Information **2015**, *6*, 536-549; doi:10.3390/info6030536

OPEN ACCESS

information

ISSN 2078-2489

www.mdpi.com/journal/information

Article

Influences of Removable Devices on the Anti-Threat Model: Dynamic Analysis and Control Strategies

Jinhua Ma *, Zhide Chen †, Wei Wu †, Rongjun Zheng † and Jianghua Liu †

Key Lab of Network Security and Cryptography, School of Mathematics and Computer Sciences, Fujian Normal University, Fuzhou, 350007, China; E-Mails: zhidechen@fjnu.edu.cn (Z.C.); weiwu81@gmail.com (W.W.); fujiandiyi009@hotmail.com (R.Z.); jianghualiu11@gmail.com (J.L.)

† These authors contributed equally to this work.

* Author to whom correspondence should be addressed; E-Mail: jinhuamam@163.com; Tel.: +86-158-0606-2482.

Academic Editors: Qiong Huang and Guomin Yang

Received: 22 May 2015 / Accepted: 20 August 2015 / Published: 24 August 2015

Abstract: With the rapid development of M2M wireless network, damages caused by malicious worms are getting more and more serious. The main goal of this paper is to explore the influences of removable devices on the interaction dynamics between malicious worms and benign worms by using a mathematical model. The model takes two important network environment factors into consideration: benign worms and the influences of removable devices. Besides, the model's basic reproduction number is obtained, along with the correct control conditions of the local and global asymptotical stability of the worm-free equilibrium. Simulation results show that the effectiveness of our proposed model in terms of reflecting the influences of removable devices on the interaction dynamics of an anti-treat model. Based on numerical analyses and simulations, effective methods are proposed to contain the propagation of malicious worms by using anti-worms.

Keywords: M2M wireless network; malicious worms; benign worms; interaction dynamics; basic reproduction number

1. Introduction

Worm is a program that can run by itself and can replicate and spread autonomously in the network. With the rapid development of information technology, M2M technologies have been widely used in mobile communication, medical care, military reconnaissance, and so on. An M2M wireless network is a network which is based on the intelligent interaction among smart devices, and it is a blending of several heterogeneous networks, such as WAN (Wide Area Network), LAN (Local Area Network) and PAN (Personal Area Network), its application has evolved widely. According to the 2015 Symantec Global Internet Security Threat Report [1], the year 2014 was a year with far-reaching vulnerabilities, faster attacks, files held for ransom, and far more malicious code than in previous years. While people are enjoying the convenience, the damages caused by malicious worms and their variants in M2M wireless network are becoming increasingly serious, due to the variety of network forms, the openness of information, the mobility of communication applications, the security vulnerability of operating systems, the complexity of network nodes, and so on. The most significant difference between a traditional computer network infection and M2M wireless network is that the latter evolved much faster and can cause broader and more dangerous harm, as the latter contains more mobile devices and wireless devices.

Currently, a number of detection and defense technologies have been proposed to contain worm propagation, but they cannot fundamentally solve those problems. In addition to benign worms, there exist beneficial worms which can dynamically proactive defense against the malicious worm propagation and patch for the susceptible hosts. Thus benign worms can solve the malicious worm propagation problem to a large degree and they have been a potential solution to restrain and resist the spread of malicious worms. Even though users lack cybersecurity awareness or take poor security measures, benign worms also can maintain the network security. Therefore, worm-anti-worm strategy is a best-effort approach to contain the spread of malicious worms. That is why in this paper we first consider using benign worms to counter the malicious worms. Motivated by this, we propose a novel dynamical model to study the dynamics of interaction infection between malicious worms and benign worms. Through theory analysis and simulation, this article studies the dynamical behaviors of the two-worm interaction.

As we all know, removable devices provide another way other than the Internet for the spread of worms. However, nearly all previous models [2–15] ignore the fact that worms can infect not only the computers but also many kinds of external wireless or wired removable devices, e.g., external hard drives, USB drives, mobile phones, wireless handheld devices, *etc*. With the development of WiFi and M2M wireless network technology, the M2M wireless network has a certain large coverage area in large cities, and even in some remote areas. While people are enjoying the convenience, worms can exploit the various wireless networks and threaten the cyber space. According to the Symantec security response, the first wireless worm appeared in 2004, which exploited vulnerabilities in the Symbian OS and propagated through Bluetooth wireless connections. Different from the spreading form of worms in traditional networks, worms can inadvertently send copies of themselves to some other nodes that can be infected. Studies show that, due to most wireless protocols allowing neighborhood discovery, proximity of wireless devices can promote worm propagation. Besides, the mobility of removable devices helps to transport worms to a lager geographic space and allows them to last for a longer time.

Therefore, it is important to study the dynamics of interaction infection between computers and removable devices. Motivated by this, we propose a novel dynamical model based on the above facts.

In this article, we analyze the malicious worm propagation in an M2M wireless network by using the mathematical model. We consider the influences of removable devices on the interaction dynamics between malicious worms and benign worms in our model. By investigating the local stability of the worm-free equilibrium, we obtain the basic reproduction number. By choosing a suitable Lyapunov function, we prove the asymptotical stability of worm propagation. Crucially, we obtain the effective threshold of controlling the spread of malicious worms.

The rest of this paper is organized as follows. Section 2 describes some related works of worm propagation models. Section 3 presents the novel worm anti-treat model and gives the relevant proofs of stability. Simulation and control strategies are given in Section 4. Finally, Section 5 concludes this paper.

