axioms

MDPI

Article

A Malware Propagation Model Considering Conformity Psychology in Social Networks

Qingyi Zhu [1,*], Yuhang Liu [2], Xuhang Luo [2] and Kefei Cheng [2]

[1] School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[2] Chongqing Key Laboratory of Computer Network and Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
* Correspondence: zhuqy@cqupt.edu.cn

Abstract: At present, malware is still a major security threat to computer networks. However, only a fraction of users with some security consciousness take security measures to protect computers on their own initiative, and others who know the current situation through social networks usually follow suit. This phenomenon is referred to as conformity psychology. It is obvious that more users will take countermeasures to prevent computers from being infected if the malware spreads to a certain extent. This paper proposes a deterministic nonlinear SEIQR propagation model to investigate the impact of conformity psychology on malware propagation. Both the local and global stabilities of malware-free equilibrium are proven while the existence and local stability of endemic equilibrium is proven by using the central manifold theory. Additionally, some numerical examples and simulation experiments based on two network datasets are performed to verify the theoretical analysis results. Finally, the sensitivity analysis of system parameters is carried out.

Keywords: malware propagation; conformity psychology; stability analysis; numerical simulation; sensitivity analysis

check for updates

Citation: Zhu, Q.; Liu, Y.; Luo, X.; Cheng, K. A Malware Propagation Model Considering Conformity Psychology in Social Networks. *Axioms* **2022**, *11*, 632. https://doi.org/10.3390/axioms11110632

Academic Editor: Joao Paulo Carvalho

Received: 9 September 2022
Accepted: 4 November 2022
Published: 10 November 2022

1. Introduction

Malware is a program that can obtain unauthorized access and perform malicious tasks on a computer system [1]. In essence, malware can perform a sequence of operations to obtain control of the operating system so it can interrupt system operations, spy on users, and steal sensitive data [2]. With the development of modern malware programs, fileless malware has been developed, which does not need traditional executables to perform its operations. The fileless malware works directly within the memory of the target system instead of the hard drive [3,4]. With the application of obfuscation techniques in malware development, the detection of new malware will become even more difficult than ever before [5–7].

Much effort has been made over recent years to deal with the threat of malware; however, it is still a severe risk in cyberspace. For example, by the end of 2016, the Mirai virus had infected more than 500,000 devices and performed Distributed Denial of Service (DDoS) attacks against many corporations and governments, including the French data service provider, the major Internet service of America, and a telecommunication service provider in Liberia [8]. In 2017, the earliest version of WannaCry was discovered by researchers from Fortinet [9]. It attacked more than 230,000 computers in over 150 countries and organizations, ranging from the UK National Health Service, the Bank of China, the Russian Interior Ministry, to FedEx [10]. Moreover, some viruses have been developed to launch advanced persistent threats (APTs) on industrial control systems, such as Stuxnet, Industroyer, and Triton [11,12]. In this context, it is extremely important to understand the propagation behavior of malware and then propose efficient control strategies to prevent its spread.

In the classical propagation models, the susceptible-infected-recovered (SIR) [13,14] and susceptible-exposed-infected-recovered (SEIR) [15–17] models are widely used, which depict the basic propagation process clearly. In [18], the perturbation method was used to obtain the asymptotic solution of the SEIR model. Bentaleb and Amine [19] used the Lyapunov function to prove that the disease-free equilibrium is globally asymptotically stable in the two-strain SEIR model. In [20], Khouzani et al. introduced the optimal control strategy to control the spread of malware. To study the computer virus propagation, the work [21] proposed a novel method that integrated the evolutionary computing paradigm to analyze the nonlinear dynamical behaviors of the model. In [22], the authors carried out numerical simulations on the trend of safety entropy creatively. Meanwhile, some prototype SEIR models, such as the SLBS model, have been investigated [23,24].

Quarantine is an early intervention measure to control the population of infected individuals [25]. In the study of malware propagation, some researchers have investigated the quarantine strategy in the SEIR model [26,27]. During the propagation of malware, one can quarantine the infected nodes by closing the connection between infected nodes and other nodes [28]. In [29], Piqueira and Batistela used the numerical approach to obtain the parameter conditions of two equilibria in both saturated and unsaturated cases of the quarantine population, respectively. However, most existing work neglects the effect of user awareness on malware propagation.

Individuals can be influenced by the behaviors of others and begin to imitate them, which is referred to as conformity psychology [30]. In the early stage of malware distribution, people will tell their friends what happened to them when their computers are infected, and their friends will be more alert. When the malware starts to become known to the general public, some people realize the threat of malware and will take some precautions against malware; then more people will follow suit [31]. Thus, malware propagation can be controlled by raising user security awareness. In [32], the authors proposed an SEIRS with vaccination and quarantine states (SEIRS-QV) model considering the impacts of user awareness, network delay, and diverse configuration of nodes. Moreover, many researchers considered the impact of user awareness on the spread of malware (e.g., [33,34]). Moreover, social networks as a carrier of information dissemination can affect user awareness by sharing messages about malware. Thus, it is necessary to study the characteristics of social networks in information transmission.

With more and more people chatting online, online social networks have become an important part of people's lives. The trust between online users allows information to spread quickly through social networking applications [35,36]. Hence, disseminating information about the spread of malware through social networks can make the public recognize the risk level. Then, the public can consciously take some preventive measures to avoid being infected, such as upgrading the firewall and running the security software. Many researchers focused on the characteristics of social networks [37–39]. Jia et al. [40] considered the heterogeneity of infection rates and proposed an HSID model to describe the spread of viruses in social networks. Owing to the importance of describing the information dissemination process of social networks, Du and Wang [41] studied a reaction–diffusion malware propagation model with mixed delays. In [42], the authors investigated a fear effect where information about the impact of the virus from different networks can cause people to feel fear and confusion. Clearly, user awareness is an important factor in preventing virus propagation.

This paper aims to explore the impact of conformity psychology on malware propagation. Section 2 gives the description of the formulated model. In Section 3, the dynamic behavior of malware-free equilibrium and endemic equilibrium are explored. In Sections 4–6, the numerical simulations, experimental analysis, and sensitivity analysis are given, respectively. Section 7 presents conclusions to end this work.

2. Assumptions and Model Formulation

In this section, we classify all the computers into five categories: susceptible, exposed, infected, quarantined, and recovered computers. Susceptible computers mean they are vulnerable to malware. Exposed computers represent a class of computers that have been infected with malware but have not yet broken out and cannot infect others. An infected computer can infect other susceptible computers. Quarantined computers mean computers are disconnected but still alive. Quarantined computers will eventually be transferred to the recovered state and become immune to current malware. Let $S(t), E(t), I(t), Q(t), R(t)$ represent their corresponding densities, respectively, and the equation $S(t) + E(t) + I(t) + Q(t) + R(t) = 1$ at time t is valid.

In the modeling of malware propagation, the bilinear incidence rate βSI is used to represent the rate of susceptible computers becoming exposed computers, which is affected by the number of susceptible and infected computers. β is denoted as the rate of malware contact transmission and infection. User awareness plays a significant role in controlling the number of infected computers. So, β^{-mI} is usually used to describe the impact of psychology [43,44]. Here, m is a non-negative parameter to measure the impact of information dissemination. The effects of information about the number of exposed, infected, and quarantined computers are expressed as m_E, m_I, and m_Q in social networks, respectively. Hence, the effect of conformity is given by M_e= $\mathrm{e}^{-m_E E - m_I I - m_Q Q}$.

Then, the following assumptions are made for this model.

(A1) Information is spread steadily and evenly on social networks. It is supposed that exposed computers have a lower impact on user awareness than infected and quarantined computers, since the more damage malware causes, the more people worry about the malware.

(A2) Let ϕ represent the probability of people adopting quarantine to address the problem of infected computers, and let γ denote the probability of quarantined computers reconnecting to the network.

(A3) As computers can deteriorate over time and be physically damaged, the mortality rate μ must be in the model. Suppose that the recruitment rate is equal to the mortality rate.

Remark 1. *As the model will eventually reach a dynamic equilibrium, the total number of nodes will eventually remain stable, which means that the recruitment rate is infinitely close to the mortality rate. If not, the total number will keep decreasing or increasing with time $t \to \infty$. Therefore, the recruitment rate is required to equal the mortality rate in order to maintain the dynamic equilibrium and be consistent with other existing efforts [28,45,46].*

The state transition connection of nodes in the model is presented in Figure 1 and the means of parameters are given in Table 1. Note that all parameters in this model are non-negative constants.

