THE JOURNAL OF CHINA UNIVERSITIES OF POSTS AND TELECOMMUNICATIONS
Volume 15, Issue 2, June 2008

XIA Wei, LI Zhao-hui, CHEN Zeng-qiang, YUAN Zhu-zhi

Commwarrior worm propagation model for smart phone networks

CLC number TN915.08 **Document** A **Article ID** 1005-8885 (2008) 02-0060-07

Abstract Commwarrior worm is capable of spreading through both Bluetooth and multimedia messaging service (MMS) in smart phone networks. According to the propagation characteristics of Bluetooth and MMS, we built the susceptible-exposed-infected-recovered-dormancy (SEIRD) model for the Bluetooth and MMS hybrid spread mode and performed the stability analysis. The simulation results show good correlation with our theoretical analysis and demonstrate the effectiveness of this dynamic propagation model. On the basis of the SEIRD model, we further discuss at length the influence of the propagation parameters such as user gather density in groups, moving velocity of smart phone, the time for worm to replicate itself, and other interrelated parameters on the propagation of the virus. On the basis of these analytical and simulation results, some feasible control strategies will be proposed to restrain the spread of mobile worm such as commwarrior on smart phone network.

Keywords smart phone, virus, spreading model, Bluetooth, MMS

1 Introduction

Smart phones with more advanced and sophisticated features are available [1]. These devices combine the functionality of mobile phones and personal digital assistants (PDA), and they gradually integrate with different networking technologies such as IEEE 802.11, Bluetooth [2], GSM, and MMS [3]. They can offer Internet connectivity, function like minicomputers, and applications or files can be downloaded from them, but some of them could carry malicious codes [4]. As a result, smart phones are simultaneously more vulnerable, more useful, and more attractive for potential attack than older mobile phones.

Smart phone mobile worms spread mainly through Bluetooth or MMS [5]. Recent occurrences of spread of mobile worms such as Cabir, Mabir, Lasco, and commwarrior [6] have been through Bluetooth or MMS.

Now the research community has started to investigate the feasibility and the propagation characteristics of smart phone virus. In Ref. [7], gather traces and controlled experiments were used to show that a large-scale Bluetooth worm outbreak is viable today. In Ref. [8], a model indicating the spread of mobile phone virus was proposed. In Ref. [9], a baseline Bluetooth worm model was proposed and its propagation property was studied. In Ref. [10], a novel approach for testing the security of MMS User Agents was proposed. But so far there has been no research on mobile worms which are capable of spreading over both Bluetooth and MMS.

Commwarrior virus is the first virus that is capable of spreading through MMS as well as through Bluetooth. Commwarrior could potentially cause much trouble than Cabir because of its capability to spread via MMS, thus allowing it to spread from one country to another easily. It will increase the risk of worm propagation and actuate a large-scale Bluetooth worm outbreak.

The accurate modeling of the epidemics is the first step to understand the impact of the infectious disease and to develop effective control strategies. Mathematical analysis and dynamics study are often used to model the disease propagation. However, many dynamic characteristic of smart phone virus are not considered in the classical SIR/SIS models.

In order to increase the accuracy and relevance of epidemic models, in this paper we propose a mobile worm model that mirrors the designs of existing smart phone worms commwarrior. On the basis of smart phone virus for the Bluetooth and MMS hybrid spread mode, we divide the phone nodes into S, E, I, R and D states and 11 kinds of state conversions. We further build an SEIRD epidemic model and analyze the influence of the propagation parameters on the propagation of smart phone virus. These parameters may be the critical features for the outbreak of the epidemic.

2 Background

2.1 Bluetooth primer

Bluetooth is a short-range radio technology that is aimed at

Received date: 2007-08-13
XIA Wei (✉), LI Zhao-hui, CHEN Zeng-qiang, YUAN Zhu-zhi
College of Information Technical Science, Nankai University, Tianjin 300071, China
E-mail: nkxw@sina.com

connecting different wireless devices under low power consumption, providing wireless connectivity in ranges from 10 m (Class 2) to 100 m(Class 1). It operates in the 2.4 GHz frequency band and its channels are shared among devices through a time division duplexing (TDD) scheme.

