IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 21, 2020, accepted February 28, 2020, date of publication March 3, 2020, date of current version March 12, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2977966

An Epidemiology-Based Model for Disclosing Dynamics of Malware Propagation in Heterogeneous and Mobile WSNs

SHIGEN SHEN[1], (Member, IEEE), HAIPING ZHOU[1], SHENG FENG[1], JIANHUA LIU[1], (Member, IEEE), HONG ZHANG[2], AND QIYING CAO[2]

[1]Department of Computer Science and Engineering, Shaoxing University, Shaoxing 312000, China
[2]College of Computer Science and Technology, Donghua University, Shanghai 201620, China

Corresponding author: Jianhua Liu (ljh_541@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61772018 and Grant 61572014, and in part by the Public Welfare Technology Research Project of Zhejiang Province under Grant LGG19F020007.

ABSTRACT Heterogeneous and mobile wireless sensor networks (HMWSNs) are generally practical in constructing smart Internet of Things. However, malware can easily propagate itself over HMWSNs and make harm such as data interception and unauthorized activities. To defend such malware, developing a model to disclose dynamics of malware propagation becomes urgently required. In this context, a heterogeneous and mobile vulnerable-compromised-quarantined-patched-scrapped (VCQPS) model is proposed by considering both the heterogeneity and mobility of HMSNs (heterogeneous and mobile sensor nodes). Then, differential equations of transition proportions among all states are achieved by analyzing the changeable quantities of HMSNs belonging to different states. Further, the existence of the stationary points of the VCQPS model is proved, upon which the malware propagation threshold is derived by calculating the reproduction number. The stability of the malware-free stationary-point is also proved. Experiments are performed to validate the stability of the malware-free stationary-point and show the effectiveness of the VCQPS model by comparing our model with traditional SIS and SIR models.

INDEX TERMS Heterogeneous and mobile wireless sensor networks, malware, epidemic theory, heterogeneity, mobility.

I. INTRODUCTION

Today, heterogeneous and mobile wireless sensor networks (HMWSNs) are the foundation of infrastructure networks such as smart homes, smart grid, and intelligent transportation, which create smart Internet of Things. In an HMWSN, heterogeneous and mobile sensor nodes (HMSNs) have heterogeneities in terms of energy, communication connection, and computation capability. They, on the other hand, are furnished with locomotive structure, so that they can move as needed after they have been initially deployed [1]. Such heterogeneities and mobility can effectively improve the scalability, the coverage and connectivity, and the dependability of the network [2], making HMWSNs be more practical in constructing smart Internet of Things than homogeneous and static WSNs.

The associate editor coordinating the review of this manuscript and approving it for publication was Chakchai So-In.

As intrusive software, malware is deliberately developed to harm and destroy computer systems, which can easily propagate itself over an HMWSN and harm the HMWSN [3]–[11]. For examples, Giannetsos *et al.* [12] and Gu *et al.* [13] gave methods to show how mal-packets can be injected into sensor nodes and propagate themselves among nodes. In a good survey, Illiano and Lupu [14] further summarized the related work on malware injection in sensor nodes and obtained general principles to detect malware. Once malware propagates over the HMWSN, it can steal, alter, and delete data sensed by nodes, and even can monitor the activity of the HMWSN without administrator permission [14]–[19]. To effectively eliminate and control malware in the HMWSN, it is necessary to explore dynamics of malware propagation for disclosing malware propagation principles, which motivates us to perform this work.

Epidemiology-based models describing communicable diseases propagation can be employed to study the dynamics of malware propagation in HMWSNs, due to the strong

similarity between infectious disease and malware in HMWSNs [20]. These models assist us in understanding how and what scale the malware will propagate in HMWSNs in the future. They also assist us in illustrating the impact factors to decide whether the malware will propagate or dissipate in HMWSNs, and thus guide administrators to design countermeasures against malware.

Herein, we propose a heterogeneous and mobile vulnerable-compromised-quarantined-patched-scrapped (VCQPS) model including states V, C, Q, P, and S, which is motivated by referring and extending the traditional SIR model. Note that this epidemiology-based model adopts states from the view of informatics to be more consistent with the habits of computer readers. Moreover, this model considers both the heterogeneity and the mobility of HMSNs.

We make contributions in this work as follows.

First, we propose a heterogeneous and mobile VCQPS model, which, to the best of our knowledge, is the first work for disclosing dynamics of malware propagation in HMWSNs.

Second, we derive differential equations of transition proportion among all states of the heterogeneous and mobile VCQPS model, which can reflect the changeable quantities of HMSNs belonging to different states.

Third, we prove the existence of the stationary points of the heterogeneous and mobile VCQPS model. We further achieve the malware propagation threshold by calculating the basic reproduction number, upon which we can deduce the condition to judge when malware in HMWSNs can propagate.

Finally, we prove the stability of the malware-free stationary-point of the heterogeneous and mobile VCQPS model, which can instruct administrators to take suitable security behaviors to suppress malware propagation.

We organize the remainder of this paper as follows. In Section II, we review related work and outline the unsolved issues of existing epidemiology-based models for HMWSNs. We analyze state transitions of HMSNs in Section III. We give the coverage area of an HMSN with random direction mobility in Section IV. We deduce the heterogeneous and mobile VCQPS model in Section V. We, in Section VI, characterize the heterogeneous and mobile VCQPS model in such aspects including proof of stationary points, calculation of the malware propagation threshold, and proof of stability of the malware-free stationary-point. We perform experiments in Section VII to validate the effectiveness of our model. Finally, conclusions are summarized.

II. RELATED WORK

Up to now, researchers have made considerable effort to develop epidemiology-based models for formulating malware propagation in WSNs. Mishra and Keshri [21] presented a susceptible-exposed-infectious-recovered-susceptible-vaccination model, which describes both the temporal and spatial characteristics of malware propagation. Sayad Haghighi *et al.* [22] proposed a geographical susceptible-infective model, which specially considers geometrical and spatial constraints of WSNs. Upadhyay and Kumari [23] formulated a susceptible-infected-terminally infected-recovered model by introducing a "terminally infected" compartment. Singh *et al.* [24] gave a susceptible-exposed-infectious-recovered-vaccinated model considering node communication radius and density. Wang *et al.* [25] integrated a discrete-time absorbing Markov process into the traditional SIS model to illustrate malware propagation in large networks with nontrivial topologies. Shakya *et al.* [26] presented a new susceptible-infectious-recovered model, which reflects spatial correlation characteristics of WSNs. Additionally, there are other representative epidemiology-based models for malware propagation in WSNs, such as a susceptible-exposed-infectious-recovered model reflecting time delay [27], a stochastic susceptible-infectious-susceptible model [28], and a susceptible-exposed-infectious-recovered model reflecting variable contact rates [29].

Some researchers have paid attention to malware propagation in heterogeneous networks. Nowzari *et al.* [30] presented a susceptible-exposed-infected-vigilant model, which characterizes dynamics of malware propagation over universal directed graphs considering node heterogeneity. Keshri *et al.* [31] achieved malware propagation dynamics using the susceptible-exposed-infectious-recovered model with a reduced scale free network, in which sensor nodes are divided into higher-degree and lower-degree ones. Qu and Wang [32] analyzed the influence of i.i.d. infection rates on the traditional susceptible-infectious-susceptible model. Yang *et al.* [33] formulated a heterogeneous susceptible-infectious-recovered-susceptible model, which reflects heterogeneous network topology. Eshghi *et al.* [34] proposed a general epidemic framework considering the heterogeneity of propagation rates.

Some researchers have studied malware propagation in mobile WSNs. Wang *et al.* [35] disclosed the dynamics of malware propagation in mobile WSNs with reaction-diffusion equations. They [36] also analyzed the process of malware propagation with pulse differential equations and further patched sensor nodes in a pulse way. Zhu *et al.* [37] considered delay reaction-diffusion equations and employed a state feedback method to effectively control unstable steady states. Other typical malware propagation models that can be employed to mobile WSNs include a susceptible-exposed-infected-recovered-susceptible model with a concrete connection pattern [38], and a complex network-based model classifying nodes into three groups: weakly-protected susceptible ones, strongly-protected susceptible ones, and infected ones [39].

However, how to disclose dynamics of malware propagation in HMWSNs has yet not solved from related work aforementioned. More especially, the first issue is how to concurrently characterize three actual factors: the heterogeneity of HMSNs, the mobility of HMSNs, and malware quarantine. The second issue is how to deduce the condition to judge

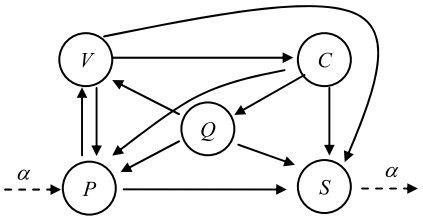


FIGURE 1. State transition diagram of an HMSN.

whether malware will propagate or dissipate. We herein solve the first issue by considering the communication connectivity and random direction model as measuring the heterogeneity and mobility of HMSNs, respectively. We further add state Q to reflect the case of malware quarantine. Then, we solve the second issue by analyzing the stationary points of our epidemiology-based model and deriving the malware propagation threshold. Compared to our previous work [40], [41], the current work not only consider the heterogeneity but also the mobility of HMSNs; on the other hand, the current work adopts a new state transition diagram for HMSNs.