2. Related Works

2.1. Existing Worm Propagation Models

In the past several decades, based on the great similarity between biological viruses and network worms, many worm propagation models were presented to understand the propagation mechanisms of worms and study the corresponding control strategies.

The classical simple epidemic models [2] only consist of two states of nodes: susceptible and infectious, which is also called the SI model. Due to the fact that the SI model does not consider the cases where the infected and infectious nodes are patched or removed, it is not suitable for a real situation. The Kermack-McKendrick epidemic model [3] (also known as KM model) makes up the shortcoming of SI model, and considers an additional removal state, the nodes translate from the susceptible to the infectious or to the removal state. Paper [4] proposed an extended stochastic diffusion model for the KM model in which the infectivity of an individual depends on the time since the individual became infective [5]. The article [6] provided a two-factor worm model based on the classical epidemic KM model, it carefully analyzed the propagation of Red Code by considering more external factors (one is the dynamic countermeasures taken by ISPs and users, the other is the slowed down worm infection rate because of network congestion and troubles to some routers). Later, many extended models were proposed, e.g., SEIRS model [7], VEISV model [8], SEIQRS model [9], SEIDQV model [10], which separate nodes' states into more varieties and consider passive recovery measures without adding active defense measures.

Worm-Anti-Worm (WAW) models consider two kinds of worms: a malicious worm and a benign worm [11]. Benign worm proactive defenses against the malicious worm propagation and patches for the susceptible hosts. Models [12–15] explored the interaction dynamics between malicious worms and benign worms. When the benign worm is absent, a WAW model is subject to the two-factor model.

To capture the influences of removable devices on the spread of worm, some worm models have been proposed. Based on the KM model, Song *et al.* presented a model to characterize the essential properties of AutoRun worms, in which a removable device would be infected with a certain rate if it was used on an infectious computer and then it can infect other computers whenever in was used on them [16]. In [17,18], Yang *et al.* addressed the influences of removable devices on the spread of viruses and investigated more complex dynamics. These models provide a reasonable qualitative understanding of the conditions under considering the influences of removable devices.

2.2. The Limitation of Existing Worm Propagation Models

Researchers have qualitatively understood the propagation mechanisms of worms and studied the corresponding control strategies by using mathematical modeling. Unfortunately, to our knowledge, none of the existing models have researched the influences of removable devices on the interaction dynamics between malicious worms and benign worms.

2.3. Our Proposed Worm Propagation Model

In our model, based on the diversity of nodes types in M2M wireless network, we explore the influences of removable devices on the interaction dynamics between malicious worms and benign worms. We take two important network environment factors into consideration: benign worms and the influences of removable devices. We find the basic reproduction number of our model and the correct control conditions of the local and global asymptotical stabilities of the worm-free equilibrium. We also obtain the effective threshold of controlling the spread of malicious worms. Furthermore, simulation results show the effectiveness of our model. Finally, effective control strategies are proposed to combat malicious worms.

3. The Model

In a wireless M2M network, we divide nodes into two types: fixed nodes and removable nodes. Fixed nodes are fixed computers, while removable nodes are wireless mobile devices with networking capability, such as mobile phones and tablet computers, or removable devices with no networking capability, such as hard drives and USB drives. The worm propagation behavior on fixed nodes is similar to the spreading behavior of worms in a traditional network, but different from it when it comes to removable devices. All the wireless removable devices autonomously roam in the network: when wireless devices are connected to network and move to the sensing area of nodes, the worms can detect possible vulnerabilities in the equipment and prepare for the infections. When removable devices without networking capability are connected to computers, the worms that exist in them can infect susceptible computers; moreover, they also can be infected by worms that exist in those computers.

Our model is based on the following assumptions: (1) Our model falls under the category of a homogeneous worm propagation model, that means, our model ignores the network topology and it is based on the concept of a network fully-connected graph; (2) We assume that the number of total fixed nodes is N, total removable nodes is R_N and other states of nodes do not change in unit time t; (3) We assume that removable devices are used equally in the whole network; (4) Since the number of removable devices users is huge, and the users exist in all over the network, we assume that removable nodes are uniform distribution in the whole network; (5) All newly fixed nodes and removable nodes accessed the network are susceptible; (6) Once fixed nodes are immunized, they will gain permanent immunity and can no longer be infected by malicious worms; (7) We assume all nodes will remain in their state when they get out of the network; (8) Wireless removable devices' worms have no space constrains and can be connected to a network to carry out a wider range of transmission.

In our model, all nodes are in six compartments: susceptible fixed nodes (S)-nodes are healthy but are not immune to AutoRun worms; fixed nodes infected by malicious worm (I); fixed nodes infected by benign worm (B); immunized nodes (V)-nodes have been immunized by anti-virus program, firewall or benign worms; susceptible removable nodes (R_S)-removable nodes without malicious worms; infected removable nodes (R_I)-removable nodes have infected by malicious worm and can infect other susceptible nodes. At any time t, the total fixed nodes are $N(t)=S(t)+I(t)+B(t)+V(t)$, and the total removable nodes are $R_N(t)=R_S(t)+R_I(t)$. The six states and state transition in our model are shown in Figure 1.

The notations in Figure 1 are listed as follows. b_1 and b_2 respectively are the number of new fixed and removable nodes join the network. ω_1 and ω_2 represent the immunized rate of susceptible fixed nodes and susceptible removable nodes by using anti-virus program and firewall, respectively. β_1 and β_2 are the effective infection rates of malicious worms and benign worms, respectively. μ_1 and μ_2 respectively represent the obsolescence rate of fixed nodes and removable nodes. δ is the self-destruct rate of benign worms after completing repair work. λ is the online rate of removable nodes.