Bluetooth has a wide range of applications, and almost all smart phones have a wireless module which enables the transmission of data to other Bluetooth-enabled devices and also enables the user to work in hands-free mode. A recent study from IDC estimates that there will be over 922 million Bluetooth-enabled devices worldwide by 2008. As do most technological developments, Bluetooth devices quickly attracted the attention of researchers on smart phone viruses and worms [11].

2.2 MMS primer

MMS is a standard for telephony messaging systems that allow sending messages that include multimedia objects (images, audio, video, rich text) and not just text as in short message service (SMS). MMS has been deployed world wide and across both GSM/GPRS and CDMA networks.

The fact that viruses aimed at smart phones are targeting MMS has raised concerns, considering the costs involved in sending such a message from one network to another or from one country to another. It will increase the worm propagation scope and actuate a large-scale Bluetooth worm outbreak.

2.3 Propagation mode of commwarrior

Commwarrior is a worm that operates on Symbian Series 60 devices. Smart phone owners are concerned over the appearance of commwarrior mobile virus that spreads via both Bluetooth and MMS messages, which was first reported in the wild in Ireland in January 2005. At present, commwarrior has undergone several mutations, but it mainly spreads through Bluetooth and MMS.

2.3.1 Bluetooth replication

Commwarrior replicates over Bluetooth wireless connections via randomly named SIS files. The SIS file contains the executable and boot components of the worm, named commwarrior.exe and commrec.mdl, respectively. The SIS file contains settings that will automatically execute commwarrior.exe when the SIS file is installed.

The commwarrior worm will search for other Bluetooth devices when it is activated. When it finds other devices, commwarrior will attempt to transfer a copy of itself to one device after another. If a target device goes out of range or rejects the file transfer, then commwarrior will search for another device.

2.3.2 Replication via MMS

MMS messages are multimedia messages that can be sent between Symbian smart phones and other phones that support MMS messaging. Commwarrior replicates via MMS when MMS messages that contain the infected SIS file are being sent to other users. The phone numbers from which the commwarrior-affected MMS messages are being sent are read from the phone address book. Commwarrior sends infected MMS messages, based on a user's messaging behavior, so that all messages sent to the infected phone will get infected MMS as response.

3 Connectivity of Bluetooth network

Currently, most smart phones have Bluetooth. An infected smart phone can only infect neighboring phones within its coverage radius of Bluetooth signal; by this way these smart phones form a Bluetooth phone network automatically. Every phone is a node of this network.

For propagation of Bluetooth worm, a determining factor is connectivity of the phone network. If the connectivity is not good enough, there is little chance to actuate a large-scale Bluetooth worm outbreak [7]. According to the relation of network connectivity, we present the formula for node average degree $\overline{k}$.

In the mobile environment, we denote $\overline{k}$ as the node average degree in unit time. We assume that nodes are uniformly distributed and several parameters are defined: r is coverage radius of the Bluetooth signal, σ is the distribution density of smart phones, and Δt is the time required for the worm to replicate itself. Then, we study the average degree of the node within Δt

All nodes of this coverage area are not infected within this time frame. Worm replication may fail because devices move out of each other's radio range within this replication period.

While the node moves, we suppose that the node lay in O_1 at the previous moment. In Fig. 1, after one Δt , the node moves to O_2, i.e. $O_1O_2=v\,\Delta t$ .When the node is with the pace v rectilinear motion at the uniform velocity, node of area among straight line AB and straight line CD can go through at least one Δt only, just probably have enough time to be infected. So we call the area between straight line AB and straight line CD as the region corresponding to effective virus propagation.

