Research Article

Modeling and Control of Malware Propagation in Wireless IoT Networks

Qing Yan,1 Lipeng Song,2 Chenlu Zhang,1 Jing Li,1 and Shanshan Feng1

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

Academic Editor: Jingyu Feng

Copyright © 2021 Qing Yan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wireless Internet of Things (IoT) devices densely populate our daily life, but also attract many attackers to attack them. In this paper, we propose a new Heterogeneous Susceptible-Exposed-Infected-Recovered (HSEIR) epidemic model to characterize the effect of heterogeneity of infected wireless IoT devices on malware spreading. Based on the proposed model, we obtain the basic reproduction number, which represents the threshold value of diffusion and governs that the malware is diffusion or not. Also, we derive the malware propagation scale under different cases. These analyses provide theoretical guidance for the application of defense techniques. Numerical simulations validated the correctness and effectiveness of theoretical results. Then, by using Pontryagin’s Minimum Principle, optimal control strategy is proposed to seek time-varying cost-effective solutions against malware outbreaks. More numerical results also showed that some control strategies, such as quarantine and vaccination, should be taken at the beginning of the malware outbreak immediately and become less necessary after a certain period. However, the repairing and fixing strategy, for example applying antivirus patches, would be keep on going constantly.

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 ac-
tivities 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
technology and experience with
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
traffic-aware patching scheme to select important inter-
mediate nodes to patch and apply this to the IoT system
with limited patching resources and response time con-
straint. On the basis of the difference of intelligent device’s
dissemination capacity and discriminant ability, Li and
Cui [21] discussed a dynamic malware propagation model
to study the malware propagation in industrial Internet of
Things. Considering both the heterogeneity and mobility
of sensor nodes, Shen and Zhou [22] proposed a heter-
ogeneous and mobile vulnerable-compromised-quar-
tained-patched-scrapped (VCQPS) model. In [7], Elsawy
et al. defined spatial firewalls to control malware
spreading in Wireless Network. Gao and Zhuang [23]
studied worm propagation with saturated incidence and
spreading in Wireless Network. In [6], Farooq and Zhu proposed an analytical model to study the
D2D propagation of malware in wireless IoT networks.

Motivated by the abovementioned research, we
propose a Heterogeneous Susceptible-Exposed-Infected-
Recovered (HSEIR) model, which characterizes the in-
fluence 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 is different due to the factors of its topology links
and processing capacity. As far as we know, little work has
been done on the heterogeneity of wireless devices. In this
work, we make contributions as follows:

(1) We propose a HSEIR model. To the best of our
knowledge, this is the first work for disclosing dy-
namics of malware propagation in the wireless IoT
network.

(2) We derive differential equations of the HSEIR model,
which can reflect the number of wireless devices
belonging to different states varying with time.

(3) We discuss the malware propagation threshold by
the proposed model. We also proof the stability of
equilibrium, upon which we can judge the malware
spread scale.

(4) We study control strategy in two aspects. One is
optimal control to minimize the number of infected
devices (including exposed and infected nodes) and
the corresponding cost of the strategies during the
process of spreading. And, the other one is to control
the malware illness upon the malware propagation
threshold.

The remainder of this paper is organized as follows. In
Section 2, we establish the HSEIR model in IoT wireless
networks. In Section 3, we analyze the dynamics of the
proposed model. In Section 4, control strategies by
Pontryagin’s Minimum Principle and malware propa-
gation threshold are discussed. Section 5 gives the details
of numerical simulation of the model. Conclusions and
discussion are given in Section 6.

2. The HSEIR Model

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

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
a and the proportion of wireless devices infected by the
nodes with strong spreading capabilities is 1 − a. The total
device population N is divided into four different com-
partments (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 in-
fected 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 com-
part. 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:

\[
\begin{align*}
S & \quad \rightarrow \quad E + R \\
E & \quad \rightarrow \quad I + R \\
I & \quad \rightarrow \quad R \\
R & \quad \rightarrow \quad S \\
\end{align*}
\]
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

\[
\frac{d(S + E + I + R)}{dt} = \frac{dN}{dt} = \Lambda - dN - \theta I \leq \Lambda - dN, \tag{2}
\]

and after a simple computation, we have

\[
N(t) \leq \frac{\Lambda}{d} + \left( N(0) - \frac{\Lambda}{d} \right) e^{-dt}. \tag{3}
\]

Then, we have

\[
\limsup_{t \to \infty} N(t) \to \frac{\Lambda}{d}. \tag{4}
\]