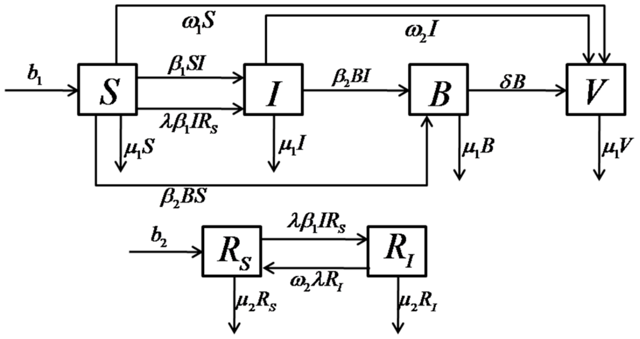


Figure 1. State transition diagram of our model.

Let $\lambda\beta_1=\beta_3, \lambda\omega_2=\omega_3$, based on Figure 1 we can obtain the equations of the model as follows:

$$\begin{cases}\dfrac{dS(t)}{dt}=b_1-\beta_1 S(t)I(t)-\beta_2 B(t)S(t)-\beta_3 S(t)R_I(t)-\omega_1 S(t)-\mu_1 S(t)\\ \dfrac{dI(t)}{dt}=\beta_1 S(t)I(t)+\beta_3 S(t)R_I(t)-\beta_2 B(t)I(t)-\omega_2 I(t)-\mu_1 I(t)\\ \dfrac{dB(t)}{dt}=\beta_2 B(t)S(t)+\beta_2 B(t)I(t)-\delta B(t)-\mu_1 B(t)\\ \dfrac{dV(t)}{dt}=\omega_1 S(t)+\omega_2 I(t)+\delta B(t)-\mu_1 V(t)\\ \dfrac{dR_S(t)}{dt}=b_2-\beta_3 I(t)R_S(t)+\omega_3 R_I(t)-\mu_2 R_S(t)\\ \dfrac{dR_I(t)}{dt}=\beta_3 I(t)R_S(t)-\omega_3 R_I(t)-\mu_2 R_I(t)\end{cases} \tag{1}$$

From system Equation (1), we can set the model's feasible region as

$$\mathrm{U}=\{(S,I,B,V,R_S,R_I)\in R_+^6 : S,I,B,V,R_S,R_I\geq 0, S+I+B+V=N, R_S+R_I=R_N\}$$

U is positively invariant for system Equation (1), we will analyze the stabilities of Equation (1) in the set U.

3.1. The Basic Reproductive Number of Our Model

The basic reproductive number R_0, is a key concept in epidemiology, and it is one of the most important and most valuable ideas that mathematical thinking has brought to epidemic theory [19]. In epidemiology, the meaning of R_0 is that the number of susceptible nodes infected by an infected node in its entire infectious time. When $R_0 \leq 1$, it means the worms in the network will be cleared finally. When $R_0 > 1$, we can predict that the worms will be prevalent. Thus, we can control the propagation of worms by controlling R_0.

By counting, we can easily obtain the equilibriums of model (1). The worm-free equilibrium is $P_0=(S_0,I_0,B_0,V_0,R_{S0},R_{I0})=(\frac{b_1}{\omega_1+\mu_1},0,0,\frac{\omega_1 b_1}{\mu_1(\omega_1+\mu_1)},\frac{b_2}{\mu_2},0)$, the endemic equilibrium is $P_1=(S_1,I_1,B_1,V_1)$, where:

$$\begin{aligned}
&S_1=\left(\sqrt{B^2-4AC}-B\right)/\left(2A\right),\\
&I_1=\left(a_3-\beta_2 S_1\right)/\beta_2,\\
&B_1=\left(b_1-a_4 S_1-a_1 I_1\right)/a_3,\\
&V_1=b_1/\mu_1-S_1-I_1-B_1
\end{aligned}$$

$$R_{S1}=b_2/\mu_2-R_{I1},\ R_{I1}=\beta_2 b_2 I_1/\left[\mu_2(\beta_3 I_1+a_2)\right],$$

$$a_1=\omega_2+\mu_1,\ a_2=\omega_3+\mu_2,\ a_3=\delta+\mu_1,\ a_4=\omega_1+\mu_1,$$

$$\begin{aligned}
&A=-\beta_2\beta_3\left(a_1\beta_1-a_3\beta_1-a_4\beta_2\right),\\
&B=-A\left(a_2/\beta_2+a_3/\beta_3\right)-b_1\beta_2{}^2\beta_3-a_3\beta_2\beta_3{}^2 b_2/\mu_2,\\
&C=b_1\beta_2\left(a_3\beta_3+a_2\beta_2\right)
\end{aligned}$$

In order to obtain the basic reproductive number R_0, let $\vec{x}=(I,B,R_I,V,S,R_S)^T$, and $\frac{d\vec{x}}{dt}=F(\vec{x})-V(\vec{x})$, where

$$F(\vec{x})=\left(\beta_1 SI+\beta_3 SR_I\ \beta_2 SB+\beta_2 BI\ \beta_3 IR_S\ 0\ 0\ 0\right)^T$$

$$V(\vec{x})=\begin{pmatrix}\beta_2 BI+a_1 I\\ a_3 B\\ a_2 R_I\\ \mu_1 V-\omega_1 S-\omega_2 I-\delta B\\ \beta_1 SI+\beta_2 BS+\beta_3 SR_I+a_4 S-b_1\\ \beta_3 IR_S+\mu_2 R_S-\omega_3 R_I-b_2\end{pmatrix}$$