III. STATE TRANSITIONS OF HMSNS

In the heterogeneous and mobile VCQPS model, state V means that an HMSN has software bugs and is vulnerable to be contaminated by malware. C means that the HMSN has been compromised and mastered by malware, from which malware can contaminate its neighbor HMSNs in state V by sending packets each other. Q means that the HMSN is quarantined because it has malware after intrusion detection. P means that the compromised HMSN has been removed the existed malware via the HMWSN IDS, therefore it becomes secure at present and can prevent from the known malware. S means that the HMSN is scrapped for the reasons of battery depletion, physical damage, or deliberate destruction by the existed malware.

Figure 1 portrays the state transition diagram of an HMSN. In essence, an HMSN changes its state due to the behaviors of the malware and the HMWSN IDS, which are operated by attackers and administrators, respectively. For an HMSN, its state is P at the beginning. The state is changed from P to V, once attackers scan the HMSN and discover its software bugs, and thus the attackers can propagate malware into the HMSN. Afterwards, the state is changed from V to C, once the attackers constantly launch attacks and successfully inject malware into the HMSN. Further, the state is changed from C to Q, once malware existed in the HMSN is detected and the administrators quarantine the HMSN. Moreover, when an HMSN in states Q and P encounters the unknown malware, its state will change into state V for it lacks immunity and becomes vulnerable. Generally, administrators launch the HMWSN IDS to scan and remove the malware resided in every HMSN, and also patch vulnerable HMSNs for preventing them from the unknown malware. These behaviors make states V, C, and Q change into state P. Additionally, any HMSN may occur hardware and software faults or is deliberately destroyed by malware, which lets states V, C, Q, and P turn into state S. These scrapped HMSNs are usually taken place of new HMSNs, since most HMSNs cannot be fixed. In this manner, new HMSNs are added into the HMWSN, whose number is the same as one of those scrapped HMSNs. Therefore, in Fig.1 we portray the incoming dashed arrow to denote the new HMSNs added, and the outgoing dashed arrow to be the scrapped HMSNs.

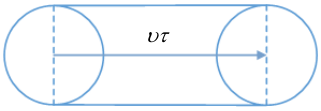


FIGURE 2. Coverage area of an HMSN moving from one point to another.

IV. COVERAGE AREA OF A MOBILE HMSN WITH RANDOM DIRECTION MOBILITY

Without loss of generality, we consider an HMWSN employ the Random Direction Mobility model [42]. In this context, an HMSN can freely move anyplace in the area covered by the HMWSN. At time t it randomly selects its direction $\omega_t \in [0, 2\pi)$ following a uniform distribution, in other words, it does not have any given or special direction. The value of its velocity $v_t \in [0, v_{\max}]$ at time t is randomly taken, which follows a normal distribution or a uniform distribution. After a random time following an exponential distribution, the HMSN changes its direction and velocity with new random values. Note that these stochastic processes for direction and velocity selection are generally unrelated to each other.

We next analyze the number of HMSNs communicating with a mobile HMSN from mean field theory. Let $r_{\min}$ be the minimum communication radius of an HMSN. υ and τ are the mean moving velocity and the mean moving time of all mobile HMSNs, respectively. As illustrated in Fig. 2, the coverage area ς is the area of two semicircle with radius $r_{\min}$ plus the area of a rectangle with width $2r_{\min}$ and length $\upsilon\tau$, i.e.,

$$\varsigma = \pi r_{\min}^2 + 2r_{\min}\upsilon\tau. \tag{1}$$

V. HETEROGENEOUS AND MOBILE VCQPS MODEL

We consider that the heterogeneity of HMSNs is characterized by their communication connectivity. In this manner, all HMSNs are separated as N sets, and an HMSN belonging to the same set has the same communication connectivity. We denote $n \in \{1, 2, \cdots, N\}$ as the communication connectivity of an HMSN belonging to set n. Let V_n^t, C_n^t, Q_n^t, P_n^t, and S_n^t be the proportions of set n in states V, C, Q, P, and S at time t, respectively. We can easily obtain

$$V_n^t + C_n^t + Q_n^t + P_n^t + S_n^t = 1 \tag{2}$$

at any time. From [15], we assume the initial proportion of HMSNs belonging to set n in state C is β, i.e.,

$$C_n^0 = \beta, 0 < \beta < 1. \tag{3}$$

The initial proportions of HMSNs belonging to set n in states Q, P, and S are 0, i.e.,

$$Q_n^0 = P_n^0 = S_n^0 = 0. \tag{4}$$

Therefore, the initial proportion of HMSNs belonging to set n in state V is

$$V_n^0 = 1 - \beta. \tag{5}$$

From complex network theory, the probability χ_n^t that an HMSN belonging to set n in state V sends packets to one of compromised HMSNs is

$$\chi_n^t = \frac{1}{< d >} \sum_{n=1}^{N} \delta_n \varepsilon_n C_n^t, \tag{6}$$

where $< d >$ is the mean degree (communication connectivity) of the HMWSN, and δ_n and ε_n are the probability and the propagation ability of an HMSN having communication connectivity n, respectively. These variables satisfy

$$\sum_{n=1}^{N} \delta_n = 1 \tag{7}$$

and

$$\langle d \rangle = \sum_{n=1}^{N} n\delta_n. \tag{8}$$

We next analyze the decremental proportion that vulnerable HMSNs belonging to set n change into compromised ones. Let φ be the density of all HMSNs with a uniform distribution in the HMWSN, and ϕ_{xy}^n be the probability of HMSNs in set n transforming from $x \in \{V, C, Q, P, S\}$ to $y \in \{V, C, Q, P, S\}$. For a vulnerable HMSN belonging to set n, it is compromised by malware with probability ϕ_{VC}^n when communicating with a compromised HMSN. When an HMSN moves from a point to another, it can communicate with $\varsigma\varphi$ neighbors from (1). Such communications, however, do not necessarily make any neighbor become a compromised HMSN; only a vulnerable neighbor may be compromised. Therefore, there are $\varsigma\varphi V_n^t \cdot \varsigma\varphi\chi_n^t$ vulnerable-compromised pairs for the HMWSN. Further, the number that vulnerable HMSNs belonging to set n are changed into compromised ones is $\phi_{VC}^n \cdot \varsigma\varphi V_n^t \cdot \varsigma\varphi\chi_n^t$; the corresponding proportion is $\phi_{VC}^n \varsigma\varphi V_n^t \chi_n^t$.

We now examine transition proportions among all states from Fig. 1. For vulnerable HMSNs belonging to set n at time t, the incremental proportions of changing from states P and Q are equal to the probability ϕ_{PV}^n times the proportion P_n^t and the probability ϕ_{QV}^n times the proportion Q_n^t, i.e., $\phi_{PV}^n P_n^t$ and $\phi_{QV}^n Q_n^t$, respectively. The decremental proportions of changing into states P and D are equal to the probability ϕ_{VP}^n times the proportion V_n^t and the probability ϕ_{VD}^n times the proportion V_n^t, i.e., $\phi_{VP}^n V_n^t$ and $\phi_{VD}^n V_n^t$, respectively. As a result, the differential proportion of vulnerable HMSNs belonging to set n at time t, i.e., $\dot{V}_n^t$, is

$$\dot{V}_n^t = \phi_{QV}^n Q_n^t + \phi_{PV}^n P_n^t - \phi_{VC}^n \varsigma\varphi V_n^t \chi_n^t - \phi_{VP}^n V_n^t - \phi_{VS}^n V_n^t. \tag{9}$$

Similarly, we can obtain the differential proportions of compromised, quarantined, patched, and scrapped HMSNs belonging to set n at time t, i.e., $\dot{C}_n^t$, $\dot{Q}_n^t$, $\dot{P}_n^t$, and $\dot{S}_n^t$, are

$$\dot{C}_n^t = \phi_{VC}^n \varsigma\varphi V_n^t \chi_n^t - \phi_{CQ}^n C_n^t - \phi_{CP}^n C_n^t - \phi_{CS}^n C_n^t, \tag{10}$$

$$\dot{Q}_n^t = \phi_{CQ}^n C_n^t - \phi_{QV}^n Q_n^t - \phi_{QP}^n Q_n^t - \phi_{QS}^n Q_n^t, \tag{11}$$

$$\dot{P}_n^t = \alpha + \phi_{VP}^n V_n^t + \phi_{CP}^n C_n^t + \phi_{QP}^n Q_n^t - \phi_{PS}^n P_n^t, \tag{12}$$

and

$$\dot{S}_n^t = \phi_{VS}^n V_n^t + \phi_{CS}^n C_n^t + \phi_{QS}^n Q_n^t + \phi_{PS}^n P_n^t - \alpha, \tag{13}$$

respectively. Thus far, we obtain the heterogeneous and mobile VCQPS model as illustrated in (9)–(13) subject to (2)–(5). Note that we add the proportion α to the proportion P_n^t in (12) and conversely subtract it from the proportion S_n^t in (13), for reflecting the fact that administrates should replace the irreparably scrapped HMSNs with new patched ones to make the HMWSN work normally.

VI. CHARACTERISTICS OF THE HETEROGENEOUS AND MOBILE VCQPS MODEL

A. STATIONARY POINTS

We herein analyze the heterogeneous and mobile VCQPS model and obtain its stationary points, which will be used to compute the malware propagation threshold deciding whether the malware will propagate or dissipate in the HMWSN. From the mathematical view of differential equations, a stationary point of the VCQPS model is the value $(V_n^*, C_n^*, Q_n^*, P_n^*, S_n^*)$ at time t^* such that

$$\forall t > t^*, \quad (V_n^t, C_n^t, Q_n^t, P_n^t, S_n^t) = (V_n^*, C_n^*, Q_n^*, P_n^*, S_n^*). \tag{14}$$

In other words, $(V_n^t, C_n^t, Q_n^t, P_n^t, S_n^t)$ is invariable for all $t > t^*$, upon which we can obtain the following theorem.

