Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 746803, 14 pages
http://dx.doi.org/10.1155/2014/746803

Research Article

Spread and Control of Mobile Benign Worm Based on Two-Stage Repairing Mechanism

Meng Wang, Zhide Chen, Li Xu, and Huan Zhan

Key Lab of Network Security and Cryptography, School of Mathematics and Computer Sciences, Fujian Normal University, Fuzhou, Fujian 350007, China

Correspondence should be addressed to Zhide Chen; zhidechen@fjnu.edu.cn

Received 29 April 2014; Accepted 21 September 2014; Published 10 November 2014

Academic Editor: Junjie Wei

Both in traditional social network and in mobile network environment, the worm is a serious threat, and this threat is growing all the time. Mobile smartphones generally promote the development of mobile network. The traditional antivirus technologies have become powerless when facing mobile networks. The development of benign worms, especially active benign worms and passive benign worms, has become a new network security measure. In this paper, we focused on the spread of worm in mobile environment and proposed the benign worm control and repair mechanism. The control process of mobile benign worms is divided into two stages: the first stage is rapid repair control, which uses active benign worm to deal with malicious worm in the mobile network; when the network is relatively stable, it enters the second stage of postrepair and uses passive mode to optimize the environment for the purpose of controlling the mobile network. Considering whether the existence of benign worm, we simplified the model and analyzed the four situations. Finally, we use simulation to verify the model. This control mechanism for benign worm propagation is of guiding significance to control the network security.

1. Introduction

In recent years, with the widespread of smartphone, Android, IOS, and other operating systems have occupied a certain market share in the mobile phone market. The increasingly complex mobile network environment brings us convenience, as well as various temptations and threats. Latest security report shows that the number of traditional virus remains stable, while the mobile device virus has increased dramatically, with nearly 50 times comparing to last year. The trends suggest that, in the current network security situation, businesses and consumers should continue to strengthen their security, including network security measures to ensure the security and order of the network environment. Faced with the wide variety of malicious viruses transmitted infections way, we need to adopt equally effective way to keep the security of mobile network environment.

Worms are malicious codes with the featrues of autonomous replication and self-propagation in a network. Because of the Code Red worm events and the outbreak of the Slammer worm, people have updated their knowledge of the great harmfulness of the worm. With the vigorous development of the mobile network environment, mobile phones become more and more popular, and mobile malicious code also gradually shows the trend of the outbreak. Mobile environment malicious codes are not simplly called worms, trojan, or virus. Most of them are mixed-type and can bring great harm to the mobile network. Most of these malicious codes are bundled in application softwares and have a high risk to learn or steal personal information data. Moreover, the current mobile smart phone and other mobile devices both have a large number of vulnerabilities, which makes mobile malicious worm outbreaks become a great potential threat.

Researchers try to use various methods to fight for the worm. In the traditional network, the existing research has successfully designed the benign worms to fight against malicious worms [1]. But in the mobile network environment, it has some differences due to worms' intelligent, autonomous, and rapidly moving features. Hazards of mobile malware worm have begun to be obvious. Using benign worms to fight mobile worms are becoming a new emergency response technology.

1.1. Motivation. A worm is a program with the featrues of autonomous replication and self-propagation in other systems. Since the Morris worm outbreak in 1989, 2003, and 2004 is the outbreak period of Blaster and Sasser. About four years later, Conficker worm emerged in November 2008, become one of the most notorious worms in history. Similarly, in the present mobile network environment, the spread way of the worm transfers from the MMS (multimedia messaging service) to the mobile application. The ways of transmission are more and more abundant. Before the mobile worms threat inevitably breaks out, we need a reasonable method to use benign worms against malicious worms.

A mobile worm can seize the victim mobile device by running a malicious exploit, and this infected mobile device will, in turn, scan and infect other mobile devices in the mobile network. Mobile worm may perform malicious activities, like steal data, send credentials to attackers, and send premium SMSs, to name a few. Lack of network security and mitigation measures can cause the worm attack to propagate through the network infrastructure, consuming overall bandwidth and causing other damage, which is potentially financially devastating. The attackers take advantage of the destructive behavior and vast spread of the worms through the network and take over a great number of systems, amplifying the damage and thus making trace-back more difficult [2].

Currently, for mobile intelligent terminals, the most effective way of worm infection prevention is to patch the mobile phone operating system and the corresponding mobile applications timely. But it is often difficult to achieve: (1) there is a large number of various various patches for different mobile operating systems; (2) mobile malware worm spreads rapidly and the number of vulnerability is also increasing all the time; (3) the security awareness of mobile smart phone users is weak, which may lead to unconscious infection; (4) for those mobile smart phones having been sold, it is almost impossible to carry out a unified operating system version upgrade.

In order to control the spread of the worm, various detection and prevention methods have been proposed, but they are difficult to solve the problem fundamentally. The benign worm proposed by Castañeda et al. is a worm favorable for traditional worm [3]. Benign worms with dynamic characteristics of active defense can fundamentally remove malicious worms and repair network environment.

In mobile environment, the spread of the worm is much more difficult to control, for the transmission is various. There are a lot of things to think about when we use benign worm to control and remove mobile malicious worms, such as the repairing problem for patch download, load and congestion for network brought by benign worms' delivery, and the trustworthiness problem of benign worms. In the vast growing mobile network market, security protection is the necessary prerequisite to avoid huge losses. Therefore, our motivation is to propose control mechanism for benign worm propagation on the basis of mobile environment.

1.2. Contribution. Our main contributions of the research on the control of mobile benign worm transmission are as the following points.

(1) In this research, we analyzed the worm propagation characteristic in the mobile environment. The result shows that benign worms, with the repairing features, will remove the malicious worm and repair the patch in two stages after being put into use. We stress that benign worms can repair mobile intelligent terminal in the mobile network and also stress the controllability of benign worm. Benign worm should be with self-destruction function to assure the quality of the network after the network returns to normal.

(2) We analyzed the traditional model of KM (Kermack-Mckendrick) and TF (two-factor) according to the characteristics of mobile network, and we put forward a two-stage benign worm propagation and control mechanism, which can effectively control and remove malicious worms. We proposed the detection and scanning methods of benign worm in the mobile network environment. There are timing simple scanning ways based on mobile phone station and more comprehensive ways of penetration test scanning. We take the repairing form of multiple patches to prevent the patch site from easily malicious use.

The remaining part of this paper is organized as follows. Section 2 gives the simple introduction and analysis of benign worm and the existing mechanism of transmission. Section 3 puts forward the mobile repair mechanism of mobile benign worm. Section 4 describes the two stages of mobile benign worm propagation mechanism, and the corresponding model is given. In Sections 5 and 6, we analyze the state of the model, conduct the analysis and comparison for two-stage propagation model with the help of simulation experiment, and conclude the optimal condition. Section 7 concludes the paper.

2. Related Work

The importance of network security has always been stressed; Cohen studied the security problems of independent transmission code [4]. The study of worm propagation and control mechanism has always been one of the hot research topics, and the research on how benign worms control the propagation of malicious worms is the hottest topic.

With the rapid development of mobile network and the common use of mobile phones, malicious code has transmitted from the traditional network to the mobile network; mobile phone security issues is facing a huge threat. Mobile applications also provide a new medium for the worm propagation. It has been a certain trend that malicious worms carrying the trojans, viruses, and other malicious codes invade the mobile network. When developing the mobile market, it is important to guarantee the safety of the mobile network.

Benign worm is a novel method to prevent worm, it draws on the worm propagation mechanisms to combat worms. When the worm outbreaks on the network, you can construct the corresponding benign worm and spread it so that it can automatically patch, repair, or remove worms. The defects of the benign worm are scanning speed, the diffusion speed, and scope. It should be carefully designed and good self-control

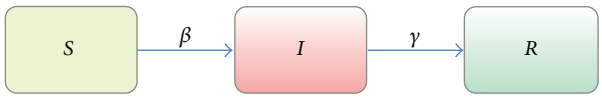

Figure 1: State transition of KM.

mechanism should be essential, or benign worm will also cause network paralysis. Frank divided benign worms into four categories, namely, passive benign worms, proactive benign worms, worms, and hybrid benign worm-based IDS. Dan et al. further divided benign worms into three categories, namely, patch worms, grabbed worms, and mixed worms. On this basis, Zhou et al. subdivided benign worms and established a mathematical model for various worms on the basis of two-factor model. He established a mathematical model for passive worms firstly. Modeling and simulation by the above scholars basically divided benign worms into three types: confrontation, active dissemination, and monitoring of drivers. However, all the analysis and design are made for worms of Internet; thus, the worms in the mobile environment can not be fight well.

Current research focuses primarily on mobile worm propagation, the worm propagation model, defense mechanisms, and control strategies.