Because

$$W_1 = DF(P_0) = \begin{pmatrix} \beta_1 S_0 & 0 & \beta_3 S_0 & 0 & 0 & 0 \\ 0 & \beta_2 S_0 & 0 & 0 & 0 & 0 \\ \beta_3 R_S & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and

$$W_2 = DV(P_0) = \begin{pmatrix} a_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & a_3 & 0 & 0 & 0 & 0 \\ 0 & 0 & a_2 & 0 & 0 & 0 \\ -\omega_2 & -\delta & 0 & \mu_1 & -\omega_1 & 0 \\ \beta_1 S_0 & \beta_2 S_0 & \beta_3 S_0 & 0 & a_4 & 0 \\ \beta_1 R_{S0} & 0 & -\omega_3 & 0 & 0 & \mu_2 \end{pmatrix}$$

the spectral radius of $W_1 W_2^{-1}$ is $\rho = \max(\rho_1, \rho_2)$, where

$$\rho_1 = \frac{\beta_1 S_0 + \sqrt{\beta_1{}^2 S_0{}^2 + 4\frac{a_1}{a_2}\beta_3{}^2 S_0 R_{S0}}}{2a_1} = \frac{\frac{\beta_1 b_1}{\omega_1 + \mu_1} + \sqrt{\beta_1{}^2 \frac{b_1^2}{(\omega_1 + \mu_1)^2} + 4\frac{\omega_2 + \mu_1}{\omega_3 + \mu_2}\beta_3{}^2 \frac{b_1}{\omega_1 + \mu_1} \cdot \frac{b_2}{\mu_2}}}{2(\omega_2 + \mu_1)}$$

and

$$\rho_2 = \frac{\beta_2 S_0}{a_3} = \frac{\beta_2 b_1}{(\mu_1 + \delta)(\mu_1 + \omega_1)}$$

According to the Theorem in [20], we know the basic reproductive number of model Equation (1) is $R_0 = \rho = \max(\rho_1, \rho_2)$. Especially, ρ_1 and ρ_2 respectively are the basic reproductive number of malicious worms and benign worms in our model. In this paper we will use $R_0 = \rho = \max(\rho_1, \rho_2)$ to analyze the stabilities of system Equation (1).

3.2. The Stability Analysis for Worm-Free Equilibrium P_0

In epidemiology, one equilibrium of a propagation model represents one final spreading trend of worms. The aim of this section is to prove the correctness of the basic reproductive number R_0 by analyzing the stability of worm-free equilibrium, and to get the correct control conditions of worm-free equilibrium by adjusting R_0.

3.2.1. The Local Asymptotical Stability of Worm-free Equilibrium P_0

Theorem 1. *When $R_0 \le 1$, the unique worm-free equilibrium P_0 is locally asymptotically stable in the model's feasible region U, and unstable when $R_0 > 1$.*

Proof. The Jacobian matrix at the worm-free equilibrium P_0 is

$$J(P_0)=\begin{pmatrix} -a_4 & -\beta_1 S_0 & -\beta_2 S_0 & 0 & 0 & -\beta_3 S_0 \\ 0 & \beta_1 S_0 - a_1 & 0 & 0 & 0 & \beta_3 S_0 \\ 0 & 0 & \beta_2 S_0 - a_3 & 0 & 0 & 0 \\ \omega_1 & \omega_2 & \delta & -\mu_1 & 0 & 0 \\ 0 & -\beta_3 R_{S0} & 0 & 0 & -\mu_2 & \omega_3 \\ 0 & \beta_3 R_{S0} & 0 & 0 & 0 & -a_2 \end{pmatrix}.$$

The corresponding eigenvalues of $J(P_0)$ are $\lambda_1=-\mu_1, \lambda_2=-\mu_2, \lambda_3=-a_4, \lambda_4=\beta_2 S_0 - a_3$, $\lambda_5=(D+E)/2, \lambda_6=(D-E)/2$, where $E=\sqrt{\beta_1{}^2 S_0{}^2+4\beta_3{}^2 S_0 R_{S0}+(a_2-a_1)^2+2\beta_1 S_0(a_2-a_1)}$, and $D=\beta_1 S_0-(a_1+a_2)$. $a_2 \le a_1$ because $0 \le \lambda \le 1, \mu_2 \le \mu_1, \omega_3=\lambda\omega_2 \le \omega_2$. According to the stability theory in [21], we know that the sufficient conditions are $\lambda_i<0$ for the six-dimensional model to be asymptotically stable, where $i=1,2,3,4,5,6$. All parameters of this model are assumed to be positive. Obviously, in this model $\lambda_1<0$, $\lambda_2<0$, and $\lambda_3<0$. If $\lambda_4<0$, it is equivalent to $\beta_2 S_0/a_3<1$, that is $\rho_2<1$. Because:

$$\begin{aligned}
\lambda_6 &= (D+E)/2 \\
&= \frac{\beta_1 S_0+(a_2-a_1)}{2}-a_2+\frac{\sqrt{[\beta_1 S_0+(a_2-a_1)]^2+4\beta_3{}^2 S_0 R_{S0}}}{2} \\
&\le \frac{\beta_1 S_0+\sqrt{\beta_1{}^2 S_0{}^2+4\beta_3{}^2 S_0 R_{S0}}}{2}-a_2 \\
&\le \frac{\beta_1 S_0+\sqrt{\beta_1{}^2 S_0{}^2+4\frac{a_1}{a_2}\beta_3{}^2 S_0 R_{S0}}}{2}-a_2 \\
&= a_2\Big(\frac{a_1}{a_2}\cdot\frac{\beta_1 S_0+\sqrt{\beta_1{}^2 S_0{}^2+4\frac{a_1}{a_2}\beta_3{}^2 S_0 R_{S0}}}{2}-1\Big) \\
&= a_2\Big(\frac{a_1}{a_2}\cdot\rho_1-1\Big)
\end{aligned}$$

If $\lambda_6<0$, it is approximatively equal to $\rho_1<1$. Therefore, when the condition meets $R_0=\rho=\max(\rho_1,\rho_2)<1$, the propagation of malicious worms will be controlled. According to Routh-Hurwits criterion [22], the unique worm-free equilibrium P_0 is locally asymptotically stable. When $R_0>1$, it means that $J(P_0)$ has two or three positive eigenvalues, therefore P_0 is an unstable saddle point in the model's feasible region U . This proof is completed. □

3.2.2. The Global Asymptotical Stability of Worm-free Equilibrium P_0

Theorem 2. *When $R_0 \le 1$, the worm-free equilibrium P_0 is globally asymptotically stable in the model's feasible region U, and unstable when $R_0>1$.*

Proof. From the first equation in system Equation (1), we can get $S(t)' \le b_1-(\omega_1+\mu_1)S$, so $S(t)\le b_1/(\omega_1+\mu_1)+\left[S(0)-b_1/(\omega_1+\mu_1)\right]e^{-(\omega_1+\mu_1)t}$. Thus, when $t\to\infty$, $S(t)\le b_1/(\omega_1+\mu_1)$. Similarly, from the fifth equation in Equation (1), we can get $R_S(t)^{'} \le b_2 - \mu_2 R_S$, so $R_S(t) \le b_2/\mu_2 + \left[R_S(0) - b_2/\mu_2\right]e^{-\mu_2 t}$. Thus, when $t \to \infty$, $R_S(t) \le b_2/\mu_2$. To measure the global asymptotical stability of worm-free equilibrium, we choose a Lyapunov function like this: $L(t) = I(t)R_I(t) + B(t)R_I(t) + R_S(t)$. Its time derivative along the solutions to the model Equation (1) is

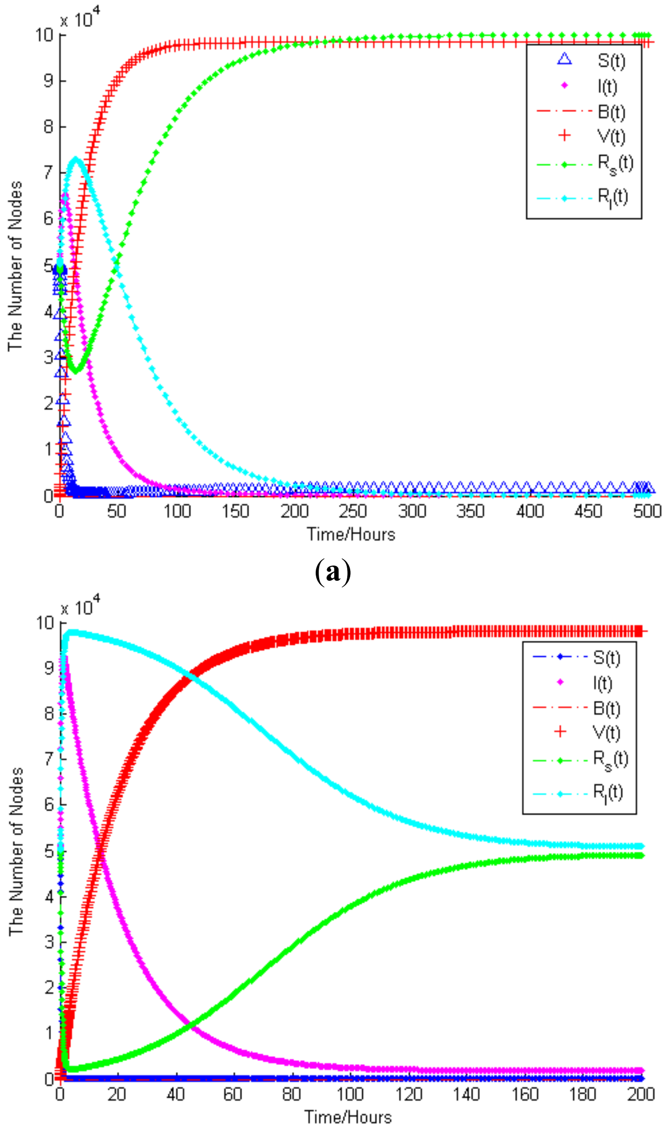
$$\begin{aligned}
L^{'} &= B^{'}R_I + BR_I^{'} + I^{'}R_I + IR_I^{'} + R_S^{'} \\
&= \left[\beta_2 BS + \beta_2 BI - a_3 B\right]R_I + \left(\beta_3 IR_S - a_2 R_I\right)B + \left(\beta_1 SI + \beta_3 SR_I - \beta_2 BI - a_1 I\right)R_I + \left(\beta_3 IR_S - a_2 R_I\right)I + R_S^{'} \\
&\le \left[\beta_2 BSR_I - a_3 BR_I\right] + B\left(\beta_3 IR_S - a_2 R_I + R_S^{'}\right) + IR_I\left(\beta_1 S - a_1 - a_2 + \beta_3 SR_I/I + \beta_3 R_S I/R_I\right) \\
&\le a_3 BR_I\left(\beta_2 S/a_3 - 1\right) + b_1 B\left(1 - 2\mu_2 R_N/b_2\right) + IR_I\left[\beta_1 S - 2a_1 + \sqrt{\left(\beta_3 SR_I/I + \beta_3 R_S I/R_I\right)^2}\right] \\
&\le a_3 BR_I\left(\beta_2 S/a_3 - 1\right) - b_1 B + IR_I\left[\beta_1 S - 2a_1 + \sqrt{\left(\beta_3 SR_I/I\right)^2 + 4\beta_3^{2} SR_S}\right] \\
&\le a_3 BR_I\left(\beta_2 S/a_3 - 1\right) - b_1 B + IR_I\left(\beta_1 S - 2a_1 + \sqrt{\beta_1^{2} S^2 + 4\frac{a_1}{a_2}\beta_3^{2} SR_S}\right) \\
&\le a_3 BR_I\left(\rho_1 - 1\right) + 2a_1 IR_I\left(\rho_2 - 1\right) \\
&\le 0
\end{aligned}$$

