Research Article

Modeling and Control of Malware Propagation in Wireless IoT Networks

Qing Yan, Lipeng Song, Chenlu Zhang, Jing Li, and Shanshan Feng

1School of Data Science and Technology, North University of China, Taiyuan 030051, Shanxi, China
2School of Mechanical, Electrical & Information Engineering, Shan Dong University, Weihai 264209, Shandong, China

Correspondence should be addressed to Lipeng Song; slp880@gmail.com

Received 8 April 2021; Accepted 18 May 2021; Published 15 June 2021

1. Introduction

The smart Internet of Things (IoT), such as intelligent transportation, smart homes, smart grid, and the next industrial revolution (i.e., Industry 4.0), are embedded in billions of wireless devices. Often, wireless devices rely heavily on the wireless connectivity such as WiFi, Bluetooth, and Zigbee [1, 2]. Wireless networks (WNs), as a kind of new information and communication network, connect the physical systems to cyber worlds. In addition, WNs have gained widespread application in IoT including healthcare, public safety, agriculture, and retail due to their low power consumption, flexible networking, unlimited potential, and relevant other features [3–5].

However, the development of IoT brings a series of new challenges to cyber security. On the one hand, the low cost and short time-to-market nature of wireless IoT devices make them, such as sensors, actuators and smart appliances, expose to a high risk of malware infiltration. In addition, most IoT devices are left to operate on consumer premises without regular maintenance. On the other hand, the majority of wireless IoT devices are installed and controlled by consumers with limited security background. Even consumers may be willing to accept to install certain processes or applications on their devices in exchange for incentives without realizing the fact that this may cause attack [6]. In reality, there are hundreds of malware attacks against IoT that occur every year around the world, and each incident affects production and economy greatly.

Malware (Trojan, virus, and worms) is an intrusive software. It is designed for a variety of criminal and hostile activities such as spying, threatening for monetary benefit, or controlling a large population of devices [7]. The academic research focuses on the spread of malware from the following perspectives: detection technology and mathematical modeling [8–12]. Based on multidimensional hybrid features extraction and analysis, Li and Xu [8] proposed a novel method to detect Android malware. In [9], Du and Liu proposed a packet-based malicious...
payload detection and identification algorithm using the deep learning method. However, the above method to detect the malware cannot predict malware spread scale and explore the key factors affecting the spread of malware. In the wireless IoT network, malware hostile activities naturally extend to physical threats and can be launched by one wireless device and spread to another device [13]. Propagation vectors such as services or functions may be used to propagate malware due to different vulnerabilities that emerge across different technologies such as IoT or IPv6 and the lack of experience in technical implementation. As a result, the propagation process is difficult to detect and observe. Based on our understanding of the technology and experience with historic attacks, modeling approaches are used to predict propagation dynamics and to explore influential factors [14–19]. Recently, Chen and Cheng [20] proposed a novel propagation dynamics and to explore influential factors historic attacks, modeling approaches are used to predict understanding of the technology and experience with the process is difficult to detect and observe. Based on our knowledge, this is the first work for disclosing dynamics of malware propagation in the wireless IoT network.

Motivated by the abovementioned research, we propose a Heterogeneous Susceptible-Exposed-Infected-Recovered (HSEIR) model, which characterizes the influence of infected wireless devices’ heterogeneity in malware spreading. In our model, a node is a wireless IoT device. And the ability of wireless devices to spread the malware spreading.

In this section, we describe the novel HSEIR model, which considers the heterogeneity of infected wireless devices in malware spreading.

2. The HSEIR Model

2.1. The States and State Transitions in HSEIR Model. In our model, we assume that the proportion of wireless devices infected by the nodes with weak spreading capabilities is \( \alpha \) and the proportion of wireless devices infected by the nodes with strong spreading capabilities is \( 1 - \alpha \). The total device population \( N \) is divided into four different compartments (susceptible (S), exposed (E), infected (I), and recovered (R)). Every device may be in one of such compartments at time tick \( t \).