Theorem 1: The heterogeneous and mobile VCQPS described by (9)–(13) has stationary points.

Proof: After the VCQPS arrives at its stationary points at time t^*, $(V_n^t, C_n^t, Q_n^t, P_n^t, S_n^t)$ will be invariable. In this manner, the differential proportions of all states are equal to 0 for all $t > t^*$. We can therefore obtain

$$\begin{cases} \phi_{QV}^n Q_n^t + \phi_{PV}^n P_n^t - \phi_{VC}^n \varsigma\varphi V_n^t \chi_n^t - \phi_{VP}^n V_n^t - \phi_{VS}^n V_n^t = 0 \\ \phi_{VC}^n \varsigma\varphi V_n^t \chi_n^t - \phi_{CQ}^n C_n^t - \phi_{CP}^n C_n^t - \phi_{CS}^n C_n^t = 0 \\ \phi_{CQ}^n C_n^t - \phi_{QV}^n Q_n^t - \phi_{QP}^n Q_n^t - \phi_{QS}^n Q_n^t = 0 \\ \alpha + \phi_{VP}^n V_n^t + \phi_{CP}^n C_n^t + \phi_{QP}^n Q_n^t - \phi_{PS}^n P_n^t - \phi_{PV}^n P_n^t = 0 \\ \phi_{VS}^n V_n^t + \phi_{CS}^n C_n^t + \phi_{QS}^n Q_n^t + \phi_{PS}^n P_n^t - \alpha = 0 \end{cases} \tag{15}$$

After solving (15), we can obtain two stationary points Γ^{Fr} and Γ^{En} as

$$\Gamma^{Fr} = (V_n^{Fr}, C_n^{Fr}, Q_n^{Fr}, P_n^{Fr}, S_n^{Fr}) \tag{16}$$

and

$$\Gamma^{En} = (V_n^{En}, C_n^{En}, Q_n^{En}, P_n^{En}, S_n^{En}), \tag{17}$$

respectively. Here,

$$V_n^{Fr} = \frac{\alpha\phi_{PV}^n}{\phi_{VP}^n\phi_{PS}^n + \phi_{VS}^n\phi_{PS}^n + \phi_{VS}^n\phi_{PV}^n}, \tag{18}$$

$$C_n^{Fr} = 0, \tag{19}$$

$$Q_n^{Fr} = 0, \tag{20}$$

$$P_n^{Fr} = \frac{\alpha(\phi_{VS}^n + \phi_{VP}^n)}{\phi_{VP}^n\phi_{PS}^n + \phi_{VS}^n\phi_{PS}^n + \phi_{VS}^n\phi_{PV}^n}, \tag{21}$$

$$\begin{aligned} S_n^{Fr} &= 1 - V_n^{Fr} - C_n^{Fr} - Q_n^{Fr} - P_n^{Fr} \\ &= 1 - \frac{\alpha(\phi_{PV}^n + \phi_{VS}^n + \phi_{VP}^n)}{\phi_{VP}^n\phi_{PS}^n + \phi_{VS}^n\phi_{PS}^n + \phi_{VS}^n\phi_{PV}^n}, \end{aligned} \tag{22}$$

$$V_n^{En} = \frac{\kappa^n}{\eta^n}, \tag{23}$$

$$C_n^{En} = \frac{\iota^n(\alpha\phi_{PV}^n\phi_{VC}^n\varsigma\varphi\eta^n - \kappa^n(\phi_{VS}^n\phi_{PV}^n + \phi_{PS}^n(\phi_{VP}^n + \phi_{VS}^n)))}{\eta^n(\iota^n\phi_{CS}^n\phi_{PV}^n + \phi_{QS}^n\phi_{CQ}^n\phi_{PV}^n + \kappa^n\iota^n\phi_{PS}^n - \phi_{QV}^n\phi_{CQ}^n\phi_{PS}^n)}, \tag{24}$$

$$Q_n^{En} = \frac{\phi_{CQ}^n}{\iota^n}C_n^{En}, \tag{25}$$

$$P_n^{En} = \frac{\alpha}{\phi_{PS}^n} - \frac{\kappa^n\phi_{VS}^n}{\phi_{PS}^n\eta^n} - \frac{\iota^n\phi_{CS}^n + \phi_{QS}^n\phi_{CQ}^n}{\iota^n\phi_{PS}^n}C_n^{En}, \tag{26}$$

and

$$S_n^{En} = 1 - V_n^{En} - C_n^{En} - Q_n^{En} - P_n^{En}, \tag{27}$$

where

$$\kappa^n = \phi_{CQ}^n + \phi_{CP}^n + \phi_{CS}^n, \tag{28}$$

$$\iota^n = \phi_{QV}^n + \phi_{QP}^n + \phi_{QS}^n, \tag{29}$$

and

$$\eta^n = \frac{\phi_{VC}^n\varsigma\varphi}{< d >}\sum_{n=1}^{N}\delta_n\varepsilon_n. \tag{30}$$

Thus, the proof is completed. □

Note that the stationary points obtained by Theorem 1 have different practical meanings. We call Γ^{Fr} be the malware-free stationary-point indicating malware disappearance from the HMWSN, since the proportion C_n^{Fr} is equal to 0 after the VCQPS model arrives at Γ^{Fr}. However, Γ^{En} is called by the endemic stationary-point meaning malware propagation in the HMWSN, since the proportion C_n^{En} is larger than 0 after the VCQPS model arrives at Γ^{En}. Therefore, all administrators look forward to the stationary point Γ^{Fr} for the reason that malware in the HMWSN will die out based on continuous security behaviors made by administrators. On the contrary, administrators do their utmost to keep away from the stationary point Γ^{En} for the obvious reason that malware in the HMWSN will propagate and HMSNs with proportion C_n^{En} will be compromised to interrupt the general operation of the HMWSN.

B. MALWARE PROPAGATION THRESHOLD IN HMWSNS

We now pay attention to the malware propagation threshold in HMWSNs, which can instruct administrators to take suitable security behaviors to suppress malware propagation. This threshold provides the condition to judge when malware in the HMWSN can propagate, after it is employed to disclose the dynamics of the VCQPS model. From the view of mathematics, the threshold is acquired by computing the basic generation number, which is equal to the average value of compromised HMSNs converted from the primary HMSNs in state C.

Theorem 2: A malware propagation threshold exists in the HMWSN characterized by the VCQPS model.

Proof: We employ the next-generation matrix method [43] to complete the proof. From this method, the malware propagation threshold μ is equal to "the spectral radius of the next-generation matrix" [43]. In other words, $\mu = \rho(\mathbf{E}_{\Gamma^{Fr}}\mathbf{F}_{\Gamma^{Fr}}^{-1})$, where $\rho(\cdot)$ denotes the spectral radius, $\mathbf{E}_{\Gamma^{Fr}}$ denotes the advent rate matrix of HMSNs in state C at the stationary point Γ^{Fr}, $\mathbf{F}_{\Gamma^{Fr}}$ denotes the transition rate matrix of HMSNs at the stationary point Γ^{Fr}, and $\mathbf{F}_{\Gamma^{Fr}}^{-1}$ denotes the inverse of matrix $\mathbf{F}_{\Gamma^{Fr}}$. Let

$$\tilde{\mathbf{E}} = [e_C] = \left[\phi_{VC}^n\varsigma\varphi V_n^t\chi_n^t\right], \tag{31}$$

and

$$\tilde{\mathbf{F}} = [f_C] = \left[\phi_{CQ}^n C_n^t + \phi_{CP}^n C_n^t + \phi_{CS}^n C_n^t\right], \tag{32}$$

satisfying

$$\tilde{\mathbf{E}} - \tilde{\mathbf{F}} = \left[\phi_{VC}^n\varsigma\varphi V_n^t\chi_n^t - \phi_{CQ}^n C_n^t - \phi_{CP}^n C_n^t - \phi_{CS}^n C_n^t\right] \tag{33}$$

Therefore, we can obtain the advent rate matrix $\mathbf{E}_{\Gamma^{Fr}}$ as

$$\mathbf{E}_{\Gamma^{Fr}} = \left[\frac{\partial e_C}{\partial C_n^t}\right]_{\Gamma^{Fr}} = \left[V_n^{Fr}\eta^n\right], \tag{34}$$

and the transition rate matrix $\mathbf{F}_{\Gamma^{Fr}}$ as

$$\mathbf{F}_{\Gamma^{Fr}} = \left[\frac{\partial f_C}{\partial C_n^t}\right]_{\Gamma^{Fr}} = \left[\phi_{CQ}^n + \phi_{CP}^n + \phi_{CS}^n\right] = [\kappa^n]. \tag{35}$$

Further, we can obtain the malware propagation threshold μ as

$$\mu = \rho(\mathbf{E}_{\Gamma^{Fr}}\mathbf{F}_{\Gamma^{Fr}}^{-1}) = \frac{V_n^{Fr}\eta^n}{\kappa^n}. \tag{36}$$

Thus, the proof is completed. □

C. STABILITY ANALYSIS OF THE MALWARE-FREE STATIONARY-POINT

Lyapunov stability theory [44] is generally applied to analyze the stability properties of a system consisting of differential equations. In this manner, we adopt the same tool to make stability analysis of the heterogeneous and mobile VCQPS model. There are two most commonly used concepts: *locally asymptotically stable* and *globally asymptotically stable*. A stationary-point ψ^* is judged to be locally asymptotically stable if all solutions of the system that start near ψ^* keep near ψ^* for all time and, moreover, these all solutions tend towards ψ^* as $t \to \infty$. This judgment is usually performed according to all eigenvalues of the characteristic determinant of a Jacobian matrix [45]. Differently, a stationary-point ψ^* is globally

asymptotically stable if it is stable given an arbitrary valid value. The corresponding proof is more difficult to achieve, because the whole process includes how to skillfully define a Lyapunov function and how to prove that the stationary-point ψ^* is globally attractive.