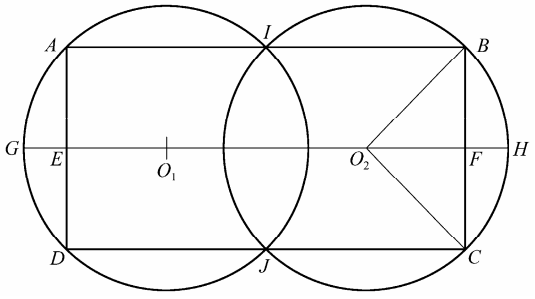

Fig. 1 Coverage area of mobile node within Δt

We define h to be the width of the propagating effective region,

$$h = AD = \sqrt{4r^2 - (\Delta t)^2 v^2} \tag{1}$$

The area of valid coverage region of Bluetooth signal in one second is defined as follows:

$$S = vh + \pi\left(\frac{h}{2}\right)^2 \tag{2}$$

Then, we can build this average degree formula:

$$\bar{k} = \sigma S - 1 = \sigma\left(v\sqrt{4r^2 - (\Delta t)^2 v^2} + \pi r^2 - \frac{\pi}{4}(\Delta t)^2 v^2\right) - 1 \tag{3}$$

4 SEIRD propagation model

This paper adds the dormancy state D to the basic SIR propagation model and proposes a new propagation model SEIRD for Bluetooth and MMS hybrid spread mode.

4.1 Node state with Bluetooth worm propagation

The smart phone Bluetooth virus is the active attack virus, similar to the worm affecting Internet. So we can draw lessons from the research approach which deals with the propagation of the worm in the traditional network. The study on worm often adopts classical epidemic model such as susceptible-infected (SI), susceptible-infected-susceptible (SIS), and model susceptible-infected-removed (SIR) [12] .

In the SIS propagation model, it is supposed that an infected phone can be recovered but can again become susceptible. It actually imitated only the partial statues of the smart phone Bluetooth worm propagation. Generally, the recovered nodes always have immunological functions, such as patches for protection, and we can use the SIR model to perform research at this moment.

In the SIR model, it is assumed that during the propagation of smart phone virus, nodes change state according to the following law: $\mathrm{S} \to \mathrm{I} \to \mathrm{R}$. Therefore, the average degree of smart phone Bluetooth worm propagation model-based nodes is:

$$\frac{\mathrm{d}I(t)}{\mathrm{d}t} = \beta\bar{k}S(t)I(t) - \gamma I(t) \tag{4}$$

where β is the infection rate, γ is the rate of removal from infectious nodes, and $\bar{k}$ is node average degree which is defined in Eq. (3).

Because Bluetooth worm constantly probes for Bluetooth devices, it will lead to exhaustion of the battery of infected phone. So in this model we increased the dormancy state D. In the dormancy state, smart phone is shut down because the battery is exhausted, thus this state will not facilitate the propagation of the virus. We should also notice that, after some dormancy state, smart phone recharge and resume activity, and the virus can continue to spread. So in this model, we also need to increase two kinds of state conversions: $\mathrm{D} \to \mathrm{I} \to \mathrm{I} \to \mathrm{D}$.

4.2 Node state with MMS propagation

The spread mode of MMS is similar to email virus. According to the already studied relevant literature of propagation characteristic of email virus in Refs. [13−15] and phone MMS virus, we divide the phone node into S, E, I and R states and 7 kinds of state conversions. This kind of model can simulate virus spread through MMS in the smart phone network.

4.3 SEIRD model

In this paper, we propose an MMS and Bluetooth mix SEIRD model. As shown in Fig. 2, we divide the phone node into S, E, I, R and D states and 11 kinds of state conversions, among them: S→I, I→D, D→I, E→I(β) are related to propagation mode in Bluetooth; S→E, E→S, E→R, E→I(μ) are related to propagation mode in MMS; and S→R, I→R, and I→S are commonly related to Bluetooth and MMS.