(i) S: the wireless devices in this compartment have not been infected by malware, but they are vulnerable to malware \( M \)

(ii) E: the wireless devices in this compartment are exposed to the attacks but do not exhibit due to the latent time requirement

(iii) I: the wireless devices in this compartment are infected and may infect other devices

(iv) R: the wireless devices in this compartment are vaccinated and are immune to \( M \)

We make the following assumptions:

(1) Once the wireless devices are vaccinated, they will be permanently immune and cannot be infected by \( M \) any more

(2) The nature death rate is extremely small. In reality, the service life of the wireless device is far more than the time from malware appearance to the end of the attack

At time \( t = 0 \), all nodes are in the susceptible compartment. Once the malware M intrudes into the system, a node may move from one state to another, as shown in Figure 1, which illustrates the state transition diagram of a node. Table 1 shows the parameters involved in this paper. The nodes changing their states upon the following rules:
Due to the partial efficiency of the vaccine, there is only $\eta$ fraction of the vaccinated susceptible nodes that move to $R$ state per unit time.

The remaining susceptible devices move to the exposed state, and the new exposed devices at time $t$ are given by the expression $a\beta_1 I(t)S(t) + (1 - a)\beta_2 I(t)S(t)$, where $\beta_1$ and $\beta_2$ stand for the transmission coefficient of devices with weak spreading capability and strong capability and $a$ and $1 - a$ represent the fraction of susceptible devices targeted by devices with weak spreading capability and strong capability, respectively.

The exposed devices transit into $I$ with $\gamma$ when the malware begins actively, where $\gamma$ is the mean latent period.

Using some sufficient defense mechanisms, a portion of the exposed, infectious devices can recover at rates $\delta$ and $\phi$, respectively:

\[
\begin{align*}
\frac{dS}{dt} &= \Lambda - [a\beta_1 I + (1 - a)\beta_2 I]S - \eta S - dS, \\
\frac{dE}{dt} &= [a\beta_1 I + (1 - a)\beta_2 I]S - \gamma E - \delta E - dE, \\
\frac{dI}{dt} &= \gamma E - \phi I - dI - \theta I, \\
\frac{dR}{dt} &= \eta S + \delta E + \phi I - dR.
\end{align*}
\]

**3. Model Analysis**

In this section, we firstly calculate the malware-free, malware-existence equilibria and the basic reproduction number of the HSEIR model. Then, we proof the local and global stability of each equilibria.

**3.1. Equilibria and Basic Reproduction Number.**

Summing the right hand of (1), we have

\[
d(S + E + I + R) = \frac{dN}{dt} = \Lambda - dN - \theta I \leq \Lambda - dN,
\]

and after a simple computation, we have

\[
N(t) \leq \frac{\Lambda}{d} + \left(\frac{N(0) - \Lambda}{\Lambda}\right)e^{-dt}.
\]

Then, we have

\[
\limsup_{t \to \infty} N(t) \to \frac{\Lambda}{d}.
\]

One can verify that the positive cone $\mathbb{R}_+^4$:

\[
\Omega = \left\{ (S, E, I, R) \in \mathbb{R}_+^4 | 0 \leq S + E + I + R \leq \frac{\Lambda}{d} \right\}.
\]

Denote that the region $\Omega$ is the positively invariant of system (1).

Next, we calculate the basic reproduction number $R_0$ by the method of van den Driessche and Watmough [24]. $R_0$ is a threshold value of the epidemiological model, which indicates the number of wireless IoT devices infected by an infectious device during its average period of illness at the beginning of the disease, when all are susceptible. It is easy to obtain that system (1) always has a malware-free equilibrium $P_0 = (S_0, E_0, I_0, R_0) = ((\Lambda/d + \eta), 0, 0, (\Lambda \eta/d + \eta))$, and the associated next generation matrices are given by $R_0$:

\[
F = \left( \begin{array}{ccc}
0 & \frac{\Lambda}{d + \eta} [a\beta_1 + (1 - a)\beta_2] \\
0 & 0
\end{array} \right),
\]

\[
V = \left( \begin{array}{ccc}
\gamma + \delta + d & 0 \\
-\gamma & \phi + d
\end{array} \right).
\]

Then, the basic reproduction number $R_0$ of the system is as:

\[
R_0 = \rho(FV^{-1}) = \frac{\Lambda \gamma (a\beta_1 + (1 - a)\beta_2)}{(d + \eta)(\gamma + \delta + d)(d + \phi + \theta)}.
\]