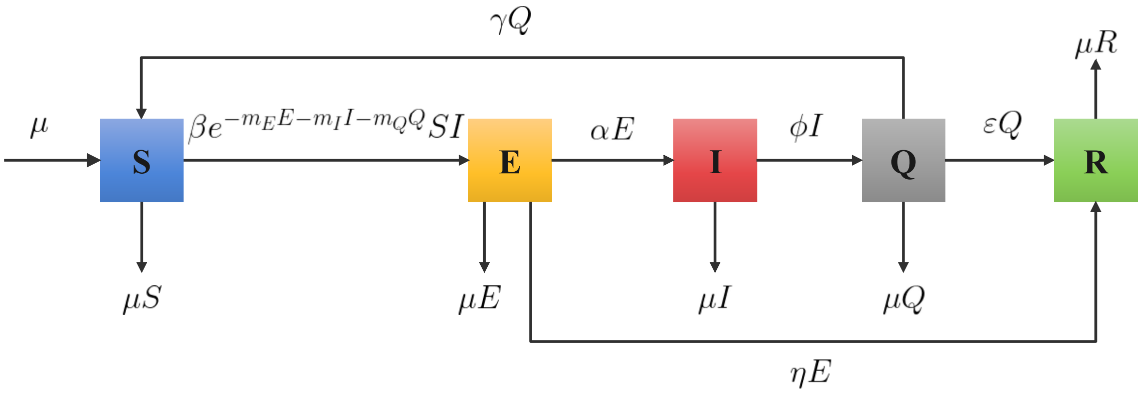


Figure 1. The transfer diagram of the model.

Table 1. Parameter interpretations.

Parameter	Description	Initial Value	Source
α	Rate of exposed computers becoming infected computers.	0.008	[26]
β	Rate of susceptible computers becoming exposed computers.	0.053	[26]
ϕ	Rate of infected computers being quarantined.	0.05	[26]
γ	Rate of susceptible computers becoming exposed computers.	0.02	-
η	Recovery rate for the exposed computers.	0.0008	[26]
ε	Rate of quarantined computers becoming susceptible computers.	0.005	[26]
μ	Recruitment and mortality rate.	0.001	-
m_E, m_I, m_Q	The impact of social networks corresponding to E, I, Q.	0.2, 0.3, 0.3	-

The corresponding ordinary differential equations are shown as:

$$\begin{cases} \frac{dS}{dt} = \mu + \gamma Q - \beta e^{-m_E E - m_I I - m_Q Q} SI - \mu S, \\ \frac{dE}{dt} = \beta e^{-m_E E - m_I I - m_Q Q} SI - \eta E - \alpha E - \mu E, \\ \frac{dI}{dt} = \alpha E - \phi I - \mu I, \\ \frac{dQ}{dt} = \phi I - \gamma Q - \varepsilon Q - \mu Q, \\ \frac{dR}{dt} = \varepsilon Q + \eta E - \mu R. \end{cases} \tag{1}$$

Thus, the feasible region Ψ of system (1) is defined as:

$$\Psi = \{(S, E, I, Q, R) \in \mathbb{R}^{+5} | S + E + I + Q + R = 1\},$$

which is a positively invariant set, and the system has been normalized. Due to the equation $S(t) + E(t) + I(t) + Q(t) + R(t) = 1$, the system (1) can be written as:

$$\begin{cases} \frac{dE}{dt} = \beta e^{-m_E E - m_I I - m_Q Q}(1 - E - I - Q - R)I - \eta E - \alpha E - \mu E, \\ \frac{dI}{dt} = \alpha E - \phi I - \mu I, \\ \frac{dQ}{dt} = \phi I - \gamma Q - \varepsilon Q - \mu Q, \\ \frac{dR}{dt} = \eta E + \varepsilon Q - \mu R. \end{cases} \tag{2}$$

In the following parts, both the local and global asymptotic stabilities will be the focus of our discussion.

3. Stability Analysis of the Equilibria

In this section, we will calculate the basic reproduction number R_0 and explore the local asymptotic stability and global asymptotic stability in the region Ψ.

3.1. Local Stability of the Equilibria

The malware-free equilibrium $E_0 = (1, 0, 0, 0, 0)$ is obtained from system (2) in the original state. Here, matrix $\mathcal{F}$ and $\mathcal{V}$ represent the additional infection terms and the transformation of other terms, respectively. So, we can obtain:

$$\mathcal{F} = \begin{pmatrix} e^{-m_E E - m_I I - m_Q Q}(1 - E - I - Q - R)I \\ 0 \\ 0 \end{pmatrix},$$

$$\mathcal{V} = \begin{pmatrix} \eta E + \alpha E + \mu E \\ \phi I + \mu I - \alpha E \\ \gamma Q + \varepsilon Q + \mu Q - \phi I \\ \mu R - \varepsilon Q - \eta E \end{pmatrix}.$$

The Jacobian matrices of $\mathbb{F}$ and $\mathbb{V}$ at the malware-free equilibrium E_0 are:

$$F = \begin{pmatrix} 0 & \beta & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$V = \begin{pmatrix} \alpha+\eta+\mu & 0 & 0 \\ -\alpha & \phi+\mu & 0 \\ 0 & -\phi & \gamma+\varepsilon+\mu \end{pmatrix}.$$

According to the matrices F and V, the matrix $J = FV^{-1}$ can be followed as:

$$J = FV^{-1} = \begin{pmatrix} \frac{\beta\alpha}{(\phi+\mu)(\eta+\alpha+\mu)} & \frac{\beta}{\phi+\mu} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

The basic reproduction number R_0 of system (2) is given exactly by the spectral radius of the matrix:

$$R_0 = \rho(FV^{-1}) = \frac{\beta\alpha}{(\phi+\mu)(\eta+\alpha+\mu)}. \tag{3}$$

Theorem 1. *E_0 is locally asymptotically stable with respect to Ψ if $R_0 < 1$.*

Proof of Theorem 1. We can obtain the Jacobian matrix of system (2) with respect to malware-free equilibrium:

$$\mathbf{J}(E_0) = \begin{pmatrix} -\alpha-\eta-\mu & \beta & 0 & 0 \\ \alpha & -\phi-\mu & 0 & 0 \\ 0 & \phi & -\gamma-\varepsilon-\mu & 0 \\ \eta & 0 & \varepsilon & -\mu \end{pmatrix}.$$

The eigenvalue of $\mathbf{J}(E_0)$ can be expressed as:

$$|\lambda E - \mathbf{J}(E_0)| = \begin{vmatrix} \lambda+\alpha+\eta+\mu & -\beta & 0 & 0 \\ -\alpha & \lambda+\phi+\mu & 0 & 0 \\ 0 & -\phi & \lambda+\gamma+\varepsilon+\mu & 0 \\ -\eta & 0 & -\varepsilon & \lambda+\mu \end{vmatrix},$$

and the characteristic equation is:

$$(\lambda^2 + b_1\lambda + b_2)(\lambda+\gamma+\varepsilon+\mu)(\lambda+\mu) = 0,$$

where

$$b_1 = \alpha+\eta+\phi+2\mu, \qquad b_2 = \beta\alpha(\frac{1}{R_0} - 1).$$

According to the Vieta theorem, the roots of this characteristic equation are negative real parts only if $R_0 < 1$. The proof is completed. □

3.2. Existence and Local Stability of Endemic Equilibrium

Theorem 2. *System* (2) *has a unique endemic equilibrium E^* if $R_0 \geq 1$.*

Proof of Theorem 2. The endemic equilibrium (E^*, I^*, Q^*, R^*) of system (2) is shown as:

$$E^* = a_1 I^*, \qquad Q^* = a_2 I^*, \qquad R^* = a_3 I^*,$$

where

$$a_1 = \frac{\phi+\mu}{\alpha}, \qquad a_2 = \frac{\phi}{\gamma+\varepsilon+\mu}, \qquad a_3 = \frac{\eta a_1 + \varepsilon a_2}{\mu},$$
$$a_4 = 1 + a_1 + a_2 + a_3,$$

and

$$m = m_E a_1 + m_Q a_2 + m_I.$$

The equation about I^* is given by:

$$1 - a_4 I^* = \frac{\mathrm{e}^{mI^*}}{R_0}. \tag{4}$$

The Equation (4) can be divided into two equations:

$$y_1 = 1 - a_4 I^*, \tag{5}$$

$$y_2 = \frac{\mathrm{e}^{mI^*}}{R_0}. \tag{6}$$

Due to $0 \le I^* \le 1$, we can see that Equation (5) is monotonically decreasing, and its maximum value is 1. Similarly, Equation (6) is monotonically increasing, and its minimum value is $\frac{1}{R_0}$. If and only if $R_0 \ge 1$, the curves of Equations (5) and (6) have one point of intersection. It means that the endemic equilibrium exists if and only if $R_0 > 1$. □

Theorem 3. *The endemic equilibrium E^* of system (2) is locally asymptotically stable if $R_0 > 1$.*

Proof of Theorem 3. In the central manifold theory, we consider parameter β as a bifurcation parameter [47]. When R_0 = 1, the bifurcation parameter β is given by:

$$\beta_0 = \frac{(\phi+\mu)(\eta+\alpha+\mu)}{\alpha}.$$

It can be easily verified that Jacobian matrix **J** at $\beta = \beta_0$ has a right eigenvector (corresponding to the zero eigenvalue) given by **W** $=(\omega_1, \omega_2, \omega_3, \omega_4)^T$, where

$$\omega_1 = \phi+\mu, \omega_2 = \alpha, \omega_3 = \frac{\alpha\phi}{\gamma+\varepsilon+\mu}, \omega_4 = \frac{\eta(\phi+\mu)(\gamma+\varepsilon+\mu)+\varepsilon\phi\alpha}{\mu(\gamma+\varepsilon+\mu)}.$$