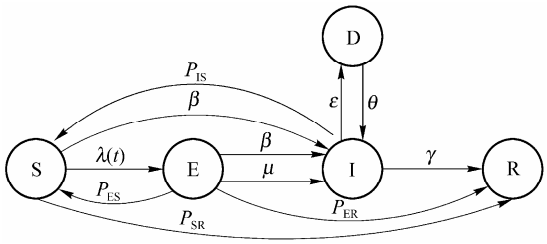

Fig. 2 Smart phone state conversions

In Fig. 2, $\lambda(t)$ is the rate at which susceptible smart phones become exposed (latent); P_{ER} is the probability that exposed (latent) smart phones under the prerequisite of nonactive MMS virus get overall technical support (kill virus and immunity) and directly remove the virus; P_{ES} is the probability that exposed (latent) smart phones gain partial technical support (kill virus) and become susceptible; γ is the probability that infectious smart phones gain overall technical support and become removed; P_{IS} is the probability that infectious smart phones get partial technical support (kill virus) and become susceptible; μ is the probability that exposed (latent) smart phones become infectious, because users have opened the multimedia message and have opened the attached virus file; P_{SR} is the probability that susceptible smart phones obtain immunity, resulting in the removal of the virus (recovered or are isolated); ε is the probability that infectious smart phones whose battery are exhausted through Bluetooth technology enter the dormancy state; θ is the probability that the dormant

smart phones become infectious after being recharged. Then SEIRD model can be described with the following differential Eq. (5):

$$\begin{cases} \dfrac{\mathrm{d}S(t)}{\mathrm{d}t} = P_{\mathrm{ES}}E(t) + P_{\mathrm{IS}}I(t) - \beta\bar{k}S(t)I(t) - \lambda(t)S(t) - P_{\mathrm{SR}}S(t) \\ \dfrac{\mathrm{d}E(t)}{\mathrm{d}t} = \lambda(t)S(t) - \beta\bar{k}E(t)I(t) - (\mu + P_{\mathrm{ES}} + P_{\mathrm{ER}})E(t) \\ \dfrac{\mathrm{d}I(t)}{\mathrm{d}t} = \beta\bar{k}(S(t) + E(t))I(t) + \mu E(t) + \theta D(t) - (\gamma + P_{\mathrm{IS}} + \varepsilon)I(t) \\ \dfrac{\mathrm{d}R(t)}{\mathrm{d}t} = \gamma I(t) + P_{\mathrm{ER}}E(t) + P_{\mathrm{SR}}S(t) \\ \dfrac{\mathrm{d}D(t)}{\mathrm{d}t} = \varepsilon I(t) - \theta D(t) \\ N = S(t) + E(t) + I(t) + R(t) + D(t) \\ \bar{k} = \sigma(v\sqrt{4r^2 - (\Delta t)^2 v^2} + \pi r^2 - \dfrac{\pi}{4}(\Delta t)^2 v^2) - 1 \\ \lambda(t) = w\eta \dfrac{I(t)}{N} \dfrac{S(t)}{S(t) + I(t)} \end{cases} \tag{5}$$

where β is the infection rate, and value range is 0–1; $S(t)$ is the number of susceptible nodes at time t; $E(t)$ is the number of exposed (latent) nodes at time t; $R(t)$ is the number of recovered nodes at time t; $D(t)$ is the number of dormancy nodes at time t; N is the total number of the nodes in the whole smart phones network; $\bar{k}$ is average degree within node radio radius; Constant w in $\lambda(t)$ gives the expression of average contact quantity of each smart phone user; η is the probability that the infected phone propagates the virus to its contacts, according to the unique infection mode of MMS virus, when we imitate MMS virus propagation, generally we assume η=1.0.

