

## RESEARCH ARTICLE

# A Mobility-Based Epidemic Model for IoT Malware Spread

BO-RUI CHEN<sup>1</sup>, SHIN-MING CHENG<sup>1,2</sup>, (Member, IEEE), AND  
MAINA BERNARD MWANGI<sup>1</sup>, (Graduate Student Member, IEEE)

<sup>1</sup>Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei 10607, Taiwan

<sup>2</sup>Research Center for Information Technology Innovation, Academia Sinica, Taipei 11529, Taiwan

Corresponding author: Maina Bernard Mwangi (d10915815@mail.ntust.edu.tw)

This work was supported in part by the National Science and Technology Council (NSTC), Taiwan, under Grant 111-2218-E-011-010-MBK.

**ABSTRACT** With the rapid advancement of technology, IoT has become inseparable from human lives. IoT is extensively used in transport, healthcare, and manufacturing, among other sectors. However, this technology lacks sufficient security defense capabilities, thus becoming a highway for malicious actors. IoT networks use infrastructure-based (INF) and device-to-device (D2D) communications to propagate data. The INF communication utilizes technologies such as WLAN, LTE, GPRS, and GSM to relay information from source to destination. The D2D paradigm, on the other hand, is a close-proximity communication in which sensors exchange data in a multi-hop manner. Since malware can utilize both D2D and INF links to spread out, IoT networks are exceptionally vulnerable to attacks. Therefore, we propose Susceptible-Exposed-Infected-Recovered-Dead (SEIRD) model to examine the dynamics of IoT malware spread via INF and D2D communications. We analyze the impacts of mobility on infection propagation and illustrate that our model adequately captures IoT malware spread behaviors through mathematical analysis and simulations. We also compute the malware transmission threshold, which can be used as a guideline to mitigate and suppress an attack.


**INDEX TERMS** Epidemic theory, Internet of Things, IoT malware, propagation modeling.

## I. INTRODUCTION

With sensing, communication, and computation capabilities, the Internet of Things (IoT) can enable various kinds of interactions between humans and machines and create new applications to fulfill human needs, thereby receiving significant attention in recent years. As shown in Fig. 1, the IoT typically consists of IoT application servers, infrastructure edge nodes for data relaying (known as intermediate nodes), and end-side sensors and actuators (known as IoT devices). However, acting as a cyber-physical system, the IoT has become a new target for adversaries since malicious behaviors in cyberspace might result in monetary gains or information leakage. In this case, the safety and privacy of users who enjoy the IoT applications might be significantly

affected, and the security issue in IoT has been an ever-growing concern [1].

Among the existing attacks on IoT, the most infamous one is a large-scale spread of malicious codes and malware, where IoT devices are infected, acted as bots, and made to perform stealthy actions, such as overloading a service or encrypting the whole system of a victim [2], [3]. The simple architecture of the IoT devices with constrained resources and without a user-friendly interface makes the propagation of the malware more and more severe [4]. The propagation of the IoT malware is done through infrastructure-based (denoted as INF) communication technologies like GSM/UMTS/LTE/GPRS and WLAN through intermediate nodes. Typically, it is achieved by performing address space scanning via Telnet or SSH protocols [5]. Recently, proximity-based wireless media (also known as device-to-device (D2D) communications) are exploited by malware to spread via Wi-Fi Direct, NFC, or BLE connections [6].

The associate editor coordinating the review of this manuscript and approving it for publication was Jose Saldana .

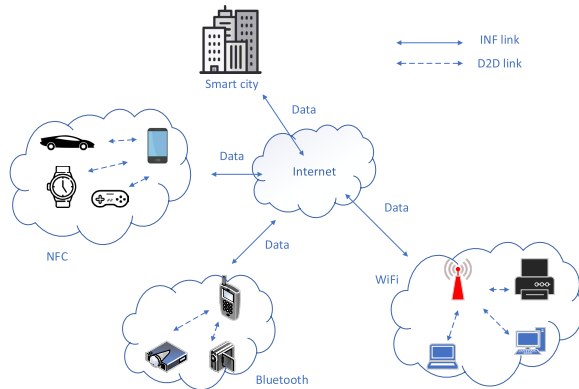


FIGURE 1. IoT network architecture with different transmission links.

To estimate the effects of propagation and the corresponding threat of the malware in IoT (e.g., outbreak), modeling of spreading behavior is necessary. Typically, we apply epidemic theory to model IoT malware diffusion in wired and wireless networks since malware propagation can be likened to the spread of pathogens in humans [7]. In particular, Susceptible-Infectious (SI) [8], [9], [10], Susceptible-Infectious-Susceptible (SIS) [11], [12], [13], [14], and Susceptible-Infectious-Recovered (SIR) [15], [16], [17] models are widely applied. Many variants such as Susceptible–Exposed–Infected–Recovered (SEIR) [18], [19], [20], Susceptible-Active-Dormant-Immune (SADI) [21], and Heterogeneous-Susceptible-Infected-Recovered-Dead (HSIRD) [22] are developed by introducing additional states and their corresponding parameters. By considering propagation via both INF and D2D transmission links [8], [13], [17], [21], the epidemic models become more complicated but better suited for modeling the spreading behavior of realistic IoT malware.

Node mobility aggravates the spread of malware by increasing the contact rate between the infected gadgets and the susceptible ones [10], [23]. In particular, mobility causes a node's neighbor to change constantly, thus increasing nodes' contact rate. The effects of mobility on malware spread have been studied in [17], [21], and [24]. Furthermore, in [17] and [21], authors model malware diffusion via both D2D and INF transmission links. However, unlike our proposed model, these studies assume that the infection spread only happens after a node has moved, thus failing to capture the spreading behavior during the movement.

This paper explores the implications of node mobility and dual communication schemes (INF and D2D) on IoT malware propagation through epidemic modeling. Specifically, our contributions are summarized below.

- We propose a mobility-based SEIRD model to study IoT malware spread. SEIRD model accurately captures the dynamics of mobile IoT malware propagation by covering the essential aspects of infection spread from inception to recovery and death of the IoT devices upon damage or power depletion. Unlike the traditional

SEIRD, our model considers the impacts of dual propagation schemes (INF and D2D) and node mobility on the spread of malware.

- We conduct mathematical analysis of the proposed model, including computing the malware transmission threshold, which can serve as a security guideline to mitigate an attack.
- Through rigorous experimental evaluations, we validate the effectiveness of the proposed model in capturing realistic dynamics of IoT malware. From the results in section V, it is evident that most propagation models such as [13] and [19] significantly underestimate the extent of malware diffusion by failing to consider key IoT aspects such as mobility and the use of INF and D2D communications.

The rest of the paper is arranged as follows: section II reviews the related work and the background information, while section III introduces the proposed model and the state transition diagram. Then, in section IV, we provide mathematical analysis, including the computation of malware transmission threshold. Next, section V presents the simulation setup, results, and comparative analysis. Finally, section VI states the conclusion of the study.

## II. RELATED WORK

### A. IoT MALWARE

The widespread adoption and development of IoT technology raise significant security and data privacy concerns. For instance, limited memory capacity, computational ability, and battery power make it challenging to implement intensive security defense mechanisms in IoT gadgets. As a result, IoT networks have become highly vulnerable to attacks. Additionally, IoT users lack the necessary knowledge regarding security measures that need to be undertaken to deter malicious actors. Therefore, there is a dire need to understand IoT malware attack behaviors and spread patterns in order to develop effective mitigation strategies to curb them. Different malware types have varying spreading and attacking techniques. For example, [25] studied android malware propagation behaviors and their attack methods. The authors classified android malware based on the installation mode, malicious behaviors, and activation method. Malware in android gadgets is mainly spread through SMS and WIFI. Initially, a malicious program is injected into popular applications, which are re-uploaded to the android app market for the users to download. After gaining access to a device, the malware obtains the remote control permissions and launches an attack. Once in the host device, android malware can spread through WIFI and SMS.

DDoS is the most common attack technique against IoT. Through this method, attackers gather an army of bots and block the target network's services [7]. Koliass et al. [5] investigated the formation and spread of botnets such as Mirai and Hajime. Botnets have three main parts: the command and control (C&C) server, bots, and botmaster. The botmaster can access the bots through SSH or Telnet [2]. Bots are

recruited into the botnet until the botmaster meets the desired target number. During the attack execution, the C&C server informs the bots about the target's IP address and the attack mode, such as traffic attacks on HTTP or TCP. DDoS attacks severely compromise service availability, data security, and privacy.

## B. EPIDEMIC MODELS

Epidemic models originated from the study of human viruses. This modeling technique continues to be widely used to examine the spread of pathogens [40] and is equally popular in studying malware propagation. Epidemic models are primarily derived from states such as susceptible (S), infected (I), exposed (E), vaccinated (V), quarantined (Q), recovered (R), and dead (D). The typical models are SIS [11], [12], [13], [14], SI [8], [9], [10], and SIR [15], [16], [17]. As discussed below, these traditional models, alongside other advanced ones with many states, have been extensively used to study the spread of malware.