Then, the left eigenvector (corresponding to the zero eigenvalue) is given by **V** = (v_1, v_2, v_3, v_4). Meanwhile, according to the calculation of the equation of **VJ** = 0 and **VW** = 1, the solution of vector **V** can be easily obtained:

$$v_1 = \frac{1}{\phi+\alpha+\eta+2\mu}, \qquad v_2 = \frac{\eta+\alpha+\mu}{\alpha(\phi+\alpha+\eta+2\mu)}, \qquad v_3 = 0, \qquad v_4 = 0.$$

Assume that $x_1 = E, x_2 = I, x_3 = Q, x_4 = R$. Hence, we have

$$\mathbf{f}_1 = \sum_{i,j,k=1}^{4} v_k w_i \frac{\partial^2 f_k(0,0)}{\partial x_i \partial x_j},$$

$$\mathbf{f}_2 = \sum_{i,j,k=1}^{4} v_k w_i \frac{\partial^2 f_k(0,0)}{\partial x_i \partial \beta}.$$

All of the second-order derivatives are calculated at the malware-free equilibrium and $\beta = \beta_0$. Then, the solutions of $\mathbf{f}_1$ and $\mathbf{f}_2$ are:

$$\begin{aligned}\mathbf{f}_1 &= -2\beta v_1(w_1 w_2(m_E+1) + 2w_2^2(m_E+1) + w_2 w_3(m_Q+1) + w_2 w_4) \\ &= -\frac{2\alpha\beta(H + \mu\alpha\phi(m_Q+1) + \gamma\phi\alpha)}{\mu(\phi+\alpha+\eta+2\mu)(\gamma+\varepsilon+\mu)},\end{aligned}$$

where

$$H = \mu(\gamma+\varepsilon+\mu)((\phi+\mu)(m_E+1) + 2\alpha(m_I+1) + \eta(\phi+\mu)),$$

and

$$\mathbf{f}_2 = v_1 w_2 = \frac{\alpha}{\phi+\alpha+\eta+2\mu}.$$

After the above calculation, we can draw the conclusion that $\mathbf{f}_1 < 0$ and $\mathbf{f}_2 > 0$, a transcritical bifurcation occurs at $R_0 = 1$. □

3.3. Global Stability of the Malware-Free Equilibrium

Theorem 4. *The malware-free equilibrium E_0 is globally asymptotically stable if $R_0 < 1$.*

Proof of Theorem 4. We use the theorem in [48] to prove the global stability of the malware-free equilibrium. Let $X = (R)$ and $Z = (E, I, Q)$ denote the uninfected group and the infected group, respectively, where $X_0 = (0)$ and $Z_0 = (0, 0, 0)$. $U_0 = (X_0, Z_0)$ denotes the disease-free equilibrium of this system. Then, the conditions (H1) and (H2) should be satisfied.

(H1) For $\frac{dX}{dt} = F(X, 0)$, X_0 is globally asymptotically stable;

(H2) G(X,Z) = AZ $-\widehat{G}(X,Z), with\ \widehat{G}(X,Z) \leq 0, for\ (X,Z) \in \Omega$;

Then, the derivative of X is the following:

$$\frac{dX}{dt} = F(X, Z) = \varepsilon Q + \eta E - \mu R.$$

At $Z = Z_0$, $G(X, 0) = 0$. Now, $\frac{dX}{dt} = F(X, 0) = -\mu X$, as $t \to \infty$, $X \to X_0$. Thus, $X = X_0$, and condition (H1) is satisfied. From system (2), we obtain:

$$\frac{dZ}{dt} = G(X, Z) = AZ - \widehat{G}(X, Z),$$

where

$$A = \begin{pmatrix} \alpha+\eta+\mu & \beta & 0 \\ -\alpha & \phi+\mu & 0 \\ 0 & -\phi & \gamma+\varepsilon+\mu \end{pmatrix},$$

and

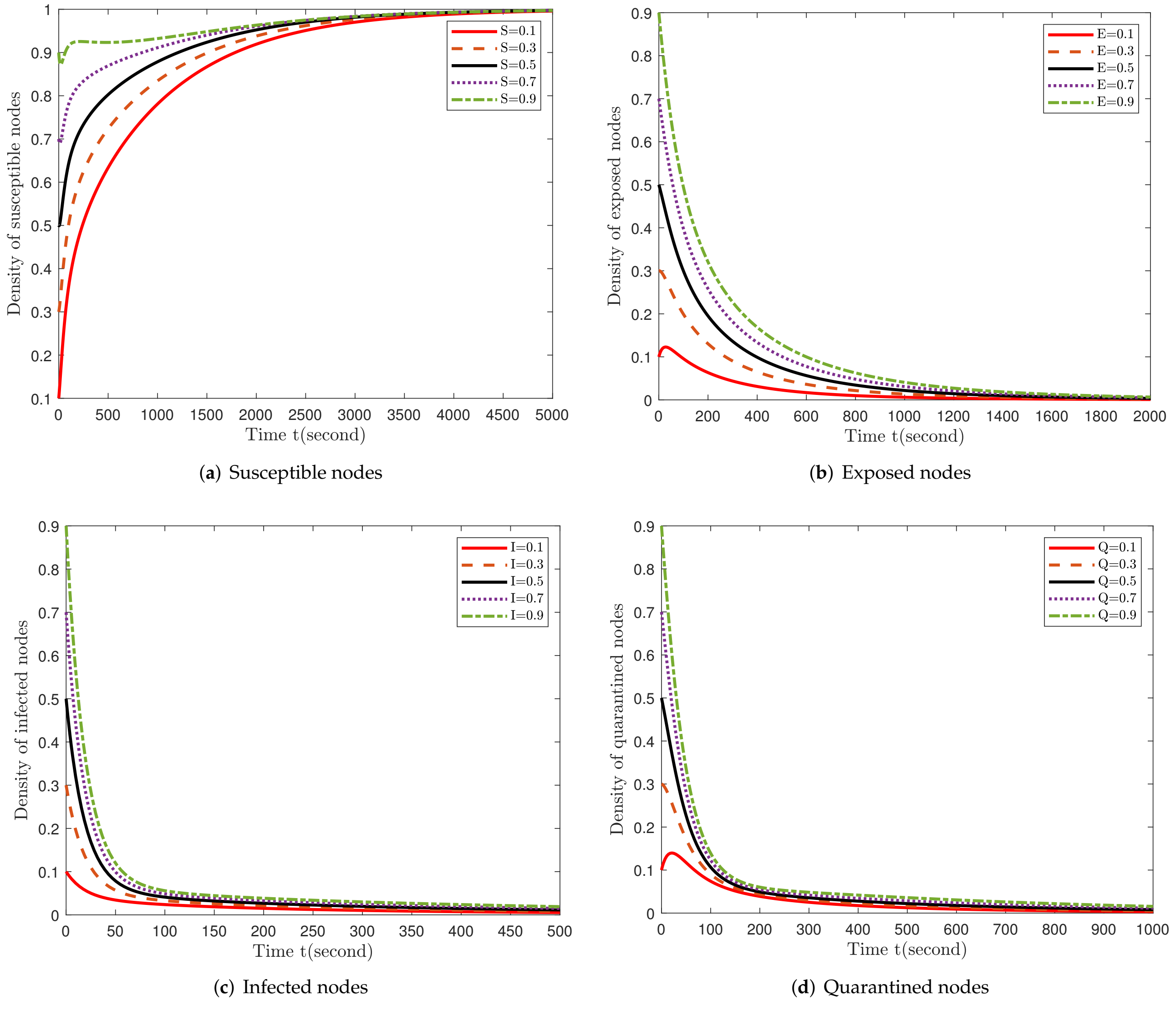
$$\widehat{G}(X, Z) = \begin{pmatrix} \beta I(1 - \mathrm{e}^{-m_E E - m_I I - m_Q Q} S) \\ 0 \\ 0 \end{pmatrix}.$$

Due to $I \geq 0$, $0 < \mathrm{e}^{-m_E E - m_I I - m_Q Q} \leq 1$ and $0 \leq S \leq 1$, so $\widehat{G}(X, Z) \geq 0$. As we know that A is an M-matrix, both conditions (H1) and (H2) are satisfied. Hence, the malware-free equilibrium E_0 is globally asymptotically stable if $R_0 < 1$. □

4. Numerical Simulations

In this section, we carry out a series of numerical simulations to demonstrate the dynamic behavior of the SEIQR model and the impact of the parameters on the infected nodes. Here, the initial densities of five components are given as $S_0 = 0.45, E_0 = 0.2$, $I_0 = 0.15, Q_0 = 0.12$, and $R_0 = 0.08$, respectively. The parameter values of the malware propagation model are given in Table 1. Based on Equation (3) and parameters in Table 1, we can obtain $R_0 = 0.8483 < 1$.