Now we analyze the stability of Eq. (5). Let

$$\frac{\mathrm{d}S(t)}{\mathrm{d}t} = 0,\ \frac{\mathrm{d}E(t)}{\mathrm{d}t} = 0,\ \frac{\mathrm{d}I(t)}{\mathrm{d}t} = 0,\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} = 0,\ \frac{\mathrm{d}D(t)}{\mathrm{d}t} = 0 \tag{6}$$

From $\dfrac{\mathrm{d}R(t)}{\mathrm{d}t} = 0$, we can obtain:

$$I(\infty) = 0,\ E(\infty) = 0,\ S(\infty) = 0$$

Then from Eq. (5), we can draw

$$R(\infty) = N,\ D(\infty) = 0$$

Thus the stable solution of Eq. (5) is

$$S(\infty) = 0,\ E(\infty) = 0,\ I(\infty) = 0,\ R(\infty) = N,\ D(\infty) = 0 \tag{7}$$

4.4 Simulation results

We have the total number of the nodes in the whole smart phones network as N=1 000 000 (according to the needs of research, expanding or reducing arbitrarily). Assume that the number of average contacts of each MMS user is r = 10. Initial state infected node I (0)=1, then $S(0)=N-1$, $E(0)=0$, $R(0)=0$, $D(0)=0$. We supposed that the average time interval of most users receiving the letters twice is $t_{\mathrm{S}} + t_{\mathrm{E}}$ =200 min in MMS frequent application environment, i.e. $t_{\mathrm{S}} = t_{\mathrm{E}}$ =100 min. This means that 1/100 of the exposed (latent) user's state changes in unit time under uniform distribution: among them, 1/5 of these users can add the immune means voluntarily under the condition of not being infected by the virus, i.e. P_{ER} = 0.002; 1/10 of the users can deal with virus mail, but did not have the appropriate immunity, i.e. P_{ES} = 0.001, then $\mu = 1/100 - P_{\mathrm{ER}} - P_{\mathrm{ES}}$ = 0.007. In addition, we assume that the average time required by the users from the time of infection to time of getting technical support is 50 min, among them 1/10 of the users cannot regain appropriate immunity after killing the virus, i.e. $P_{\mathrm{IS}} = 1/(50\times10)$ = 0.002, then $\gamma = 1/50 - P_{\mathrm{IS}}$ = 0.018. Other parameters are: σ = 0.005, r = 10, v = 20, β = 0.25/N, ε = 0.03, θ = 0.05, and Δt = 0.1.

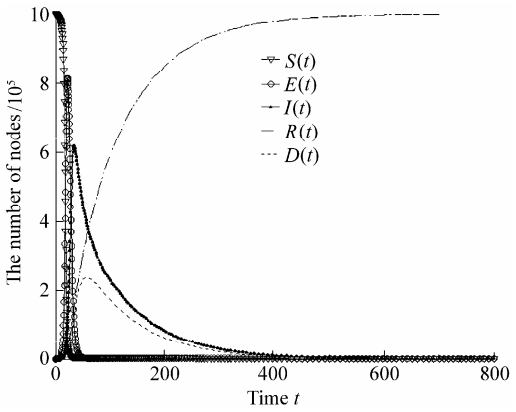

Fig. 3 SEIRD model simulation result

The simulation result indicates that the SEIRD model developed here shows good correlation with the results of our theoretical analysis. This model perfectly simulates the Bluetooth and MMS hybrid spread mode of the virus and leads to a better understanding and prediction of the scale and speed at which the commwarrior worm spreads in smart phone network.

Other parameters are shown in Table 1.

Table 1 Propagation model parameter

Parameter	Meaning	Value range or unit
σ	Distribution density of smart phones (uniform distribution)	0.001–4/m^2
r	Coverage radius of Bluetooth signal	0.1–30 m
v	Moving velocity of smart phone (uniform velocity)	m·s^{-1}
Δt	The time for worm to replicate itself	0.01–0.5 s

5 Parameter analysis and emulation

The propagation of smart phone virus through Bluetooth and MMS hybrid spread mode is influenced by several factors. We will make use of the SEIRD model to simulate the result with regards to the influence of the factors described in this paper. Because of the imitation time granularity relatively small, it can not compare and fit with statistics of the relatively large granularity in the real world. So, we select a

group of observed data in which every factor being parameterized is already selected on a simulation basis and then trace the diffusion law of this virus in different influence degrees of this parameter by changing the value of the parameter.