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

\[
\Omega = \left\{ (S, E, I, R) \in \mathbb{R}^4_+ | 0 \leq S + E + I + R \leq \frac{\Lambda}{d} \right\}. \tag{5}
\]

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 \( R_0 \):

\[
F = \begin{pmatrix} 0 & \frac{\Lambda}{d + \eta} (a \beta_1 + (1-a) \beta_2) \\ 0 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} \gamma + \delta + d & 0 \\ -\gamma & \phi + d \end{pmatrix}.
\]

Then, the basic reproduction number \( R_0 \) of the system is as:

\[
R_0 = \rho(FV^{-1}) = \frac{\Lambda \gamma (a \beta_1 + (1-a) \beta_2)}{(d + \eta) (\gamma + \delta + d) (d + \phi + \theta)}. \tag{7}
\]

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

\[
\begin{align*}
S^* &= \frac{\Lambda}{(a \beta_1 + \beta_2 - a \beta_2) I^* + (d + \eta)} \\
E^* &= \frac{d + \phi + \theta I^*}{\gamma} \\
I^* &= \frac{(R_0 - 1) (d + \eta)}{(a \beta_1 + \beta_2 - a \beta_2)} \\
R^* &= \frac{\delta E^* + \phi I^* + \eta S^*}{d}.
\end{align*} \tag{8}
\]
Table 1: Nations and parameter values in the model.

| Nation | Explanation |
|--------|-------------|
| N(t)   | Total number of wireless devices at time t |
| S(t)   | Number of susceptible devices at time t |
| E(t)   | Number of exposed devices at time t |
| I(t)   | Number of infected devices at time t |
| R(t)   | Number of recovered devices at time t |
| a      | The proportion of wireless devices infected by weak spreading capabilities |
| 1 - a  | The proportion of wireless devices infected by strong spreading capabilities |
| β₁     | Infection rate of devices with weak spreading capabilities |
| β₂     | Infection rate of devices with strong spreading capabilities |
| λ      | The recruitment rate |
| d      | The natural death rate |
| γ      | State transition rate from E to I |
| δ      | State transition rate from E to R |
| φ      | State transition rate from I to R |
| η      | State transition rate from R to S |
| θ      | Malware-related death rate |

3.2. Stability of Equilibrium

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:

\[
(\lambda + d + \vartheta)(\lambda + \gamma + \delta + d) - \frac{\lambda \gamma (a\beta_1 + \beta_2 - a\beta_2)}{\eta + d} = 0.
\]

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.

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

\[
J(P_0) = \begin{pmatrix}
-(\eta + d) & \frac{\lambda (a\beta_1 - \beta_2 - a\beta_2)}{\eta + d} & 0 \\
0 & -(\gamma + \delta + d) & \frac{\lambda (a\beta_1 + \beta_2 - a\beta_2)}{\eta + d} \\
\eta & \gamma & -d
\end{pmatrix}.
\]

and its characteristic equation is

\[
\det(\lambda I - J(P_0)) = 0.
\]

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

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

Then,

\[
L' = \gamma' + (\gamma + \delta + d)L',
\]

\[
= [\gamma S(a\beta_1 + \beta_2 - a\beta_2) - (\gamma + \delta + d)(\vartheta + d + \theta)]I,
\]

\[
\leq [\gamma S(a\beta_1 + \beta_2 - a\beta_2) - (\gamma + \delta + d)(\vartheta + d + \theta)]I,
\]

\[
= (\gamma + \delta + d)(\vartheta + d + \theta)(R_0 - 1)I.
\]
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 $R_0 = 1$ and $S = S_0$, the only compact invariant subset in the set $L' \leq 0$ is also the singleton $P_0$; therefore, the largest invariant subset in the set $\{ (dL/dt) = 0 \}$ also is 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.

\[\square\]

**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:

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

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

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

By direct calculations, we have that

\[
V' = \left[ a \beta_1 + (1 - a) \beta_2 \right] \gamma S^* I^* \left( 1 - \frac{S}{S^*} \right) \left( 1 - \frac{SI}{S^* I^*} \right)
+ \left[ a \beta_1 + (1 - a) \beta_2 \right] \gamma S^* I^* \left( 1 - \frac{E}{E^*} \right) \left( \frac{SI}{S^* I^*} - \frac{E^*}{E} \right)
+ (\gamma + \delta + d) \gamma E^* \left( 1 - \frac{I}{I^*} \right) \left( \frac{E}{E^*} - \frac{1}{I^*} \right)
- \gamma (d + \eta) \frac{(S^* - S)^2}{S}.
\]

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

then

\[
(a \beta_1 + (1 - a) \beta_2) S^* I^* = (\gamma + \delta + d) E^*.
\]

\[
(14)
\]

\[
(15)
\]

\[
(16)
\]

\[
(17)
\]

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.