2.1. Mobile Worm Propagation Model. A lot of spread about malicious codes of mobile phones is focused on the Bluetooth worm, such as Cabir and CommWarrior, whose spread is to find and infect other infectious mobile devices by physical proximity. Kostakos, deployed bluetooth monitor equipment in a British town, found that only eight percent of users turn on their bluetooth devices, which largely limits the possibility of worm propagation [5]. Hui et al.'s research focuses on population density, bluetooth radius, and the node rate, the results of which point out that various quarantine methods can reduce the potential of virus greatly [6]. Compared with the worms propagating through the close geographical position, the worms propagating through the Internet have faster propagation speed and can infect more equipment. The damage to infrastructure of mobile environment is more serious. Mobile smart phones face the similar vulnerabilities as traditional PCs. For example, Mulliner et al. describe a smart phone GSM/WiFi-concept to verify the buffer overflow vulnerability [7]. At the same time the smart phone market breaks out, the mobile security is facing a potential threat.

An accurate model of worm can have certain effect on observing the worm propagation. The model has a certain ability to identify weaknesses in the propagation process and can provide accurate prediction to reduce losses. Due to the similarity of worm propagation and spread of infectious diseases, infectious disease model is often used to establish the worm propagation model. A number of the existing models are not always applicable to the specific situation. Here we first introduce the KM model and TF model simply.

In the KM model, we assume that some infected individuals either recover or die in popular infections. An individual is immune to the worm permanently after recovering from the infection. These immune individuals, like the death ones,

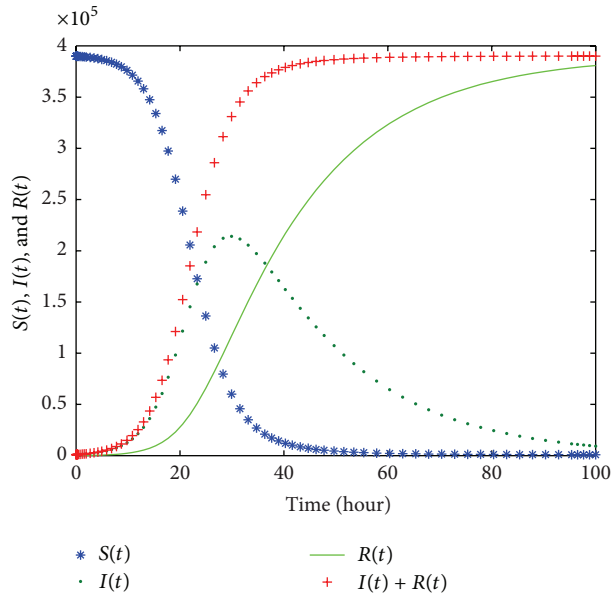

Figure 2: The simulation of KM mode.

will be finally removed. So we give a definition that the individual of this model is always in three states: susceptible, infected or removed. In the process any individual is in one of the following states: changing from susceptible state to infected state, changing from infected state to removed state, or permanent staying in susceptible state. The status transition diagram is shown in Figure 1.

In the figure, β represents infection rate. γ represents the probability of removal from infection group. $S(t)$ represents the number of susceptible user at time t; $I(t)$ represents the number of infected users at time t. $R(t)$ represents the number of removed users from the infected users. N is the total number of users. The model is

$$\begin{aligned} \frac{dS}{dt} &= -\beta SI, \\ \frac{dI}{dt} &= \beta SI - \gamma I, \\ \frac{dR}{dt} &= \gamma I, \\ S(t) + I(t) + R(t) &= N, \quad 0 \le S(t), I(t), R(t) \le N. \end{aligned} \tag{1}$$

For the KM model, when an infected user acquires immunity, it is removed from the network, and then the total number of users in the network becomes $N - 1$ instead of N. Simulation is shown in Figure 2. We set $N = 400000$, $\beta = 0.98/N$, and $\gamma = 0.22$. KM model involves the immune status of the infectious individual and describes the trend of worm propagation trend accurately. However, KM does not involve the susceptible users and the situation that infectious user can resist the worms through patching.

TF model is the expansion of traditional infectious disease model and KM model. The model involves the dynamics strategies of the user and operator, and the situation that

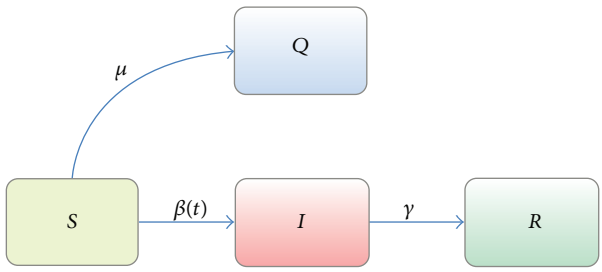

Figure 3: State transition of TF mode.

infection rates decline due to network congestion and other issues. Its state transition diagram is shown in Figure 3.

Parameters $\beta(t)$, $R(t)$, and $Q(t)$ are all function of time t. The model is shown as follows:

$$\begin{aligned}
\frac{dS(t)}{dt} &= -\beta(t) S(t) I(t) - \frac{dQ(t)}{dt}, \\
\frac{dR(t)}{dt} &= \gamma I(t), \\
\frac{dQ(t)}{dt} &= \mu S(t) (I(t) + R(t)), \\
\beta(t) &= \beta_0 \left[1 - \frac{I(t)}{N}\right]^{\eta}, \\
N &= S(t) + I(t) + R(t) + Q(t), \\
0 \le S(t), &\quad I(t), R(t), Q(t) \le N.
\end{aligned} \tag{2}$$

$\beta(t)$ represents the infection rate at time t, $I(t)$ represents the number of infected user at time t, and $R(t)$ represents the number of individual immune from infection at time t. $Q(t)$ represents the number of individuals immunized before infection at time t. β_0, γ, and μ are constants. We can get $dI(t)/dt = \beta(t)S(t)I(t) - \gamma I(t)$. Trend of the spread of TF model is shown in Figure 4.

TF model is an extension of the infectious disease model and KM model, which is more suitable to describe the spread of the worm. However, the model does not consider that the individuals being infected can be patched or upgrade the system to fight worms. There are still some deficiencies when describing the mobile worm propagation. Zhou et al. proposed the corresponding analysis and simulation based on TF model of active benign worms and hybrid benign worm propagation model [1].

In recent years, there are studies on the worm-anti-worm (WAW) model [8], such as the propagation process of malicious worms and benign worms in the network environment. And some models based on WAW various amendments are proposed to adapt to changing network environment. According to these existing models, we combine the features of mobile network environment and propose the control mechanism for mobile benign worm propagation, which will be introduced in detail in the model part of this paper.

2.2. Worm Detection, Defense, and Repair Mechanism. Defense mechanism for worms and other malicious code has been carried out all the time. As for mobile networks, Bose and Shin [9] proposed the method with malicious code propagation based on behavior anomaly detection, which is based on MMS/SMS. Van Ruitenbeek et al. also studied the relevant defense styles and various propagation effects [10]. Researches are constantly to continue.

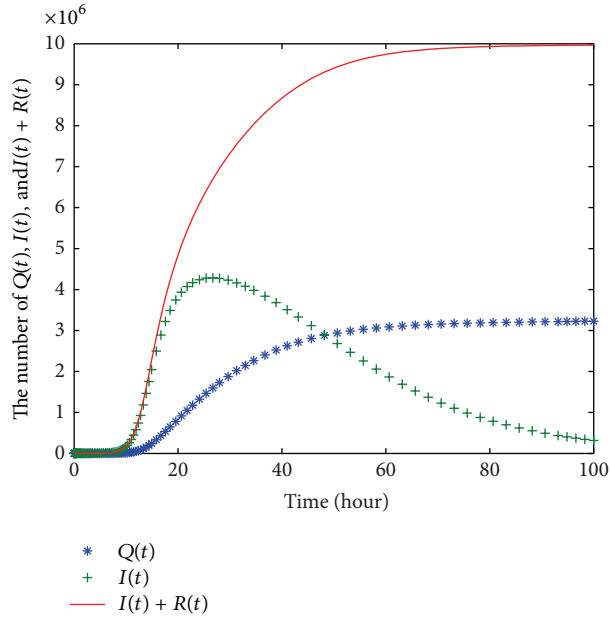

Figure 4: The simulation of TF mode.

Compared with the research of defense mechanism in the mobile network, the traditional research on the Internet is more mature. Niels presented a defense based on virtual honeypot framework to detect and block network worms [11]. And Laurent used this defense architecture to successfully prevent the worm Blaster [12]. Zheng et al. also made a quick lightweight cloud-based scanning benign worm proactive mechanism to control the spread of worms [13]. It is possible to learn in the detection of mobile network, but it also is a long-term project to maintain a network security. We need to know the information of the network at real time. With the thought of traditional penetration test, we can use benign worm to conduct penetration test for mobile network environment, which can do the important prework for us to prevent the damage caused by worms.