5.1 Effects of λ (*t*)

$\lambda(t)$ has great influence on the spread of the smart phone virus. If there is the communication gather characteristic between the MMS users (some people have relatively higher communication density because the contact is close), then the spread relation of MMS with virus is mutual. $\lambda(t)$ has shown such a characteristic: in the system of the limited capacity, the speed at which the infection spreads is related to the relative number of susceptible nodes to that of the infected nodes in the whole smart phone network and is also related to the relative distribution density in the whole network.

5.2 Effects of *w* (users' gather density in groups)

Users' gather density in groups w means the number of contact users of each phone node. With regards to email or MMS virus propagation, it is an important influencing parameter. Users' gather density in groups $w > 0$ indicated that information exchange between users disobeys uniform distribution within the whole system, and traffic flow and time density of information exchange between users in the group are higher than the exchange among the groups. In this way, the size of w will influence velocity and scale of the virus eruption: the increase in the value of w (i.e. the higher the number of contacts in the group) will promote the spread of the virus, and the time corresponding to virus infection and outbreak will also be shortened. In Fig. 4, the simulation result indicates under the condition of w=1, w=10, w=100, w=200, and w=500, five conditions for the propagation of the comm-warrior worm in smart phone network.

From Fig. 4, we can see when w is smaller, the scale of the virus propagation is small and the time corresponding to worm out break is relatively low. On the contrary, when the value of w is high, the scale of virus propagation is large and the time corresponding to worm outbreak is relatively high. When w increases to certain value, change of w fetching value has little influence on virus-infection scale and the time corresponding to the outbreak of the worm. The rational theory analysis is: when the number of infected users in the network is already quite high, the possibility that virus-infected MMS being sent by infected users is being received by immune users or already infected users will also increase. These users play a certain role in reducing the spread of the virus. So the peak of the scale of virus propagation could not reach N.

In order to reduce the influence of w, phone users should often manage address book and delete the cell-phone number that cannot be often contacted during the infection by the MMS virus. In this way, it will slow down the spread of the virus and reduce the expenses resulting from the MMS sent automatically by the virus.

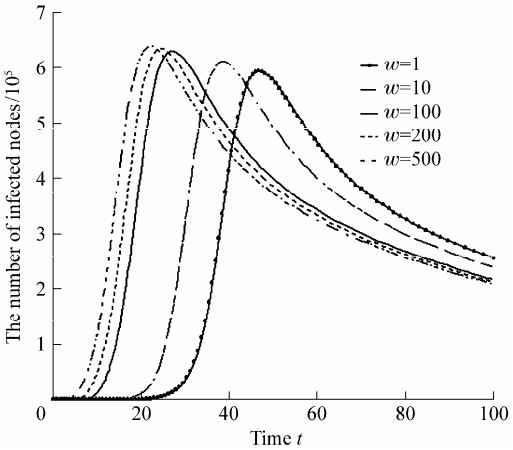

Fig. 4 Effects of w

5.3 Effects of parameter *v*

Based on Eq. (2), we find

$$s_1 = v\sqrt{4r^2 - (\Delta t)^2 v^2} \tag{8}$$

$$s_2 = \pi r^2 - \frac{\pi}{4}(\Delta t)^2 v^2 \tag{9}$$

Then $S = s_1 + s_2$.

Figure 5 shows the curves of v-s_1, v-s_2, and v-S. Curve v-S shows the direct influence of the moving velocity of smart phone on areas of valid propagation region and also shows the indirect influence of moving velocity of smart phones on average degree i.e. the effects on speed of propagation of the virus. Among them, r = 10, Δt = 0.2. From Fig. 5 we can see that there is a phone moving velocity v at which S becomes maximum.

