendation based friendship selection (orfs) for navigating smarter social objects in siot, Microprocessors and Microsystems 80 (2021) 103358.

[14] R. M.S., S. Pattar, R. Buyya, V. K.R., S. Iyengar, L. Patnaik, Social internet of things (siot): Foundations, thrust areas, systematic review and future directions, Computer Communications (2019) 32–57.

[15] B. Hammi, S. Zeadally, R. Khatoun, J. Nebhen, Survey on smart homes: Vulnerabilities, risks, and countermeasures, Computers & Security 117 (2022) 102677.

[16] J. H. Han, J. Y. Lee, Digital healthcare industry and technology trends, in: 2021 IEEE International Conference on Big Data and Smart Computing (BigComp), 2021, pp. 375–377.

[17] H. Taslimasa, S. Dadkhah, E. C. P. Neto, P. Xiong, S. Ray, A. A. Ghorbani, Security issues in internet of vehicles (iov): A comprehensive survey, Internet of Things 22 (2023) 100809.

[18] S. Pourmohseni, M. Ashtiani, A. A. Azirani, A computational trust model for social iot based on interval neutrosophic numbers, Information Sciences 607 (2022) 758–782.

[19] N. Jiang, J. Chen, R.-G. Zhou, C. Wu, H. Chen, J. Zheng, T. Wan, Pan: Pipeline assisted neural networks model for data-to-text generation in social internet of things, Information Sciences (2020) 167–179.

[20] M. E. J. Newman, M. Girvan, Finding and evaluating community structure in networks, Physical Review E 69 (2004) 026113.

[21] D. Ferraris, C. Fernandez-Gago, Y. Assouyat, H. Labiod, W. Haiguang, J. Lopez, Trust dynamicity for iot: How do i trust your social iot cluster?, Internet of Things (2025) 101529.

[22] C. Gan, Y. Qian, A. Liu, Q. Zhu, Search-driven virus spreading on social internet of things: A dynamical perspective, Communications in Nonlinear Science and Numerical Simulation (2022) 106624.

[23] C. Marche, M. Nitti, Trust-related attacks and their detection: A trust management model for the social iot, IEEE Transactions on Network and Service Management 18 (2021) 3297–3308.

[24] J. H. Smith, N. D. Bastian, A ranked solution for social media fact checking using epidemic spread modeling, Information Sciences (2022).

[25] Y. Wu, H. Huang, N. Wu, Y. Wang, M. Z. A. Bhuiyan, T. Wang, An incentive-based protection and recovery strategy for secure big data in social networks, Information Sciences 508 (2020) 79–91.

[26] M. López, A. Peinado, A. Ortiz, An extensive validation of a sir epidemic model to study the propagation of jamming attacks against iot wireless networks, Computer Networks 165 (2019) 106945.

[27] A. Al Kindi, D. Al Abri, A. Al Maashri, F. Bait-Shiginah, Analysis of malware propagation behavior in social internet of things, International Journal of Communication Systems 32 (2019) e4102.

[28] Q. Zhu, G. Zhang, X. Luo, C. Gan, An industrial virus propagation model based on scada system, Information Sciences (2023) 546–566.

[29] D. Zhao, L. Wang, Z. Wang, G. Xiao, Virus propagation and patch distribution in multiplex networks: Modeling, analysis, and optimal allocation, IEEE Transactions on Information Forensics and Security 14 (2019) 1755–1767.

[30] Y. Chen, Y. Mao, L. Cui, S. Leng, Y. Wei, X. Chen, A two layer model of malware propagation in a search engine context, in: IEEE InfoCom Workshops, 2018, pp. 21–26.

[31] C. Fu, X.-Y. Liu, J. Yang, L. T. Yang, S. Yu, T. Zhu, Wormhole: The hidden virus propagation power of the search engine in social networks, IEEE Transactions on Dependable and Secure Computing 16 (2019).

[32] B. Ostermaier, K. Römer, F. Mattern, M. Fahrmair, W. Kellerer, A real-time search engine for the web of things, in: 2010 Internet of Things (IOT), 2010, pp. 1–8.

[33] M. Nitti, V. Pilloni, D. D. Giusto, Searching the social internet of things by exploiting object similarity, in: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 2016, pp. 371–376.

[34] G. Wu, L. Xie, H. Zhang, J. Wang, S. Shen, S. Yu, Stsir: An individual-group game-based model for disclosing virus spread in social internet of things, Journal of Network and Computer Applications 214 (2023) 103608.

[35] H. Zhang, X. Hu, Y. Shen, H. Xu, S. Shen, R. Li, Mitigating malware propagation in social internet of things using an exact markov-chain-based epidemic method, IEEE Internet of Things Journal 12 (2025) 24104–24118. doi:10.1109/JIOT.2025.3554230.