3. Mobile Benign Worms Repair Mechanisms

We studied a two-stage mobile benign worm propagation mechanism. We set that, in a mobile network environment, there are several mobile base stations, as well as many ordinary mobile devices. The mobile base station can put benign worms on the mobile devices in a certain area, and control the behavior of benign worms according to the specific situation, which will help the repair mode of benign worms to be better adapted for the current network. In the repair mode of benign worm based on mobile base station, we need to

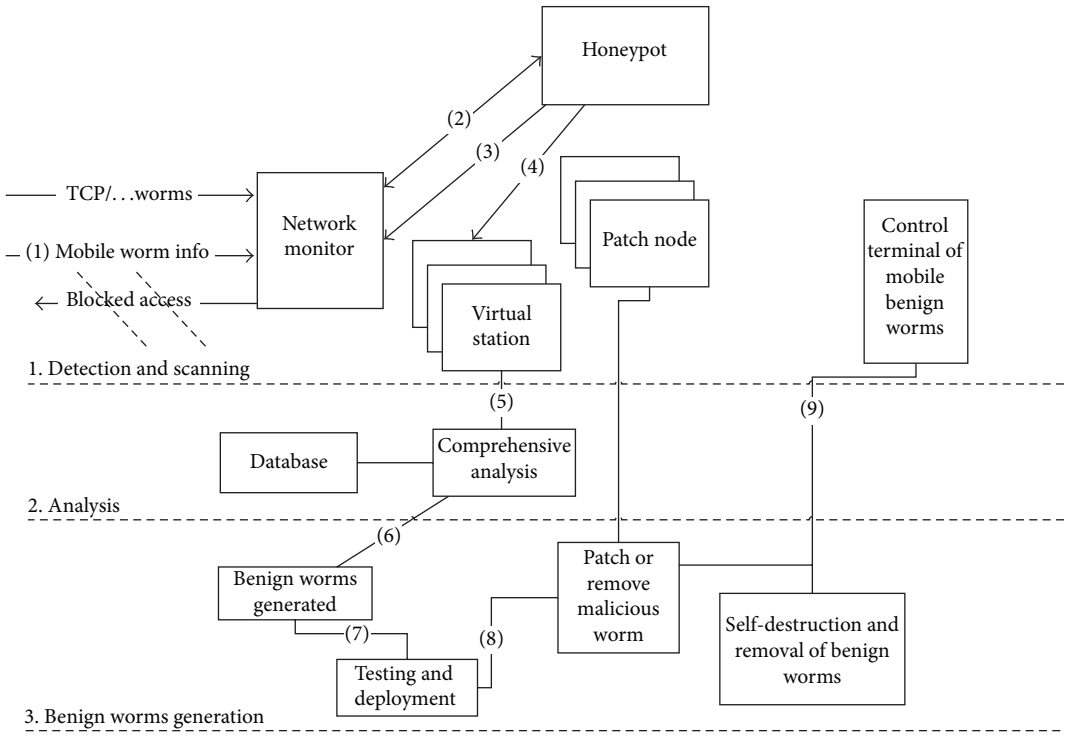

Figure 5: Benign worm mechanism based on honeypot.

consider the performance of mobile base station, trustworthiness, antiforgery attacks, and other issues. Benign worms need to be carefully designed, but according to the actual situation, it is very difficult to design a large number of corresponding benign worms, so before the implementation of the security mechanism, we need to conduct network penetration test, collect and analyze the common security problems, and design relatively common benign worms to response to rapidly changing network. When a new security issue arises, benign worms can submit the issue to the control center, then, according to the characteristics of security issue, we put in some existing benign worms to repair the network timely, so we can have enough time to design targeted benign worms.

Similar to Figure 5, when the malicious worms outbreaks, we put benign worms into use. According to the network situation, in the early stage, benign worms use active scanning mode. The scanning mode is divided into simple scanning and automatic penetration test, the purpose of which is to detect and remove malicious worm or patch the vulnerable of mobile individuals. In order to prevent the malicious use of the mobile base station or in case that the load is too large, we set some patch nodes where benign worms can connect to and remove individuals' vulnerability in mobile station within their coverage.

We set conditions to distinguish the two stages of benign worm repair mechanism. When the network is detected that the number of malicious worms is less than the number of benign worm. Now we set $M = Ut/I(t)$; then, we can send a signal to benign worm and switch the mode to passive clear mode according to the value of M that we set, in order to reduce the load on the mobile network. We call this condition switching condition. With the reduction of malicious worms, benign worms take measures of self-destruction after completing removal and repairing tasks and withdraw from the network activity to further reduce the network load.

Benign worm detection module is divided into simple automatic scanning and automatic penetration test. Simple scanning is based on the feature library to scan the mobile intelligent terminal within the coverage. When the feature matches, it is considered that the individual is infected with malicious worms. Automatic penetration test makes use of existing process automation, integration tools, and combined with benign worm's own initiative. It is mainly divided into two parts: one is the master control terminal and the other is a penetration test worm. In the main control terminal, scanning should be done as a basic work. It is important for us to define common vulnerabilities and viruses in mobile network environment. Only in this way can we judge and create the benign worm in the first place. We use integrated wireless security scanning tools to generate report and first-hand information quickly. Then we analyze the common mobile security vulnerabilities, integrate the virus database, and set harm degree according to the risk level of vulnerabilities.

Then we need to analyze the mobile benign worm's penetrating strategy. This strategy includes two aspects: one is the selection strategy of test worm and the other is the propagation strategy of the test worm. Through analyzing the risk of vulnerabilities in the mobile network, we first determine what kind of test worms is used for penetration test. Secondly, we determine which propagation strategy benign worm will take

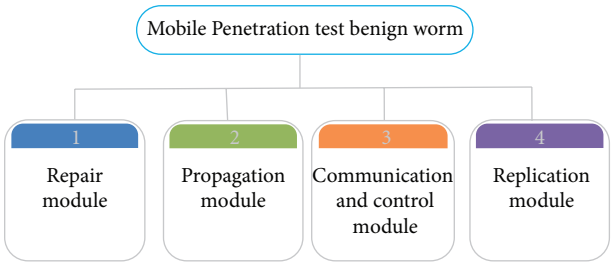

Figure 6: Composition of a penetration testing benign worm.

to spread in mobile networks according to the distribution of vulnerabilities and viruses.

How to assemble benign worm is a very important issue in detecting and repairing process. Generally benign worm is made of repairing module, transport module, communication and control module, and replication module. In addition to repair module, other modules can all be generic and we can replace the content of benign worms repairing module according to the situation.

We need to create a database that contains the repair code for known vulnerabilities or viruses. When detecting a known vulnerability, according to the information which matches the database, we can connect to the nearest node in the mobile network to download patch.

Penetration test benign worm is composed of several parts: the repairing module, transport module, communication and control module, and replication module. According to the communication strategy, the main control terminal uses assembled penetrantion testing benign worm to attack individual mobile intelligent terminal. Then it establishes a transmission channel between the main control terminal and the target individual. Copies of benign worm are transmitted to the individual mobile terminal through transport channels. In the process, the benign worms continuously exchange information with the main control and control the behavior of benign worm. Figure 6 is the composition of a penetration testing benign worm.

4. Mobile Benign Worm Propagation Model

In the mobile network environment, due to the constraints of network bandwidth, the patch site vulnerable, and benign worms' trustworthiness, we established the benign worm propagation model by means of two-stage infection treatment methods. When a malicious worm outbreaks, benign worms will take active mode for rapid processing at first time. Late in the propagation, malicious worms will be suppressed in a certain degree. Benign worms take passive mode, so as to reduce the load of the mobile network bandwidth, avoiding network congestion. When benign worm are patching the vulnerable phones, we use the patch method based on the range of machine base station and timely control the worm. When the parameter M reaches a certain value, the mode of the benign worm can be changed into passive clear mode.

We classify active mode into three situations:

(1) Benign worms only patch all susceptible phones with vulnerabilities.

(2) Benign worms only remove malicious worms.

(3) Benign worms patch all susceptible phones with vulnerabilities and remove malicious worms.

Mobile populations are divided into four types:

(1) Susceptible mobile individuals (S). It is vulnerable to malicious worms and patching benign worms.

(2) Infectious mobile individuals (I). It is infected by malicious worms.

(3) Benign infectious mobile individuals (U). It is infected by benign worms.

(4) Removal mobile individuals (R). Malicious worm may be removed by clearing, marked vulnerability patches, and so forth. Also as mobile phone user may be flashed, safety awareness insufficiency and other factors, it may again become susceptible individual phone.

Here, we set the parameters of the model.