Some propagation models primarily focus on the spread of malware over long distances, usually through INF links. For example, [9] and [26] proposed SI model for malware propagation in large-scale networks. In [9], propagation happens mainly within groups with different infection rates, but in [26], malware spreads across groups through the search engine. Although individual groups have different numbers and categories of devices, the authors in [26] assume that the infection rate is homogeneous. In [12] and [27], the authors propose SIS model for malware propagation. In [27], the authors calculate immunization and infection probability based on the Markov chain. Moreover, infection rates are heterogeneous due to different link weights. Authors in [12] suggest that there is a relationship between the sender and the receiver, and thus the links between the nodes are bidirectional and have the same infection rate. SIR propagation model is studied in [15] and [25]. Wei et al. [15] considered interest-based communities where nodes with similar interests connect. This form of connection forms multi-layered complex networks conducive to malware propagation. Olivier et al. [28] applied game theory to derive Susceptible-Infected-Resistant (SIR) model for botnet propagation. In addition to the classic S-I states, the authors added the "resistant" state (R) to refer to patched and password-protected gadgets. However, despite the gainful contribution in controlling and suppressing botnet spread, this paper fails to consider the impact of mobility and dual communication schemes (INF and D2D) on the infection spread.

Yi et al. [41] used epidemic theory to develop a novel Unacquired-Acquired-Hibernated (UAH) model for information dissemination in the industrial IoT. The authors categorized the IoT gadgets into three compartments where nodes are classified based on whether they have acquired/not acquired and disseminated information and whether they have hibernated or are active.

Le et al. [31] applied SEIQVS (Susceptible-Exposed-Quarantined-Vaccinated-Susceptible) model to study the

spread of malware in Wi-Fi routers. The authors conducted mathematical analysis and simulations to analyze and validate their model.

In a bid to more realistically capture the behaviors of malware propagation through INF links, more complicated epidemic models have emerged. For example, [29] proposed SISV model for malware spread in multiplex networks. This model combined the features of classic SIS and SIR models. In [19], authors suggested Susceptible-Delitescent (Exposed)-Infected-Recovered (SD(E)IR) model, where nodes in state E/D are not immediately infected after receiving malware; the infection occurs only when a user opens a malicious file. The two papers consider homogeneous infection probability, which does not reflect the effect of different transmission links. Guillen et al. [30] introduced SCIRAS (Susceptible-Carrier-Infectious-Recovered-Attacked-Susceptible) model for studying zero-day attacks in IoT. The various states of the model make it possible to analyze different stages of the malware propagation process, making the model more accurate and realistic. Using stochastic SIRS and SEIRS models, Arash et al. [7] analyzed IoT botnet propagation dynamics in complex networks. The authors compared the results from the two models and concluded that SEIRS was more suitable for modeling botnets as it reflects their long incubation periods. Arash et al. [34] used SIRS epidemiology model, comprising micro (initial infection) and macro (spread) sub-models, to study the propagation of cross-platform malware. The macro model was significantly influenced by the contact rate via a USB connection. The analysis of the macro model illustrated that the malware mutation ability remarkably impacts the infection spread as it decimates the immunity rate.

For D2D malware propagation, SIS model is proposed in [11] and [14]. In [11], the authors studied botnet formation in wireless IoT networks and discovered that node density profoundly affects malware spread dynamics. Shen et al. [14] used a discrete-time SIS model to study malware spread in heterogeneous WSNs. However, these studies consider the D2D link as the only channel through which malware propagates. Liu et al. [10] proposed a mobile SI model to study malware propagation in ad hoc wireless networks. The authors proposed two spread mechanisms, i.e., communication and diffusion modes. Zhou et al. [35] applied the attack-defense game model (SID) to study malware propagation in WSNs. Shen et al. [32] introduced SNIRD model for malware propagation in heterogeneous WSNs while [24] proposed (vulnerable-compromised-quarantined-patched-scrapped) VCQPS for malware propagation in mobile heterogeneous WSNs. In [24], a random walk model is used to depict the mobility of the sensors. A similar heterogeneous susceptible-infected-recovered-dead (HSIRD) model is proposed in [22] to examine malware diffusion where WSNs have different connectivity capabilities. Zhang et al. [33] used the SEIRD model to study malware diffusion in heterogeneous WSNs based on the cellular automaton concept.

**TABLE 1.** Epidemiology-based models for malware propagation.

Research work	Link type	Mobility	Malware type	Infection timing
SI [9], [26], SIS [12], [27], SIR [15], [25], [28], SISV [29], SDIR [19], SEIRS [7], [18], SCIRAS [30], SEIQVS [31]	INF	x	IoT malware	periodically
SI [10], VCQPS [24], HSIRD [22]	D2D	o	WSN malware	after each movement
SIS [11], [14], SNIRD [32], SEIRD [33], SIRS [34], SID [35], SEIRV [36], SIR [37], SEIRS [38]	D2D	x	WSN malware	periodically
SI [8], SIS [13], SLIQRE [39]	INF/D2D	x	malware	periodically
SIR [17], SADI [21],	INF/D2D	o	malware	after each movement
SIR [40]	INF/D2D	o	human virus	after each movement
SIR [16], UAH [41]	D2D	x	information	periodically
Proposed SEIRD	INF/D2D	o	IoT malware	during each movement

Achar et al. [36] used a fractional derivative-based SEIRV model to study the spread of worms in wireless sensor networks. The authors argued that the frail defense mechanisms of sensors make them attractive targets for attacks. Through mathematical analysis and simulations, the authors discovered that node density and the sensor's communication capabilities significantly contribute to the dissemination of worms in WSNs.

Jiang et al. [37] used the SIR model to study virus propagation control mechanisms WSNs. The authors found out that the average degree of nodes, the communication radius of devices, and the probability of virus infection significantly inhibited the control mechanism.

Yu et al., [38] proposed a  $SEI^2RS$  malware dissemination model for cyber-physical systems. The authors categorized the  $I$  state into infected nodes with low infection ability and the infection nodes with high infection ability. The authors argued that newly infected nodes propagate malware at a lower rate as compared to nodes infected earlier.

Some authors focus more on malware propagation through both INF and D2D communication links. For example, [8] proposed SI model to simulate malware spread in generalized social networks. In [39], the authors used six states, including susceptible (S), latent (L), infected (I), quarantined (Q), recovered (R), and dead (E), (SLIQRE), to analyze IoT malware dissemination. Acarali et al. [13] also considered INF and D2D transmission links and proposed SIS model to investigate malware spread dynamics in IoT-based WSNs. In addition to multiple transmission links, [17], [21] incorporated node mobility to study malware propagation in social IoT networks. However, contrary to our proposed model, [17], [21] assume that the infection only happens after the node movement, thus ignoring the infection during the movement. Wang et al. [21] proposed SADI (Susceptible-Active-Dormant-Infected) to model the propagation of worms in hierarchical social networks. In [17], the authors argue that IoT users might have multiple devices and, thus, malware propagation happens not only through INF and D2D but also via self-infection by IoT users possessing more than one gadget.

As depicted in the discussion above, only a handful of studies in the existing literature consider mobility, INF transmission, and D2D links in modeling IoT malware spread. Furthermore, the only two papers [21] and [17] that have employed the three aspects (mobility, INF, and D2D) have not adequately captured the effect of mobility on the spread of malware. Therefore, we aim to fill this gap in our proposed mobility-based SEIRD model by incorporating D2D and INF transmission links and correctly modeling node mobility to reflect malware spread effects during and after node movement.

### III. SYSTEM MODEL

As stated previously, the main aim of this paper is to explore the dynamics of IoT malware propagation where mobility and the use of dual communication schemes (INF and D2D) are involved. IoT gadgets have a simple architecture with constrained resources, resulting in weak defense capabilities. Additionally, the lack of security awareness by the users exposes IoT infrastructure to malware attacks. As highlighted in [2], most IoT gadget users continue using the default passwords, while others use simple and predictable passwords that attackers can easily bypass. Due to these reasons, brute-force and DoS attacks have become rampant as IoT technology advances. Therefore, in this paper, we assume that IoT devices have security vulnerabilities due to their weak defense capabilities and the use of weak or default passwords, which give room for brute-force and DoS attacks. Before presenting the proposed model in subsection III-B, we first introduce the Gauss-Markov model, which has been used to generate node mobility in this paper. Later, in subsections III-C and III-D we briefly discuss D2D and INF communication schemes, respectively.

#### A. GAUSS-MARKOV MOBILITY MODEL

The proposed SEIRD model utilizes the Gauss-Markov model (GMM) as the basis of its mobility. Usually, researchers use GMM to simulate non-stationary machine-to-machine networks, where machines can include sensors, computers, or IoT gadgets [42]. GMM describes the velocity (given by



$v_{t_i}$ ) and direction of the device at time  $t_i$  (expressed as  $d_{t_i}$ ) based on their corresponding values at time  $t_{i-1}$ . GMM is expressed as shown in (1).

$$v_{t_i} = \chi_v v_{t_{i-1}} + (1 - \chi_v)\mu_v + \chi_s(\alpha_v \sqrt{1 - \chi_v^2})$$

$$d_{t_i} = \chi_d d_{t_{i-1}} + (1 - \chi_d)\mu_d + \chi_s(\alpha_d \sqrt{1 - \chi_d^2}), \quad (1)$$

where  $i = 1, 2, 3, \dots$  and the notations  $\chi_v$  and  $\chi_d$  are tuning parameters within the range of 0 and 1.  $\chi_v$  and  $\chi_d$  are used to introduce a degree of randomness in the computation of the speed and direction. If both parameters are 0, it implies that the movement trajectory is completely random, whereas if they are both 1, the trajectory is linear. The parameters  $\mu_v$  and  $\mu_d$  denote the average speed and mean direction, respectively. Notations  $\alpha_v$  and  $\alpha_d$  are stationary, independent, and uncorrelated Gaussian processes with a mean of zero. Finally,  $\chi_s$  is a conversion parameter to model the randomness. To eliminate the mobility randomness, parameter  $\chi_s$  is set to 0, while complete randomness is modeled by setting  $\chi_s$  to 1. We, therefore, set this parameter to 1.