We can know that only at P_0, $L(t)^{'} = 0$. According to the LaSalle's invariance principle in [23], when $R_0 \le 1$, the worm-free equilibrium P_0 is globally asymptotically stable in the model's feasible region U . When $R_0 > 1$, it means that $L(t)^{'} > 0$ and P_0 is unstable in U . This proof is completed. □

4. Simulations and Control Strategies

4.1. Simulations

In this section, we will analyze the stability of our model and the influences of removable devices on the interaction dynamics between the malicious worms and the benign worms, by using MATLAB simulation tool. First, we set $b_1 = b_2 = 100, \beta_1 = 2\times10^{-6}, \beta_2 = 2\times10^{-5}, \omega_1 = 0.06, \omega_2 = 0.05, \omega_3 = 0.035$, $\mu_1 = \mu_2 = 0.001, \delta = 0.5, \lambda = 1$. At the beginning, the number of all kinds of nodes are $\left(S(0), I(0), B(0), V(0), R_S(0), R_I(0)\right) = \left(50000, 50000, 0, 0, 50000, 50000\right)$. We can obtain the basic reproduction number $R_0 = 0.6306 < 1$ by using above parameters. The results are shown in Figure 2a. It shows that the two kinds of malicious worms (I and R_I) will gradually disappear, which proves the correctness of Theorems 1 and 2. When $\beta_1 = 2\times10^{-5}$ and other parameters do not change, $R_0 = 6.3063 > 1$, and we can see the results in Figure 2b. Different from Figure 2a, the two kinds of malicious worms in Figure 2b are prevalent in network, and all states reach their equilibrium points. This is also consistent with Theorems 1 and 2.



(**a**)

(**b**)

Figure 2. (**a**) When $R_0 \le 1$, worm-free equilibrium is globally asymptotically stable; (**b**) When $R_0 > 1$, the two kinds of malicious worms will be prevalent.

In the third experiment, we will evaluate the effects of benign worms. Let $\omega_1 = 0.04, \omega_2 = \omega_3 = 0.03, B(0) = 50$, and leave the other arguments intact. The results are shown in Figure 3. It shows that benign worms can not only decrease the number of two kinds of malicious infected nodes, but can also reduce the malicious worm propagation speed. However, when $\rho_1 > 1 > \rho_2$, benign worms cannot change the prevalent propagation phenomenon of malicious worms; when $\rho_2 > \rho_1 > 1$, these two kinds of malicious infected nodes are all died out, the prevalent propagation phenomenon of malicious worms is changed by benign worms. The conclusion provides a strong theoretical basis to take effective measures to control the large-scale spreading of malicious worms.

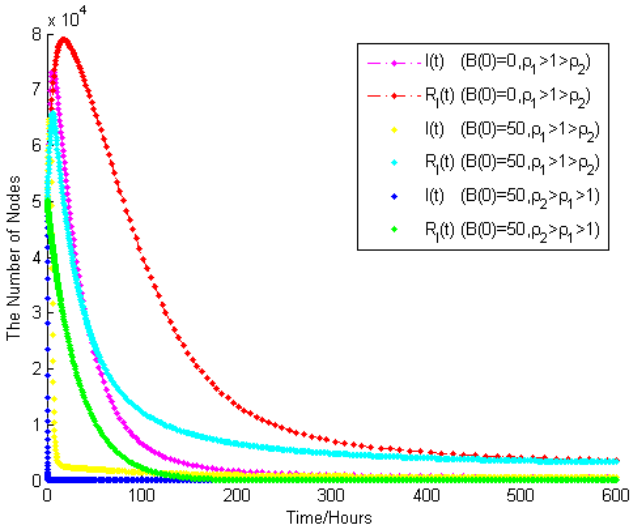


Figure 3. Effect of benign worms.