$I(t)$: the number of infectious phones at time t.

$U(t)$: the number of benignly infectious phones at time t.

$R(t)$: the number of phones removed from the infectious phones at time t.

$Q(t)$: the number of phones removed from the susceptible phones at time t.

$P(t)$: the number of phones removed from the benignly infectious phones at time t.

$S(t)$: the number of susceptible phones at time t.

$\beta_1(t)$: infection rate of the worm at time t.

$\beta_2(t)$: infection rate of the benign worm at time t.

η_1: parameter of the infection rate of the worm.

η_2: parameter of the infection rate of the benign worm.

μ: removal rate of susceptible phones.

α: removal rate of infectious phones.

θ: removal rate of benignly infectious phones.

N: total number of hosts under consideration.

T: time delay.

γ_1: removal rate of phones from benignly infectious to removed phones.

Situation 1. Benign worms only patch all susceptible phone individuals. The status is $S \rightarrow Q$, as is shown in the Figure 7.

According to Figure 8, it shows that we can get that, from time t to the time $t + \Delta t$, the change formula of infectious phones is as follows:

$$I(t+\Delta t) - I(t) = \beta_1(t) I(t) S(t) t - \frac{dR(t)}{dt}\Delta t. \quad (3)$$

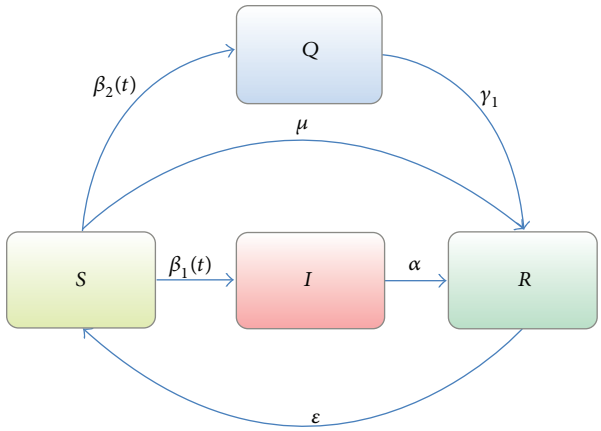

Figure 7: State transition of Situation 1.

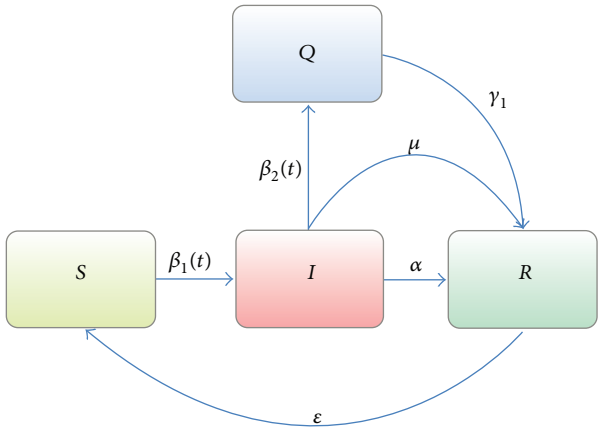

Figure 8: State transition of Situation 2.

So we have

$$\frac{dI(t)}{dt} = \beta_1(t) I(t) S(t) - \frac{dR(t)}{dt}. \tag{4}$$

We get the change formula of $U(t)$:

$$U(t+\Delta t) - U(t) = \beta_2(t) U(t) S(t) \Delta t - \frac{dP(t)}{dt}\Delta t. \tag{5}$$

So we also have

$$\frac{dU(t)}{dt} = \beta_2(t) U(t) S(t) - \frac{dP(t)}{dt}. \tag{6}$$

By definition, θ is the removal rate of benign worm, and we can get

$$\frac{dP(t)}{dt} = \theta U(t). \tag{7}$$

And because at any moment, we all have

$$S(t) + I(t) + R(t) + Q(t) + U(t) + P(t) = N. \tag{8}$$

We substitute $S(t)$ into (4) and can get

$$\begin{aligned}\frac{dS(t)}{dt} &= -\beta_1(t) I(t) S(t) - \beta_2(t) U(t) S(t) \\ &\quad - \frac{dQ(t)}{dt} + \varepsilon R(t).\end{aligned} \tag{9}$$

According to the epidemic rate of rumors in biology, we can get the $Q(t)$

$$\frac{dQ(t)}{dt} = \mu(I(t) + R(t) + Q(t) + P(t)) S(t). \tag{10}$$

As the malicious worm removal rate is, we get

$$\frac{dR(t)}{dt} = \alpha I(t) - \varepsilon R(t). \tag{11}$$

According to the existing mobile worm propagation model and the two-factor model, we can get the equations of two transmission rate:

$$\begin{aligned}\beta_1(t) &= \beta_1\left(1 - \frac{I(t)+U(t)}{N}\right)^{\eta_1}, \\ \beta_2(t) &= \beta_2\left(1 - \frac{I(t)+U(t)}{N}\right)^{\eta_2}.\end{aligned} \tag{12}$$

Then we can get the model:

$$\begin{aligned}\frac{dI(t)}{dt} &= \beta_1(t) I(t) S(t) - \frac{dR(t)}{dt}, \\ \frac{dU(t)}{dt} &= \beta_2(t) U(t) S(t) - \frac{dP(t)}{dt}, \\ \frac{dP(t)}{dt} &= \theta U(t), \\ \frac{dR(t)}{dt} &= \alpha I(t) - \varepsilon R(t), \\ \frac{dQ(t)}{dt} &= \mu(I(t) + R(t) + U(t) + P(t)) S(t), \\ \frac{dS(t)}{dt} &= -\beta_1(t) I(t) S(t) - \beta_2(t) U(t) S(t) \\ &\quad - \frac{dQ(t)}{dt} + \varepsilon R(t), \\ \beta_1(t) &= \beta_1\left(1 - \frac{I(t)+U(t)}{N}\right)^{\eta_1}, \\ \beta_2(t) &= \beta_2\left(1 - \frac{I(t)+U(t)}{N}\right)^{\eta_2}, \\ N &= S(t) + I(t) + R(t) + Q(t) + U(t) + P(t).\end{aligned} \tag{13}$$

Situation 2. Benign worms only remove malicious worms. The status is $I \rightarrow R$, as is shown in the Figure 8.

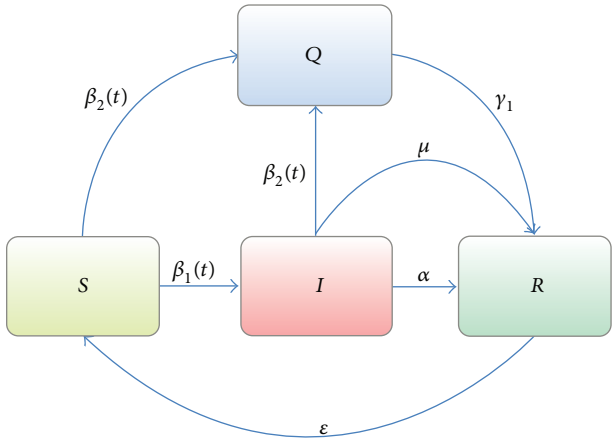

Figure 9: State transition of Situation 3.

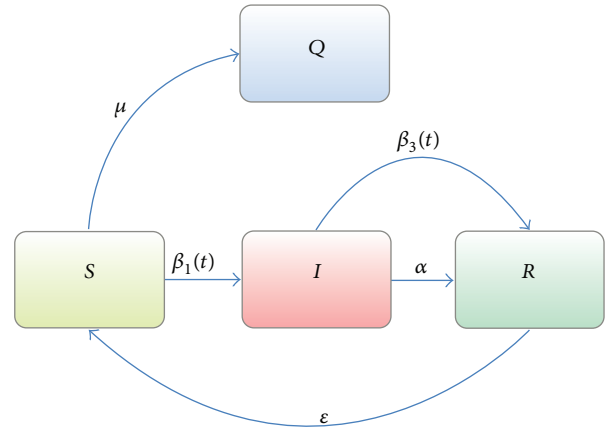

Figure 10: State transition of passive mode.