[36] C. Gan, A. Liu, Q. Zhu, Y. Zhu, Y. Xiang, J. Liu, Social tie-driven coupling propagation of user awareness and information in device-to-device communications, Computer Networks 237 (2023) 110087.

[37] D. Nithya, V. Madhusudanan, B. Murthy, R. Geetha, N. X. Mung, N.-N. Dao, S. Cho, Delayed dynamics analysis of sei2rs malware propagation models in cyber–physical systems, Computer Networks 248 (2024) 110481.

[38] C. Fu, C. Peng, X.-Y. Liu, L. T. Yang, J. Yang, L. Han, Search engine: The social relationship driving power of internet of things, Future Generation Computer Systems 92 (2019) 972–986.

[39] A. A. Kindi, D. A. Abri, A. A. Maashri, F. Bait-Shiginah, Analysis of malware propagation behavior in social internet of things, International Journal of Communication Systems (2019) e4102.

[40] Y. Hayel, Q. Zhu, Epidemic protection over heterogeneous networks using evolutionary poisson games, IEEE Transactions on Information Forensics and Security 12 (2017) 1786–1800.

[41] M. Ahmad, S. Ali, J. Tariq, I. Khan, M. Shabbir, A. Zaman, Combinatorial trace method for network immunization, Information Sciences 519 (2020) 215–228.

[42] X. Han, Q. Tan, Dynamical behavior of computer virus on internet, Applied Mathematics & Computation 217 (2010) 2520–2526.

[43] A. Sobhani, A. Keshavarz-Haddad, A distributed patching scheme for controlling mobile malware infection, in: 2015 23rd Iranian Conference on Electrical Engineering, 2015, pp. 187–192.

[44] K. A. Kabir, K. Kuga, J. Tanimoto, Analysis of sir epidemic model with information spreading of awareness, Chaos, Solitons & Fractals 119 (2019) 118–125.

[45] J. Amador, J. R. Artalejo, Stochastic modeling of computer virus spreading with warning signals, Journal of the Franklin Institute (2013).

[46] C. Gan, X. Yang, Theoretical and experimental analysis of the impacts of removable storage media and antivirus software on viral spread, Communications in Nonlinear Science & Numerical Simulation 22 (2015) 167–174.

[47] L. Yang, X. Yang, Y. Wu, The impact of patch forwarding on the prevalence of computer virus: A theoretical assessment approach, Applied Mathematical Modelling 43 (2017) 110–125.

[48] L. Yang, M. Draief, X. Yang, Heterogeneous virus propagation in networks: a theoretical study: L.x. yang, m. draief and x. yang, Mathematical Methods in the Applied Sciences 40 (2016).

[49] L. Feng, L. Song, Q. Zhao, H. Wang, Modeling and stability analysis of worm propagation in wireless sensor network, Mathematical Problems in Engineering,2015,(2015-9-2) 2015 (2015) 1–8.

[50] R. C. Robinson, An Introduction to Dynamical Systems: Continuous and Discrete, American Mathematical Society, 2004.

[51] E. X. DeJesus, C. Kaufman, Routh-hurwitz criterion in the examination of eigenvalues of a system of nonlinear ordinary differential equations, Physical Review A 35 (1987) 5288.

[52] H. K. Khalil, Lyapunov stability, Control systems, robotics and automation 12 (2009) 115.

[53] M. Y. Li, J. S. Muldowney, A geometric approach to global-stability problems, SIAM Journal on Mathematical Analysis 27 (1996).

[54] M. Cai, W. Wang, Y. Cui, H. E. Stanley, Multiplex network analysis of employee performance and employee social relationships, Physica A: Statistical Mechanics and its Applications 490 (2018) 1–12.

[55] B. Nettasinghe, V. Krishnamurthy, K. Lerman, Diffusion in social networks: Effects of monophilic contagion, friendship paradox, and reactive networks, IEEE Transactions on Network Science and Engineering 7 (2020) 1121–1132.

[56] S. Memarian, B. Farahani, E. Nazemi, Social internet of things: Interoperability and autonomous computing challenges, in: International Conference on Omni-layer Intelligent Systems, 2020, pp. 1–7.

[57] S. Talbi, A. Bouabdallah, Interest-based trust management scheme for social internet of things, Journal of Ambient Intelligence and Humanized Computing 11 (2020) 1129–1140.

[58] H. R. Thieme, Asymptotically autonomous differential equations in the plane, The Rocky Mountain Journal of Mathematics 24 (1994).

[59] J. Leskovec, A. Krevl, SNAP Datasets: Stanford large network dataset collection, `http://snap.stanford.edu/data`, 2014.