In Figure 2, it is evident that different initial densities of five components converge to the malware-free equilibrium with parameter values in Table 1 and the basic reproduction number $R_0 = 0.8483 < 1$. However, we further consider the case when malware infections become more powerful ($\beta = 0.1$ and $\alpha = 0.1$), so $R_0 = 1.9261 > 1$. Then, all solutions converge to the endemic equilibrium as shown in Figure 3. From these curves in Figures 2 and 3, it is obvious that the system is asymptotically stable.



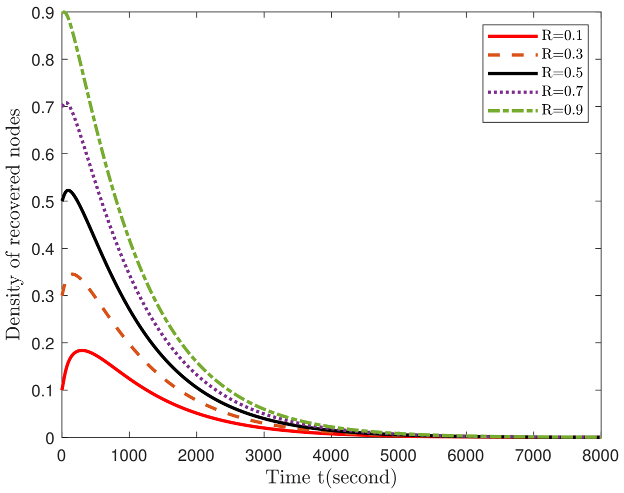
(**a**) Susceptible nodes

(**b**) Exposed nodes

(**c**) Infected nodes

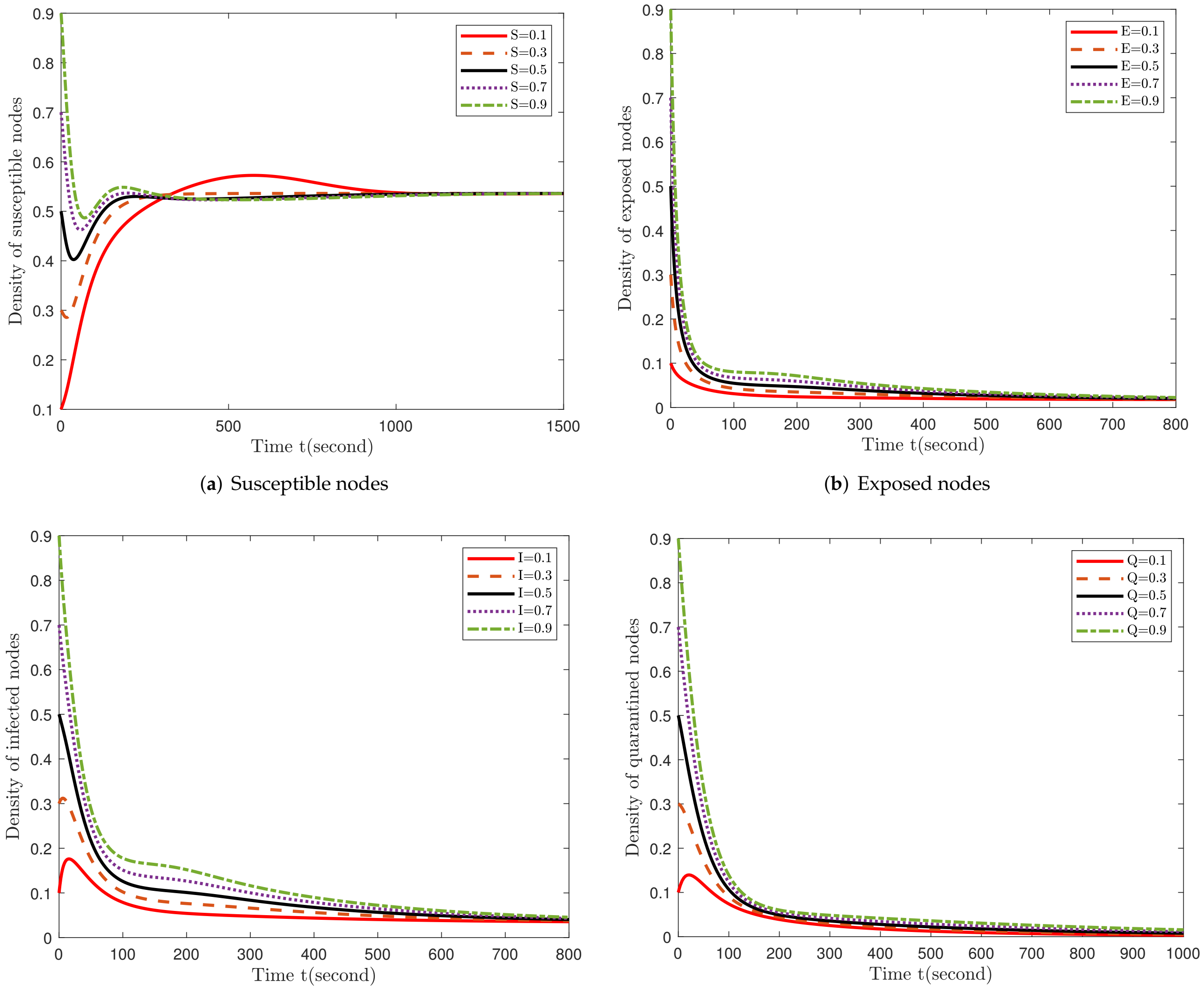
(**d**) Quarantined nodes

Figure 2. *Cont.*



(**e**) Recovered nodes

Figure 2. Different initial densities of susceptible, exposed, infected, quarantined, and recovered nodes with respect time *t* under parameters in Table 1.



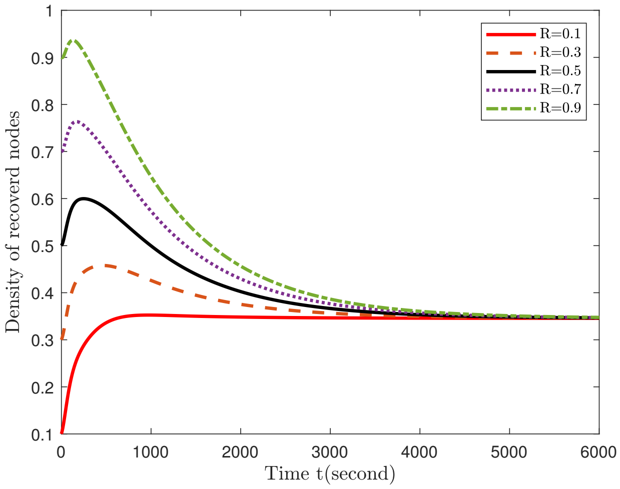
(**a**) Susceptible nodes

(**b**) Exposed nodes

(**c**) Infected nodes

(**d**) Quarantined nodes

Figure 3. *Cont.*



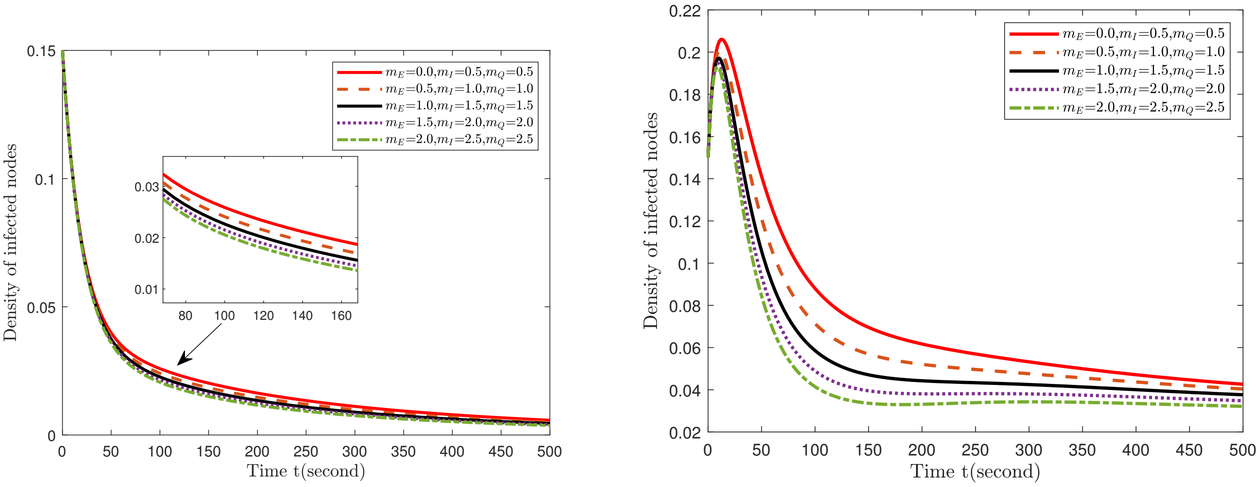
(**e**) Recovered nodes

Figure 3. Different initial densities of susceptible, exposed, infected, quarantined, and recovered nodes with respect time t under parameters in Table 2.