According to the known, we can obtain two different variations equations:

$$\begin{aligned}\frac{dU(t)}{dt} &= \beta_2(t)U(t)I(t) - \frac{dP(t)}{dt},\\ \frac{dI(t)}{dt} &= \beta_1(t)I(t)S(t) - \beta_2(t)U(t)I(t) - \frac{dR(t)}{dt}.\end{aligned} \tag{14}$$

So we can get the benign worm propagation model in Situation 2:

$$\begin{aligned}\frac{dI(t)}{dt} &= \beta_1(t)I(t)S(t) - \beta_2(t)U(t)I(t) - \frac{dR(t)}{dt},\\ \frac{dU(t)}{dt} &= \beta_2(t)U(t)I(t) - \frac{dP(t)}{dt},\\ \frac{dP(t)}{dt} &= \theta U(t),\\ \frac{dR(t)}{dt} &= \alpha I(t) - \varepsilon R(t),\\ \frac{dQ(t)}{dt} &= \mu(I(t) + R(t) + Q(t) + P(t))S(t),\\ \frac{dS(t)}{dt} &= -\beta_1(t)I(t)S(t) - \beta_2(t)U(t)S(t)\\ &\quad - \frac{dQ(t)}{dt} + \varepsilon R(t),\\ \beta_1(t) &= \beta_1\left(1 - \frac{I(t)+U(t)}{N}\right)^{\eta_1},\\ \beta_2(t) &= \beta_2\left(1 - \frac{I(t)+U(t)}{N}\right)^{\eta_2},\\ N &= S(t) + I(t) + R(t) + Q(t) + U(t) + P(t),\end{aligned} \tag{15}$$

Situation 3. Benign worms patch all vulnerable phones and remove malicious worms.

As is shown in the Figure 9, when benign worms patch susceptible phone individuals, the status is $S \rightarrow Q$. When benign worms remove malicious worms, the status is $I \rightarrow R$.

According to the Figure 10, we can get

$$\frac{dU(t)}{dt} = \beta_2(t)U(t)I(t) + \beta_2(t)U(t)S(t) - \frac{dP(t)}{dt}. \tag{16}$$

According to the same rules, we can draw the change formula of $I(t)$:

$$\frac{dI(t)}{dt} = \beta_1(t)I(t)S(t) - \beta_2(t)U(t)I(t) - \frac{dR(t)}{dt}. \tag{17}$$

So we get the model:

$$\begin{aligned}\frac{dI(t)}{dt} &= \beta_1(t)I(t)S(t) - \beta_2(t)U(t)I(t) - \frac{dR(t)}{dt},\\ \frac{dU(t)}{dt} &= \beta_2(t)U(t)I(t) + \beta_2(t)U(t)S(t) - \frac{dP(t)}{dt},\\ \frac{dP(t)}{dt} &= \theta U(t),\\ \frac{dR(t)}{dt} &= \alpha I(t) - \varepsilon R(t),\\ \frac{dQ(t)}{dt} &= \mu(I(t) + R(t) + U(t) + P(t))S(t),\\ \frac{dS(t)}{dt} &= -\beta_1(t)I(t)S(t) - \beta_2(t)U(t)S(t)\\ &\quad - \frac{dQ(t)}{dt} + \varepsilon R(t),\\ \beta_1(t) &= \beta_1\left(1 - \frac{I(t)+U(t)}{N}\right)^{\eta_1},\\ \beta_2(t) &= \beta_2\left(1 - \frac{I(t)+U(t)}{N}\right)^{\eta_2},\\ N &= S(t) + I(t) + R(t) + Q(t) + U(t) + P(t).\end{aligned} \tag{18}$$

In the later period of benign worm control and repair mechanism, the number of malicious worms is less than the number of benign worm. Now we set $M = Ut/I(t)$. The benign worm's mode is changed into passive clear pattern

according to the value of M that we set. This can effectively reduce the burden of mobile networks. And at this stage, the benign worms will destroy themselves with the reduction of the malicious worms. When the switching condition is met, benign worms switch to the second phase of the passive clearing mode. Delay T exists when switching. Passive mobile benign worm in the actual case is slower than malicious worm. $\beta_3(t)$ represents the scanning rate of benign worm at time t. β_3 is the initial value.

According to change formula, we can get

$$\frac{dI(t)}{dt} = \beta_1(t) I(t) S(t) - \beta_3(t) U(t-T) I(t) - \frac{dR(t)}{dt},$$
$$\frac{dU(t)}{dt} = -M\beta_3(t) U(t-T) I(t) - \frac{dP(t)}{dt}. \tag{19}$$

The model is

$$\begin{aligned}
\frac{dI(t)}{dt} &= \beta_1(t) I(t) S(t) - \beta_3(t) U(t-T) I(t) - \alpha I(t)\\
\frac{dU(t-T)}{dt} &= -M\beta_3(t) U(t-T) I(t) - \theta U(t-T)\\
\frac{dP(t-T)}{dt} &= \theta U(t-T)\\
\frac{dR(t)}{dt} &= \alpha I(t) + \beta_3(t) U(t-T) I(t) - \varepsilon R(t)\\
\frac{dQ(t)}{dt} &= \mu(I(t) + R(t)) S(t)\\
\frac{dS(t)}{dt} &= -\beta_1(t) I(t) S(t) - \frac{dQ(t)}{dt} + \varepsilon R(t)\\
\beta_1(t) &= \beta_1\left(1 - \frac{I(t) + U(t-T)}{N}\right)^{\eta_1}\\
\beta_3(t) &= \beta_2\left(1 - \frac{U(t-T)}{N}\right)^{\eta_2}\\
N &= S(t) + I(t) + R(t) + Q(t) + U(t-T) + P(t-T)\\
0 &\le S(t), \quad I(t), R(t), U(t-T), Q(t) \le N.
\end{aligned} \tag{20}$$

5. State Analysis of the Model

In order to facilitate analysis of the model, we simplify the model. Here we consider the state transition relations among susceptible, infectious, benign infectious, and removal individuals. Its state transition figure is shown in Figure 11.

Here we set β_1, β_2, and β_3 as constants. β_2 is the probability of susceptible ones infected by benign worms. β_3 is the probability of infectious ones infected by benign worms. With the process of propagation control model, the numbers of groups for four types are in constant change and there is also a certain probability of death. We set the corresponding death rate of four groups as $\omega_1, \omega_2, \omega_3$, and ω_4. The proportion of susceptible phones actually involved in the propagation model is set as λ. So we get a simplified model formula as follows:

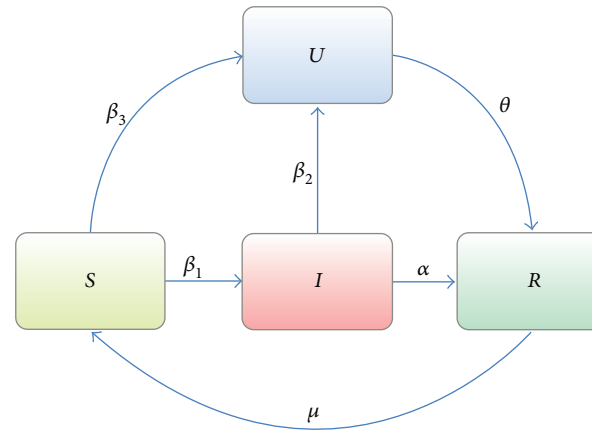

Figure 11: State transition of simplified model.

$$\begin{aligned}
\frac{dS(t)}{dt} &= \lambda N - (\omega_1 + \mu) S - \beta_1 SI - \beta_3 SU,\\
\frac{dI(t)}{dt} &= \beta_1 SI - \beta_2 UI - (\omega_2 + \alpha) I,\\
\frac{dU(t)}{dt} &= \beta_2 UI + \beta_3 SU - (\omega_4 + \theta) U,\\
\frac{dR(t)}{dt} &= \alpha I + \theta U + \mu S - \omega_3 R.
\end{aligned} \tag{21}$$

Analyzing this model, we first detect equilibrium of the model. For the propagation model, we analyze the model in Situation 3 as an example. In this process, there should be at least four states: no infection status $(S, 0, 0, R)^T$, worm infection status $(S, I, 0, R)^T$, benign worm infection status $(S, 0, U, R)^T$, and interactive infection status $(S, I, U, R)^T$.

(1) No infection status $(S, 0, 0, R)^T$: in this case, I, U, and P are 0, and its steady-state value is

$$\overline{S} = \frac{\lambda N}{(\omega_1 + \mu)}, \qquad \overline{R} = \frac{\mu}{\omega_3}\overline{S}. \tag{22}$$

We analyze the eigenvalues of Jacobean matrix in the model equations and get four characteristic values as follows:

$$\begin{aligned}
\lambda_1 &= -(\omega_1 + \mu),\\
\lambda_2 &= \beta_1\overline{S} - (\omega_2 + \alpha),\\
\lambda_3 &= \beta_3\overline{S} - (\omega_4 + \theta),\\
\lambda_4 &= -\omega_3.
\end{aligned} \tag{23}$$

In order to obtain system stability, characteristic values are required to satisfy the following conditions:

$$\begin{aligned}
\overline{S} &< \frac{\omega_2 + \alpha}{\beta_1},\\
\overline{S} &< \frac{\omega_4 + \theta}{\beta_3}.
\end{aligned} \tag{24}$$

If any of these conditions does not meet the requirements, the system would be unstable.