Mobility in the proposed model will affect the number of IoT devices that can communicate directly at any given time. The communication range is given by  $r$ , and thus, a neighbor of the IoT device  $i$  in D2D communication is defined as any node  $j$  that is within the communication radius of node  $i$ , i.e.,

$$D2D_{Neighbor_i} = \{j | \psi(i, j) \leq r\}, \quad (2)$$

where  $\psi$  is the distance between  $i$  and  $j$  and  $D2D_{Neighbor_i}$  will change over time.

### B. SEIRD MODEL

This paper employs the SEIRD model to study mobile IoT malware's propagation dynamics. We choose this model for its suitability in accurately capturing the essential stages of the infection process. As opposed to the classical SIR model, the additional E and D states appropriately reflect the incubation period and the death of IoT devices upon power depletion, respectively. The SEIRD model categorizes the population of devices into five states: susceptible, exposed, infected, recovered, and dead. These states are briefly explained below.

#### 1) SUSCEPTIBLE STATE (S)

Nodes in  $S$  state have security shortcomings, are neither infected nor patched, and are vulnerable to malware attacks. Also, immunized devices that lose their immunity are categorized as susceptible since they can get attacked again.

#### 2) EXPOSED STATE (E)

Susceptible nodes that receive a malicious file transit to state  $E$ . IoT devices in the exposed state contain malware that can be activated once the user opens the malicious file. However, since nodes in state  $E$  are already compromised, they can propagate malware to the susceptible nodes they contact, thus exposing them to malware. Specifically, nodes in the  $E$  state are infected but do not depict the infection symptoms, such

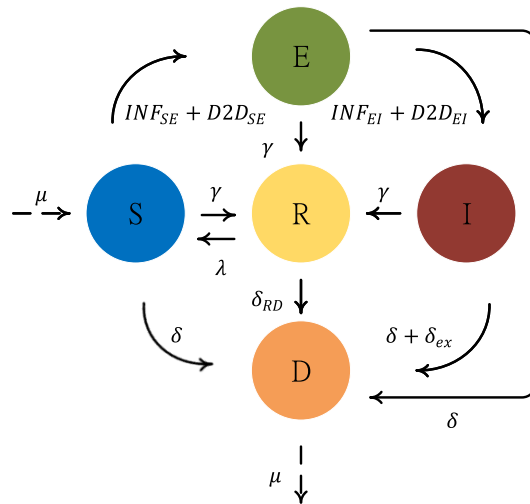


FIGURE 2. SEIRD transition diagram.

as high power consumption rates and increased processing activities.

#### 3) INFECTED STATE (I)

IoT devices in state  $E$  transit to state  $I$  once a user opens a malicious file. Therefore, infected gadgets can propagate infection to other vulnerable devices in the network. In this state, the malware is active and running in the IoT devices, increasing the power consumption rate due to increased processing activities.

#### 4) RECOVERED STATE (R)

The IoT devices that are cleared of malware and equipped with the updated antivirus software belong to the  $R$  state. These nodes can resist and detect the malware spreading in the network.

#### 5) DEAD STATE (D)

Since IoT devices are battery-powered, they may deplete their power and transit to state  $D$ . If a device's power runs out, it is regarded as dead since it cannot communicate with the others in the network.

The state transition diagram in Fig 2 illustrates how nodes shift from one state to another during the infection process. When nodes in the  $S$  state get exposed to malware, they transit to state  $E$  at the rate of  $INF_{SE} + D2D_{SE}$ . If susceptible nodes are patched, they shift to the  $R$  state at the rate of  $\gamma$ . Furthermore, susceptible nodes may die when they deplete their battery power and move to state  $D$  at the rate of  $\delta$ . After infection, nodes in  $E$  state shift to  $I$  class at the rate of  $INF_{EI} + D2D_{EI}$ . However, if a node in the exposed state is recovered, it transits to state  $R$  at the rate of  $\gamma$ . Exposed nodes that die transit to  $D$  state at the rate of  $\delta$ . Similarly, infected nodes recover at the rate of  $\gamma$  or die at the rate of  $\delta + \delta_{ex}$ . Recovered nodes can lose immunity and become susceptible again at the rate of  $\lambda$ . Nodes in the  $R$  state can

TABLE 2. Notations and description.

Notations	Explanation
$\mu$	Birth rate / discard rate.
$\gamma$	Probability of successful patching.
$\lambda$	Probability of losing immunity.
$\delta$	Probability of a node exhausting power.
$\delta_{ex}$	The probability of exhausting power due to malware.
$r$	IoT device's D2D transmission radius.
$R_d$	Malware decline rate caused by reduced infected devices.
$R_s$	Malware scanning rate through D2D.
$R_c$	Contact rate on the social network.
$R_o$	Probability of a user opening a malware file.
$P_{EI}$	Probability to transit from state $E$ to $I$ through D2D.
$P_{suc}$	Success rate of malware transmission through INF.

also die at the rate of  $\delta_{RD}$ . Damaged and irreplaceable dead nodes are discarded from state  $D$  at the rate of  $\mu$  and replaced at state  $S$  with the same rate of  $\mu$ . The birth rate is set to be equal to the discard rate to simulate a closed system in which nodes eliminated from the system are actively replaced to ensure continuity. From Fig. 2, the death rate of the infected nodes is higher than that of other nodes because malware activities consume more battery power causing IoT devices to die faster.

Table 2 shows the notations used in this paper and their descriptions. There are  $N$  IoT devices in the network, which are divided into  $k$  groups based on node degree, i.e.,  $G_1 + G_2 + G_3 + \dots, G_k = N$ . In each group, the population of  $S, E, I, R,$  and  $D$  at any point in time add up to 1, i.e.,  $S_k^t + E_k^t + I_k^t + R_k^t + D_k^t = 1$ .

The SEIRD model can be expressed as shown in (3).

$$\begin{aligned}
 S_k^t &= S_k^{t-1} + \mu - INF_{SE}S_k^{t-1} - D2D_{SE}S_k^{t-1} \\
 &\quad - \delta S_k^{t-1} - \gamma S_k^{t-1} + \lambda R_k^{t-1}, \\
 E_k^t &= E_k^{t-1} + INF_{SE}S_k^{t-1} + D2D_{SE}S_k^{t-1} \\
 &\quad - INF_{EI}E_k^{t-1} - D2D_{EI}E_k^{t-1} - \gamma E_k^{t-1} - \delta E_k^{t-1}, \\
 I_k^t &= I_k^{t-1} + INF_{EI}E_k^{t-1} + D2D_{EI}E_k^{t-1} - \gamma I_k^{t-1} \\
 &\quad - (\delta + \delta_{ex})I_k^{t-1}, \\
 R_k^t &= R_k^{t-1} + \gamma(S_k^{t-1} + E_k^{t-1} + I_k^{t-1}) - \delta_{RD}R_k^{t-1} - \lambda R_k^{t-1}, \\
 D_k^t &= D_k^{t-1} - \mu + \delta(S_k^{t-1} + E_k^{t-1}) + \delta_{RD}R_k^{t-1} \\
 &\quad + (\delta + \delta_{ex})I_k^{t-1}. \tag{3}
 \end{aligned}$$

### C. D2D PROPAGATION

The probability of an IoT device receiving malware via D2D transmission is given by  $D2D_{SE}$ . Since IoT devices can be infected along the path of movement, we define the area covered by the moving device in any given group  $k$  as  $\Lambda_k$  and is given by (4).

$$\Lambda_k = \pi r^2 + 2r \cdot v_{avg} t_{step}, \tag{4}$$

where  $v_{avg}$  is average velocity of the moving devices in group  $G_k$ , and  $t_{step}$  is the time step between  $t$  and  $t - 1$ . Besides, we consider the density of the compromised IoT devices, i.e.,  $\rho_{EI}$ , in the total area covered by the moving devices in all the

groups ( $\Lambda$ ) as shown in (5).

$$\rho_{EI} = \frac{E + I}{\Lambda}, \tag{5}$$

where  $E$  and  $I$  are the total number of devices in exposed and infected states, respectively, i.e.,

$$\begin{aligned}
 E &= \frac{\sum E_k^{t-1} G_k}{N}, \\
 I &= \frac{\sum I_k^{t-1} G_k}{N}. \tag{6}
 \end{aligned}$$