Table 2. The initial parameter values in our simulations.

Parameter	α	β	γ	ϕ	η	ε	μ	m_E	m_I	m_Q
Value	0.1	0.1	0.2	0.05	0.0008	0.005	0.001	0.2	0.3	0.3

The impact of conformity psychology plays a crucial role in the dynamic behavior of infected nodes. However, the dissemination of information about malware is influenced by social networks. Thus, we utilize the parameters m_E, m_I, and m_Q to represent the impact of social networks corresponding to exposed, infected, and quarantined computers, respectively. Figure 4 shows the curves about the density of infected nodes, which is influenced by different sets of values for m_E, m_I, and m_Q. Figure 4a shows that the conformity psychology contributes very little to reduce exposed nodes when the density of infected nodes decreases and $R_0 < 1$. It mean that most people do not care about the malware when it has not infected enough nodes, especially if the malware is not contagious enough. From these curves of Figure 4b, we can see that the density of infected nodes shows a trend of increasing rapidly at the beginning of malware propagation. As the infected nodes reach a certain size, many computer users hear information about malware through social networks. Due to the conformity psychology, most users may take some proper security measures to protect their computers. The bigger values of m_E, m_I, and m_Q means that the social network is more powerful in spreading information. Then, many people are aware of the danger of malware and will strengthen the security of their own computers and inform their acquaintances about the protection methods. After that, malware will no longer infect computers on a large scale. In this context, conformity psychology works well in limiting the spread of malware.



(**a**) $R_0 < 1$ (**b**) $R_0 > 1$

Figure 4. The density of infected nodes over time under different values of m_E, m_I, and m_Q for $R_0 < 1$ and $R_0 > 1$.

In Figure 5, we set different values of the quarantine rate ϕ to study the effectiveness of the quarantine measure. From Figure 5, we can draw a conclusion that the density of infected nodes will decrease with the increase of the value of ϕ. The higher quarantine rate will reduce the number of infected nodes to avoid more nodes being infected.

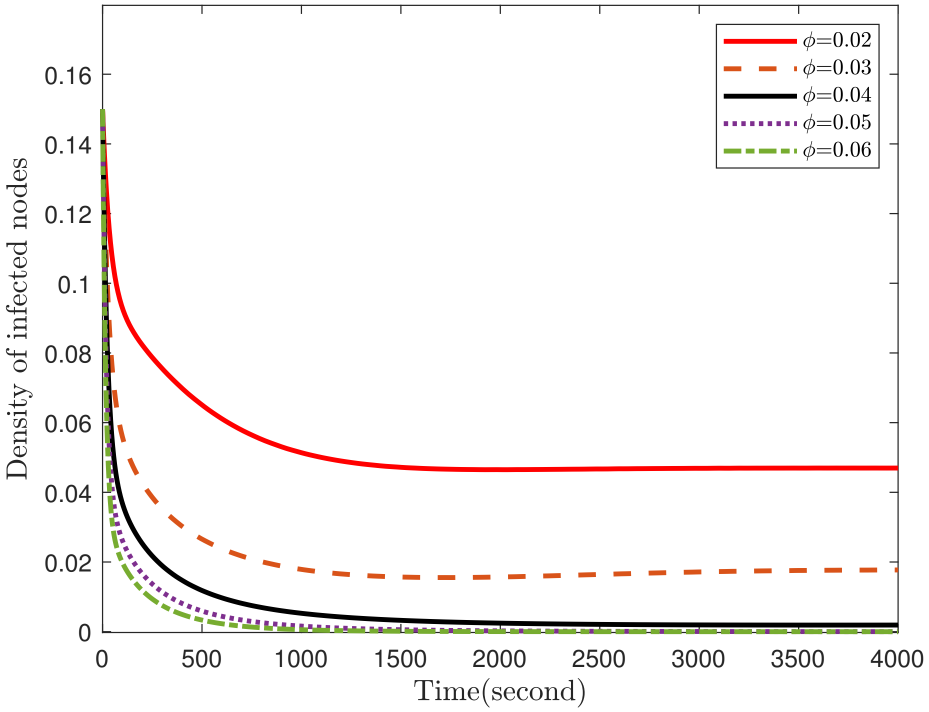


Figure 5. The impact of the quarantined rate ϕ on the infected nodes with respect to time.

5. Experimental Analysis

In this section, we will perform a series of experiments based on two real datasets. The one dataset consists of 55,863 nodes and 858,490 edges from Reddit hyperlink network [49]. The other dataset consists of 81,306 nodes and 1,768,149 edges from Twitter [50]. The emulation program will be used to simulate the state transition of computers during malware propagation.

To compare with Section 4, S, E, I, Q, R indicate numerical simulation results, and S_r, E_r, I_r, Q_r, R_r are the output results of Algorithm 1. The experiments (Examples 1 and 2) will validate the theoretical results with real datasets and analyze the important parameters. In Examples 1 and 2, we will use the Reddit and Twitter datasets to validate the model.

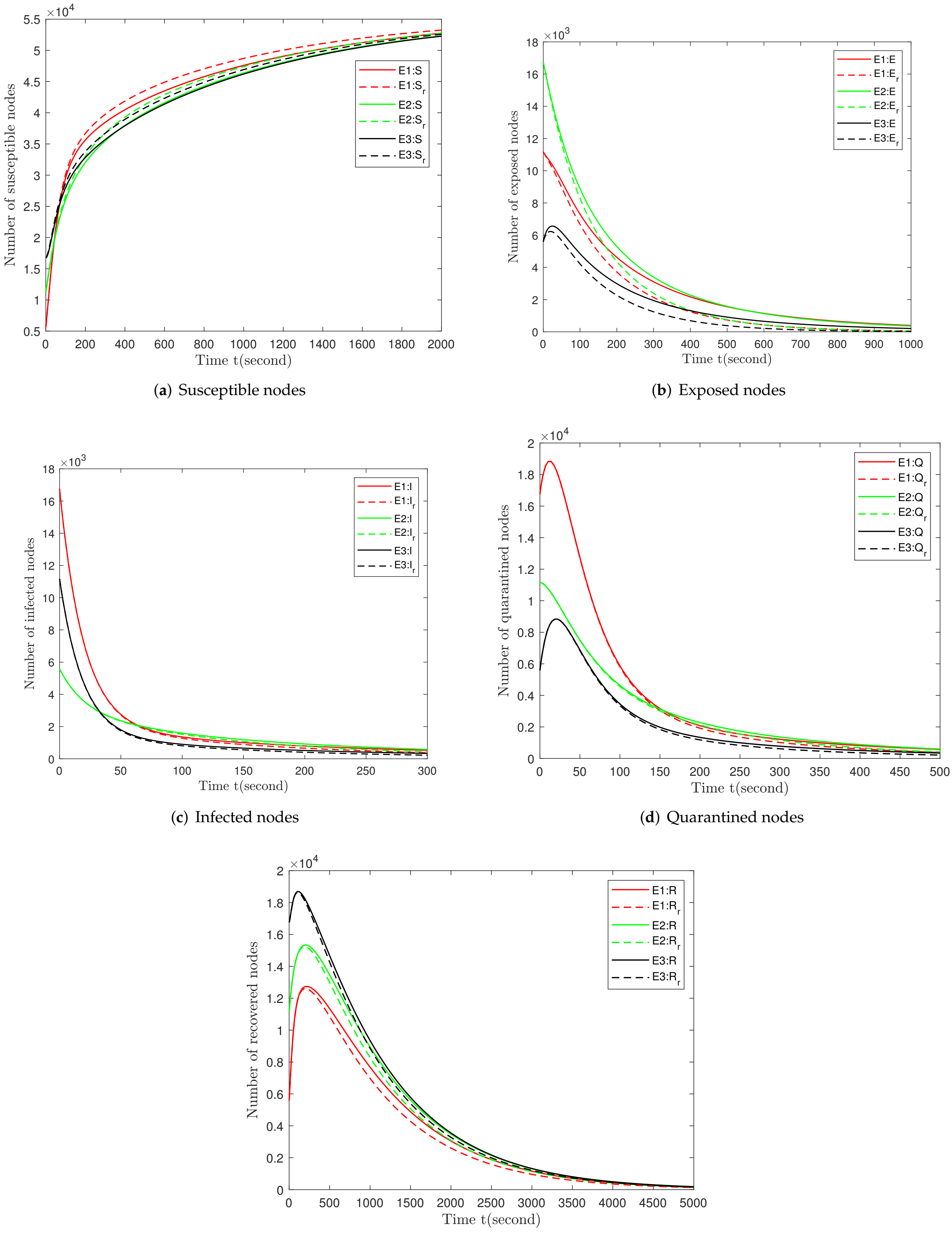
The main algorithm for validating this model is given below:

Algorithm 1: The state transformation of computers on the Internet

```
Input: Input the network G=(v,e) which is given by the set of data and the original
       number of nodes per state
Output: Output the number of nodes in each state at time $t^*$
some description;
for t=0 to $t^*$ with the step of 1 do
    new nodes will be born with probability $\mu$ and all in state S
    if node(i) in the S state and alive then
        if neighbor nodes of node(i) is I then
            it will turn to E with probability $\beta M_e$;
        else
            its state remains unchanged;
        end
    else if node(i) is in the E state and alive then
        if neighbor nodes of node(i) is I then
            it will turn to I with probability $\eta$ ;
        else
            it will turn to R with probability $\alpha$ or its state remains unchanged;
        end
    else if node(i) is in the I state and alive then
        it will turn to Q with probability $\phi$ or its state remains unchanged
    else if node(i) is in the Q state and alive then
        it will turn to R with probability $\varepsilon$, or turn to S with probability $\gamma$, or its
          state remains unchanged;
    else if node(i) is in the R state and alive then
        its state remains unchanged;
    else
        each state of the node dies naturally with probability $\mu$;
    end
end
```

Example 1. *System (1) will evolve with the parameters in Table 1, and the initial conditions on the Reddit dataset are given as:*
(E1) (S(0),E(0),Q(0),I(0),R(0)) = (5586,11173,16758,16758,5588),
(E2) (S(0),E(0),Q(0),I(0),R(0)) = (11173,16758,5585,11173,11174),
(E3) (S(0),E(0),Q(0),I(0),R(0)) = (16758,5586,11173,5588,16758).

Figure 6 demonstrates the progression of system (1) under the initial numbers of Example 1 and the parameter values in Table 1.



(**a**) Susceptible nodes

(**b**) Exposed nodes

(**c**) Infected nodes

(**d**) Quarantined nodes

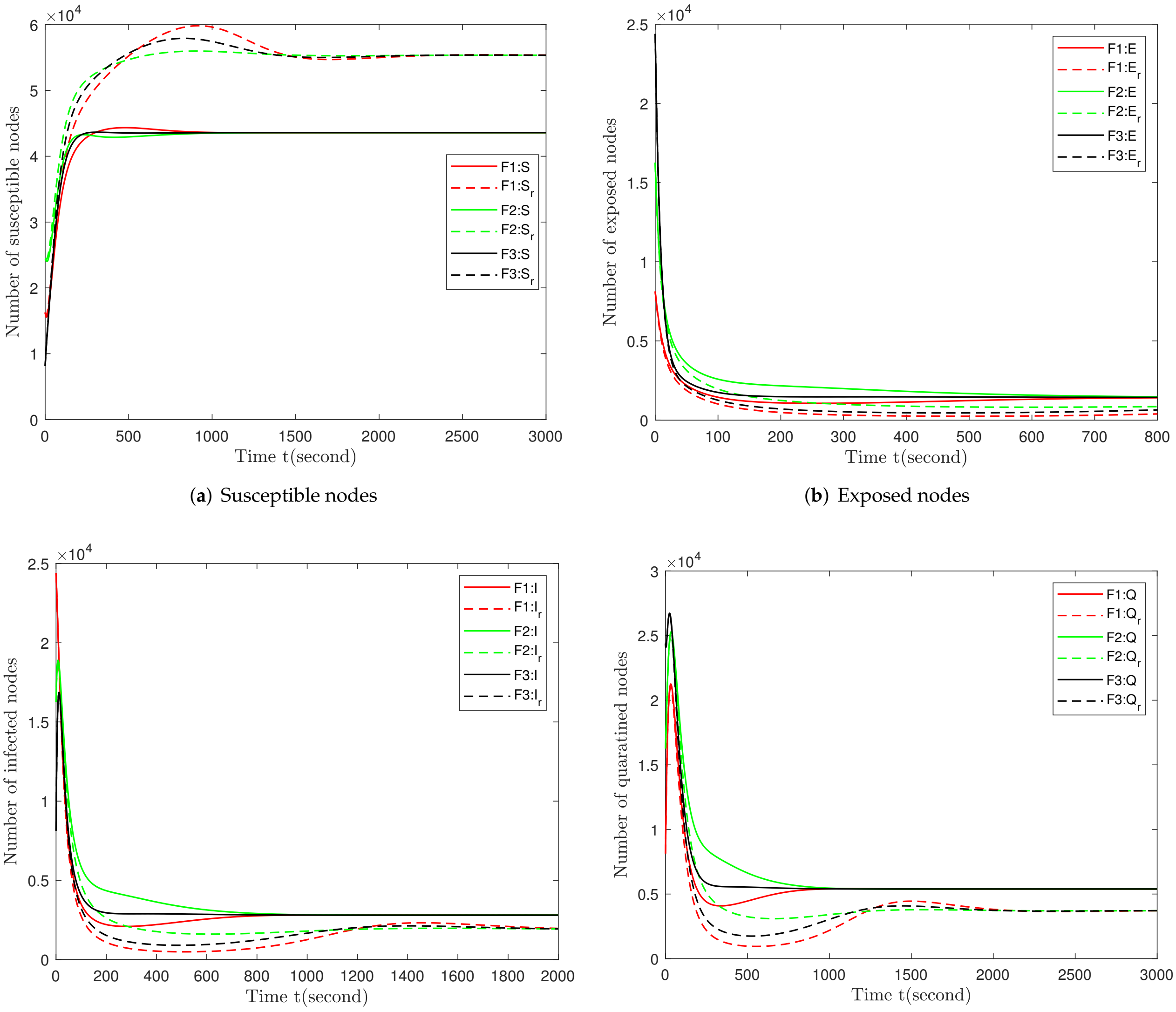
(**e**) Recovered nodes

Figure 6. Trends of the numbers of different nodes for the Reddit dataset.

From Figure 6, we can see that the real dataset and the numerical simulation results are basically the same. With different initial values, the number of nodes in each state eventually tends to stabilize. This means that the stability of the system is not affected by the initial conditions as time passes. This proves the validity of the proposed model.

Example 2. *System (1) will evolve with the parameters in Table 2 and the below initial conditions on the Twitter dataset:*
(F1) (S(0),E(0),Q(0),I(0),R(0)) = (8132,16261, 24391, 24391, 8131),
(F2) (S(0),E(0),Q(0),I(0),R(0)) = (16261, 24392, 8131, 16261, 16261),
(F3) (S(0),E(0),Q(0),I(0),R(0)) = (24391, 8131,16262, 8131, 24391).

Figure 7 depicts the evolution of the two kinds of simulations under Example 2, and they both reach stability. This proves the feasibility of the model and the theoretical results in Section 3. From these five plots, we can see that Figure 7a,b show a larger deviation than the remaining three plots after reaching stability. One possible reason for this is that the two are simulated in different ways.



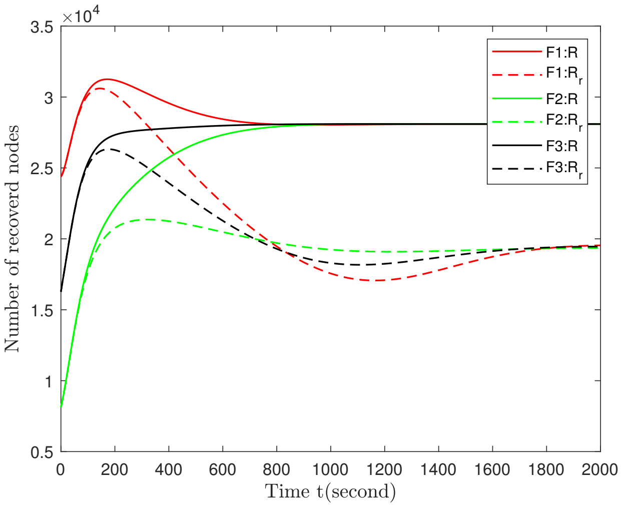
(**a**) Susceptible nodes

(**b**) Exposed nodes

(**c**) Infected nodes

(**d**) Quarantined nodes

Figure 7. *Cont.*



(**e**) Recovered nodes

Figure 7. Trends the numbers of different nodes for the Twitter dataset.

6. Sensitivity Analysis

R_0 is an important parameter to determine whether the malware will die out after its break-out. If $R_0 < 1$, the number of infected computers will decrease to zero in a period of time. If $R_0 > 1$, we will reach the opposite conclusion. Hence, we have to figure out how to reduce R_0 below one by controlling system parameters. By calculating various partial derivatives of R_0, it is obvious that $\frac{\partial R_0}{\partial \beta}$, $\frac{\partial R_0}{\partial \alpha} > 0$ and $\frac{\partial R_0}{\partial \phi}$, $\frac{\partial R_0}{\partial \mu}$, $\frac{\partial R_0}{\partial \eta}$, $\frac{\partial R_0}{\partial \alpha} < 0$, and we can obtain the relationship between R_0 and the other parameters. R_0 has an increasing relationship with β and α, but R_0 decreases along with the increase of ϕ, μ, η, and α. Furthermore, we need the sensitivity of R_0 about different parameters.