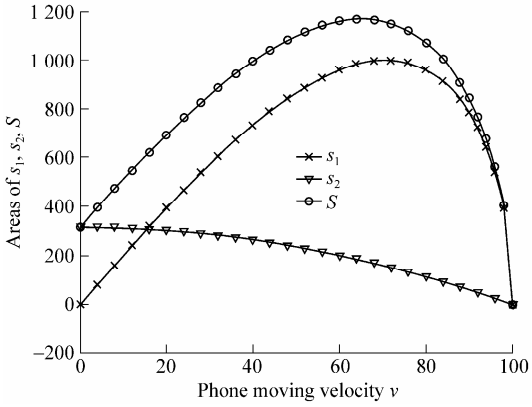

Fig. 5 Curves of v-s_1, v-s_2, v-S

From Fig. 5 we can see that s_2 has little influence on S when the value of Δt is small. So we will only discuss s_1.

We have $s_1' = 0$, (i.e. $(v\sqrt{4r^2-(\Delta t)^2v^2})' = 0$). Then, we obtain $s_{1\max} = 2r^2/\Delta t$ when $v = \sqrt{2}r/\Delta t$. The virus spreads fastest under this smart phone moving velocity v. We call this velocity the worst velocity, i.e. $v_{\text{worst}} = \sqrt{2}r/\Delta t$.

The obatined result shows that when the moving velocity $v < v_{\text{worst}}$, rising the velocity will increase the average degree of the node and enlarge the areas of valid propagation region, and then accelerate the worm propagation. When $v = v_{\text{worst}}$, the average degree of the node and the areas of valid propagation region will reach maximum. So, the propagation of the worm is the fastest at this time. When $v > v_{\text{worst}}$, increase in the velocity will decrease the average degree of the node and shrink the areas of valid propagation region, and then reduce the propagation of the worm. To reduce the moving velocity of smart phones which are close to the worst velocity, node will slow down the spread of the virus.

When $v = 2r/\Delta t$, from Eq. (2) we get $S = 0$. At this time, the virus cannot spread. Bluetooth is a short-range radio technology. When the smart phone moves very fast, the devices will move out of each other's radio range within Δt . The virus cannot spread. So when $v > 2r/\Delta t$, mobile nodes will not facilitate the spread of the virus.

5.4 Effects of virus replication time Δt

The time Δt corresponding to the spread of the virus from one smart phone to another smart phone reflects the spreading ability of this virus. The smaller the value of Δt , the stronger is the virus propagation ability in the mobile environment. Investigating the calculation Eq. (3) for the average degree of the node at unit time in the mobile environment, we can see that when r, v is not altered, the smaller Δt is and the larger the average degree becomes. So reducing Δt will facilitate the spread of the virus.

5.5 Effects of parameter σ

Only when the node average degree $\bar{k} > 0$, the virus can spread. We have

$$\delta = v\sqrt{4r^2-(\Delta t)^2v^2} + \pi r^2 - \frac{\pi}{4}(\Delta t)^2v^2 \tag{10}$$

Then

$$\sigma > \frac{1}{\delta} \tag{11}$$

Only when Eq. (11) is satisfied, the virus can spread. According to SEIRD epidemic model and Eq. (3), we can see that the heavier the node distribution density, the larger is the average degree of the node, and then it will accelerate the propagation of the virus.

5.6 Effects of parameter r

From Eq. (3), we can see that increase in the coverage radius of Bluetooth signal r will increase node average degree and accelerate the virus propagation.

6 Conclusions

Smart phones have become increasingly popular. However, the flexibility of running third-party software also leaves the smart phones open to malicious viruses. Recent occurrences of mobile worms such as Cabir, Mabir, and commwarrior have created growing concerns over the security of data stored in smart phones. Generally, all these worms use Bluetooth or MMS communication as their infection channel. In particular, commwarrior is the first virus that is capable of spreading using MMS as well as Bluetooth. Commwarrior could be potentially more troublesome than other viruses. But there has been no research on mobile worms which are capable of spreading over both Bluetooth and MMS.