To obtain the infection force due to the D2D link ( $D2D_{SE}$ ), we compute the product of the mobility area,  $\Lambda_k$ , the density of the infected devices,  $\rho_{EI}$ , and the scanning rate ( $R_s$ ). The resultant  $D2D_{SE}$  is given by (7).

$$D2D_{SE} = \Lambda_k \rho_{EI} R_s. \tag{7}$$

With the increasing number of infected devices in the IoT network, malware will quickly spread out, and after the malware saturation point, the population of state  $I$  will start declining. This phenomenon will effectively reduce the number of devices transiting from states  $E$  to  $I$ . We, therefore, define the decline rate ( $R_d$ ), which we can use to obtain the value of  $D2D_{EI}$ .

$$D2D_{EI} = (1 - R_d I) P_{EI}. \tag{8}$$

### D. INF PROPAGATION

For the long-distance (INF) transmission, we define social network  $S_{net}$ . To determine the connectedness of the social network, we define the adjacency matrix  $N \times N$ . If  $S_{i,j} = 1$ , there is a connection between nodes  $i$  and  $j$ , otherwise,  $S_{i,j} = 0$ , and  $i$  and  $j$  are not connected.  $INF_{SE}$  is the probability that the device receives malware through long-distance transmission. Because IoT devices in the same group,  $G_k$ , have the same degree, they have an equal probability of contacting an infected device,  $O_k(E + I)$ , i.e.,

$$O_k(E + I) = \frac{\phi_k G_k}{\sum \phi_j G_j} (E + I), \tag{9}$$

where  $\phi_k$  is the degree of  $G_k$ . By multiplying  $O_k(E + I)$  with the contact rate and success rate, we obtain  $INF_{SE}$  as

$$INF_{SE} = R_c \cdot P_{suc} O_k(E + I). \tag{10}$$

After receiving the malware file, IoT users do not open it immediately. Therefore, the probability of a user opening a malicious file depends on the opening rate and the number of infected devices among friends. Since many friends might trust that the malware file is safe, the user's alert level might be low. We, therefore, define the infection rate,  $INF_{EI}$  as

$$INF_{EI} = O_k R_o I. \tag{11}$$

Due to malware activity, infected devices are more likely to run out of power faster than uninfected ones. Therefore, the death rate of the  $I$  state is increased by  $\delta_{ex}$ . The death rate

of the recovered nodes,  $\delta_{RD}$ , is determined by the number of infected IoT devices that transit to  $R$  and  $\delta_{RD}$  is given as

$$\delta_{RD} = \delta + I\gamma\delta_{ex}. \quad (12)$$

When there are many infected IoT devices,  $\delta_{RD}$  approaches  $\delta + \delta_{ex}$ . For simulation purposes in section V, we initialize  $I_k^0$  to a small value,  $\tau$ , whereby  $0 \leq \tau \leq 1$ . The other states are initialized as shown below.

$$\begin{aligned} E_k^0 &= R_k^0 = D_k^0 = 0, \\ S_k^0 &= 1 - \tau. \end{aligned} \quad (13)$$

## IV. MATHEMATICAL ANALYSIS

### A. EQUILIBRIUM POINTS

In malware spread modeling, two types of equilibrium points are of interest to researchers: endemic equilibrium (EE) and malware-free equilibrium (MFE) points. At equilibrium, the rate of change in all states is zero, i.e.,

$$\begin{aligned} \Delta S &= \mu - INF_{SE}S_k^{t-1} - D_2D_{SE}S_k^{t-1} \\ &\quad - \delta S_k^{t-1} - \gamma S_k^{t-1} + \lambda R_k^{t-1} = 0, \\ \Delta E &= INF_{SE}S_k^{t-1} + D_2D_{SE}S_k^{t-1} - INF_{EI}E_k^{t-1} \\ &\quad - D_2D_{EI}E_k^{t-1} - \gamma E_k^{t-1} - \delta E_k^{t-1} = 0, \\ \Delta I &= INF_{EI}E_k^{t-1} + D_2D_{EI}E_k^{t-1} - \gamma I_k^{t-1} \\ &\quad - (\delta + \delta_{ex})I_k^{t-1} = 0, \\ \Delta R &= \gamma(S_k^{t-1} + E_k^{t-1} + I_k^{t-1}) - \delta_{RD}R_k^{t-1} - \lambda R_k^{t-1} = 0, \\ \Delta D &= -\mu + \delta(S_k^{t-1} + E_k^{t-1}) + \delta_{RD}R_k^{t-1} \\ &\quad + (\delta + \delta_{ex})I_k^{t-1} = 0. \end{aligned} \quad (14)$$

The endemic equilibrium point refers to the stability point at which the number of nodes in all the states remains constant after a certain duration,  $t^*$ , and there is malware in the network. That is,  $\forall t > t^*$ ,  $\Delta S = \Delta E = \Delta I = \Delta R = \Delta D = 0$ , where  $\Delta$  is the rate of change from time  $t - 1$  to  $t$ , and  $I \neq 0$ ,  $E \neq 0$ . At this point, the malware transmission threshold value (discussed in subsection IV-B) is greater than one, implying that malware will persist in the network unless intervention measures are undertaken. The EE point, denoted as  $S_k^E, E_k^E, I_k^E, R_k^E, D_k^E$ , can be expressed as shown below.

$$\begin{aligned} S_k^E &= \frac{\mu(\delta\delta_{RD} - \delta\lambda + \gamma\delta_{RD}) + \lambda(\mu\gamma - \delta_{RD} + \delta)}{(INF_{SE} + D_2D_{SE} + \delta + \gamma)(\delta\delta_{RD} - \delta\lambda + \gamma\delta_{RD})}, \\ E_k^E &= \frac{S_k^E(INF_{SE} + D_2D_{SE})}{INF_{EI} + D_2D_{EI} + \gamma + \delta}, \\ I_k^E &= \frac{E_k^E(INF_{EI} + D_2D_{EI})}{\gamma + \delta + \delta_{ex}}, \\ R_k^E &= \frac{\gamma\mu - \delta_{RD} + \delta}{\delta_{RD}(\delta + \gamma) - \delta\lambda}, \\ D_k^E &= 1 - S_k^E - E_k^E - I_k^E - R_k^E. \end{aligned} \quad (15)$$

Different from endemic equilibrium, at MFE, the rate of change in all the states is 0, but there is no malware in the network. After a certain time period,  $t^*$ , the population of the infected and exposed states will settle at zero, thus

rendering the network malware-free. The MFE point, denoted as  $S_k^F, E_k^F, I_k^F, R_k^F, D_k^F$ , can be expressed as

$$\forall t > t^*, (S_k^t, E_k^t, I_k^t, R_k^t, D_k^t) = (S_k^F, E_k^F, I_k^F, R_k^F, D_k^F). \quad (16)$$

After time,  $t^*$ ,  $\Delta S = \Delta E = \Delta I = \Delta R = \Delta D = 0$ , where  $\Delta$  is the rate of change from time  $t - 1$  to  $t$ . Also, at MFE,  $I = E = 0$ ,  $\forall t > t^*$ . As shown in (17), the population of devices in states  $E, I, S, R$ , and  $D$  at the MFE point is given by

$$\begin{aligned} E_k^F &= I_k^F = 0, \\ S_k^F &= \frac{\mu(\delta + \lambda)}{\delta\lambda + \delta\gamma + \delta^2}, \\ R_k^F &= \frac{\mu\gamma}{\delta\lambda + \delta\lambda + \delta^2}, \\ D_k^F &= 1 - S_k^F - R_k^F. \end{aligned} \quad (17)$$

The MFE point is achieved when the malware spread threshold value is below one, as discussed in the subsequent subsection. Malware-free equilibrium point analysis can be used to highlight the parameter values that need to be adjusted to ensure that the malware dies off from the network. This can be achieved through the computation of the malware transmission threshold.

### B. MALWARE TRANSMISSION THRESHOLD

Here, by calculating the SEIRD malware transmission threshold,  $\sigma$ , we provide an indicator of the effectiveness of the current security measures. The transmission threshold plays an important role in modeling malware propagation as it indicates whether malware in the network will survive and persist in the future or fade away after some time. To compute  $\sigma$ , we use the Next-generation matrix method (NGM) presented in [43]. The transmission threshold,  $\sigma$ , is expressed as the spectral radius (denoted as  $\Gamma$ ) of the NGM, i.e.,

$$\sigma = \Gamma(\mathbf{AB}^{-1}), \quad (18)$$

where  $\mathbf{A}$  is the advent rate matrix, and  $\mathbf{B}$  is the transition rate matrix at MFE. Matrices  $\mathbf{A}$  and  $\mathbf{B}$  are generated from infectious classes  $E$  and  $I$ . The advent rate matrix,  $\mathbf{A}$ , comprises only the parameters that cause new infections, i.e., the parameters that cause susceptible nodes to become compromised. Matrix  $\mathbf{B}$  is derived from the parameters that transmit the infection, e.g., the parameters that make exposed nodes transit to I state. These two matrices are shown below.