It can be seen that system (1) has a malware-existence equilibrium $P^* = (S^*, E^*, I^*, R^*)$ in $\Omega$ if $R_0 > 1$, which satisfies that

\[
\begin{align*}
S^* &= \frac{\Lambda}{(a\beta_1 + \beta_2 - a\beta_2)}}{I^* + (d + \eta)}, \\
E^* &= \frac{d + \phi + \theta}{\gamma} I^*, \\
I^* &= \frac{(R_0 - 1)(d + \eta)}{(a\beta_1 + \beta_2 - a\beta_2)} I^*, \\
R^* &= \frac{\delta E^* + \phi I^* + \eta S^*}{d}.
\end{align*}
\]
Table 1: Nations and parameter values in the model.

<table>
<thead>
<tr>
<th>Nation</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>N(t)</td>
<td>Total number of wireless device at time t</td>
</tr>
<tr>
<td>S(t)</td>
<td>Number of susceptible devices at time t</td>
</tr>
<tr>
<td>E(t)</td>
<td>Number of exposed devices at time t</td>
</tr>
<tr>
<td>I(t)</td>
<td>Number of infected devices at time t</td>
</tr>
<tr>
<td>R(t)</td>
<td>Number of secured devices at time t</td>
</tr>
<tr>
<td>a</td>
<td>The proportion of wireless devices infected by weak spreading capabilities nodes</td>
</tr>
<tr>
<td>1−a</td>
<td>The proportion of wireless devices infected by strong spreading capabilities nodes</td>
</tr>
<tr>
<td>β₁</td>
<td>Infection rate of devices with weak spreading capabilities</td>
</tr>
<tr>
<td>β₂</td>
<td>Infection rate of devices with strong spreading capabilities</td>
</tr>
<tr>
<td>Λ</td>
<td>The recruitment rate</td>
</tr>
<tr>
<td>δ</td>
<td>State transition rate from E to I</td>
</tr>
<tr>
<td>φ</td>
<td>State transition rate from I to R</td>
</tr>
<tr>
<td>η</td>
<td>State transition rate from S to R</td>
</tr>
<tr>
<td>θ</td>
<td>Malware-related death rate</td>
</tr>
</tbody>
</table>

3.2. Stability of Equilibrium

Let $N(t)$, $S(t)$, $E(t)$, $I(t)$, and $R(t)$ be the number of infected, susceptible, exposed, infected, and secured devices at time $t$, respectively. The infection dynamics of these devices can be modelled as:

$$
\begin{align*}
\frac{dN}{dt} &= \Lambda - \beta_1 N S - \theta N R \\
\frac{dS}{dt} &= \beta_1 N S - \delta S E \\
\frac{dE}{dt} &= \delta S E - \gamma E I \\
\frac{dI}{dt} &= \gamma E I - \phi I R \\
\frac{dR}{dt} &= \phi I R - \eta R 
\end{align*}
$$

where $\Lambda$ is the recruitment rate of new devices, $\beta_1$ is the infection rate of devices with weak spreading capabilities, $\theta$ is the malware-related death rate, $\delta$ is the state transition rate from $E$ to $I$, $\gamma$ is the state transition rate from $E$ to $R$, $\phi$ is the state transition rate from $I$ to $R$, $\eta$ is the state transition rate from $S$ to $R$, and $\Lambda$ is the recruitment rate.

The malware-free equilibrium $P_0$ is determined by solving:

$$
\begin{align*}
0 &= \Lambda - \beta_1 N_0 S_0 - \theta N_0 R_0 \\
0 &= \beta_1 N_0 S_0 - \delta S_0 E_0 \\
0 &= \delta S_0 E_0 - \gamma E_0 I_0 \\
0 &= \gamma E_0 I_0 - \phi I_0 R_0 \\
0 &= \phi I_0 R_0 - \eta R_0
\end{align*}
$$

3.2. Stability of Equilibrium

Lemma 1. The malware-free equilibrium $P_0$ of system (1) is locally asymptotically stable if $R_0 < 1$, and unstable if $R_0 > 1$.