Although the VCQPS model has two stationary points, we only analyze the stability of the malware-free stationary-point. This is because finding what conditions to result in the malware-free stationary-point is practical for securely managing the HMWSN, whereas the endemic stationary-point should be avoided.

Theorem 3: The malware-free stationary-point Γ^{Fr} *is locally asymptotically stable if* $\mu < 1$ *, whereas* Γ^{Fr} *is unstable if* $\mu \geq 1$.

Proof: We can reduce the VCQPS model as four differential equations describing the proportion dynamics of V_n^t, C_n^t, Q_n^t, and P_n^t, since

$$S_n^t = 1 - V_n^t - C_n^t - Q_n^t - P_n^t \tag{37}$$

can be inferred from V_n^t, C_n^t, Q_n^t, and P_n^t.

From "stability theory for ordinary differential equations" [45], the stationary point Γ^{Fr} is locally asymptotically stable if and only if all eigenvalues of the characteristic determinant of $\mathbf{J}(\Gamma^{Fr})$ are less than 0, where $\mathbf{J}(\Gamma^{Fr})$ is the Jacobian matrix of the VCQPS model arriving at Γ^{Fr}. Therefore, we first present the Jacobian matrix $\mathbf{J}$ of the VCQPS model as (38), shown at the bottom of this page. Further, the Jacobian matrix of the VCQPS model arriving at Γ^{Fr} is obtained as

$$\mathbf{J}(\Gamma^{Fr}) = \begin{bmatrix} -\phi_{VP}^n - \phi_{VS}^n & -V_n^{Fr}\eta^n & \phi_{QV}^n & \phi_{PV}^n \\ 0 & V_n^{Fr}\eta^n - \kappa^n & 0 & 0 \\ 0 & \phi_{CQ}^n & -\iota^n & 0 \\ \phi_{VP}^n & \phi_{CP}^n & \phi_{QP}^n & -\phi_{PS}^n - \phi_{PV}^n \end{bmatrix}. \tag{39}$$

We denote ν and $\mathbf{G}$ be the eigenvalue and the identity matrix, respectively. The eigenfunction of matrix $\mathbf{J}(\Gamma^{Fr})$ can be obtained as

$$\begin{aligned} &\left|\nu\mathbf{G} - \mathbf{J}(\Gamma^{Fr})\right| \\ &= \begin{vmatrix} \nu+\phi_{VP}^n+\phi_{VS}^n & V_n^{Fr}\eta^n & -\phi_{QV}^n & -\phi_{PV}^n \\ 0 & \nu - V_n^{Fr}\eta^n+\kappa^n & 0 & 0 \\ 0 & -\phi_{CQ}^n & \nu+\iota^n & 0 \\ -\phi_{VP}^n & -\phi_{CP}^n & -\phi_{QP}^n & \nu+\phi_{PS}^n+\phi_{PV}^n \end{vmatrix} \\ &= (\nu^2 + (\phi_{PS}^n + \phi_{PV}^n + \phi_{VP}^n + \phi_{VS}^n)\nu + \phi_{VP}^n\phi_{PS}^n \\ &\quad +\phi_{VS}^n\phi_{PS}^n + \phi_{VS}^n\phi_{PV}^n) \\ &\quad \cdot(\nu - V_n^{Fr}\eta^n + \kappa^n) \cdot (\nu + \iota^n) \end{aligned} \tag{40}$$

Thus, all eigenvalues can be obtained as

$$\nu_1 = \frac{-\sigma^n + \sqrt{(\sigma^n)^2 - 4(\phi_{VP}^n\phi_{PS}^n + \phi_{VS}^n\phi_{PS}^n + \phi_{VS}^n\phi_{PV}^n)}}{2}, \tag{41}$$

$$\nu_2 = \frac{-\sigma^n - \sqrt{(\sigma^n)^2 - 4(\phi_{VP}^n\phi_{PS}^n + \phi_{VS}^n\phi_{PS}^n + \phi_{VS}^n\phi_{PV}^n)}}{2}, \tag{42}$$

$$\nu_3 = V_n^{Fr}\eta^n - \kappa^n = (\mu - 1)\kappa^n, \tag{43}$$

and

$$\nu_4 = -\iota^n, \tag{44}$$

where

$$\sigma^n = \phi_{PS}^n + \phi_{PV}^n + \phi_{VP}^n + \phi_{VS}^n. \tag{45}$$

Obviously,

$$\nu_1 < \frac{-\sigma^n + \sqrt{(\sigma^n)^2}}{2} = 0, \tag{46}$$

$\nu_2 < 0$, $\nu_3 < 0$ if $\mu < 1$, and $\nu_4 < 0$. As a result, the malware-free stationary-point Γ^{Fr} is locally asymptotically stable if $\mu < 1$, whereas Γ^{Fr} is unstable if $\mu \geq 1$. Thus, the proof is completed. □

Next, we employ a Lyapunov function, which is a continuous real-valued and scalar one, to examine the global stability of stationary points for the heterogeneous and mobile

$$\begin{aligned} \mathbf{J} &= \begin{bmatrix} \frac{\partial \dot{V}_n^t}{\partial V_n^t} & \frac{\partial \dot{V}_n^t}{\partial C_n^t} & \frac{\partial \dot{V}_n^t}{\partial Q_n^t} & \frac{\partial \dot{V}_n^t}{\partial P_n^t} \\ \frac{\partial \dot{C}_n^t}{\partial V_n^t} & \frac{\partial \dot{C}_n^t}{\partial C_n^t} & \frac{\partial \dot{C}_n^t}{\partial Q_n^t} & \frac{\partial \dot{C}_n^t}{\partial P_n^t} \\ \frac{\partial \dot{Q}_n^t}{\partial V_n^t} & \frac{\partial \dot{Q}_n^t}{\partial C_n^t} & \frac{\partial \dot{Q}_n^t}{\partial Q_n^t} & \frac{\partial \dot{Q}_n^t}{\partial P_n^t} \\ \frac{\partial \dot{P}_n^t}{\partial V_n^t} & \frac{\partial \dot{P}_n^t}{\partial C_n^t} & \frac{\partial \dot{P}_n^t}{\partial Q_n^t} & \frac{\partial \dot{P}_n^t}{\partial P_n^t} \end{bmatrix} \\ &= \begin{bmatrix} -\phi_{VC}^n \varsigma\varphi\chi_n^t - \phi_{VP}^n - \phi_{VS}^n & -V_n^t\eta^n & \phi_{QV}^n & \phi_{PV}^n \\ \phi_{VC}^n \varsigma\varphi\chi_n^t & V_n^t\eta^n - \kappa^n & 0 & 0 \\ 0 & \phi_{CQ}^n & -\iota^n & 0 \\ \phi_{VP}^n & \phi_{CP}^n & \phi_{QP}^n & -\phi_{PS}^n - \phi_{PV}^n \end{bmatrix}. \end{aligned} \tag{38}$$

VCQPS model. Generally, the Lyapunov function is with the LaSalle invariant principle [46].

Theorem 4: The malware-free stationary-point Γ^{Fr} is globally asymptotically stable if $\mu < 1$, whereas Γ^{Fr} is unstable if $\mu \geq 1$.

Proof: To deduce the globally asymptotical stability of the malware-free stationary-point Γ^{Fr}, we define a Lyapunov function ζ^t based on (9)–(13) as

$$\zeta^t = \sum_{n=1}^{N} \frac{\delta_n \varepsilon_n C_n^t}{\kappa^n}. \tag{47}$$

Therefore, the time derivative of the Lyapunov function ζ^t along the solutions of the VCQPS model is

$$\begin{aligned}
\dot{\zeta}^t &= \sum_{n=1}^{N} \frac{\delta_n \varepsilon_n \dot{C}_n^t}{\kappa^n} \\
&= \sum_{n=1}^{N} \frac{\delta_n \varepsilon_n (\phi_{VC}^n \varsigma \varphi V_n^t \chi_n^t - \phi_{CQ}^n C_n^t - \phi_{CP}^n C_n^t - \phi_{CS}^n C_n^t)}{\kappa^n} \\
&= \sum_{n=1}^{N} \frac{\delta_n \varepsilon_n \phi_{VC}^n \varsigma \varphi V_n^t \chi_n^t}{\kappa^n} - \sum_{n=1}^{N} \delta_n \varepsilon_n C_n^t \\
&= \chi_n^t < d > \left(\sum_{n=1}^{N} \frac{\delta_n \varepsilon_n \phi_{VC}^n \varsigma \varphi V_n^t}{\kappa^n < d >} - 1 \right).
\end{aligned} \tag{48}$$