Sensitivity analysis is a method that can be used to study the sensitivity of R_0 about system parameters. The estimation of sensitive parameters should be performed with caution because even slight changes in this parameter can result in significant quantitative changes. Therefore, it is important to find out which parameters have a high impact on R_0 through sensitivity analysis.

Definition 1. *The normalized forward sensitivity index of the variable R_0, whose value is dependent on parameter x_i, is defined by (see [51,52]):*

$$\Upsilon_{x_i}^{R_0} = \frac{\partial R_0}{\partial x_i} \times \frac{x_i}{R_0}.$$

So, we can obtain:

$$\Upsilon_{\beta}^{R_0} = \frac{\partial R_0}{\partial \beta} \times \frac{\beta}{R_0} = 1 > 0, \tag{7}$$

$$\Upsilon_{\alpha}^{R_0} = \frac{\partial R_0}{\partial \alpha} \times \frac{\alpha}{R_0} = \frac{\eta + \mu}{\eta + \alpha + \mu} > 0, \tag{8}$$

$$\Upsilon_{\eta}^{R_0} = \frac{\partial R_0}{\partial \eta} \times \frac{\eta}{R_0} = -\frac{\eta}{\eta + \alpha + \mu} < 0, \tag{9}$$

$$\Upsilon_{\mu}^{R_0} = \frac{\partial R_0}{\partial \mu} \times \frac{\mu}{R_0} = -\frac{\eta + \alpha + \phi + 2\mu}{(\phi + \mu)(\eta + \alpha + \mu)} < 0, \tag{10}$$

$$\Upsilon_{\phi}^{R_0} = \frac{\partial R_0}{\partial \phi} \times \frac{\phi}{R_0} = -\frac{\phi}{\phi + \mu} < 0. \tag{11}$$

A conclusion can be drawn from the above five equations. The increase of β and α will cause R_0 increases, while an increase in η, μ, and ϕ will lead to a decrease in R_0. We set up five groups of *parameters with different values in Table 3 to evaluate the sensitivity indices of R_0. Calculating these Equations (7)–(11) with these values of parameters, we can obtain Table 4.*

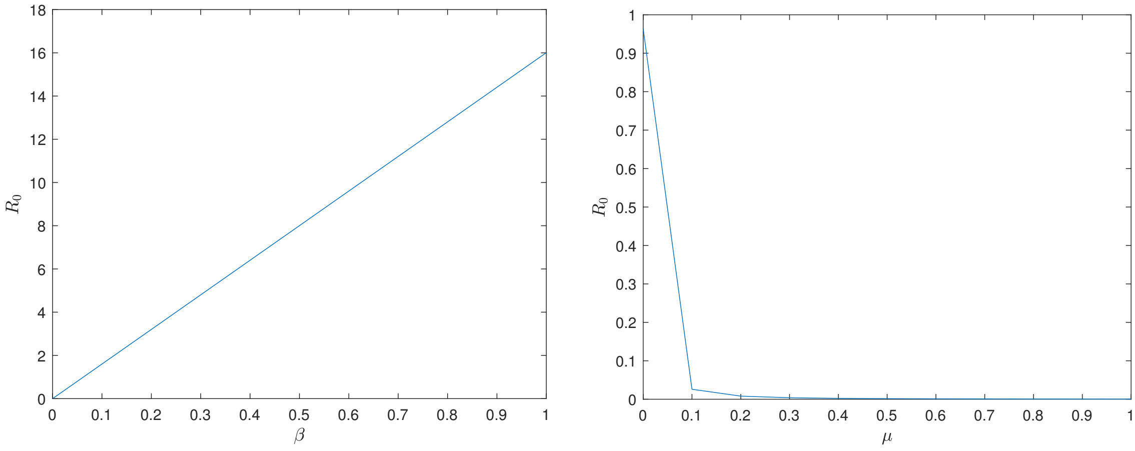
Table 3. Five groups of parameters with different values.

Parameter	β	α	η	μ	ϕ
Group 1	0.1	0.24	0.5	0.7	0.8
Group 2	0.3	0.45	0.6	0.9	0.1
Group 3	0.5	0.75	0.9	0.15	0.28
Group 4	0.7	0.8	0.28	0.4	0.53
Group 5	0.9	0.22	0.29	0.5	0.75

Table 4. The sensitivity indices of R_0.

Parameter	β	α	η	μ	ϕ
Case 1	+1.0000	+0.8333	−0.3472	−0.9528	−0.5333
Case 2	+1.0000	+0.7692	−0.3077	−1.3615	−0.1000
Case 3	+1.0000	+0.5833	−0.5000	−0.4322	−0.6512
Case 4	+1.0000	+0.4595	−0.1892	−0.7004	−0.5699
Case 5	+1.0000	+0.7822	−0.2871	−0.8950	−0.6000

The sensitivity indices of R_0 in Table 4 show that R_0 is most sensitive to β in Cases 1, 3, 4, 5, and μ in Case 2. Figure 8 is presented to describe the relationship between R_0 and β, μ, respectively.



(**a**) R_0 with respect to β

(**b**) R_0 with respect to μ

Figure 8. R_0 with respect to β and μ.

7. Conclusions

In this paper, we briefly introduce malware and some of the damages it causes first. Then, we describe some characteristics of conformity psychology, paving the way for us to study how it affects malware transmission. A deterministic nonlinear SEIQR model considering the conformity psychology in social networks is designed. We calculate the basic reproduction number R_0 and investigate the stability of the two equilibria. There is only one malware-free equilibrium, E_0, which is locally and globally stable when $R_0 < 1$ and one endemic equilibrium which is locally stable when $R_0 > 1$. The simulation results show that conformity psychology plays a great role in preventing the spread of malware. Through the result of sensitivity analysis, we can draw a conclusion that the basic reproduction number is sensitive to the parameters β and μ. Our future work will research more effective methods to control the spread of malware. We are considering complex networks to simulate malware propagation and solve the problems involved.

Author Contributions: Conceptualization, Q.Z., Y.L. and X.L.; methodology, Q.Z.; validation, Y.L. and X.L.; formal analysis, Y.L.; investigation, Y.L.; resources, Q.Z. and K.C.; writing—original draft preparation, Y.L.; writing—review and editing, Q.Z. and K.C.; supervision, Q.Z. and K.C.; funding acquisition, Q.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (Nos. 61903056 and 61702066) and the Chongqing Research Program of Basic Research and Frontier Technology (Nos. cstc2019jcyj-msxmX0681 and cstc2021jcyj-msxmX0761).

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ngo, Q.D.; Nguyen, H.T.; Le, V.H.; Nguyen, D.H. A survey of IoT malware and detection methods based on static features. *ICT Express* **2020**, *6*, 280–286. [CrossRef]
2. Verma, V.; Muttoo, S.K.; Singh, V. Multiclass malware classification via first- and second-order texture statistics. *Comput. Secur.* **2020**, *97*, 101895. [CrossRef]
3. Sudhakar; Kumar, S. An emerging threat Fileless malware: A survey and research challenges. *Cybersecurity* **2020**, *3*, 1–12. [CrossRef]
4. Mimura, M.; Tajiri, Y. Static detection of malicious PowerShell based on word embeddings. *Internet Things* **2021**, *15*, 100404. [CrossRef]
5. Pektaş, A.; Acarman, T. Classification of malware families based on runtime behaviors. *J. Inf. Secur. Appl.* **2017**, *37*, 91–100. [CrossRef]
6. Chen, T.; song Zhang, X.; yuan Li, H.; Wang, D.; Wu, Y. Propagation modeling of active P2P worms based on ternary matrix. *J. Netw. Comput. Appl.* **2013**, *36*, 1387–1394. [CrossRef]
7. Chen, T.; song Zhang, X.; Li, H.; da Li, X.; Wu, Y. Fast quarantining of proactive worms in unstructured P2P networks. *J. Netw. Comput. Appl.* **2011**, *34*, 1648–1659. [CrossRef]
8. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and Other Botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]
9. Akbanov, M.; Vassilakis, V.G.; Logothetis, M.D. Ransomware detection and mitigation using software-defined networking: The case of WannaCry. *Comput. Electr. Eng.* **2019**, *76*, 111–121. [CrossRef]
10. Adams, C. Learning the lessons of WannaCry. *Comput. Fraud. Secur.* **2018**, *2018*, 6–9. [CrossRef]
11. Zhou, P.; Gu, X.; Nepal, S.; Zhou, J. Modeling social worm propagation for advanced persistent threats. *Comput. Secur.* **2021**, *108*, 102321. [CrossRef]
12. Hartmann, L.; Wendzel, S. Anomaly Detection in ICS based on Data-history Analysis. In Proceedings of the European Interdisciplinary Cybersecurity Conference, Rennes, France, 18 November 2020; pp. 1–2.
13. Kumari, S.; Upadhyay, R.K. Exploring the behavior of malware propagation on mobile wireless sensor networks: Stability and control analysis. *Math. Comput. Simul.* **2021**, *190*, 246–269. [CrossRef]
14. Martín del Rey, A.; Casado Vara, R.; Rodríguez González, S. A computational propagation model for malware based on the SIR classic model. *Neurocomputing* **2021**, *484*, 161–171. [CrossRef]
15. Dong, N.P.; Long, H.V.; Khastan, A. Optimal control of a fractional order model for granular SEIR epidemic with uncertainty. *Commun. Nonlinear Sci. Numer. Simul.* **2020**, *88*, 105312. [CrossRef] [PubMed]
16. Han, S.; Lei, C. Global stability of equilibria of a diffusive SEIR epidemic model with nonlinear incidence. *Appl. Math. Lett.* **2019**, *98*, 114–120. [CrossRef]
17. Yang, Y.; Xu, L. Stability of a fractional order SEIR model with general incidence. *Appl. Math. Lett.* **2020**, *105*, 106303. [CrossRef]
18. Wang, X.; Wei, L.; Zhang, J. Dynamical analysis and perturbation solution of an SEIR epidemic model. *Appl. Math. Comput.* **2014**, *232*, 479–486. [CrossRef]
19. Bentaleb, D.; Amine, S. Lyapunov function and global stability for a two-strain SEIR model with bilinear and non-monotone incidence. *Int. J. Biomath.* **2019**, *12*, 1950021. [CrossRef]
20. Karyotis, V.; Khouzani, M. *Malware Diffusion Models for Modern Complex Networks: Theory and Applications*; Morgan Kaufmann: Burlington, MA, USA, 2016; pp. 139–154.
21. Raja, M.A.Z.; Mehmood, A.; Ashraf, S.; Awan, K.M.; Shi, P. Design of evolutionary finite difference solver for numerical treatment of computer virus propagation with countermeasures model. *Math. Comput. Simul.* **2022**, *193*, 409–430. [CrossRef]
22. Tang, W.; Liu, Y.J.; Chen, Y.L.; Yang, Y.X.; Niu, X.X. SLBRS: Network Virus Propagation Model based on Safety Entropy. *Appl. Soft Comput.* **2020**, *97*, 106784. [CrossRef]
23. Yang, F.; Zhang, Z. Hopf bifurcation analysis of SEIR-KS computer virus spreading model with two-delay. *Results Phys.* **2021**, *24*, 104090. [CrossRef]
24. Yang, F.; Zhang, Z.; Zeb, A. Hopf bifurcation of a VEIQS worm propagation model in mobile networks with two delays. *Alex. Eng. J.* **2021**, *60*, 5105–5114. [CrossRef]