Proof. The Jacobian matrix of system (1) at $P_0$ is

$$
J(P_0) = \begin{pmatrix}
-(\eta + d) & 0 & \frac{\Lambda (a\beta_2 - \beta_2 - a\beta_1)}{\eta + d} & 0 \\
0 & -(\gamma + d + \delta) & \frac{\Lambda (a\beta_1 + \beta_2 - a\beta_2)}{\eta + d} & 0 \\
0 & \gamma & -(d + \phi + \theta) & 0 \\
\eta & \delta & -\phi & \lambda - d
\end{pmatrix}
$$

and its characteristic equation is

$$
\det(\lambda I - J(P_0)) = 0
$$

It is clear that (10) has two negative roots $\lambda_1 = -d$ and $\lambda_2 = -(d + \eta)$, and other roots of (10) are determined by the following equation:

$$
(\lambda + d + \phi + \theta)(\lambda + \gamma + \delta + d) - \frac{\Lambda \gamma (a\beta_1 + \beta_2 - a\beta_2)}{\eta + d} = 0. 
$$

If $R_0 < 1$, all roots of (11) have negative real parts, so all roots of (10) have negative real parts. Therefore, the malware-free equilibrium $P_0$ is locally asymptotically stable by the Hurwitz criterion. If $R_0 > 1$, the root of (11) has both positive and negative real parts, so the malware-free equilibrium $P_0$ is unstable. □

Theorem 1. The malware-free equilibrium $P_0$ of (1) is globally asymptotically stable if $R_0 \leq 1$, and unstable if $R_0 > 1$.

Proof. Consider the Lyapunov function as

$$
L = \gamma E + (\gamma + d + \delta)(I).
$$

Then,

$$
L' = \gamma' + (\gamma + d + \delta)I', \\
\leq [\gamma S(a\beta_1 + \beta_2 - a\beta_2) - (\gamma + d + \delta)(\phi + d + \theta)]I, \\
\leq [\gamma S_0(a\beta_1 + \beta_2 - a\beta_2) - (\gamma + d + \delta)(\phi + d + \theta)]I, \\
= (\gamma + d + \delta)(\phi + d + \theta)(R_0 - 1)I.
$$

(13)
Thus, $L' \leq 0$ when $R_0 \leq 1$. The equality is holding if and only if $R_0 = 1$, $E = 0$, and $S = S_0$ or $E = 0$ and $S = S_0$, or $R_0 = 1$ and $S = S_0$. If $R_0 = 1$, $E = 0$, and $S = S_0$, then the only compact invariant subset in the set $L' \leq 0$ is the singleton $P_0$, if $E = 0$ and $S = S_0$, the only compact invariant subset in the set $L' \leq 0$ is also the singleton $P_0$. If $R_0 > 1$, we have $(dL/dt) > 0$. Finally, taking into account $L(E, I) = \gamma E + (\gamma + \delta + d)I$ and LaSalle invariance principle [25], the result follows. This means that the malware will disappear with time varying if the basic reproduction number is less than one.

**Theorem 2.** The malware-existence equilibrium $P^*$ of (1) is globally asymptotically stable if $R_0 > 1$, and unstable if $R_0 < 1$.

**Proof.** For system (1), we consider the following Lyapunov function:

$$V = \gamma \left( S - S^* - \ln \frac{S}{S^*} \right) + \gamma \left( E - E^* - \ln \frac{E}{E^*} \right) + (\gamma + \delta + d) \left( 1 - I^* - \ln \frac{I}{I^*} \right).$$

Then, the derivative of $V$ along solutions of system (1) is

$$V' = \gamma S \left( 1 - \frac{S^*}{S} \right) + \gamma E \left( 1 - \frac{E^*}{E} \right) + (\gamma + \delta + d) \left( 1 - \frac{I^*}{I} \right).$$