Further, the derivative $\dot{\zeta}^t$ at the stationary point Γ^{Fr} is

$$\begin{aligned}
\dot{\zeta}_{\Gamma^{Fr}}^t &= \chi_n^t < d > \left(\sum_{n=1}^{N} \frac{\delta_n \varepsilon_n \phi_{VC}^n \varsigma \varphi V_n^{Fr}}{\kappa^n < d >} - 1 \right) \\
&= \chi_n^t \langle d \rangle \left(\frac{V_n^{Fr} \eta^n}{\kappa^n} - 1 \right) \\
&= \chi_n^t \langle d \rangle (\mu - 1),
\end{aligned} \tag{49}$$

which satisfies $\dot{\zeta}_{\Gamma^{Fr}}^t \leq 0$ if $\mu < 1$. In this way, if $\mu < 1$, $\chi_n^t = 0$ so that $\dot{\zeta}_{\Gamma^{Fr}}^t = 0$. Because $\delta_n > 0$ and $\varepsilon_n > 0$ for all $n = 1, 2, \cdots, N$, we obtain

$$\lim_{t \to \infty} C_n^t = 0. \tag{50}$$

Consequently, we obtain

$$\lim_{t \to \infty} Q_n^t = 0, \tag{51}$$

$$\lim_{t \to \infty} V_n^t = \frac{\alpha \phi_{PV}^n}{\phi_{VP}^n \phi_{PS}^n + \phi_{VS}^n \phi_{PS}^n + \phi_{VS}^n \phi_{PV}^n}, \tag{52}$$

$$\lim_{t \to \infty} P_n^t = \frac{\alpha (\phi_{VS}^n + \phi_{VP}^n)}{\phi_{VP}^n \phi_{PS}^n + \phi_{VS}^n \phi_{PS}^n + \phi_{VS}^n \phi_{PV}^n}, \tag{53}$$

and

$$\lim_{t \to \infty} S_n^t = 1 - \frac{\alpha (\phi_{PV}^n + \phi_{VS}^n + \phi_{VP}^n)}{\phi_{VP}^n \phi_{PS}^n + \phi_{VS}^n \phi_{PS}^n + \phi_{VS}^n \phi_{PV}^n}. \tag{54}$$

Therefore, the malware-free stationary-point Γ^{Fr} is globally attractive for the VCQPS model if $\mu < 1$. From Theorem 3 that the malware-free stationary-point Γ^{Fr} is locally asymptotically stable if $\mu < 1$, we have that the malware-free stationary-point Γ^{Fr} is globally asymptotically stable if $\mu < 1$; whereas Γ^{Fr} is unstable if $\mu \geq 1$. Thus, the proof is completed. □

From Theorems 3 and 4, we conclude that if $\mu < 1$, the proportions of HMSNs belonging to set n in states V, C, Q, P, and S will eventually converge to V_n^{Fr}, 0, 0, P_n^{Fr}, and S_n^{Fr}, respectively. That is, malware in the MHWSN will fade as long as administrators take security behaviors to make the MHWSN parameters achieve the condition $\mu < 1$, no matter what proportion of HMSNs belonging to set n in state C is initialized. This case should be pursued by administrators in practice for suppressing the malware propagation in the HMWSN.

VII. EXPERIMENTAL VALIDATION FOR THE VCQPS MODEL

Here, we simulate the heterogeneous and mobile VCQPS model via MATLAB R2018a. We further validate the stability of the malware-free stationary-point from Theorem 3 when the malware propagation threshold in an HMWSN $\mu < 1$ and $\mu \geq 1$, respectively. We also show the effectiveness of the VCQPS model by comparing our model with traditional SIS and SIR models.

We set simulation parameters for the VCQPS model as follows. The topology of the HMWSN that has 2,000 HMSNs is referred to [47], where the minimum degree (communication connectivity), the maximum degree, and the mean degree are 2, 20, and 4, respectively. Moreover, the propagation ability of a compromised HMSN, ε_n, is referred as $\varepsilon_n = \zeta n^\theta / (1 + \psi n^\theta)$ [48], where $\zeta = 5$, $\theta = 0.5$, and $\psi = 1$. In addition, the interval time of the HMWSN changing from one state to the next is 1 d.

A. VALIDATION FOR STABILITY OF THE MALWARE-FREE STATIONARY-POINT WHEN $\mu < 1$

In this instance, we set the probabilities of HMSNs in set n transforming from $x \in \{V, C, Q, P, S\}$ to $y \in \{V, C, Q, P, S\}$ based on the characteristics of HMSNs, as illustrated in Table 1. As a result, the malware propagation threshold satisfies $\mu < 1$ from (36).

As illustrated in Figs. 3–7, we show, when $\mu < 1$, the changeable proportions of HMSNs belonging to set n in states V, C, Q, P, and S, respectively. Fig. 3 presents that the proportions of HMSNs in state V all keep at ∼90% in the beginning ∼13 d, as the mean moving velocity of HMSNs changes from 0.1 to 1. These proportions then quickly descend to ∼2.55% that is approximately equal to V_n^{Fr} from (18), after ∼20 d. From Fig. 4, the proportions of compromised HMSNs all keep at ∼10% in the beginning ∼13 d. These proportions then quickly ascend to their maximum values, ∼77.99%, ∼78.15%, ∼78.31%, ∼78.46%, ∼78.62%, ∼78.77%, and ∼78.91% for mean moving velocities (unit m/s) $\upsilon = 0.1$, $\upsilon = 0.25$, $\upsilon = 0.4$, $\upsilon = 0.55$, $\upsilon = 0.7$, $\upsilon = 0.85$, and $\upsilon = 1$, respectively. Afterwards, all of these proportions slowly descend and tend to 0 that is the same value as C_n^{Fr} from (19). From Fig. 5, the proportions of quarantined HMSNs all keep at 0 in the beginning ∼13 d.

TABLE 1. Probabilities of HMSN state transformation.

Name	Description	Value
ϕ^n_{VC}	Probability of HMSNs in set n transforming from state V to C	0.3
ϕ^n_{VP}	Probability of HMSNs in set n transforming from state V to P	0.15
ϕ^n_{VS}	Probability of HMSNs in set n transforming from state V to S	0.0125
ϕ^n_{CQ}	Probability of HMSNs in set n transforming from state C to Q	0.1
ϕ^n_{CP}	Probability of HMSNs in set n transforming from state C to P	0.25
ϕ^n_{CS}	Probability of HMSNs in set n transforming from state C to S	0.05
ϕ^n_{QV}	Probability of HMSNs in set n transforming from state Q to V	0.005
ϕ^n_{QP}	Probability of HMSNs in set n transforming from state Q to P	0.25
ϕ^n_{QS}	Probability of HMSNs in set n transforming from state Q to S	0.0125
ϕ^n_{PV}	Probability of HMSNs in set n transforming from state P to V	0.005
ϕ^n_{PS}	Probability of HMSNs in set n transforming from state P to S	0.0125

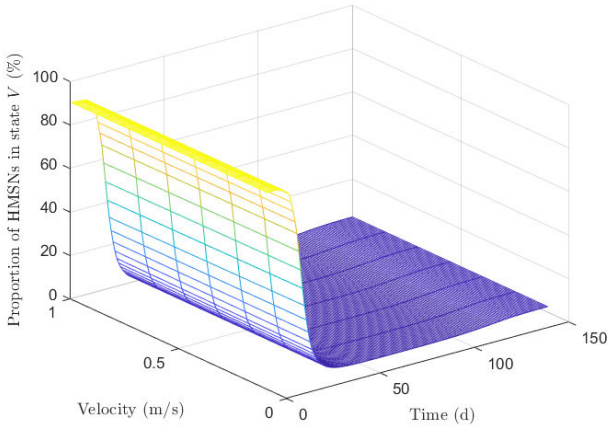


FIGURE 3. Proportion of HMSNs in state *V* according to velocity and time when $\mu < 1$.

These proportions then slowly ascend to their maximum value ∼10.63%, after ∼70 d. All of these proportions then slowly tend to 0 that is the same value as Q_n^{Fr} from (20), after ∼55 d. From Fig. 6, the proportions of currently secure HMSNs all keep at 0 in the beginning ∼13 d, then slowly ascend and finally tend to ∼83.83% that is approximately equal to P_n^{Fr} from (21). From Fig. 7, the proportion tendencies of the scrapped HMSNs are similar to those of HMSNs in state P. Nevertheless, these proportions in Fig. 7 finally tend to ∼13.61% that is approximately equal to S_n^{Fr} from (VI-A).

We can conclude that, from the above analyses, proportions of HMSNs belonging to set n in states V, C, Q, P, and S nearly tend to V_n^{Fr}, C_n^{Fr}, Q_n^{Fr}, P_n^{Fr}, and S_n^{Fr}, respectively, in spite of the different moving velocities of HMSNs. This conclusion has validated that the VCQPS model has the stationary point Γ^{Fr}, and that the malware-free stationary-point

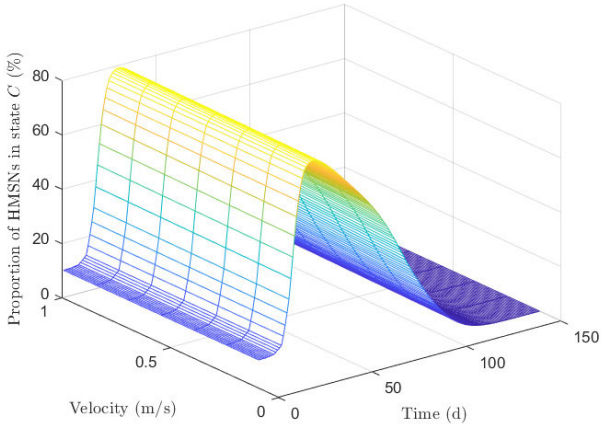


FIGURE 4. Proportion of HMSNs in state *C* according to velocity and time when $\mu < 1$.