By direct calculations, we have that

\[
V' = \left[ a \beta_1 + (1 - a) \beta_2 \right] \gamma S^* I^* \left( 1 - \frac{S}{S^*} \right) \left( 1 - \frac{SI}{S^* I^*} \right)
+ \left[ a \beta_1 + (1 - a) \beta_2 \right] \gamma S^* I^* \left( 1 - \frac{E}{E^*} \right) \left( \frac{SI}{S^* I^*} - \frac{E^*}{E} \right)
+ (\gamma + \delta + d) \gamma E^* \left( 1 - \frac{I}{I^*} \right) \left( \frac{E}{E^*} - \frac{1}{I^*} \right)
- \gamma (d + \eta) \frac{(S^* - S)^2}{S}.
\]

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) $u_2 (t)$ 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) \( u_1(t) \) 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

\[
\begin{align*}
\frac{dS}{dt} &= \Lambda - (1 - u_1(t))a \beta_1 SI - (1 - u_2(t))(1 - a)\beta_2 SI - (d + u_3(t))S, \\
\frac{dE}{dt} &= (1 - u_1(t))a \beta_1 SI + (1 - u_2(t))(1 - a)\beta_2 SI - (\gamma + \delta + d)E, \\
\frac{dI}{dt} &= \gamma E - (\theta + d + u_4(t))I, \\
\frac{dR}{dt} &= \delta E + u_4(t)I + u_3(t)S - dR.
\end{align*}
\]  

(18)

The main purpose is to minimize the number of infected devices at a minimum cost. And, as a consequence, we consider the objective functional:

\[
J(u_1, u_2, u_3, u_4) = \int_0^T \left[ E + I + \frac{K}{2}u_1^2 + \frac{W}{2}u_2^2 + \frac{P}{2}u_3^2 + \frac{Q}{2}u_4^2 \right] dt,
\]

where the parameters \( K \geq 0, W \geq 0, P \geq 0, \) and \( Q \geq 0 \) are the weight constants for the control strategies. \((K/2)u_1^2(t), (W/2)u_2^2(t), (P/2)u_3^2(t), \) and \((Q/2)u_4^2(t)\) describe the cost associated with quarantine strategy, quarantine strategy, vaccination, and repairing and fixing strategies, respectively. Our aim is to seek the optimal control functions \( \{u_1^*, u_2^*, u_3^*, u_4^*\} \), such that

\[
J(u^*_i) = \min \{J(u_i) : u_i \in U, i = 1, 2, 3, 4\},
\]

(20)

where \( U \) is the control function set defined as \( U = \{u_i : u_i(t) \) is Lebesque measure, \( 0 \leq u_i(t) \leq 1, t \in [0, T]\} \).

Next, we discuss the existence of an optimal control functions by Fleming and Rishel [26].

(1) The set of controls and the corresponding state variables are nonempty

(2) The admissible control set is convex and closed

(3) The right hand side of the optimal control system is bounded by a linear function in the state and control variables

(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 \( J(E, I, u, t) \geq c_1 (\sum_{i=1}^4 |u_i^2|)^{l/2} + c_2 \)

\[\text{Theorem 3. An optimal control pair} \ (u_1^*, u_2^*, u_3^*, \text{and} \ u_4^*) \ \text{subject to system} \ (18) \ \text{exists if the following conditions hold:}\]

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

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
\[ L(x, U) = E + I + \frac{K}{2}u_1^2 + \frac{W}{2}u_2^2 + \frac{P}{2}u_3^2 + \frac{Q}{2}u_4^2. \]  

Then, we define the Hamiltonian function \( H \) as

\[
H(x, U, \lambda) = E + I + \frac{K}{2}u_1^2 + \frac{W}{2}u_2^2 + \frac{P}{2}u_3^2 + \frac{Q}{2}u_4^2 \\
+ \lambda_1\left[\Lambda -(1 - u_1(t))a\beta_1SI -(1 - u_2(t))(1 - a)\beta_2SI -(d + u_3(t))S\right] \\
+ \lambda_2\left[(1 - u_1(t))a\beta_1SI +(1 - u_2(t))(1 - a)\beta_2SI -(\gamma + \delta + d)S\right] \\
+ \lambda_3[yE -(\theta + d + u_4(t))I] \\
+ \lambda_4[\delta E + u_4(t)I + u_5(t)S - dR].
\]

Next, we show the following theorem.