By direct calculations, we have that

$$V' = \left[ a\beta_1 + (1 - a)\beta_2 \right] \gamma S^* I^* \left( 1 - \frac{S^*}{S} \right) \left[ 1 - \frac{S E^*}{S^* I^*} \right]$$

$$+ \left[ a\beta_1 + (1 - a)\beta_2 \right] \gamma S^* I^* \left( 1 - \frac{E^*}{E} \right) \left[ \frac{S E^*}{S^* I^*} - \frac{E^*}{E^*} \right]$$

$$+ (\gamma + \delta + d) \gamma E^* \left( 1 - \frac{I^*}{I} \right) \left( \frac{E^*}{E} - \frac{I}{I^*} \right)$$

$$- \gamma (d + \eta) \left( \frac{(S - S^*)^2}{S} \right).$$

Then

$$V' \leq \gamma S^* I^* \left[ a\beta_1 + (1 - a)\beta_2 \right] \left[ \left( 1 - \frac{S^*}{S} + \ln \frac{S^*}{S} \right) + \left( 1 - \frac{I^*}{I} \frac{E^*}{IE^*} + \ln \frac{I^*}{IE^*} \right) + \left( 1 - \frac{SE^*}{S^* I^*} + \frac{SE^*}{S^* I^*} \right) \right].$$

**4. Control Strategy**

In this section, we investigate the control strategy from two aspects. Firstly, an optimal control model has been proposed by Pontryagin’s Minimum Principle. Secondly, we give some control strategies to prevent the malware outbreak from the explicit expression of the malware spreading threshold value.

For the function $f(x) = 1 - x - \ln x$, we know that if $x > 0$, $f(x) \leq 0$, and $x = 1$ leads to $f(x) = 0$. Therefore, we can obtain $V' \leq 0$, and the equality is holding if and only if $S = S^*$, $E = E^*$, $I = I^*$, and $R = R^*$. It means that the largest invariant subset, where $V' = 0$, is $P^*$. By LaSalle’s Invariance Principle [25], $P^*$ is globally asymptotically stable when $R_0 > 1$. This means that the malware will be outbreak if the basic reproduction number is more than one.

**4.1. Optimal Control Strategy Formulation.** We aim to minimize the number of infected devices (including exposed and infected nodes) and the corresponding cost of the strategies during the process of spreading. Four control functions $u_1(t)$, $u_2(t)$, $u_3(t)$, and $u_4(t)$, where $0 \leq u_1(t) \leq 1$. In particular, $u_1(t) = 0$ means no control strategy and $u_1(t) = 1$ means the maximal use of control strategy. The meanings of $u_i(t)$ are shown as follows:

(1) $u_1(t)$ is used to represent the quarantine strategy that aims to reduce the contact between wireless devices with weak spreading capabilities and susceptible devices at time $t$.

(2) $u_1(t)$ is used to represent the quarantine strategy that aims to reduce the contact between wireless devices with strong spreading capabilities and susceptible devices at time $t$. 
(3) $u_4(t)$ is used to represent the vaccination strategy that can improve the immunocompetence of susceptible devices at time $t$

(4) $u_4(t)$ is used to represent the repairing and fixing strategy that can increase the recovery rate of infected wireless devices at time $t$

The transmission dynamics of the optimal control model is formulated as

$$
\begin{aligned}
\frac{dS}{dt} &= \Lambda - (1 - u_1(t))a\beta_1SI - (1 - u_2(t))(1 - a)\beta_2SI - (d + u_3(t))S, \\
\frac{dE}{dt} &= (1 - u_1(t))a\beta_1SI + (1 - u_2(t))(1 - a)\beta_2SI - (\gamma + \delta + d)S, \\
\frac{dI}{dt} &= \gamma E - (\theta + d + u_4(t))I, \\
\frac{dR}{dt} &= \delta E + u_4(t)I + u_3(t)S - dR.
\end{aligned}
$$

\(18\)

(4) The integrand of the objective function, $E + I + (K/2)u_1^2 + (W/2)u_2^2 + (P/2)u_3^2 + (Q/2)u_4^2$, is convex.

(5) There exist constants $c_1 > 0$, $c_2 > 0$, and $l > 1$ such that the integrand of the objective cost functional is convex and satisfied $J(E, I, u_i, t) \geq c_1 (\sum_{i=1}^{4} |u_i|^2)^{l/2} + c_2$

Theorem 3. An optimal control pair $(u_1^*, u_2^*, u_3^*, u_4^*)$ subject to system (18) exists if the following conditions hold:

Proof. By the results of [27], it is easy to check that the set of controls and corresponding state variables exist. By the definition, the control set is bounded and convex. Since optimal control system (18) is bilinear in $u_i$, the right hand side of it satisfies condition 3 by using the boundedness of the solutions. Additionally, the integrand of objective function (19) is convex on the control set $U$. $E + I + (K/2)u_1^2 + (W/2)u_2^2 + (P/2)u_3^2 + (Q/2)u_4^2 \geq c_1 (\sum_{i=1}^{4} |u_i|^2)^{l/2}$ because the state variables are bounded, considering $l = 2$ and $c_1$ and $c_2$ are smaller enough.