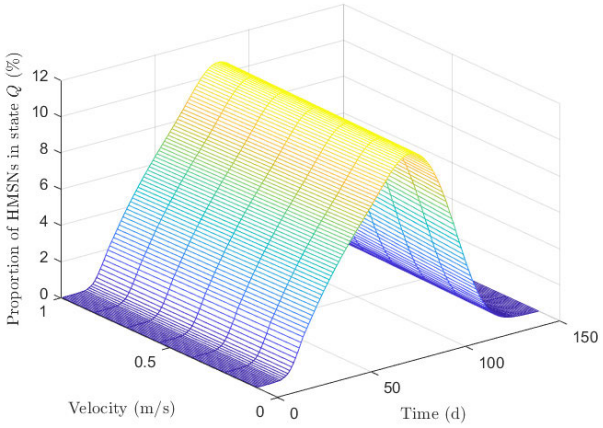


FIGURE 5. Proportion of HMSNs in state *Q* according to velocity and time when $\mu < 1$.

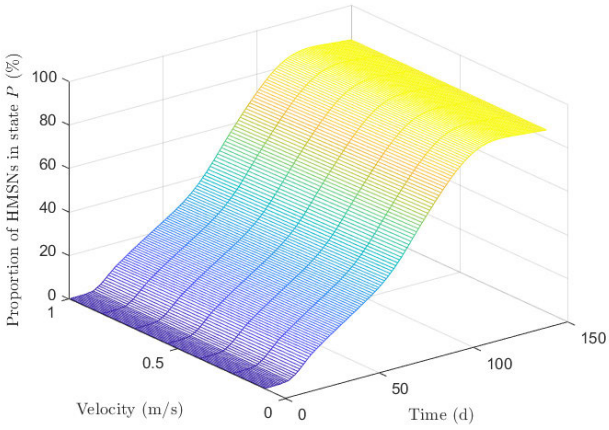


FIGURE 6. Proportion of HMSNs in state *P* according to velocity and time when $\mu < 1$.

of the heterogeneous and mobile VCQPS model is locally asymptotically stable if the malware propagation threshold satisfies $\mu < 1$. More especially, experimental results show that the proportion of compromised HMSNs finally tends

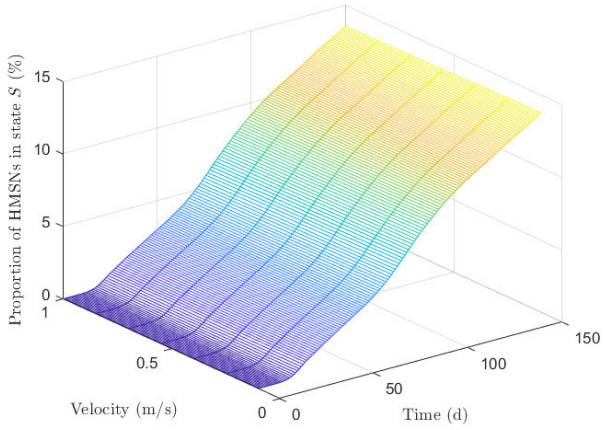


FIGURE 7. Proportion of HMSNs in state *S* according to velocity and time when $\mu < 1$.

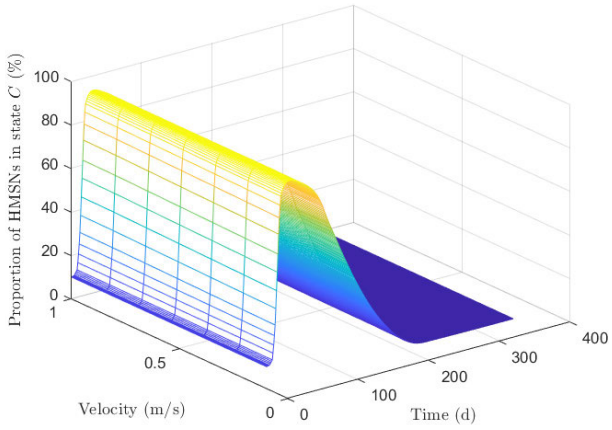


FIGURE 9. Proportion of HMSNs in state *C* according to velocity and time when $\mu \geq 1$.

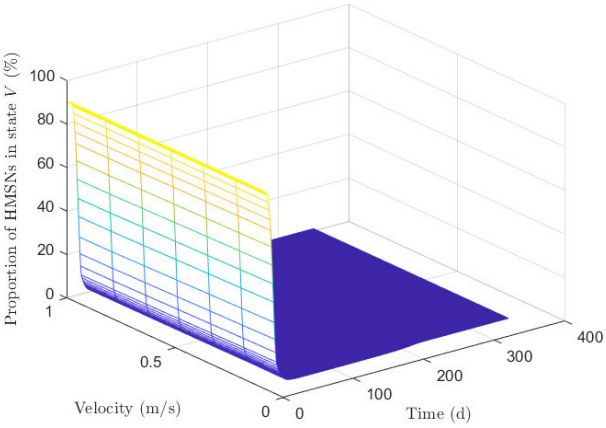


FIGURE 8. Proportion of HMSNs in state *V* according to velocity and time when $\mu \geq 1$.

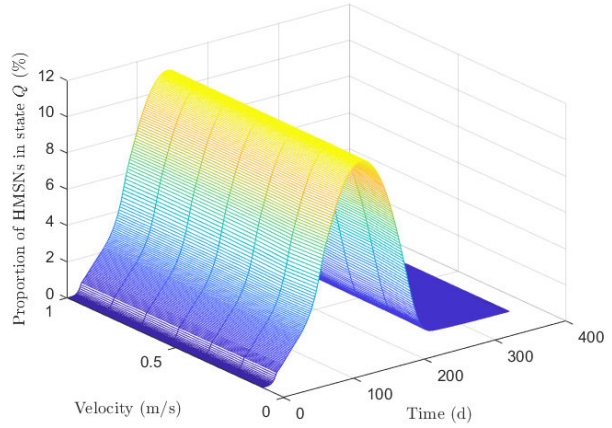


FIGURE 10. Proportion of HMSNs in state *Q* according to velocity and time when $\mu \geq 1$.

to 0, reflecting that the malware in the HMWSN will die out only if administrators continually keep current security measures. We should pursue this circumstance by controlling parameters in (30) so that the malware propagation threshold satisfies $\mu < 1$. Thus, we can restrain the malware propagation in the HMWSN.

B. VALIDATION FOR UNSTABILITY OF THE MALWARE-FREE STATIONARY-POINT WHEN $\mu \geq 1$

In this instance, we set probabilities of HMSN state transformation as those described in Table 1, except for $\phi_{VC}^{n} = 0.6$ and $\phi_{PV}^{n} = 0.01$. In this manner, the malware propagation threshold is approximately equal to 4 from (30), satisfying $\mu \geq 1$.

As illustrated in Figs. 8–12, we show, when $\mu \geq 1$, the changeable tendencies of HMSN proportions in different states. As time evolves, the eventual proportions of HMSNs belonging to set n in states V, C, Q, P, and S when $\mu \geq 1$ are ∼1.12%, ∼1.41%, ∼0.52%, ∼73.59%, and ∼23.36%, respectively. These eventual proportions are approximately equal to V_n^{En}, C_n^{En}, Q_n^{En}, P_n^{En}, and S_n^{En} from (23), (24), (25), (26), and (27), respectively.

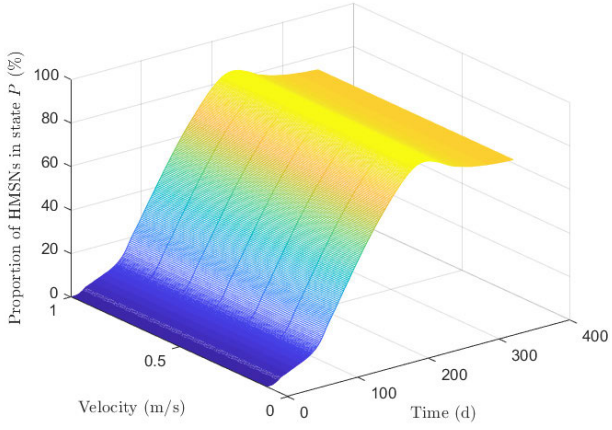


FIGURE 11. Proportion of HMSNs in state *P* according to velocity and time when $\mu \geq 1$.

Therefore, we have validated that the VCQPS model has the stationary point Γ^{En}, and that the malware-free stationary-point of the VCQPS model is unstable if the malware propagation threshold satisfies $\mu \geq 1$. Note that the eventual proportion of compromised HMSNs is more

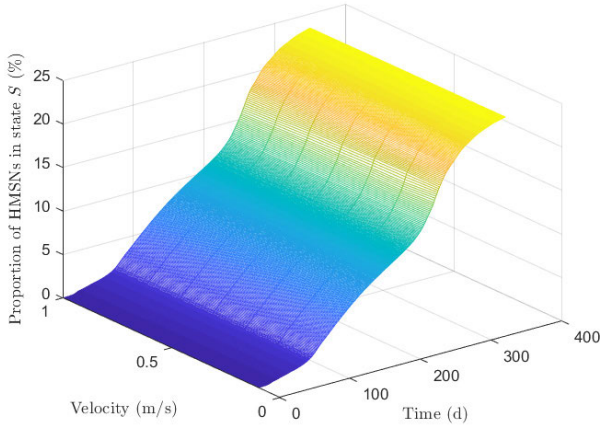


FIGURE 12. Proportion of HMSNs in state *S* according to velocity and time when $\mu \geq 1$.