**Theorem 4.** Given an optimal control pair \((u_1^*, u_2^*, u_3^*, \text{ and } u_4^*)\) and a solution \((S^*, E^*, I^*, \text{ and } R^*)\) of corresponding control system (18), there exists an adjoint variable \(\lambda_i, i = 1, \ldots, 4,\) satisfying

\[
\frac{\partial H}{\partial S} = (\lambda_2 - \lambda_1)\left[(1 - u_1(t))a\beta_1I +(1 - u_2(t))(1 - a)\beta_2\right] \\
-(d + u_3(t))\lambda_1 + u_3\lambda_4,
\]

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

\[
\frac{\partial H}{\partial I} = 1 + u_4\lambda_4 + (\lambda_2 - \lambda_1)\left[1 - u_1(t)\right]a\beta_1 \left[1 - u_2(t)\right](1 - a)\beta_2 \\
-(\theta + d + u_4(t))\lambda_3,
\]

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

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

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

where \(x = (S, E, I, R)\). Hence, the adjoint variable \(\lambda_i, i = 1, \ldots, 4,\) satisfies (23).
Consider control system (18) with \( \lambda_i(T) = 0 \). By using the optimal necessary condition, we have
\[
\frac{\partial H}{\partial u_i} = 0.
\] (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 \((\partial R_0/\partial \beta_1) > 0, (\partial R_0/\partial \beta_2) > 0, (\partial R_0/\partial \delta) > 0, (\partial R_0/\partial \alpha) < 0, (\partial R_0/\partial \eta) < 0, (\partial R_0/\partial \gamma) < 0, (\partial R_0/\partial \phi) < 0, (\partial R_0/\partial \theta) < 0, \) and \((\partial R_0/\partial d) < 0 \), which mean that \( R_0 \) increases as the parameters \( \Lambda, \gamma, \beta_1, \) 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 \( d \) and \( \theta \) is usually constant because of the properties of wireless devices. Consequently, we control the following coefficients to make \( R_0 \leq 1 \):

(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 \( \Lambda = 0.75, d = 0.001, \theta = 0.005, \beta_1 = 0.00001, \beta_2 = 0.0001, \gamma = 0.004, \eta = 0.0006, \delta = 0.003, a = 0.6, \) 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 $u_{1\max} = 0.8$, $u_{2\max} = 0.8$, $u_{3\max} = 0.7$, $u_{4\max} = 0.9$, $K = 0.3$, $W = 0.6$, $P = 0.4$, 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 strategies. 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 reduced 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 IoT devices 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 networks, 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 $R_0$, which represents the malware spreading threshold. 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 increases, the malware spreading scale will also increase. In addition, the proportion of susceptible wireless devices infected 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**

[1] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-physical systems security-a survey,” IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, 2017.

[2] B. Kuang, A. Fu, L. Zhou et al., “DO-RA: data-oriented runtime attestation for IoT devices,” Computers and Security, vol. 97, 2020.

[3] Y. Hou and J. Wang, “Investigation of wireless sensor network of the Internet of Things,” in Proceedings of the International Conference on Intelligent and Interactive Systems and Applications, pp. 21–29, London, UK, 2019.

[4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on Internet of things: architecture, enabling technologies, security and privacy, and applications,” IEEE Internet of Things Journal, vol. 4, no. 5, 2017.

[5] J. Wu, W. Jiang, Y. Mei, Y. Zhao, and T. Wang, “A survey on the progress of testing techniques and methods for wireless sensor networks,” IEEE Access, vol. 7, pp. 4302–4316, 2018.

[6] M. J. Farooq and Q. Zhu, “Modeling, analysis, and mitigation of dynamic botnet formation in wireless IoT networks,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 9, pp. 2412–2426, 2019.

[7] H. Elsawy, M. A. Kishk, and M. S. Alouini, “Spatial firewalls: quarantining malware epidemics in large scale massive wireless networks,” IEEE Communications Magazine, vol. 58, no. 9, pp. 32–38, 2020.

[8] Y. Li, G. Xu, H. Xian, L. Rao, and J. Shi, “Novel android malware detection method based on multi-dimensional hybrid features extraction and analysis,” Intelligent Automation and Soft Computing, vol. 25, no. 3, pp. 635–644, 2019.