$$\begin{aligned} \mathbf{A} &= \begin{bmatrix} \frac{\partial a_{11}}{\partial E_k^{t-1}} & \frac{\partial a_{11}}{\partial I_k^{t-1}} \\ \frac{\partial a_{21}}{\partial E_k^{t-1}} & \frac{\partial a_{21}}{\partial I_k^{t-1}} \end{bmatrix} = \begin{bmatrix} C_1 S_k^{t-1} & C_1 S_k^{t-1} \\ 0 & 0 \end{bmatrix} \\ \mathbf{B} &= \begin{bmatrix} \frac{\partial b_{11}}{\partial E_k^{t-1}} & \frac{\partial b_{11}}{\partial I_k^{t-1}} \\ \frac{\partial b_{21}}{\partial E_k^{t-1}} & \frac{\partial b_{21}}{\partial I_k^{t-1}} \end{bmatrix} \\ &= \begin{bmatrix} C_2 I_k^{t-1} + P_{EI} + \delta + \gamma & C_2 E_k^{t-1} \\ -C_2 I_k^{t-1} - P_{EI} & \delta + \delta_{ex} + \gamma - C_2 E_k^{t-1} \end{bmatrix} \end{aligned} \quad (19)$$

To compute the malware transmission threshold, we first compute the inverse of matrix  $\mathbf{B}$  ( $\mathbf{B}^{-1}$ ), which is given by

$$\frac{1}{|\mathbf{B}|} \begin{bmatrix} \delta + \delta_{ex} + \gamma - C_2 E_k^{t-1} & -C_2 E_k^{t-1} \\ C_2 I_k^{t-1} - P_{EI} & C_2 I_k^{t-1} + P_{EI} + \delta + \gamma \end{bmatrix}, \quad (21)$$

where  $C_1 = \frac{\Lambda_k}{\Lambda} R_s N + R_c P_{suc} O_k$  and  $C_2 = -R_d P_{EI} + O_k R_o$ . Following equation (21), matrix  $\mathbf{B}$  must be invertible, i.e., the determinant should not be equal to 0. Computing the determinant of matrix,  $|\mathbf{B}|$ , we obtain,

$$|\mathbf{B}| = (\delta + \delta_{ex} + \gamma)(C_2 I_k^{t-1} + P_{EI} + \delta + \gamma) - C_2 E_k^{t-1}(\delta + \gamma), \quad (22)$$

which is non-zero, and therefore matrix  $\mathbf{B}$  is invertible. Finally, we derive the malware transmission threshold (basic reproduction number) as,

$$\sigma = \frac{C_1(P_{EI} + \delta + \delta_{ex} + \gamma)S_k^f}{(P_{EI} + \delta + \gamma)(\delta + \delta_{ex} + \gamma)}. \quad (23)$$

The transmission threshold,  $\sigma$ , can be used as a security guideline to determine whether the malware is likely to die out in the future or not. For instance, when  $\sigma < 1$ , one primary case infects less than one device, implying that the malware will eventually disappear, and the IoT network will stabilize at the malware-free equilibrium point. MFE point implies that the current security measures are sufficient for mitigating an attack. On the contrary, if  $\sigma > 1$ , one index case produces more than one infection, thus implying that the malware will remain in the network if proper security interventions are not undertaken to reduce the threshold value.

From equation (23),  $P_{EI}$ ,  $\delta$ , and  $\gamma$  have the greatest implications on the threshold value. Increasing maintenance frequency for IoT devices could effectively reduce  $\delta$ , and accelerating the patching rate could increase  $\gamma$ . For the  $P_{EI}$ , it is not easy to tune as it requires users' security awareness. To control the value of  $P_{EI}$ , the network administrator can do some advocacy and improve the users' knowledge of attack protection strategies. Therefore, to reduce the value of  $\sigma$ , network administrators need to reduce the value of  $\delta$ , increase  $\gamma$  rate, and improve user security awareness.

### V. SIMULATION AND RESULTS

This section illustrates that the analytical results fit the simulation findings. For the analytical illustrations, we solved equations (3) while simulation results were achieved through performing Monte Carlo simulations, each repeated 1000 times with varying inputs. We also used the ONE simulator proposed in [44] to simulate the Gauss Markov mobility model, whereby we reset the position of IoT devices 100 times and computed the average value to use in the final simulations. The ONE simulator provides an environment to model node movement and inter-node contacts

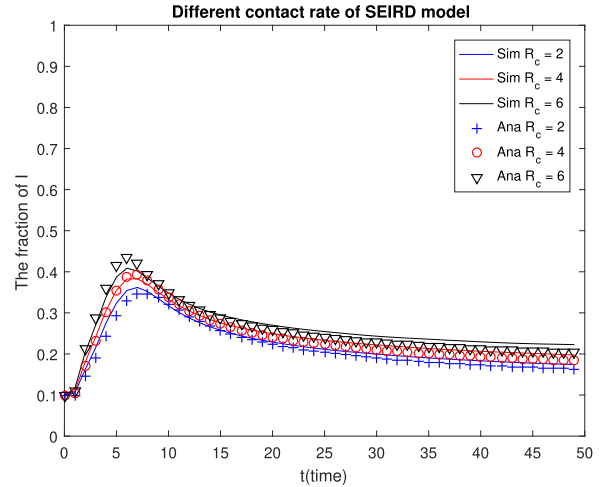


FIGURE 3. Fraction of IoT devices in State I under different  $R_c$ .

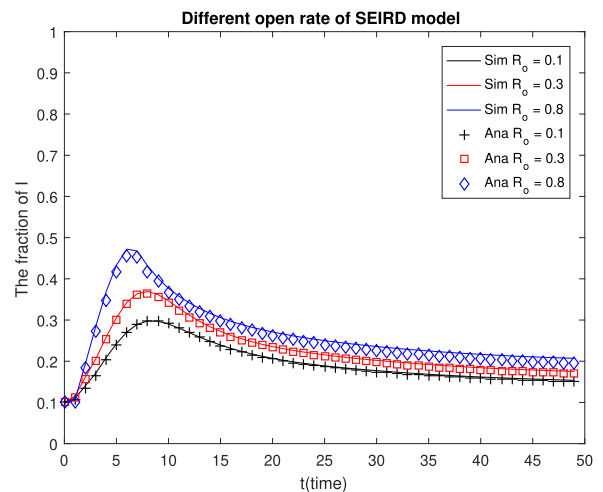


FIGURE 4. Fraction of IoT devices in State I under different  $R_o$ .

using different mobility models. Additionally, we analyzed the impact of changing specific parameter values on the malware spread rate and observed that different parameter settings profoundly affected the simulation results. Also, we performed experiments to illustrate the malware transmission threshold, i.e, when  $\sigma > 1$ , and  $\sigma < 1$ . Finally, we compared the proposed model with similar existing works, and the results are reported in subsection V-B. The parameters used in this paper are recorded in Table 3.

#### A. PARAMETER DISCUSSION

In most experiments, solid and dotted lines represent the simulation and analytical results, respectively. Similarly, we will follow this convention in our simulation illustrations. This subsection discusses the impact of modifying different parameter values on malware propagation.

Figs. 3 and 4 show the number of infected IoT devices,  $I$ , under different values of  $R_c$  and  $R_o$ , respectively. Both  $R_c$



TABLE 3. Parameter settings:-

Notation	$v$	$d$	$\mu$	$\gamma$	$\lambda$	$\delta$	$\delta_{ex}$	$r$	$R_d$	$R_s$	$R_c$	$R_o$	$P_{EI}$	$P_{suc}$
value	100	30	0.03	0.1	0.1	0.05	0.01	100	0.2	0.01	8	0.5	0.2	0.3

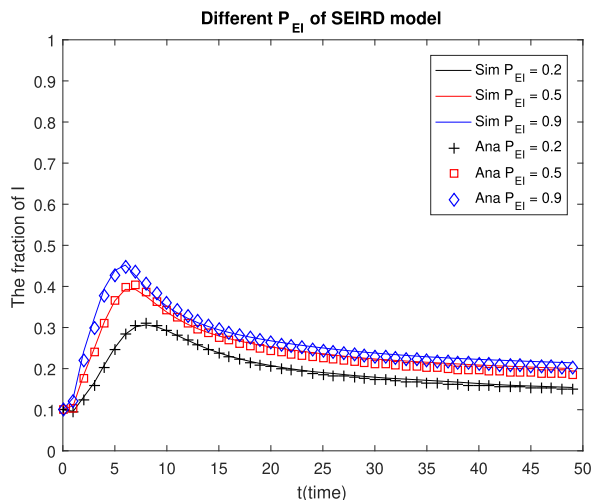


FIGURE 5. Fraction of IoT devices in State I under different  $P_{EI}$ .

(contact rate) and  $R_o$  (malware file opening rate) positively correlate with the number of infected devices in the network. Specifically, contacting friends on social networks more frequently and increasing the probability of opening a malware file exacerbates the infection spread.

Figs. 5 and 6 illustrate the population of the infected IoT devices under different values of  $P_{EI}$  and  $R_d$ . Both  $P_{EI}$  and  $R_d$  affect the infection probability in D2D transmission. While  $P_{EI}$  increases the population of infected IoT devices,  $R_d$  does not. The growth of the  $I$  state is influenced by other parameters because  $R_d$  reduces the number of devices that transit from state  $E$  to  $I$ . Because of the decline rate,  $R_d$ , the  $I$  proportion is relatively lower at time  $t$  than it was at time  $t - 1$ . Concretely, the population of infected devices increases before gradually decreasing and finally plateauing.