In order to find the optimal control solution, we should describe the Lagrangian and Hamiltonian function of control system (18). Let $x = (S, E, I, R)$, and the Lagrangian of the control system is
where $x$ satisfies system (18), there exists an adjoint variable $\lambda_i$, $i = 1, \ldots, 4$, satisfying

\[
\frac{\partial H}{\partial S} = (\lambda_2 - \lambda_4) \left[ (1 - u_i) a \beta_1 I + (1 - u_2) (1 - a) \beta_2 \right] - (d + u_4) \lambda_1 + u_3 \lambda_4,
\]

\[
\frac{\partial H}{\partial E} = 1 - \lambda_2 (d + y + \delta) + \lambda_3 y + \lambda_4 \delta,
\]

\[
\frac{\partial H}{\partial I} = 1 + u_4 \lambda_4 + (\lambda_2 - \lambda_4) S (1 - u_4) \alpha \beta_1 + (1 - u_2) (1 - a) \beta_2 \]

\[
- (\theta + d + u_4) \lambda_3,
\]

\[
\frac{\partial H}{\partial R} = -d \lambda_4.
\]

According to Pontryagin’s Maximum Principle [28], we obtain

\[
\frac{d \lambda}{dr} = \frac{\partial H(x, U, \lambda)}{\partial \lambda},
\]

where $x = (S, E, I, R)$. Hence, the adjoint variable $\lambda_i$, $i = 1, \ldots, 4$, satisfies (23).

Proof. Calculating the partial derivatives of the five states of Hamiltonian function (22), respectively, we have

\[
\frac{\partial H}{\partial S} = (\lambda_2 - \lambda_4) \left[ (1 - u_i) a \beta_1 I + (1 - u_2) (1 - a) \beta_2 \right] - (d + u_4) \lambda_1 + u_3 \lambda_4,
\]

\[
\frac{\partial H}{\partial E} = 1 - \lambda_2 (d + y + \delta) + \lambda_3 y + \lambda_4 \delta,
\]

\[
\frac{\partial H}{\partial I} = 1 + u_4 \lambda_4 + (\lambda_2 - \lambda_4) S (1 - u_4) \alpha \beta_1 + (1 - u_2) (1 - a) \beta_2 \]

\[
- (\theta + d + u_4) \lambda_3,
\]

\[
\frac{\partial H}{\partial R} = -d \lambda_4.
\]
Consider control system (18) with $\lambda_i(T) = 0$. By using the optimal necessary condition, we have

$$\frac{\partial H}{\partial u^*_i} = 0. \quad (29)$$

On the interior of the control set space, we can obtain optimal control pair solution (25).

### 4.2. Control Strategy Based on the Basic Reproductive Number

There is an important epidemiological threshold $R_0$ in the epidemic model. As we discussed in Section 3, the threshold value plays a critical role to control the malware outbreak. Moreover, we obtain the local and global stability of the worm-free equilibrium when $R_0 \leq 1$. Consequently, it is crucial to reduce the value of $R_0$ below 1, as a result of that to design the efficient security countermeasures to prevent malware outbreak.

From equation (19), we obtain $(\partial R_0/\partial \beta_i) > 0$, $(\partial R_0/\partial \beta_2) > 0$, $(\partial R_0/\partial \beta_3) > 0$, $(\partial R_0/\partial \gamma) > 0$, $(\partial R_0/\partial \alpha) < 0$, $(\partial R_0/\partial \delta) < 0$, $(\partial R_0/\partial \phi) < 0$, $(\partial R_0/\partial \theta) < 0$, and $(\partial R_0/\partial \delta) < 0$, which mean that $R_0$ increases as the parameters $\Lambda$, $\gamma$, $\beta_i$, and $\beta_2$ increase or the parameters $a$, $d$, $\delta$, $\theta$, $\phi$, and $\eta$ decrease. Figure 2 further describes the trend of $R_0$ over time with different parameters $\delta$ and $a$. However, the value of $\delta$ and $a$ is usually constant because of the properties of wireless devices. Consequently, we control the following coefficients to make $R_0 < 1$:

(i) To decrease the transmission rate of infectious devices with weak and strong spreading capabilities by increasing the security background of the consumer

(ii) To ensure configuration integrity and wipe out potential malicious software by taking into account an efficient defense mechanism

### 5. Experimental Validation for the HSEIR Model

In this section, we simulate the HSEIR model via MATLAB R2018a. We illustrate the theoretical results for system (1) by numerical simulations. Besides, by Forward-Backward Sweep Method, we obtain the optimal control strategies and show their effectiveness via comparing the trajectories of infected devices with optimal control and without optimal control.

#### 5.1. Stability of Worm-Free and Worm-Existence Equilibrium

In the real world, there are not much data about malware attacks against the IoT wireless network. Following [15, 23], we attempt to choose appropriate parameter values from the Slammer worm. Assume model parameters $\Lambda = 0.75$, $d = 0.001$, $\theta = 0.005$, $\beta_1 = 0.00001$, $\beta_2 = 0.0001$, $\gamma = 0.0004$, $\eta = 0.0006$, $\delta = 0.003$, $a = 0.6$, and $\phi = 0.005$. The initial numbers of susceptible, exposed, infected, and recovered devices are $S(0) = 350$, $E(0) = 80$, $I(0) = 20$, and $R(0) = 300$. By simple computing, we obtain that $R_0 = 0.9801 < 1$, the worm-free equilibrium $P_0 = (468.75, 0, 0, 282.15)$. Thus, by Theorem 1, the malware-free equilibrium is globally asymptotically stable, which means that when the time $t$ goes to infinity, the exposed and infected nodes will approach to 0, while the susceptible and recovered nodes will be 468.75 and 282.15. Figure 3 shows that the stable behavior of malware-free equilibrium when $R_0 = 0.9801 < 1$. From Figure 3, we can see that there only exist susceptible nodes and recovered nodes, in accordance with the conclusion in Theorem 1.

Secondly, we set the infected rate $\beta_1 = 0.0001$ and $\beta_2 = 0.001$, and the other parameters are the same as above. By equations (7) and (8), we obtain that $R_0 = 9.801 > 1$, and the malware-existence equilibrium $E^* = (30.61, 47.83, 84.18, 434.31)$. Besides, by Theorem 2, the malware-existence equilibrium is globally asymptotically stable, which means that when the time $t$ goes to infinity, the number of $S(t)$, $E(t)$, $I(t)$, and $R(t)$ is 47.83, 84.18, 30.61, and 434.31, respectively. Figure 4 shows that the stable behavior of malware-existence equilibrium when $R_0 = 9.801 > 1$. From Figure 4, we can see that infected nodes (including exposed and infectious), as well as susceptible and recovered nodes, persist at the endemic level.

#### 5.2. Sensitivity Analysis of Infected Rate of Heterogeneity Devices

In this section, we do some sensitivity analysis of parameters $a$, $\beta_1$, and $\beta_2$ to observe the malware spreading scale. Firstly, we set $a = 0.2, 0.4, 0.6$, and 0.8, while keeping other parameters the same as those in 5.1. In Figure 5, we can see that when the proportion of wireless devices infected by weak spreading capabilities nodes decreases, that is, the proportion of wireless devices infected by strong spreading capabilities nodes increases, and the speed of malware spreading goes fast, which also causes an increase in the malware spreading scale.

Secondly, we assume 0.0001 as the interval for the infection rate of devices with weak spreading capabilities to compare the malware spreading scale, as shown in Figures 6 and 7. We can see that when $a = 0.2$, parameter $\beta_1$ has little effect on the scale and speed of malware transmission, but when $a = 0.8$, the larger the parameter $\beta_1$, the faster the malware spreading and the larger of the number of infected nodes simultaneously. In Figures 8 and 9, let 0.01 be the interval for the infection rate of devices with strong spreading capabilities. The malware spreading speed as well as the spreading scale are increasing with $\beta_2$ increasing when $a = 0.2$ and $a = 0.8$. Figure 5 shows that when the proportion of wireless devices that infected by strong spreading capability nodes increases, the number of infected wireless devices also increases. When the proportion of wireless devices infected by strong spreading capabilities nodes remains unchanged, the infected rate $\beta_2$ is the main factor in malware spreading. Thus, we must control the proportion of wireless devices with strong spreading capabilities and spread the patch to them as soon as possible.