[9] C. Du, S. Liu, L. Si, Y. Guo, and T. Jin, “Using object detection network for malware detection and identification in network traffic packets,” Computers, Materials & Continua, vol. 64, no. 3, pp. 1785–1796, 2020.

[10] D.-W. Kim, G.-Y. Shin, and M.-M. Han, “Analysis of feature importance and interpretation for malware classification,” Computers, Materials & Continua, vol. 65, no. 3, pp. 1891–1904, 2020.

[11] J. Liu, Y. Zeng, J. Shi, Y. Yang, R. Wang, and L. He, “MalDetect: a structure of encrypted malware traffic detection,” Computers, Materials and Continua, vol. 60, no. 2, pp. 721–739, 2019.

[12] M. S. Arif, A. Raza, M. Rafiq, M. Bibi, and J. N. Abbasi, “Numerical simulations for stochastic computer virus propagation model,” Computers, Materials and Continua, vol. 62, no. 1, pp. 61–77, 2020.

[13] M. Knysz, X. Hu, Y. Zeng, and K. G. Shin, Open WiFi Networks: Lethal Weapons for Botnets?, Proceedings IEEE Infocom, Orlando, FL, USA, 2012.

[14] L. X. Yang, P. D. Li, X. F. Yang, Y. Xiang, and Y. Y. Tang, “Simultaneous benefit maximization of conflicting opinions: modeling and analysis,” IEEE Systems Journal, vol. 14, no. 2, pp. 1623–1634, 2020.
[15] F. W. Wang, Y. K. Zhang, C. G. Wang, J. F. Ma, and S. J. Moon, "Stability analysis of a SEIQV epidemic model for rapid spreading worms," *Computers and Security*, vol. 29, no. 4, pp. 410–418, 2010.

[16] J. N. C. Goncalves, H. S. Rodrigues, and M. T. T. Monteiro, "Optimal control measures for a susceptible-carrier-infectious-recovered-susceptible malware propagation model," *Optimal Control Applications and Methods*, vol. 40, no. 4, pp. 691–702, 2019.

[17] L. P. Song and X. Q. Ding, "Hopf bifurcation of an epidemic model with delay," *PLoS One*, vol. 11, no. 6, 2019.

[18] D. Acarali, M. Rajarajan, N. Komninos et al., "Modelling the spread of Botnet malware in IoT-based wireless sensor networks," *Security and Communication Networks*, vol. 2019, Article ID 3745619, 2019.

[19] S. Peng, S. Yu, and A. Yang, "Smartphone malware and its propagation modeling: a survey," *IEEE Communication Surveys and Tutorials*, vol. 16, no. 2, pp. 952–1041, 2014.

[20] S. M. Cheng, P. Y. Chen, C. C. Lin, and H. C. Hsiao, "Traffic-aware patching for cyber security in mobile IoT," *IEEE Communications Magazine*, vol. 55, no. 7, 2017.

[21] L. Li, J. Cui, R. Zhang et al., "Dynamics of complex networks: malware propagation modeling and analysis in Industrial Internet of Things," *IEEE Access*, vol. 8, pp. 64184–64192, 2020.

[22] S. G. Shen, H. P. Zhou, S. Feng, J. H. Liu, H. Zhang, and Q. Y. Gao, "An epidemiology-based model for disclosing dynamics of malware propagation in heterogeneous and mobile WSNs," *IEEE Access*, vol. 8, pp. 43876–43887, 2020.

[23] Q. W. Gao and J. Zhuang, "Stability analysis and control strategies for worm attack in mobile networks via a VEIQS propagation model," *Applied Mathematics and Computation*, vol. 368, Article ID 124584, 2020.

[24] P. van den Driessche and J. Watmough, "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission," *Mathematical Biosciences*, vol. 180, pp. 29–48, 2002.

[25] J. P. Lasalle, *The Stability of Dynamical Systems*, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1976.

[26] W. H. Fleming and R. W. Rishel, *Deterministic and Stochastic Optimal Control*, Springer-Verlag, Berlin, Germany, 1975.

[27] D. L. Lukes, *Differential Equations: Classical to Controlled*, Elsevier, Amsterdam, Netherlands, 1982.

[28] L. S. Pontryagin, V. G. Boltyanskii, R. V. Gamkrelidze et al., *Mathematical Theory of Optimal Processes*, Gordon and Breach Science Publishers, New York, NY, USA, 1966.

[29] S. Lenhart and J. T. Workman, *Optimal Control Applied to Biological Models*, Chapman and Hall/CRC Press, Boca Raton, FL, USA, 2007.