Next, we will evaluate the influences of different initial levels of infected removable nodes on the propagation of malicious worms. Let $\left(S(0), I(0), B(0), V(0)\right)=\left(99900,100,0,0\right)$ remain unchanged, and $\left(R_S(0), R_I(0)\right)$ is respectively equal to $\left(0,0\right),\left(99900,100\right),\left(90000,10000\right),\left(100,99900\right)$-label them as 0,1,2,3. The results are shown in Figure 4. As can be seen from Figure 4, a larger number of initial levels of infected removable nodes results in the increase of number of fixed nodes which infected by malicious worms, and can speed up the propagation speed of malicious worms.

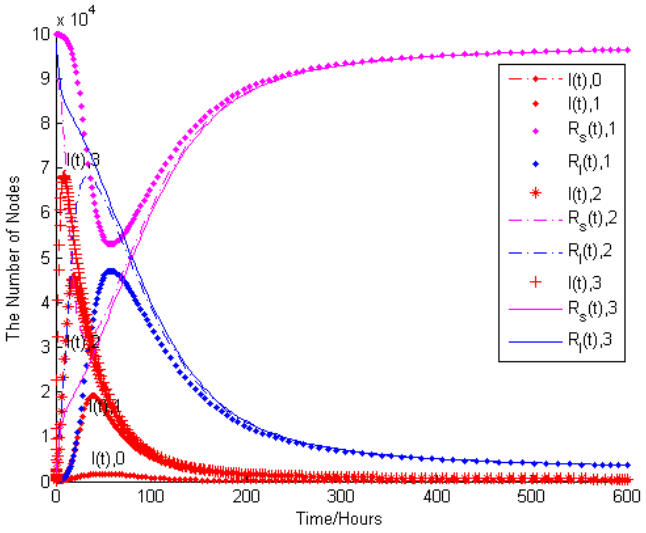


Figure 4. Influence of different initial levels of infected removable nodes.

Finally, we will evaluate the influences of different online rates of removable nodes on the propagation of malicious worms. Let λ be 0, 0.1, 0.4, 1, respectively, and $\left(S(0), I(0), B(0), V(0), R_S(0), R_I(0)\right)=\left(99900,100,0,0,50000,50000\right)$. The results are shown in Figure 5. As can be seen from Figure 5, a larger online rate of removable nodes results in the increase of the number of nodes infected by malicious worms, and also can speed up the spreading speed of malicious worms.

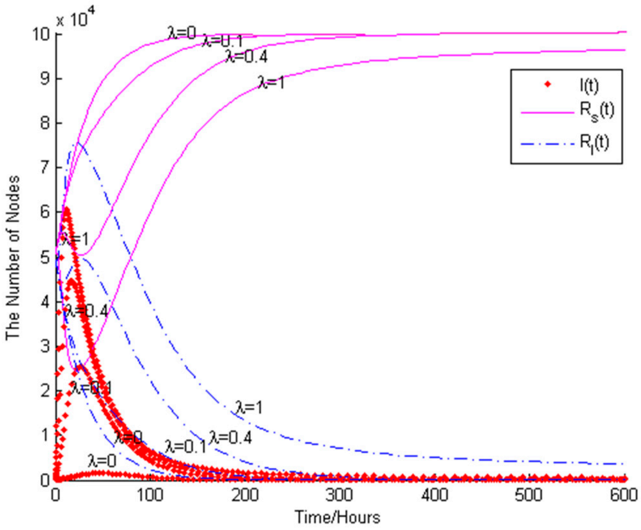


Figure 5. Influence of different online rates of removable nodes.

4.2. Control Strategies

In this paper, we focus on the influences of parameters concerned with removable devices. Through above analysis we know that a larger number of initial level of infected removable devices and a larger online rate of removable devices are all beneficial for the propagation of malicious worms. Decreasing the value of online rate of removable nodes and limiting the number of removable nodes can confine the propagation of malicious worms. Furthermore, we can increase the basic reproductive number of benign worms $\rho_2 = \frac{\beta_2 b_1}{(\mu_1 + \delta)(\mu_1 + \omega_1)}$ by increasing the value of β_2 and decreasing the value of δ, making ρ_2 larger than the basic reproductive number of malicious worms ρ_1, when $\rho_2 > \rho_1 > 1$, the malicious worms will disappear from the network.

However, the temporal form of the benign worm has several unresolved issues and limitations, such as network congestion, patching safety, and legal issues. In addition, the benign worm strategy faces two problems: (1) When the number of benign worms put into the network is small, it will be difficult to contain a great amount of malicious worms; (2) The spreading speed of benign worms will be quick without any constraints, and their proactive scans will result in the same problems as malicious worms, such as the system overload and the network congestion. Hence we cannot blindly increase the effective infection rate of benign worms and reduce their self-destruct rate to contain the propagation of malicious worms. Obviously, a larger β_2 will quickly kill off malicious worms but meanwhile a larger β_2 will bring a larger amount of traffic than that caused by malicious worms, which could greatly endanger normal network application. Thus, we should choose a reasonable value for β_2 and δ according to the actual situation of network, in order to combat malicious worms synthetically and efficiently.

5. Conclusions

In this paper, we proposed a mathematical model to explore the influences of removable devices on the interaction dynamics between malicious worms and benign worms based on diversity of nodes types in an M2M wireless network, which considers two important network environment factors: benign worms and removable devices. Firstly, we found out the model's basic reproduction number R_0, and its threshold value determines whether the malicious worms die out in the network. Numerical analysis shows that if $R_0 \leq 1$ the worm-free equilibrium is globally asymptotically stable in the model's feasible region U. Otherwise, malicious worms will be prevalent. Secondly, simulations verify the performance of our model is effective in combating with malicious worms. Finally, effective control strategies are proposed to combat malicious worms. In the future, we will take more network environment factors into consideration, e.g., the time delay of benign worms, the latent period of malicious worms, and more characteristics of an M2M network, such as communication technology, communication range, communication speed, network protocols or the capabilities of a typical device, making the adaptability of our model stronger and broader.