(2) Worm infection status $(S, I, 0, R)^T$: in this case, U is 0, and its steady-state value is

$$\begin{aligned} \lambda N &= (\omega_1 + \mu)\overline{S} + \beta_1 \overline{S}\,\overline{I}, \\ \overline{S} &= \frac{\omega_2 + \alpha}{\beta_1}, \\ \overline{R} &= \frac{\alpha \overline{I} + \mu \overline{S}}{\omega_3}. \end{aligned} \tag{25}$$

(3) Benign worm infection status: in this case, I is 0, and its steady-state value is

$$\begin{aligned} \lambda N &= (\omega_1 + \mu)\overline{S} + \beta_3 \overline{S}\,\overline{U}, \\ \overline{S} &= \frac{\omega_4 + \theta}{\beta_3}, \\ \overline{R} &= \frac{\theta \overline{U} + \mu \overline{S}}{\omega_3}. \end{aligned} \tag{26}$$

(4) Interactive infection status: in this case, malicious worms and benign worms coexist in the system. In order to determine the equilibrium point of S, I, R, and U, we have

$$\frac{dS}{dt} = 0, \qquad \frac{dI}{dt} = 0, \qquad \frac{dU}{dt} = 0, \qquad \frac{dR}{dt} = 0. \tag{27}$$

There are two key points in the differential equation. One is $N(N, 0, 0, 0)$. The point means no infection status. The other one is $X = (\overline{S}, \overline{I}, \overline{U}, \overline{R})$. It is the stable value of the system, and its value can be obtained:

$$\begin{aligned} \overline{S} &= M\beta_2, \\ \overline{I} &= N - \beta_3 M, \\ \overline{U} &= \beta_1 M - Q, \\ \overline{R} &= \frac{M(\beta_2\mu - \beta_3\alpha + \beta_1\theta) + (\alpha N - \theta Q)}{\mu}. \end{aligned} \tag{28}$$

Among them

$$\begin{aligned} M &= \frac{\lambda N}{\beta_2(\omega_1 + \mu) + \beta_1(\omega_4 + \theta) - \beta_3(\omega_1 + \alpha)}, \\ N &= \frac{\omega_4 + \theta}{\beta_2}, \qquad Q = \frac{\omega_2 + \alpha}{\beta_2}. \end{aligned} \tag{29}$$

6. Simulation

6.1. Mobile Benign Worm Modes Simulations. In order to verify the differences and effectiveness of the three mobile active worm modes and the passive worm mode after switching, we make simulation experiments with the help of Matlab. In the simulation figure, the dotted line represents the malicious worm propagation curve, while solid line represents the benign worm propagation curve. The x axis represents the time (one hour per unit), and the y axis represents the number of infectious population $I(t)$ and benignly infectious population for a dashed line $U(t)$.

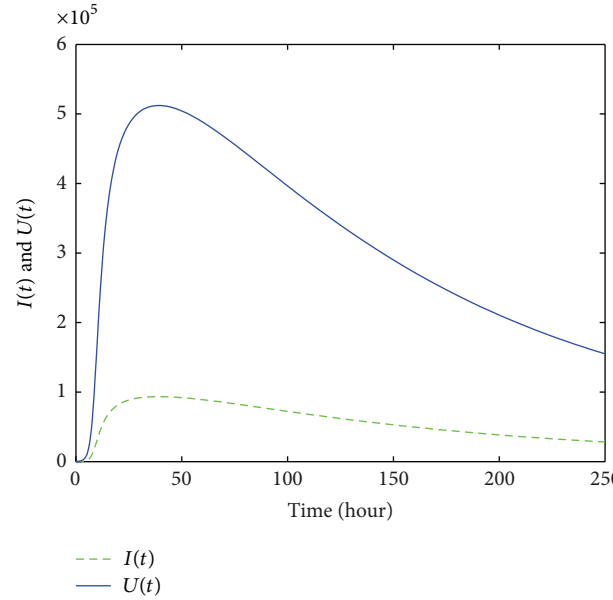

Figure 12: Mode one.

6.1.1. Mobile Active Mode One. Benign worms only patch all susceptible phones with vulnerabilities. We use simulation parameters: ($N = 1000000$, $\beta_1 = 8 * 10^{-7}$, $\beta_2 = 8 * 10^{-7}$, $\eta_1 = \eta_2 = 3$, $\mu = 6 * 10^{-8}$, $\alpha = 0.05$, $\theta = 0.004$, and $\varepsilon = 5 * 10^{-6}$). The initial values of malicious worm and benign worm are 1 and 200. Its corresponding simulation is shown in Figure 12. We can see that the patch benign worm have certain control effect on the propagation of malicious worms.

The comparing figure with TF is in Figure 13.

6.1.2. Mobile Active Mode Two. Benign worms only remove malicious worms. We use simulation parameter: ($N = 1000000$, $\beta_1 = 8 * 10^{-7}$, $\beta_2 = 8 * 10^{-7}$, $\eta_1 = \eta_2 = 3$, $\mu = 6 * 10^{-8}$, $\alpha = 0.05$, $\theta = 0.004$, and $\varepsilon = 5 * 10^{-6}$). The initial value of malicious worm and benign worm is the same as above, The corresponding simulation is shown in Figure 14, where we can see that this benign worm is weak against the malicious worms.

However, comparing with the TF model, it is clearly reflected the effectiveness of benign worms. The comparison figure is shown in Figure 15.

6.1.3. Mobile Active Mode Three. Benign worms patch all susceptible phones with vulnerabilities and remove malicious worms. This benign worms should be more powerful. We use simulation parameters: ($N = 1000000$, $\beta_1 = 8 * 10^{-7}$, $\beta_2 = 8 * 10^{-7}$, $\eta_1 = \eta_2 = 3$, $\mu = 6 * 10^{-8}$, $\alpha = 0.05$, $\theta = 0.004$, $\varepsilon = 5 * 10^{-6}$). The corresponding simulation is shown in Figure 16, where we can see that benign worms of the active

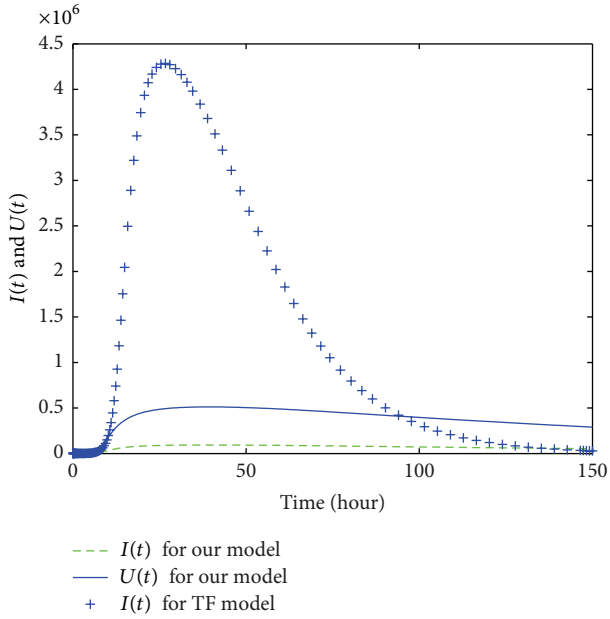

Figure 13: Mode one-TF.

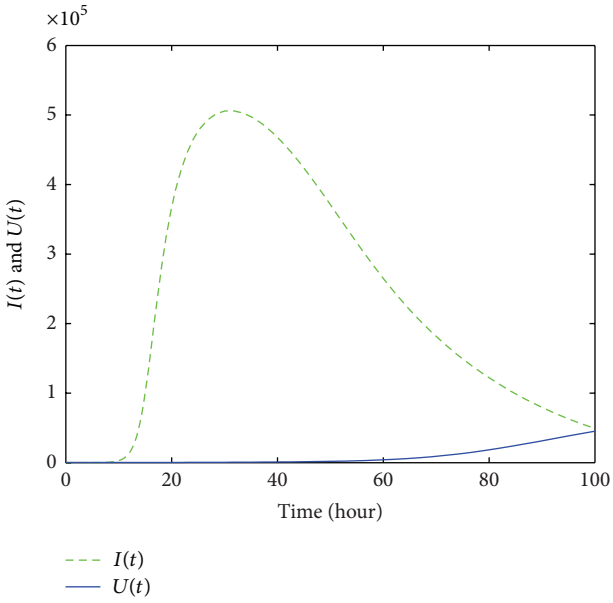

Figure 14: Mode two.