Fig. 7 demonstrates that a higher death rate,  $\delta, \delta_{ex}$ , reduces the fraction of the infected devices. The increased malware activity in infected nodes depletes devices' battery power, thus reducing the number of nodes in the  $I$  state.

As illustrated in Fig. 8, the higher the birth rate ( $\mu$ ), the smaller the proportion of the IoT devices in the  $D$  state. However, after a certain duration, a further increase in  $\mu$  does not alter the proportion of the  $D$  state. Fig. 9 illustrates the effect of  $\delta, \delta_{ex}$  on the proportion of devices in  $D$  state. A higher death rate causes more nodes to transit to state  $D$  after power depletion.

Figs. 10 and 11 show the effect of movement speed,  $v$ , on the population of  $E$  and  $I$ , respectively. The proportion of  $E$  and  $I$  states increases with speed, but after a certain threshold, the number of exposed nodes plateaus

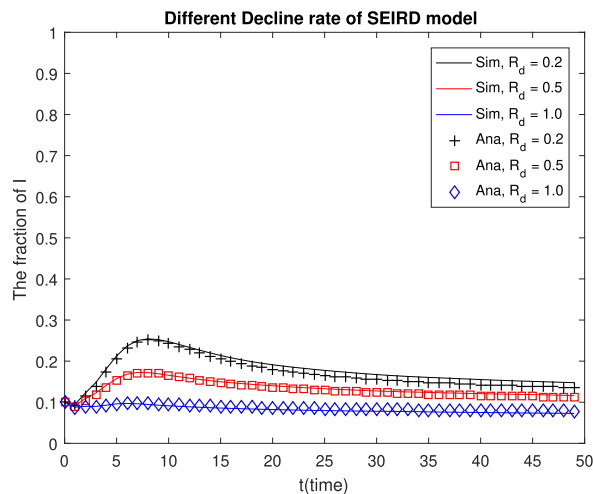


FIGURE 6. Fraction of IoT devices in State I under different  $R_d$ .

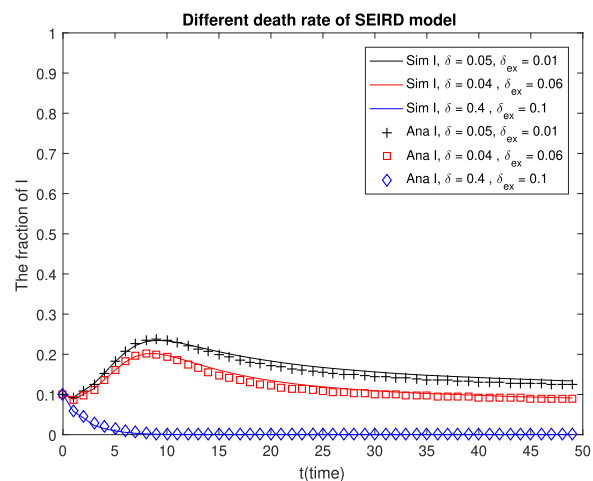


FIGURE 7. Fraction of IoT devices in State I under different  $\delta, \delta_{ex}$ .

while the number of the infected nodes decreases steadily over time.

The effects of changing the value of the communication range are shown in Figs. 12 and 13. The larger the radius, the higher the infection rate since malware can reach more target victims.

Fig. 14 illustrates the malware-free equilibrium (MFE) point, i.e., when  $\sigma < 1$ . Applying equation (23), we obtain the threshold value for MFE and as expected it is less than 1, i.e.,  $\sigma = 0.38 < 1$ . The rate of change in all states is zero, and there is no malware in the network. The MFE point implies that the current security measures are sufficient to eliminate the malware from the network. In Fig. 15, the malware threshold is greater than 1, i.e.,  $\sigma > 1$ , and mal-

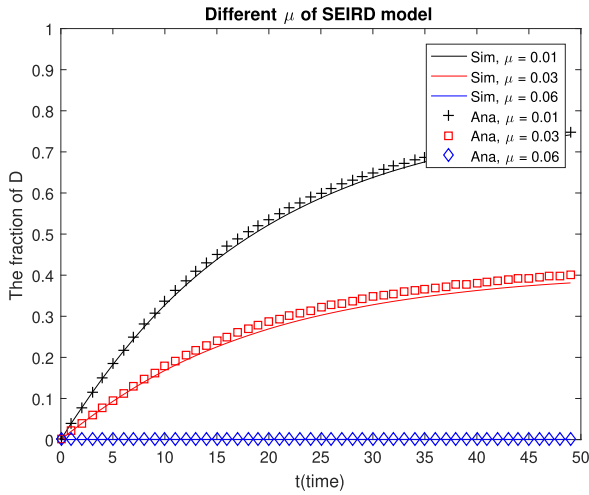


FIGURE 8. Fraction of IoT devices in State D under different  $\mu$ .

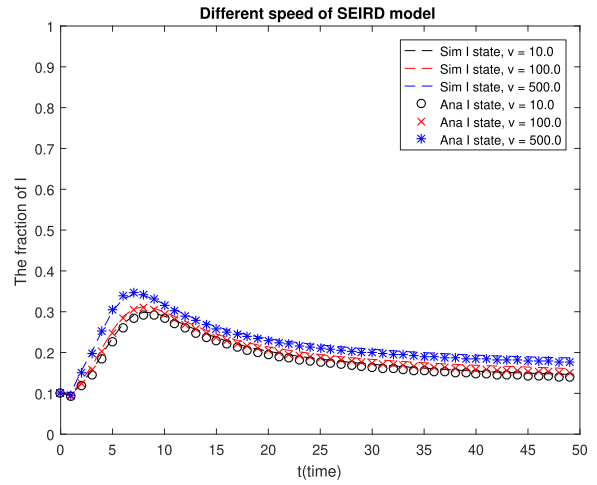


FIGURE 11. Fraction of IoT devices in State I under different speed  $v$ .

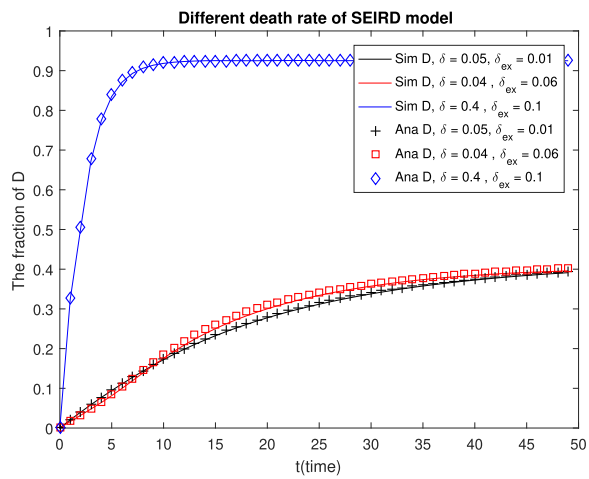


FIGURE 9. Fraction of IoT devices in State D under different  $\delta, \delta_{ex}$ .

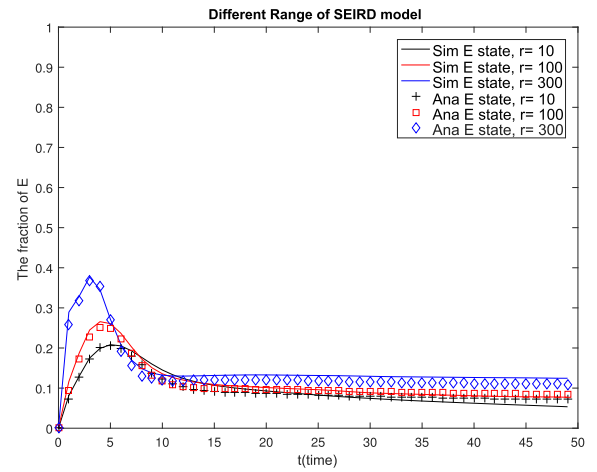


FIGURE 12. Fraction of IoT devices in State E under different radius  $r$ .

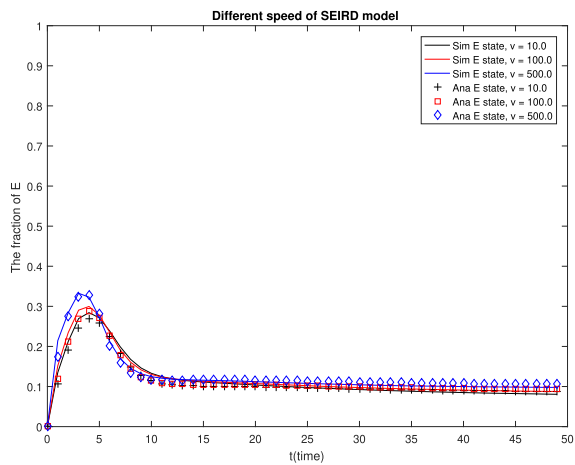


FIGURE 10. Fraction of IoT devices in State E under different speed  $v$ .