Acknowledgments

This work was supported by National Natural Science Foundation of China (NO.61202450, NO.U1405255, NO.61402110, NO.61472083), and the development project of Fujian provincial strategic emerging industries technologies: Key technologies in development of next generation Integrated High Performance Gateway, Fujian Development, and Reform Commission High-Technical (2013) 266, Fuzhou Science and Technology Bureau (No.2013-G-84), the Scientific Research Foundation for the Returned Overseas Chinese Scholars, Ministry of Education of China, and Fujian Normal University Innovative Research Team (NO.IRTL1207).

Author Contributions

The research scheme was mainly designed by Jinhua Ma, Zhide Chen, Wei Wu, Rongjun Zheng, and Jianghua Liu performed the research and analyzed the data. The paper was mainly written by Jinhua Ma. All authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. 2015 Symantec Global Internet Security Threat Report. Available online: http://www.symantec.com/security-response (accessed on 24 August 2015).
2. Anderson, R.M.; May, R.M. *Infectious Diseases of Humans: Dynamics and Control*; Oxford University Press: Oxford, UK, 1991; pp. 174–175.
3. Wood, P.H.N. The Mathematical Theory of Infectious Diseases and Its Applications. *Immunology* **1978**, *34*, 955–956.
4. Štěpán, J.; Hlubinka, D. Kermack-McKendrick epidemic model revisited. *Kybernetika* **2007**, *43*, 395–414.
5. Capasso, V.; Serio, G. A generalization of the Kermack-McKendrick deterministic epidemic model. *Math. Biosci.* **1978**, *42*, 43–61.

6. Zou, C.C.; Gong, W.; Towsley, D. Code red worm propagation modeling and analysis. In Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, 18–22 November 2002; pp.138–147.
7. Mishra, B.K.; Saini, D.K. SEIRS epidemic model with delay for transmission of malicious objects in computer network. *Appl. Math. Comput.* **2007**, *188*, 1476–1482.
8. Toutonji, O.A.; Yoo, S.M.; Park, M. Stability analysis of VEISV propagation modeling for network worm attack. *Appl. Math. Model.* **2012**, *36*, 2751–2761.
9. Mishra, B.K.; Jha, N. SEIQRS model for the transmission of malicious objects in computer network. *Appl. Math. Model.* **2010**, *34*, 710–715.
10. Yao, Y.; Xiang, W.; Qu, A.; Yu, G. Hopf bifurcation in an SEIDQV worm propagation model with quarantine strategy. *Discret. Dyn. Nat. Soc.* **2012**, doi:10.1155/2012/304868.
11. Qing, S.; Wen, W. A survey and trends on Internet worms. *Comput. Secur.* **2005**, *24*, 334–346.
12. Zhou, H.; Wen, Y.; Zhao, H. Modeling and analysis of active benign worms and hybrid benign worms containing the spread of worms. In Proceedings of the Sixth International Conference on Networking, ICN'07, Martinique, France, 22–28 April 2007; p. 65.
13. Fang, Y.H.; Zheng, X.F.; Xie, T.T. A revised benign worm-anti-worm propagation model. *Appl. Mech. Mater.* **2012**, *121*, 4340–4344.
14. Wang, F.; Zhang, Y.; Wang, C.; Ma, J. Stability analysis of an e-SEIAR model with point-to-group worm propagation. *Commun. Nonlinear Sci. Numer. Simul.* **2015**, *20*, 897–904.
15. Wang, F.; Yang, Y.; Zhang, Y.; Ma, J. Stability analysis of the interaction between malicious and benign worms. *Future Comput. Inf. Technol.* **2014**, *86*, 217.
16. Song, L.P.; Jin, Z.; Sun, G.Q. Zhang, J.; Han, X. Influence of removable devices on computer worms: Dynamic analysis and control strategies. *Comput. Math. Appl.* **2011**, *61*, 1823–1829.
17. Gan, C.; Yang, X. Theoretical and experimental analysis of the impacts of removable storage media and antivirus software on viral spread. *Commun. Nonlinear Sci. Numer. Simul.* **2015**, *22*, 167–174.
18. Zhu, Q.; Yang, X.; Ren, J. Modeling and analysis of the spread of computer virus. *Commun. Nonlinear Sci. Numer. Simul.* **2012**, *17*, 5117–5124.
19. Heffernan, J.M.; Smith, R.J.; Wahl, L.M. Perspectives on the basic reproductive ratio. *J. R. Soc. Interface* **2005**, *2*, 281–293.
20. Van den Driessche, P.; Watmough, J. Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission. *Math. Biosci.* **2002**, *180*, 29–48.
21. Robinson, R.C. *An Introduction to Dynamical Systems: Continuous and Discrete*; American Mathematical Society: Providence, RI, USA, 2012.
22. Clark, R.N. The Routh-Hurwitz stability criterion, revisited. *IEEE Control Syst. Mag.* **1992**, *12*, 119–120.
23. Bellman, R. *Stability Theory of Differential Equations*; Courier Corporation: North Chelmsford, MA, USA, 2013.