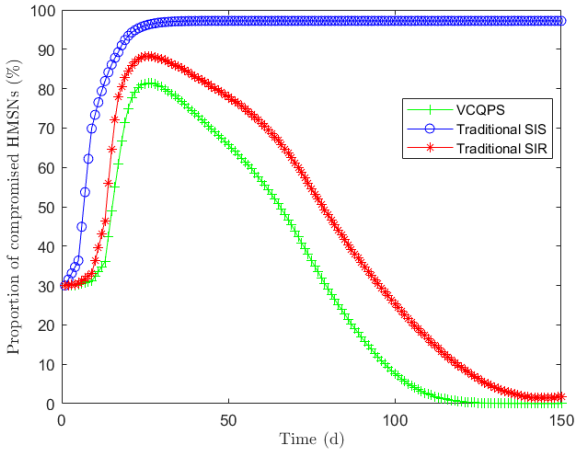


FIGURE 13. Comparison among the VCQPS, SIS, and SIR models according to the proportion of compromised HMSNs, when $\mu < 1$.

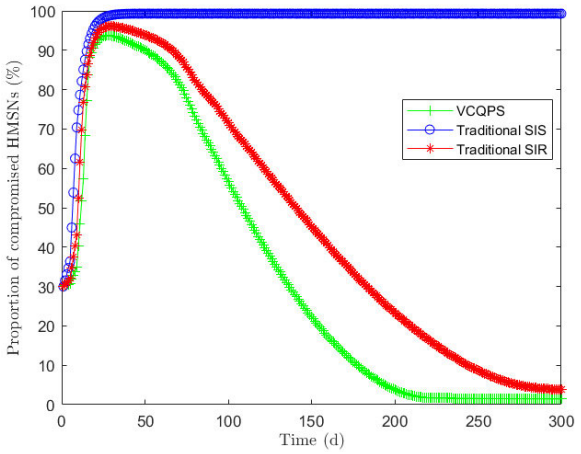


FIGURE 14. Comparison among the VCQPS, SIS, and SIR models according to the proportion of compromised HMSNs, when $\mu \geq 1$.

than 0, reflecting that the malware will propagate around the HMWSN. Moreover, the eventual proportion of scrapped HMSNs is more than ∼10%, compared to that in the case $\mu < 1$. This phenomenon is caused by malware propagation making more HMSNs be deliberately destructed. Therefore, an actual strategy adopted by administrators is to control parameters in (30) and guarantee that the malware propagation threshold does not satisfy $\mu \geq 1$. In this manner, the malware propagation in the HMWSN can be effectively constrained and thus the HMWSN can serve normally.

C. COMPARISON WITH TRADITIONAL MODELS

In order to show the effectiveness of the heterogeneous and mobile VCQPS model, we herein compare and contrast our model with the traditional and typical models—SIS and SIR. We still contemplate the same two conditions—$\mu < 1$ and $\mu \geq 1$—as those in Sections VII.A and VII.B. We perform experiments of all models with the same proportion values and network environment under the same condition. Moreover, we employ the proportion of compromised HMSNs as the comparative indicator, since the changeable proportion trend of the compromised HMSNs can obviously characterize the effectiveness of different models based on epidemic theory.

As illustrated in Figs. 13 and 14, we give the comparative results of three models based on epidemic theory under conditions $\mu < 1$ and $\mu \geq 1$, respectively. We here set the initial proportion of compromised HMSNs at 30% in order to more clearly observe the comparative results. From Fig. 13, the proportion of compromised HMSNs, achieved by the VCQPS model, quickly ascends to the maximum value ∼81.45%, and then slowly descends to 0 as the final value. The changeable proportion from the SIR model is similar to that from the VCQPS model; however, its maximum and final values are respectively ∼88.23% and ∼1.74%, both of which are more than those of the VCQPS model. This experimental result indicates the effectiveness of our model is more than that of the traditional SIR model under condition $\mu < 1$. Moreover, the effectiveness of the traditional SIS model under condition $\mu < 1$ is worst, since the final proportion value stabilizes ∼97.2% meaning that the malware will largely propagate over the HMWSN. Under condition $\mu \geq 1$ in Fig. 14, the proportions of compromised HMSNs, achieved by the VCQPS, SIR, and SIS models, approximately tend to ∼1.43%, ∼3.85%, ∼99.3%, respectively. This experimental result indicates that the malware in the HMWSN can be constrained at minimum level via the VCQPS model. As a result, the effectiveness of the heterogeneous and mobile VCQPS model is obviously most than the SIR and SIS models.

VIII. CONCLUSION

Motivated by the requirement to defend malware, we have proposed a heterogeneous and mobile vulnerable-compromised-quarantined-patched-scrapped (VCQPS) model to disclose dynamics of malware propagation in HMWSNs. This model considers both the heterogeneity and mobility of HMSNs, and reflects the characteristic of HMSN quarantine. We have derived differential equations of transition proportions among all states, which are able to indicate the changeable quantities of HMSNs belonging to different states. Further, we have proven the existence of the stationary

points of the VCQPS model, and achieved the malware propagation threshold that can make us deduce the condition to judge when malware in the HMWSN can propagate. We have also proven the stability of the malware-free stationary-point, which is able to acknowledge what condition administrators should pursue. We have finally performed experiments and compared to the traditional epidemiology-based models to validate the effectiveness of our model. Our theoretical contributions and results can instruct administrators to take suitable security behaviors to suppress malware propagation in HMWSNs.

Although this paper have addressed the issue on how to disclose the dynamics of malware propagation in HMWSNs, there are still a lot of further issues to be done in the future. One interesting issue is how to study the most efficient control strategies such as node immunity optimization, rate adjustment by optimally increasing (or decreasing) the recovery (or infection) rate, and topology optimization by optimally removing specific nodes and links. This constructs our future work to control the dynamics of malware propagation in HMWSNs.

REFERENCES

[1] S. M. Mohamed, H. S. Hamza, and I. A. Saroit, "Coverage in mobile wireless sensor networks (M-WSN): A survey," *Comput. Commun.*, vol. 110, pp. 133–150, Sep. 2017.

[2] Y.-G. Yue and P. He, "A comprehensive survey on the reliability of mobile wireless sensor networks: Taxonomy, challenges, and future directions," *Inf. Fusion*, vol. 44, pp. 188–204, Nov. 2018.

[3] L. Xiao, Y. Li, X. Huang, and X. Du, "Cloud-based malware detection game for mobile devices with offloading," *IEEE Trans. Mobile Comput.*, vol. 16, no. 10, pp. 2742–2750, Oct. 2017.

[4] J. Liu, S. Shen, G. Yue, R. Han, and H. Li, "A stochastic evolutionary coalition game model of secure and dependable virtual service in sensor-cloud," *Appl. Soft Comput.*, vol. 30, pp. 123–135, May 2015.

[5] S. Yu, G. Wang, and W. Zhou, "Modeling malicious activities in cyber space," *IEEE Netw.*, vol. 29, no. 6, pp. 83–87, Nov. 2015.

[6] S. Shen, K. Hu, L. Huang, H. Li, R. Han, and Q. Cao, "Optimal report strategies for WBANs using a cloud-assisted IDS," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 11, Jan. 2015, Art. no. 184239.

[7] 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.

[8] J. Liu, M. Xu, X. Wang, S. Shen, and M. Li, "A Markov detection tree-based centralized scheme to automatically identify malicious webpages on cloud platforms," *IEEE Access*, vol. 6, pp. 74025–74038, Nov. 2018.

[9] S. Shen, L. Huang, H. Zhou, S. Yu, E. Fan, and Q. Cao, "Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in Fog-Cloud-Based IoT networks," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1043–1054, Apr. 2018.

[10] J. Liu, J. Yu, and S. Shen, "Energy-efficient two-layer cooperative defense scheme to secure sensor-clouds," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 408–420, Feb. 2018.

[11] S. Sharmeen, S. Huda, J. H. Abawajy, W. N. Ismail, and M. M. Hassan, "Malware threats and detection for industrial mobile-IoT networks," *IEEE Access*, vol. 6, pp. 15941–15957, Mar. 2018.

[12] T. Giannetsos, T. Dimitriou, I. Krontiris, and N. R. Prasad, "Arbitrary code injection through self-propagating worms in von neumann architecture devices," *Comput. J.*, vol. 53, no. 10, pp. 1576–1593, Feb. 2010.

[13] Q. Gu, C. Ferguson, and R. Noorani, "A study of self-propagating malpackets in sensor networks: Attacks and defenses," *Comput. Secur.*, vol. 30, no. 1, pp. 13–27, Jan. 2011.

[14] V. P. Illiano and E. C. Lupu, "Detecting malicious data injections in wireless sensor networks: A survey," *ACM Comput. Surv.*, vol. 48, no. 2, Oct. 2015, Art. no. 24.

[15] S. Shen, H. Li, R. Han, A. V. Vasilakos, Y. Wang, and Q. Cao, "Differential game-based strategies for preventing malware propagation in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1962–1973, Nov. 2014.

[16] 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.