In order to devise effective defense strategies against such viruses, we build a new worm propagation model SEIRD for smart phone network. We studied the propagation characteristics of Bluetooth and MMS and then built the SEIRD model for the Bluetooth and MMS hybrid spread mode according to Commwarrior. We further analyzed the influence of the propagation parameters on the propagation of the smart phone virus and drewseveral useful conclusions.

Acknowledgements This work is supported by the National Natural Science Foundation of China (60574036), the Natural Science Foundation of Tianjin (08JCYBJC12800), the Program for New Century Excellent Talents in University (NCET2005-290) and the Science and Technology Innovation Fund of Nankai University (Z1A2006012).

References

1. Zhang Ai-hua, Zhao Lian-qiang, Shu Hua-ying. The evolution of investments decision mode in China's telecommunication. The Journal of China Universities of Posts and Telecommunications, 2007 14 (1): 122−128
2. Bluetooth Special Interest Group. Bluetooth Core Specification Version 2.0+ EDR. http://www.bluetooth.org, 2004-11
3. Andersson S. MMS Security Considerations. 3GPP TSG SA WG3 Security, 2003
4. Mulliner C. Security of smart phones, master's thesis, department of computer science. Santa Barbara, CA, USA: University of California Santa Barbara, 2006

5. Tang C. Summary of mobile threats for year 2005. [2006-04-06]. http://www.it-observer.com/pdf/dl/mobile_threat_sum.pdf
6. Lactaotao M. Security information: virus encyclopedia: symbos comwar. a: technical details. Trend Micro Incorporated, 2005
7. SU J, Chan K K W, Miklas A G, et al. A preliminary investigation of worm infections in a bluetooth environment. Proceedings of the 4th ACM Workshop on Recurring Malcode (WORM'06) Co-located with the 13th ACM Conference on Computer and Communications Security (CCS'06), Nor 3, 2006, Alexandria, VA, USA. New York, NY, USA: ACM, 2006: 9−16
8. Zheng Hui, Li Dong, Gao Zhuo. An epidemic model of mobile phone virus. The 1st International Symposium on Pervasive Computing and Applications Proceedings (SPCA'06), Aug 3−5, 2006, Urumchi, China. Piscataway, NJ, USA: IEEE Computer Society, 2006: 534−538
9. Yan Guan-hua, Hector D Flores, Leticia Cuellar, et al. Bluetooth worm propagation: mobility pattern matters. Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, Mar 20−22, 2007, Singapore. 2007: 245−256
10. Mulliner C, Vigna G. Vulnerability analysisof MMS user agents. Proceedings of 22nd Annual Computer Security Applications Conference (ACSAC'06), Dec 11−15, 2006, Miami Beach, FL, USA. Los Alamitos, CA, USA: IEEE Computer Society, 2006: 77−88
11. Carettoni L, Merloni C, Zanero S. Studying Bluetooth malware propagation: the BlueBag project. IEEE Security and Privacy, 2007, 5(2): 17−25
12. Daley D J, Gani J. Epidemic modelling: an introduction. Cambridge, UK: Cambridge University Press, 1999
13. Zou C C, Towsley D, Gong W. Email worm modeling and defense. Proceedings of 13th International Conference on Computer Communications and Networks (ICCCN'04), Oct 11−13, 2004, Chicago, IL, USA. Piscataway, NJ, USA: IEEE Computer Society, 2004: 409−414
14. Zou C C C, Towsley D. Email virus propagation modeling and analysis. Umass ECE Technical Report TR-03-CSE-04. 2003
15. Yuan Hua, Chen Guo-qing. Simulation model of e-mail virus propagation and simulation of its influence factors. Computer Engineering and Design, 2006, 27(11): 1914−1916 (in Chinese)

Biographies: XIA Wei, Ph. D. Candidate in Operational Research and Cybernetics in Nankai University. Her research interests include wireless network and information security.

CHEN Zeng-qiang, professor and the advisor for Ph. D. students in the College of Information Technology Sciences of Nankai University, his main areas of research are in computer communication technology, complex networks, adaptive control, and Chaos system. He has authored/coauthored more than 90 journal papers in these areas.