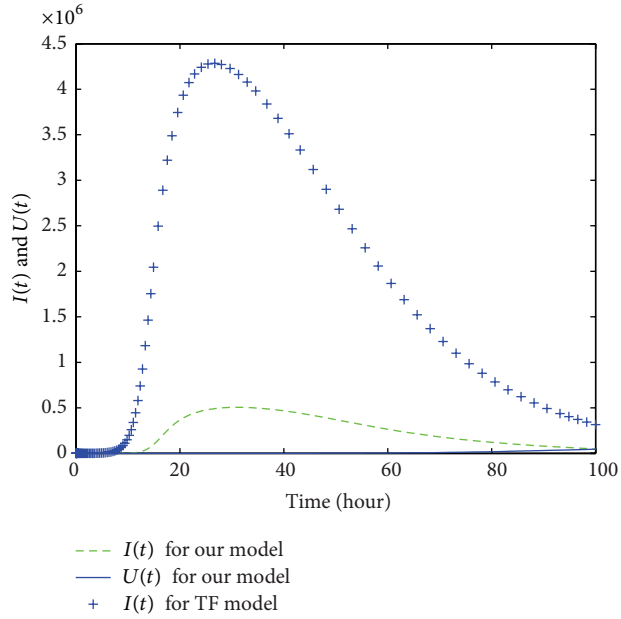

Figure 15: Mode two-TF.

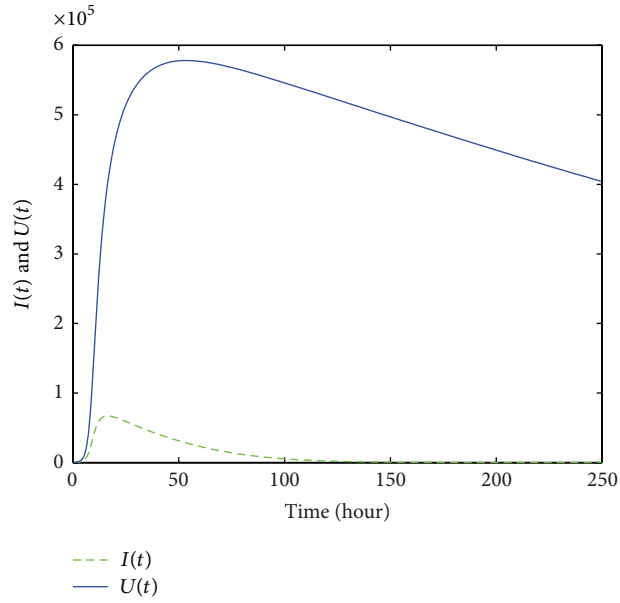

Figure 16: Mode three.

mode three have the most effective control for malicious worm.

Comparison with the TF model is in Figure 17.

Among the three active modes, the third mode has the most effective control for malicious worms. The control for the worm of the second situation is almost negligible and the first one has a certain influence. But for a specific situation, we can select benign worms of different active modes.

When the number of malicious worms is less than the number of benign worm, benign worms switch to passive scanning mode. The scanning rate is $\beta_3(t)$ and the initial value is $\beta_3 = 5 * 10^{-7}$. The delay time is 1 hour. Through the discussion of T, we can have the following conclusion.

By comparison, we can see that when M is large to a certain extent, the effect is very small, and the control becomes poor when M is less than 1. So here we take $M = 1$ or 2 for discussion. The simulation is shown in Figure 18.

When T obtains different values and M is set 2, we can see the change as shown in Figure 19.

In the mobile network environment, benign worms control the spread of the malicious worms; meanwhile, they will increase the scan frequency and load to the network to a certain extent. In the early stage of the benign worm using

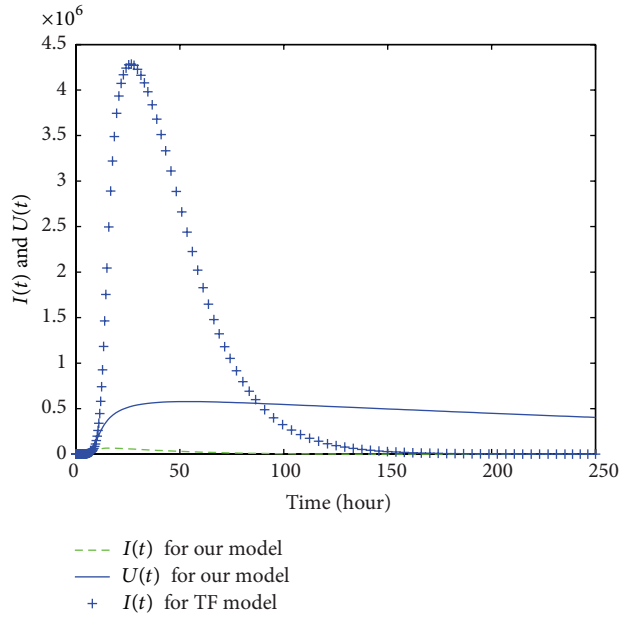

Figure 17: Mode three-TF.

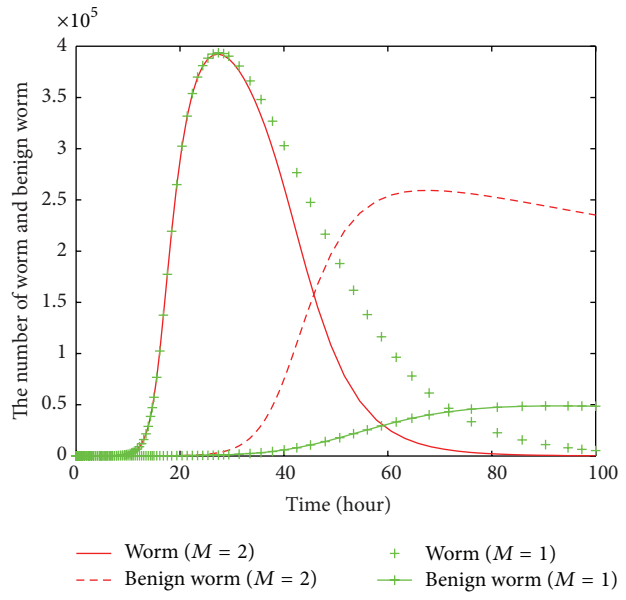

Figure 18: Comparison of different M.

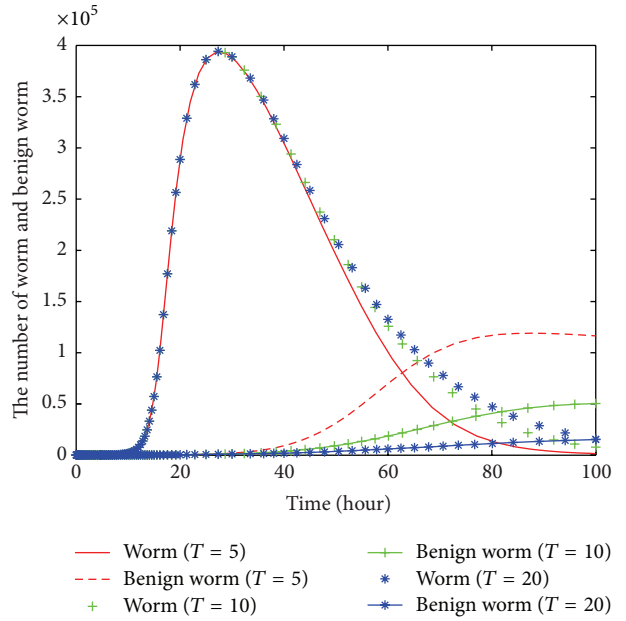

Figure 19: Comparison of different T.

active mode, it has inhibited the malicious worms on a large scale. After a certain time delay T, we need to postprocess the propagation, switching it into the passive worm pattern. Now the merits of passive worms reflected out. Benign worms will be self-destructed with the malicious worms being cleaned to ensure the fluency of the network. It is feasible for the model to remove the worms in mobile network and repair smart phone. And it has a certain guiding role to protect the safety of the mobile network in reality. Under the big trend that mobile network is in the continuous development now the security problems of mobile phone are particularly prominent. We still need to do further research on the new problems appearing in the reality.

6.2. Mobile Benign Worm States Simulations. We conduct numerical analysis for our states section. We set the parameters: $\beta_1 = 0.000012$, $\beta_2 = 0.000003$, $\beta_3 = 0.000006$, $\lambda = 0.03$, $\omega_1 = \omega_2 = \omega_4 = 0.05$, $\omega_3 = 0.02$, $N = 300000$, $\mu = 0.025$, $\alpha = 0.02$, and $\theta = 0.06$.

The numerical analysis diagram of no infection status is in Figure 20. The numerical analysis diagram of worm infection status is in Figure 21. The numerical analysis diagram of benign worm infection state is in Figure 22. The numerical analysis diagram of interaction infection state is in Figure 23.