[17] S. Shen, L. Huang, J. Liu, A. Champion, S. Yu, and Q. Cao, "Reliability evaluation for clustered WSNs under malware propagation," *Sensors*, vol. 16, no. 6, p. 855, Jun. 2016.

[18] N. R. Zema, E. Natalizio, G. Ruggeri, M. Poss, and A. Molinaro, "MeDrone: On the use of a medical drone to heal a sensor network infected by a malicious epidemic," *Ad Hoc Netw.*, vol. 50, pp. 115–127, Nov. 2016.

[19] T. Wang, Q. Wu, S. Wen, Y. Cai, H. Tian, Y. Chen, and B. Wang, "Propagation modeling and defending of a mobile sensor worm in wireless sensor and actuator networks," *Sensors*, vol. 17, no. 12, p. 139, Jan. 2017.

[20] 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, Dec. 2017.

[21] B. K. Mishra and N. Keshri, "Mathematical model on the transmission of worms in wireless sensor network," *Appl. Math. Model.*, vol. 37, no. 6, pp. 4103–4111, Mar. 2013.

[22] M. Sayad Haghighi, S. Wen, Y. Xiang, B. Quinn, and W. Zhou, "On the race of worms and patches: Modeling the spread of information in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2854–2865, Dec. 2016.

[23] R. K. Upadhyay and S. Kumari, "Bifurcation analysis of an e-epidemic model in wireless sensor network," *Int. J. Comput. Math.*, vol. 95, no. 9, pp. 1775–1805, Jun. 2018.

[24] A. Singh, A. K. Awasthi, K. Singh, and P. K. Srivastava, "Modeling and analysis of worm propagation in wireless sensor networks," *Wireless Pers. Commun.*, vol. 98, no. 3, pp. 2535–2551, Oct. 2018.

[25] X. Wang, W. Ni, K. Zheng, R. P. Liu, and X. Niu, "Virus propagation modeling and convergence analysis in large-scale networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 10, pp. 2241–2254, Oct. 2016.

[26] R. K. Shakya, K. Rana, A. Gaurav, P. Mamoria, and P. K. Srivastava, "Stability analysis of epidemic modeling based on spatial correlation for wireless sensor networks," *Wireless Pers. Commun.*, vol. 108, no. 3, pp. 1363–1377, May 2019.

[27] H. Kang, Y. Yu, B. Bao, X. Fu, and M. Sun, "Spreading dynamics of an SEIR model with delay on scale-free networks," *IEEE Trans. Netw. Sci. Eng.*, to be published. [Online]. Available: https://ieeexplore.ieee.org/document/8423094

[28] S. Xu, W. Lu, and Z. Zhan, "A stochastic model of multivirus dynamics," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 1, pp. 30–45, Jan./Feb. 2012.

[29] D. Tian, C. Liu, Z. Sheng, M. Chen, and Y. Wang, "Analytical model of spread of epidemics in open finite regions," *IEEE Access*, vol. 5, pp. 9673–9681, Apr. 2017.

[30] C. Nowzari, V. M. Preciado, and G. J. Pappas, "Optimal resource allocation for control of networked epidemic models," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 2, pp. 159–169, Jun. 2017.

[31] N. Keshri, A. Gupta, and B. K. Mishra, "Impact of reduced scale free network on wireless sensor network," *Phys. A, Stat. Mech. Appl.*, vol. 463, pp. 236–245, Dec. 2016.

[32] B. Qu and H. Wang, "SIS epidemic spreading with heterogeneous infection rates," *IEEE Trans. Netw. Sci. Eng.*, vol. 4, no. 3, pp. 177–186, Jul.-Sep. 2017.

[33] L. Yang, M. Draief, and X. Yang, "Heterogeneous virus propagation in networks: A theoretical study," *Math. Methods Appl. Sci.*, vol. 40, no. 5, pp. 1396–1413, Jun. 2017.

[34] S. Eshghi, M. H. R. Khouzani, S. Sarkar, and S. S. Venkatesh, "Optimal patching in clustered malware epidemics," *IEEE/ACM Trans. Netw.*, vol. 24, no. 1, pp. 283–298, Feb. 2014.

[35] X. Wang, Z. He, X. Zhao, C. Lin, Y. Pan, and Z. Cai, "Reaction-diffusion modeling of malware propagation in mobile wireless sensor networks," *Sci. China Inf. Sci.*, vol. 56, no. 9, pp. 1–18, Sep. 2013.

[36] X. Wang, Z. He, and L. Zhang, "A pulse immunization model for inhibiting malware propagation in mobile wireless sensor networks," *Chin. J. Electron.*, vol. 23, no. 4, pp. 810–815, Oct. 2014.

[37] L. Zhu, H. Zhao, and X. Wang, "Bifurcation analysis of a delay reaction-diffusion malware propagation model with feedback control," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 22, nos. 1–3, pp. 747–768, May 2015.

[38] M. T. Signes-Pont, A. Cortés-Castillo, H. Mora-Mora, and J. Szymanski, "Modelling the malware propagation in mobile computer devices," *Comput. Secur.*, vol. 79, pp. 80–93, Nov. 2018.
[39] W. Liu, C. Liu, Z. Yang, X. Liu, Y. Zhang, and Z. Wei, "Modeling the propagation of mobile malware on complex networks," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 37, pp. 249–264, Aug. 2016.
[40] 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, Jul. 2019.
[41] 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.
[42] M. Bouaziz and A. Rachedi, "A survey on mobility management protocols in wireless sensor networks based on 6LoWPAN technology," *Comput. Commun.*, vol. 74, pp. 3–15, Jan. 2016.
[43] P. van den Driessche and J. Watmough, "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission," *Math. Biosciences*, vol. 180, nos. 1–2, pp. 29–48, Nov./Dec. 2002.
[44] M. Vidyasagar, *Nonlinear Systems Analysis*. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.
[45] G. Teschl, *Ordinary Differential Equations and Dynamical Systems*. Providence, RI, USA: AMS, 2012.
[46] J. P. LaSalle, *The Stability of Dynamical Systems*. Philadelphia, PA, USA: SIAM, 1976.
[47] C.-H. Li, C.-C. Tsai, and S.-Y. Yang, "Analysis of epidemic spreading of an SIRS model in complex heterogeneous networks," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 4, pp. 1042–1054, Apr. 2014.
[48] G. Zhu, X. Fu, and G. Chen, "Global attractivity of a network-based epidemic SIS model with nonlinear infectivity," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 6, pp. 2588–2594, Jun. 2012.

SHIGEN SHEN (Member, IEEE) received the B.S. degree in fundamental mathematics from Zhejiang Normal University, Jinhua, China, in 1995, the M.S. degree in computer science and technology from Zhejiang University, Hangzhou, China, in 2005, and the Ph.D. degree in pattern recognition and intelligent systems from Donghua University, Shanghai, China, in 2013.

He is currently a Professor with the Department of Computer Science and Engineering, Shaoxing University, Shaoxing, China. His current research interests include the Internet of Things, cyber security, cloud computing, and game theory.

HAIPING ZHOU received the B.S. degree in food science and engineering from Nanchang University, Nanchang, China, in 2001, and the M.S. degree in theoretical physics and the Ph.D. degree in microelectronics and solid-state electronics from Guizhou University, Guiyang, China, in 2006 and 2009, respectively.

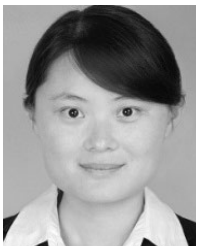
He is currently a Professor with the Department of Computer Science and Engineering, Shaoxing University, Shaoxing, China. His current research interests include complex networks and recommendation algorithm.

SHENG FENG received the B.S. degree in computing from the University of Greenwich, London, England, in 2004, and the M.S. degree in software engineering and the Ph.D. degree in pattern recognition and intelligent system from Northeastern University, Shenyang, China, in 2013 and 2017, respectively.

He is currently a Lecturer with the Department of Computer Science and Engineering, Shaoxing University, Shaoxing, China. His research interests include intelligent robot, computer vision, and wireless sensor networks.

JIANHUA LIU (Member, IEEE) received the B.S. degree in computer science and technology from Xinyang Normal University, Xinyang, China, in 2004, the M.S. degree in computer application technology from Shanghai Normal University, Shanghai, China, in 2008, and the Ph.D. degree in computer application technology from Shanghai University, Shanghai, in 2012.

He was a Visiting Scholar with the State University of New York at Buffalo State, in summer 2014. He is currently an Associate Professor with the Department of Computer Science and Engineering, Shaoxing University, Shaoxing, China. His research interests include distributed computing, wireless communications, multimedia networking, and wireless sensor networks.



HONG ZHANG received the B.S. degree in computer science and technology from Shandong Agricultural University, Tai'an, China, in 2007, and the M.S. degree in computer software and theory from Donghua University, Shanghai, China, in 2010.

She is currently an Experimental Teacher with the College of Computer Science and Technology, Donghua University. Her current research interests include the Internet of Things, cyber security, cloud computing, and game theory.

QIYING CAO received the B.S. degree from Harbin Engineering University, Harbin, China, in 1982, and the M.S. and Ph.D. degrees from Jiangsu University, Zhenjiang, China, in 1993 and 1998, respectively.

From 1999 to 2001, he was a Postdoctoral Researcher with the Chunlan Research Institute, Taizhou, China. He is currently a Professor with the College of Computer Science and Technology, Donghua University, Shanghai, China. His current research interests include pervasive computing and intelligent information processing.