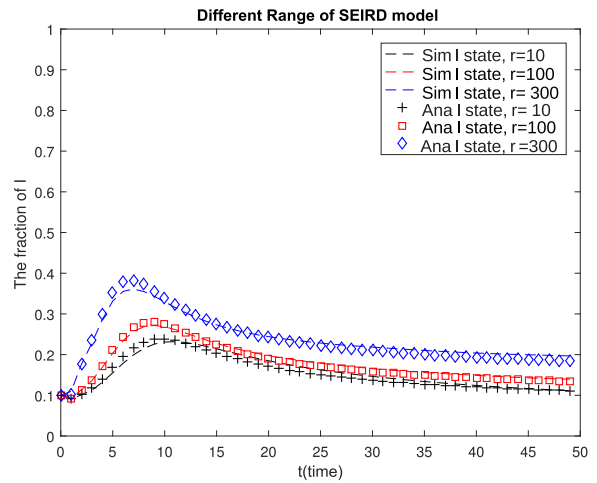


FIGURE 13. Fraction of IoT devices in State I under different radius  $r$ .

ware is present in the network since  $E \neq 0$  and  $I \neq 0$ . Specifically, applying equation (23), we obtain the malware

threshold in endemic equilibrium as  $\sigma = 2.5 > 1$ . This value indicates that the malware will remain in the network in

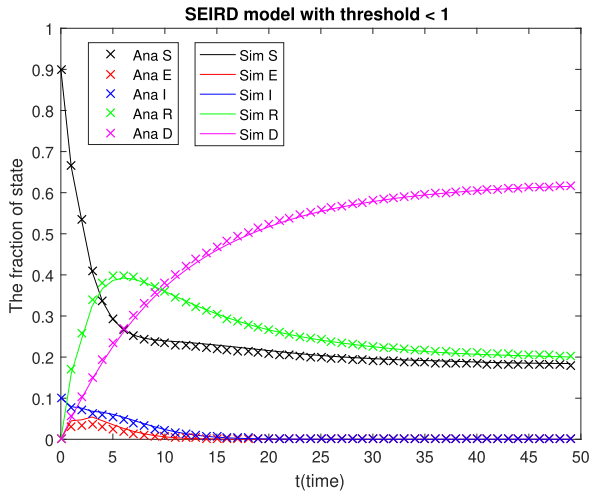


FIGURE 14. Fraction of IoT devices in each State when  $\sigma < 1$ .

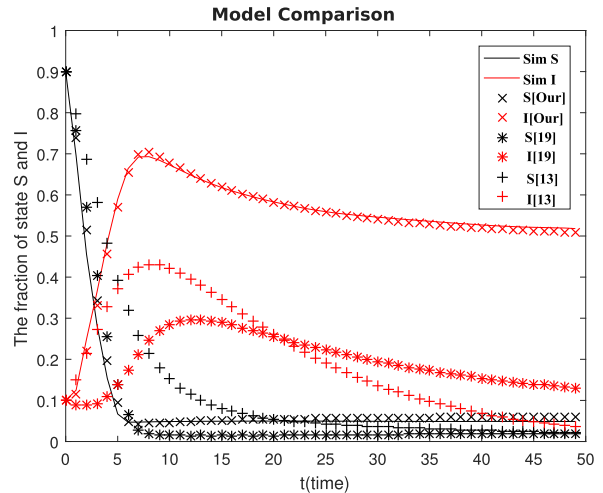


FIGURE 16. Comparison with different models.

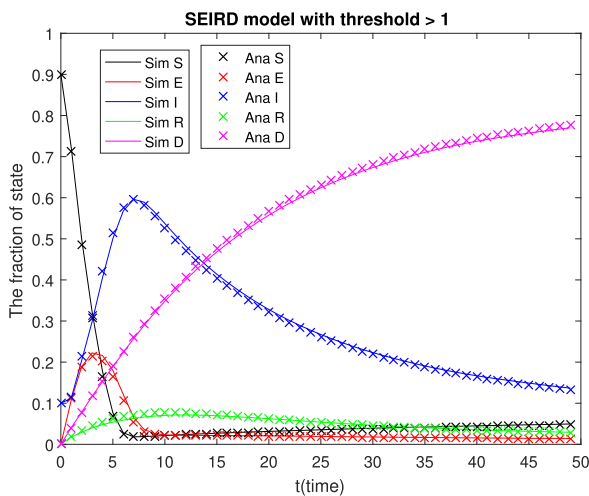


FIGURE 15. Fraction of IoT devices in each State when  $\sigma > 1$ .

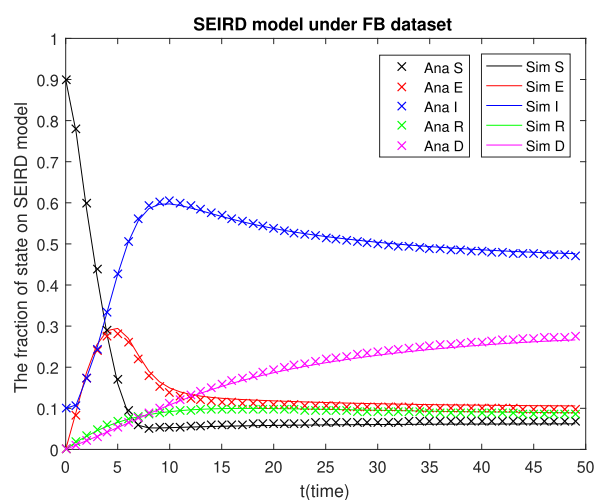


FIGURE 17. SEIRD Model under the FB dataset.

the future unless effective strategies are adopted to suppress them.

### B. MODEL COMPARISON AND FACEBOOK DATASET IMPLEMENTATION

This subsection compares the performance of the proposed work with the models presented in [13] and [19]. Fig. 16 shows the ratio of states  $I$  and  $S$  of our model and those of models proposed in [13] and [19], under the same parameter settings. Liu et al. [19] only consider long-distance transmission, while [13] studies both INF and D2D communications but ignores the role of mobility in malware propagation. From Fig. 16, the ratio of  $I$  state in [19] and [13] is not as high as that of the proposed model. Liu et al. [19] seriously underestimated malware propagation by failing to factor in the role of INF in malware spread. Acarali et al. [13] also underrated the severity of IoT malware propagation by failing to recognize the impact of mobility in the spread of malware.

Finally, we tested our model on a real-world dataset, the Facebook dataset from the Stanford Network Analysis Project (SNAP) [45]. The Facebook dataset is an undirected graph with 4,039 nodes and 88,234 edges. The simulation results presented in Fig. 17 demonstrate that the experimental findings under the FB dataset match the analytical results discussed previously.

### VI. CONCLUSION

In this paper, we proposed SEIRD epidemic model to study mobile IoT malware. In addition to mobility, we analyzed the impacts of leveraging infrastructure-based and D2D communication schemes on IoT malware spread. Our discussions and analysis demonstrated that our model adequately captures the dynamics of realistic IoT malware propagation. We conducted mathematical evaluations and computed the malware transmission threshold, which can be used as a security guideline in suppressing IoT malware attacks. When the transmission threshold value is less than one,

the malware will eventually die out even without further interventions; otherwise, it will persist in the future. Our analysis and simulation results revealed that mobility and the use of both INF and D2D connections significantly aggravate malware diffusion in IoT networks. However, we discovered that intervention measures such as increasing IoT user security awareness and improving the recovery rate could substantially reduce the extent and severity of malware spread.