In Figure 23, we studied the interaction infection status. In this case, the benign worm is introduced into the worms infected environment. Comparing Figure 21 with Figure 23, we found that the introduction of the benign worms suppresses the spread of the worm quickly and the number of infected host drops rapidly. All of these show the effectiveness of benign worm in theory. In addition, we also found that from the Figure 23 the number of susceptible individuals will get a slow rise to the equilibrium value after reaching the lowest equilibrium value. This is mainly because the death of infected individuals causes the decrease of the removal rate of susceptible hosts.

7. Conclusion

In this paper, we proposed a repairing mechanism for benign worm propagation based on the mobile network. In the detection and repairing mechanism, after collecting the problems of the whole mobile network, we can put the effective benign worms into the mobile network environment to improve the repairing efficiency when malicious worms outbreak. For

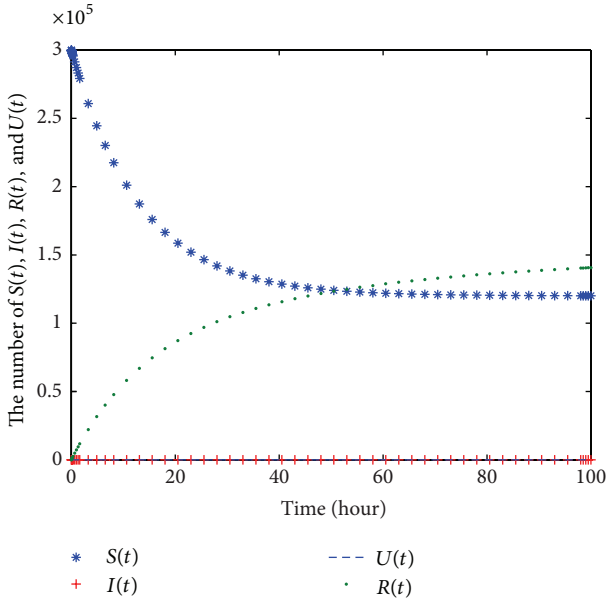

Figure 20: No infection status.

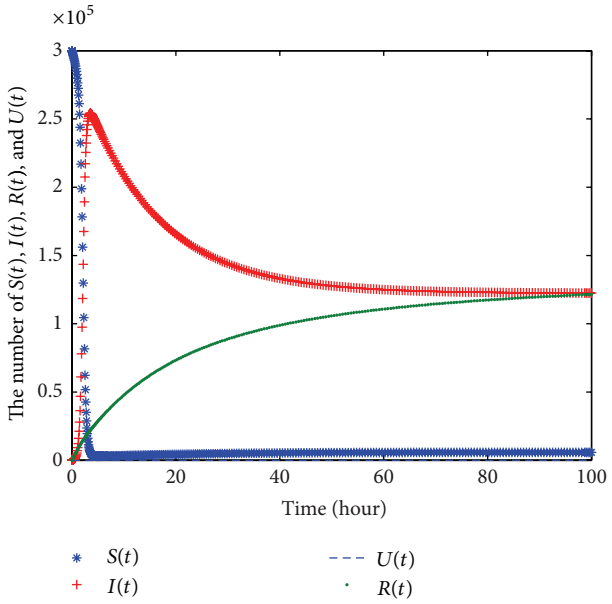

Figure 21: Worm infection status.

benign worm propagation mechanism, we first use the active mode of benign worm to quickly handle malicious worms in order to quickly release network resources occupied by malicious worms. Later after the malicious worms are under control, we switch to the passive mode and release mobile network resources further. Thus we not only ensure the safety of mobile networks, but also optimize the network correspondingly. The propagation and repairing mechanism has a certain guiding significance in the growing mobile Internet market. What is more, we need to do further research on it.

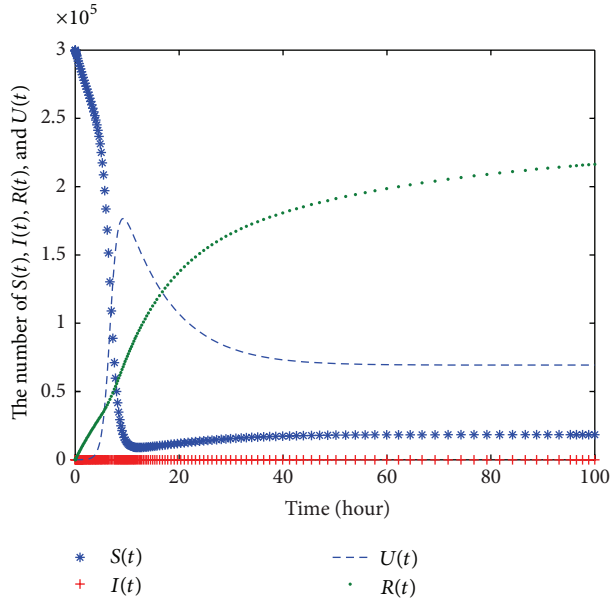

Figure 22: Benign worm infection state.

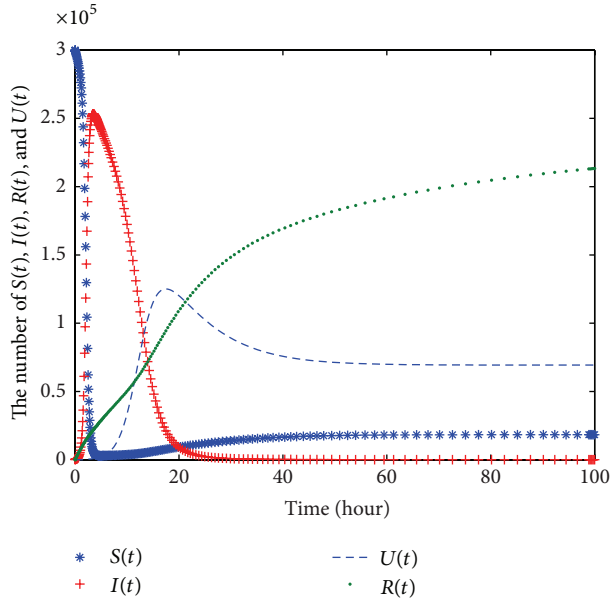

Figure 23: Interaction infection state.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported by 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), and Fujian Normal University Innovative Research Team (IRTL1207).

References

[1] H. Zhou, Y. Wen, and H. Zhao, "Modeling and analysis of active benign worms and hybrid benign worms containing the spread of worms," in *Proceedings of the 6th International Conference on Networking (ICN '07)*, p. 65, Martinique, France, April 2007.

[2] O. Toutonji and S.-M. Yoo, "Passive benign worm propagation modeling with dynamic quarantine defense," *KSII Transactions on Internet and Information Systems*, vol. 3, no. 1, pp. 96–107, 2009.

[3] F. Castañeda, E. C. Sezer, and J. Xu, "Worm vs. Worm: Preliminary study of an active counter-attack mechanism," in *Proceedings of the ACM Workshop on Rapid Malcode (WORM '04)*, pp. 83–93, ACM, October 2004.

[4] F. Cohen, "Computer viruses. Theory and experiments," *Computers and Security*, vol. 6, no. 1, pp. 22–35, 1987.

[5] V. Kostakos, "Experiences with urban deployment of Bluetooth (given at UCSD)," March 2007.

[6] Z. Hui, L. Dong, and G. Zhuo, "An epidemic model of mobile phone virus," in *Proceedings of the 1st International Symposium on Pervasive Computing and Applications (SPCA '06)*, pp. 1–5, Urumqi, China, August 2006.

[7] C. Mulliner, G. Vigna, D. Dagon, and W. Lee, "Using labeling to prevent cross-service attacks against smart phones," in *Detection of Intrusions and Malware & Vulnerability Assessment*, pp. 91–108, Springer, Berlin, Germany, 2006.

[8] S. Qing and W. Wen, "A survey and trends on internet worms," *Computers & Security*, vol. 24, no. 4, pp. 334–346, 2005.

[9] A. Bose and K. G. Shin, "Proactive security for mobile messaging networks," in *Proceedings of the 5th ACM workshop on Wireless security*, pp. 95–104, ACM, September 2006.

[10] E. Van Ruitenbeek, T. Courtney, W. H. Sanders, and F. Stevens, "Quantifying the effectiveness of mobile phone virus response mechanisms," in *Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '07)*, pp. 790–799, June 2007.

[11] P. Niels, "A virtual honeypot framework," in *Proceedings of the 12th USENIX Security Symposium*, vol. 173, San Diego, Calif, USA, August 2004.

[12] O. Laurent, *Fighting Internet Worms with Honeypots*, 2003, http://www.securityfocus.com/infocus/1740.

[13] X. Zheng, T. Li, and Y. Fang, "Strategy of fast and light-load cloud-based proactive benign worm countermeasure technology to contain worm propagation," *Journal of Supercomputing*, vol. 62, no. 3, pp. 1451–1479, 2012.