#### 5.3. Simulation of Optimal Control Strategies

In [29], Lenhart and Workman combined the Runge–Kutta fourth-
order schemes and Forward-Backward Sweep Method to get
the optimal solution. Based on their method, we conduct
some numerical simulations to illustrate the effectiveness of
the optimal control theoretic approach by using a MATLAB
code. Considering the limitation of technology and cost, we
set $u_{1\text{max}} = 0.8$, $u_{2\text{max}} = 0.8$, $u_{3\text{max}} = 0.7$, $u_{4\text{max}} = 0.9$, $K = 0.3$,
$W = 0.6$, $P = 0.4$, and $Q = 0.5$, and the initial numbers and
the other parameters are taken as the same as those in V.A.
As shown in Figure 10, we give the optimal control stra-
gies. We observe that $u_1(t)$ and $u_2(t)$, namely, quarantine
strategies to infected wireless devices with weak spreading
capabilities and strong spreading capabilities, could be re-
duced 3 seconds later from the beginning of the malware
outbreak, which saves much of quarantine costs. (This
conclusion is consistent with the use of wireless IoTdevices
that disconnected from the wireless network for a long time
are not allowed. Equally, after 8 seconds, $u_3(t)$, vaccination
strategy, could be canceled gradually. Different from the
abovementioned control strategies, $u_4(t)$, repairing and
fixing strategy, for example, applying antivirus patches,
would be keep going. In Figures 11 and 12, we illustrate the
trend of the number of exposed devices and infected devices
over time with control and without control, respectively. It is
clear that the exposed devices, as well as the infected devices,
with control are much smaller than those without control,
and we suggest that early control strategies play a significant
role on reducing the number of infected devices remarkably,
which are also cost-effective optimal strategies.

6. Conclusions and Discussion
In this paper, we have proposed a new HSEIR model to
investigate the malware propagation in wireless IoT net-
works, while considering the heterogeneity of infected
wireless IoT devices. According to the ability of wireless
devices on malware spreading, devices are divided into two
different level groups in a fuzzy way. Based on the proposed
model, we obtained the basic reproduction number $R_0$,
moreover, we analyzed the final size of malware propagation
under special cases. Numerical simulations vividly illustrate
the main results of stability analysis for system (1). Our
simulations also show that when the proportion of wireless
devices infected by strong spreading capabilities nodes in-
creases, the malware spreading scale will also increase. In
addition, the proportion of susceptible wireless devices in-
fected by weak spreading capabilities or strong spreading
capabilities devices also affects the malware propagation size.
These results will provide some useful insights on preventing the global spread of malware.

Furthermore, aiming to minimize the costs of control strategy as well as minimize the infected mobile devices, we obtained the optimal control solution by the Forward-Backward Sweep Method. At the beginning of the malware outbreak, the strategies of quarantine and vaccination can effectively control the malware propagation. As for repairing and fixing strategy, it is the essential method to control malware spreading and reduce the death rate due to the malware attack. More numerical results show the effectiveness of the optimal control strategy. Also, the analysis of $R_0$ allows us to give the efficient malware-epidemic control strategies to prevent the malware propagation through IoT wireless networks, including decreasing the transmission rate of infectious devices with weak and strong spreading capabilities by increasing the security background of the consumer and to ensure configuration integrity and wipe out potential malicious software by taking into account an efficient defense mechanism.

Although we have investigated the issue of the heterogeneity of wireless IoT devices in malware spreading, there are still some problems in this paper to be further solved.
Figure 8: Parameter $\beta_2$ at $a = 0.2$.

Figure 9: Parameter $\beta_2$ at $a = 0.8$.

Figure 10: The graph trajectories of four optimal control strategies.
How to determine the transmission capability of the infected wireless devices more accurately is still a question. In this paper, we only divided them into two different level groups in a fuzzy way. It is significant to study the case where there is a limited supply of control strategies at each instant of time.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors’ Contributions

All authors contributed equally to this work.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 61772478.

References