25. Pei, Y.; Liu, S.; Gao, S.; Li, S.; Li, C. A delayed SEIQR epidemic model with pulse vaccination and the quarantine measure. *Comput. Math. Appl.* **2009**, *58*, 135–145. [CrossRef]
26. Gao, Q.; Zhuang, J. Stability analysis and control strategies for worm attack in mobile networks via a VEIQS propagation model. *Appl. Math. Comput.* **2020**, *368*, 124584. [CrossRef]
27. Magagula, V.M.; Mungwe, S.N. Stability analysis of a virulent code in a network of computers. *Math. Comput. Simul.* **2021**, *182*, 296–315. [CrossRef]
28. Xiao, X.; Fu, P.; Dou, C.; Li, Q.; Hu, G.; Xia, S. Design and analysis of SEIQR worm propagation model in mobile internet. *Commun. Nonlinear Sci. Numer. Simul.* **2017**, *43*, 341–350. [CrossRef]
29. Piqueira, J.R.C.; Batistela, C.M. Considering quarantine in the SIRA malware propagation model. *Math. Probl. Eng.* **2019**, *2019*, 6467104. [CrossRef]
30. Badea, C.; Binning, K.R.; Sherman, D.K.; Boza, M.; Kende, A. Conformity to group norms: How group-affirmation shapes collective action. *J. Exp. Soc. Psychol.* **2021**, *95*, 104153. [CrossRef]
31. Li, D.; Du, J.; Sun, M.; Han, D. How conformity psychology and benefits affect individuals' green behaviours from the perspective of a complex network. *J. Clean. Prod.* **2020**, *248*, 119215. [CrossRef]
32. Hosseini, S.; Azgomi, M.A. The dynamics of an SEIRS-QV malware propagation model in heterogeneous networks. *Phys. A Stat. Mech. Its Appl.* **2018**, *512*, 803–817. [CrossRef]
33. Miao, Q.; Tang, X.; Quan, Y. A Novel Email Virus Propagation Model with Local Group. In Proceedings of the 2014 IEEE 11th Intl Conf on Ubiquitous Intelligence and Computing and 2014 IEEE 11th Intl Conf on Autonomic and Trusted Computing and 2014 IEEE 14th Intl Conf on Scalable Computing and Communications and Its Associated Workshops, Bali, Indonesia, 9–12 December 2014; pp. 331–336.
34. Zhu, Q.; Luo, X.; Liu, Y. Modeling and Analysis of the Spread of Malware with the Influence of User Awareness. *Complexity* **2021**, *2021*, 6639632. [CrossRef]
35. Fang, H.; Li, X.; Zhang, J. Integrating social influence modeling and user modeling for trust prediction in signed networks. *Artif. Intell.* **2022**, *302*, 103628. [CrossRef]
36. Ghafari, S.M.; Beheshti, A.; Joshi, A.; Paris, C.; Mahmood, A.; Yakhchi, S.; Orgun, M.A. A Survey on Trust Prediction in Online Social Networks. *IEEE Access* **2020**, *8*, 144292–144309. [CrossRef]
37. Yu, Z.; Lu, S.; Wang, D.; Li, Z. Modeling and analysis of rumor propagation in social networks. *Inf. Sci.* **2021**, *580*, 857–873. [CrossRef]
38. Cauteruccio, F.; Cinelli, L.; Fortino, G.; Savaglio, C.; Terracina, G.; Ursino, D.; Virgili, L. An approach to compute the scope of a social object in a Multi-IoT scenario. *Pervasive Mob. Comput.* **2020**, *67*, 101223. [CrossRef]
39. Meo, P.D. Trust Prediction via Matrix Factorisation. *ACM Trans. Internet Technol.* **2019**, *19*, 1–20. [CrossRef]
40. Jia, P.; Liu, J.; Fang, Y.; Liu, L.; Liu, L. Modeling and analyzing malware propagation in social networks with heterogeneous infection rates. *Phys. A Stat. Mech. Its Appl.* **2018**, *507*, 240–254. [CrossRef]
41. Du, B.; Wang, H. Partial differential equation modeling of malware propagation in social networks with mixed delays. *Comput. Math. Appl.* **2018**, *75*, 3537–3548. [CrossRef]
42. Bozkurt, F.; Yousef, A.; Abdeljawad, T.; Kalinli, A.; Mdallal, Q.A. A fractional-order model of COVID-19 considering the fear effect of the media and social networks on the community. *Chaos Solitons Fractals* **2021**, *152*, 111403. [CrossRef]
43. Liu, R.; Wu, J.; Zhu, H. Media/psychological impact on multiple outbreaks of emerging infectious diseases. *Comput. Math. Methods Med.* **2007**, *8*, 153–164. [CrossRef]
44. Sahu, G.P.; Dhar, J. Dynamics of an SEQIHRS epidemic model with media coverage, quarantine and isolation in a community with pre-existing immunity. *J. Math. Anal. Appl.* **2015**, *421*, 1651–1672. [CrossRef] [PubMed]
45. Yuan, H.; Chen, G. Network virus-epidemic model with the point-to-group information propagation. *Appl. Math. Comput.* **2008**, *206*, 357–367. [CrossRef]
46. Sheng, C.; Yao, Y.; Fu, Q.; Yang, W.; Liu, Y. Study on the intelligent honeynet model for containing the spread of industrial viruses. *Comput. Secur.* **2021**, *111*, 102460. [CrossRef]
47. Castillo-Chavez, C.; Song, B. Dynamical models of tuberculosis and their applications. *Math. Biosci. Eng.* **2004**, *1*, 361. [CrossRef]
48. Chavez, C.C.; Feng, Z.; Huang, W. On the computation of R_0 and its role on global stability. *Math. Approaches Emerg. Emerg. Infect. Dis. Introd.* **2002**, *125*, 31–65.
49. Social Network: Reddit Hyperlink Network. Available online: http://snap.stanford.edu/data/soc-RedditHyperlinks.html (accessed on 9 September 2022).
50. Social Circles: Twitter. Available online: http://snap.stanford.edu/data/ego-Twitter.html (accessed on 9 September 2022).
51. Ndaïrou, F.; Area, I.; Nieto, J.J.; Torres, D.F. Mathematical modeling of COVID-19 transmission dynamics with a case study of Wuhan. *Chaos Solitons Fractals* **2020**, *135*, 109846. [CrossRef] [PubMed]
52. Chitnis, N.; Hyman, J.M.; Cushing, J.M. Determining Important Parameters in the Spread of Malaria Through the Sensitivity Analysis of a Mathematical Model. *Bull. Math. Biol.* **2008**, *70*, 5. [CrossRef] [PubMed]