## REFERENCES

- [1] M. Frustaci, P. Pace, G. Aloï, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.
- [2] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai botnet," in *Proc. 26th USENIX Secur. Symp.*, Aug. 2017, pp. 1093–1110.
- [3] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019.
- [4] S.-M. Cheng, P.-Y. Chen, C.-C. Lin, and H.-C. Hsiao, "Traffic-aware patching for cyber security in mobile IoT," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 29–35, Jul. 2017.
- [5] C. Koliass, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.
- [6] C. O'Flynn, "A lightbulb worm? Details of the Philips Hue smart lighting design," in *Proc. Blackhat*, Aug. 2016, pp. 1–48. [Online]. Available: <https://www.blackhat.com/docs/us-16/materials/us-16-O'Flynn-A-Lightbulb-Worm-wp.pdf>
- [7] A. Mahboubi, S. Camtepe, and K. Ansari, "Stochastic modeling of IoT botnet spread: A short survey on mobile malware spread modeling," *IEEE Access*, vol. 8, pp. 228818–228830, 2020.
- [8] S.-M. Cheng, W. C. Ao, P.-Y. Chen, and K.-C. Chen, "On modeling malware propagation in generalized social networks," *IEEE Commun. Lett.*, vol. 15, no. 1, pp. 25–27, Jan. 2011.
- [9] S. Yu, G. Gu, A. Barnawi, S. Guo, and I. Stojmenovic, "Malware propagation in large-scale networks," *IEEE Trans. Knowl. Data Eng.*, vol. 27, no. 1, pp. 170–179, Jan. 2015.
- [10] B. Liu, W. Zhou, L. Gao, H. Zhou, T. H. Luan, and S. Wen, "Malware propagations in wireless ad hoc networks," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 6, pp. 1016–1026, Nov./Dec. 2018.
- [11] M. J. Farooq and Q. Zhu, "Modeling, analysis, and mitigation of dynamic botnet formation in wireless IoT networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 9, pp. 2412–2426, Sep. 2019.
- [12] X. Wang, B. Song, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Group-based susceptible-infectious-susceptible model in large-scale directed networks," *Secur. Commun. Netw.*, vol. 2019, pp. 1–9, Jan. 2019.
- [13] D. Acarali, M. Rajarajan, N. Komninos, and B. B. Zarpelão, "Modelling the spread of botnet malware in IoT-based wireless sensor networks," *Secur. Commun. Netw.*, vol. 2019, pp. 1–13, Feb. 2019.
- [14] S. Shen, H. Ma, E. Fan, K. Hu, S. Yu, J. Liu, and Q. Cao, "A non-cooperative non-zero-sum game-based dependability assessment of heterogeneous WSNs with malware diffusion," *J. Netw. Comput. Appl.*, vol. 91, pp. 26–35, Aug. 2017.
- [15] Y. Wei, Y. Tao, N. Yang, and S. Leng, "On modeling malware propagation in interest-based overlapping communities," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.
- [16] N. Kawabata, Y. Yamasaki, and H. Ohsaki, "Modeling restrained epidemic routing on complex networks," in *Proc. IEEE 43rd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2019, pp. 285–290.
- [17] A. Al Kindi, D. Al Abri, A. Al Maashri, and F. Bait-Shiginah, "Analysis of malware propagation behavior in social Internet of Things," *Int. J. Commun. Syst.*, vol. 32, no. 15, p. e4102, Oct. 2019.
- [18] T. Gardner, C. Beard, and D. Medhi, "Using SEIRS epidemic models for IoT botnets attacks," in *Proc. DRCN*, Mar. 2017, pp. 1–8.
- [19] W. Liu and S. Zhong, "Web malware spread modelling and optimal control strategies," *Sci. Rep.*, vol. 7, no. 1, pp. 1–19, Feb. 2017.
- [20] H. Xia, L. Li, X. Cheng, X. Cheng, and T. Qiu, "Modeling and analysis botnet propagation in social Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7470–7481, Aug. 2020.
- [21] T. Wang, C. Xia, S. Wen, H. Xue, Y. Xiang, and S. Tu, "SADI: A novel model to study the propagation of social worms in hierarchical networks," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 1, pp. 142–155, Jan. 2019.
- [22] S. Shen, H. Zhou, S. Feng, L. Huang, J. Liu, S. Yu, and Q. Cao, "HSIRD: A model for characterizing dynamics of malware diffusion in heterogeneous WSNs," *J. Netw. Comput. Appl.*, vol. 146, Nov. 2019, Art. no. 102420.
- [23] P.-Y. Chen, S.-M. Cheng, and M.-H. Sung, "Analysis of data dissemination and control in social internet of vehicles," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2467–2477, Aug. 2018.
- [24] S. Shen, H. Zhou, S. Feng, J. Liu, H. Zhang, and Q. Cao, "An epidemiology-based model for disclosing dynamics of malware propagation in heterogeneous and mobile WSNs," *IEEE Access*, vol. 8, pp. 43876–43887, 2020.
- [25] G. Meng, M. Patrick, Y. Xue, Y. Liu, and J. Zhang, "Securing Android app markets via modeling and predicting malware spread between markets," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1944–1959, Jul. 2019.
- [26] Y. Chen, Y. Mao, L. Cui, S. Leng, Y. Wei, and X. Chen, "A two layer model of malware propagation in a search engine context," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2018, pp. 21–26.
- [27] B. Song, X. Wang, W. Ni, Y. Song, R. P. Liu, G.-P. Jiang, and Y. J. Guo, "Reliability analysis of large-scale adaptive weighted networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 651–665, 2020.
- [28] O. Tsemogne, Y. Hayel, C. Kamhoua, and G. Deugoué, "Game theoretic modeling of cyber deception against epidemic botnets in Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2678–2687, Feb. 2022.
- [29] D. Zhao, L. Wang, Z. Wang, and G. Xiao, "Virus propagation and patch distribution in multiplex networks: Modeling, analysis, and optimal allocation," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1755–1767, Jul. 2019.
- [30] J. D. Hernandez Guillen, A. Martin del Rey, and R. Casado-Vara, "Security countermeasures of a SCIRAS model for advanced malware propagation," *IEEE Access*, vol. 7, pp. 135472–135478, 2019.
- [31] D. T. Le, T. T. Tran, K. Q. Dang, R. Alkanhel, and A. Muthanna, "Malware spreading model for routers in Wi-Fi networks," *IEEE Access*, vol. 10, pp. 61873–61891, 2022.
- [32] S. Shen, H. Zhou, S. Feng, J. Liu, and Q. Cao, "SNIRD: Disclosing rules of malware spread in heterogeneous wireless sensor networks," *IEEE Access*, vol. 7, pp. 92881–92892, 2019.
- [33] H. Zhang, S. Shen, Q. Cao, X. Wu, and S. Liu, "Modeling and analyzing malware diffusion in wireless sensor networks based on cellular automaton," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 11, Nov. 2020, Art. no. 155014772097294.
- [34] A. Mahboubi, S. Camtepe, and H. Morarji, "A study on formal methods to generalize heterogeneous mobile malware propagation and their impacts," *IEEE Access*, vol. 5, pp. 27740–27756, 2017.
- [35] H. Zhou, S. Shen, and J. Liu, "Malware propagation model in wireless sensor networks under attack–defense confrontation," *Comput. Commun.*, vol. 162, pp. 51–58, Oct. 2020.
- [36] S. J. Achar, C. Baishya, and M. K. A. Kaabar, "Dynamics of the worm transmission in wireless sensor network in the framework of fractional derivatives," *Math. Methods Appl. Sci.*, vol. 45, no. 8, pp. 4278–4294, May 2022.
- [37] L. Jiang, H. Pan, J. He, R. Li, C. Xu, Q. Xu, Y. Dai, F. Dong, and J. Tong, "Control mechanism of virus propagation in wireless sensor networks based on analytic hierarchy process," *Secur. Commun. Netw.*, vol. 2022, pp. 1–16, May 2022.
- [38] Z. Yu, H. Gao, D. Wang, A. A. Alnuaimi, M. Firdausi, and A. M. Mostafa, "SEI2RS malware propagation model considering two infection rates in cyber–physical systems," *Phys. A, Stat. Mech. Appl.*, vol. 597, Jul. 2022, Art. no. 127207.
- [39] Y. Shen, S. Shen, Z. Wu, H. Zhou, and S. Yu, "Signaling game-based availability assessment for edge computing-assisted IoT systems with malware dissemination," *J. Inf. Secur. Appl.*, vol. 66, May 2022, Art. no. 103140.



[40] R. Goel and R. Sharma, "Mobility based SIR model for pandemics—With case study of COVID-19," in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining (ASONAM)*, Dec. 2020, pp. 110–117.

[41] Y. Yi, Y. Yang, K. Cheng, Y. Wu, and X. Wang, "Information dissemination with service-oriented incentive mechanism in industrial Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16897–16907, Sep. 2022.

[42] R. He, B. Ai, G. L. Stüber, and Z. Zhong, "Mobility model-based non-stationary mobile-to-mobile channel modeling," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4388–4400, Jul. 2018.

[43] P. Van Den Driessche and J. Watmough, "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission," *Math. Biosci.*, vol. 180, nos. 1–2, pp. 29–48, Nov. 2002.

[44] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," in *Proc. 2nd Int. ICST Conf. Simul. Tools Techn.*, 2009, pp. 1–10.

[45] J. Leskovec and A. Krevl. (Jun. 2014). *SNAP Datasets: Stanford Large Network Dataset Collection*. [Online]. Available: <http://snap.stanford.edu/data>



**SHIN-MING CHENG** (Member, IEEE) received the B.S. and Ph.D. degrees in computer science and information engineering from the National Taiwan University, Taipei, Taiwan, in 2000 and 2007, respectively.

He was a Postdoctoral Research Fellow with the Graduate Institute of Communication Engineering, National Taiwan University, from 2007 to 2012. Since 2012, he has been a Faculty Member of the Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei, where he is currently an Associate Professor. Since 2017, he has been with the Research Center for Information Technology Innovation, Academia Sinica, Taipei, where he is currently a Joint Appointment Associate Research Fellow. His current research interests include secure mechanism design and cybersecurity platform development in 4G/5G and the IoT networks. He also investigates the robustness issue of machine learning. He received the K. T. Li Young Researcher Award from ACM Taipei/Taiwan Chapter, in 2014, the IEEE PIMRC 2013 Best Paper Award, the IEEE Trustcom 2020 Best Paper Award, and the CISC 2020 & 2021 Best Paper Award.



**BO-RUI CHEN** received the M.Sc. degree in computer science and information engineering from the National Taiwan University of Science and Technology, Taipei, Taiwan, in 2020. His research interest includes malware propagation modeling in IoT networks.



**MAINA BERNARD MWANGI** (Graduate Student Member, IEEE) received the M.Sc. degree in computer science and information engineering from the National Taiwan University of Science and Technology, Taipei, Taiwan, in 2021, where he is currently pursuing the Ph.D. degree in computer science and information engineering. His research interests include the IoT and AI security.

...