Journal of Computer and System Sciences 79 (2013) 586–595

Contents lists available at SciVerse ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Modeling the dynamics of worm propagation using two-dimensional cellular automata in smartphones

Sancheng Peng [a], Guojun Wang [b,*], Shui Yu [c]

[a] School of Computer Science, Zhaoqing University, Zhaoqing, 526061, China
[b] School of Information Science and Engineering, Central South University, Changsha, 410083, China
[c] School of Information Technology, Deakin University, 221 Burwood HWY, Burwood, VIC 3125, Australia

ARTICLE INFO

Article history:
Received 1 March 2012
Received in revised form 29 September 2012
Accepted 8 November 2012
Available online 14 December 2012

Keywords:
Smartphones
Worm propagation
Bluetooth
Cellular automata

ABSTRACT

Smartphones combine the communication capabilities of cellphones and the functions of PDA (personal digital assistant), which enable us to access a large variety of ubiquitous services, such as surfing the web, sending/receiving emails, MMS, and online shopping. However, the availability of these services provided by smartphones increases the vulnerability to worm attacks. In addition, modeling on worm propagation in smartphones is particularly challenging because it is difficult to piece together dynamics from pair-wise device interactions. To characterize the propagation dynamics of worms in smartphones, we propose an efficient worm propagation modeling scheme using a two-dimensional cellular automata based on the epidemic theory. A set of suitable local transition rules is designed for the two-dimensional cellular automata in this scheme. Moreover, this scheme integrates an infection factor to evaluate the spread degree of infected nodes, and a resistance factor to evaluate the degree that susceptible nodes resist. Five classes of epidemic states are considered: susceptible, exposed, infected, diagnosed, and recovered. We explore a strategy for simulating the dynamics of worm propagation process from a single node to the entire network. The effectiveness and rationality of the proposed model have been validated through extensive simulations.

1. Introduction

Smartphones combine the wireless communication capabilities of cellphones and the functionalities of personal digital assistants (PDAs). They can be used to surf the web, send/receive emails, store and play music, and take photographs and videos. In addition, most smartphones use an application-based interface, which allows users to download individual programs that can perform a variety of tasks. Canalys [1] published its final worldwide country-level Q2 2011 smart phone market estimates in August 1, 2011, showing a substantial market growth in all regions of the world. Globally, the market grows 73% year-on-year, with around 107.7 million units shipped in the second quarter of 2011.

As the popularity of smartphones increases, the number of smartphones on the market is steadily increasing. To more and more users, smartphones are becoming an integral part of their everyday lives. Moreover, most smartphones are now being equipped with advanced features, such as e-mail access and multimedia messaging, which increases their vulnerability to infection. Yet, fewer smartphones are being designed to guard against worm attacks, which makes them a more appealing target to hackers and worm writers.

* Corresponding author.
E-mail address: csgjwang@mail.csu.edu.cn (G. Wang).

0022-0000/$ – see front matter
http://dx.doi.org/10.1016/j.jcss.2012.11.007

Worms are self-replicating computer viruses, which can propagate through computer networks without any human intervention. They have been rampant in the Internet for more than two decades. Since 2004, worms have been known to spread among smartphones and other mobile devices through wireless networks. The first known worm in smartphones emerged in June 2004. It was called Cabir [2] and was propagated through Bluetooth [3,4] as an infection vector.

There are various channels used by malware in smartphones to transmit an infection to other susceptible smartphones. Smartphones can be subjected to various attack vectors, such as SMS, Bluetooth, WiFi, Web browsers, and emails. These become a step stone that allows a hacker to have access to personal information on personal smartphones. In this paper, we focus on proximity based communication channels, namely, we concentrate our study on modeling and analysis of Bluetooth-based worm propagation, which provides a means of message transfer similar to the method of spreading infectious diseases. A preliminary version of this paper appeared in [5].

Mathematical epidemiology has existed for over a hundred years. Epidemic modeling is used to imitate the spreading of infectious diseases for a given population, such as H1N1, SARS, and influenza. Infected individuals spread the virus to healthy individuals that they contact with. We can use this model to predict the transmission rate of mobile malware in smartphones based on contact via proximity.

Since Internet worms are similar to biological viruses in their self-replicating and propagative behaviors, epidemiological models for analyzing the propagation of Internet worms is nothing new to us, as there has been tremendous interest in modeling the propagation of Internet worms over the past decades [6–8]. The study of computer worms in general, and Internet worms in particular, is a very popular topic of research.

The security issue regarding worm propagation that exploits geographic proximity of wireless-enabled devices has received significant attention in recent years. Many efforts have been made to model the propagation behaviors of worms in wireless networks, such as wireless sensor networks [9] and wireless ad-hoc networks [10]. Most epidemic models have focused almost entirely on the technology of the differential equations [9] and the Markov chain [10].

Although most previous work can provide some valuable insight into the characteristics and dynamics of worm propagation, the models based on differential equations fail to capture the local characteristics of spreading processes, nor do they include interaction behaviors among individuals. Furthermore, the models based on the Markov chain are difficult to describe the spatial–temporal process of worm propagation.

Cellular automata (CA) [11] can overcome these drawbacks and has been used as an efficient alternative method to characterize epidemic spreading [12–15] and malware propagation [16]. Generally speaking, cellular automata can model the computation capability characterizing physical, biological, or environmental complex phenomena, such as growth processes, reaction–diffusion systems, epidemic models, and the spread of forest fire.

Even though CAs have been used for several decades in the domain of computational models, modeling worm propagation has rarely been utilized to its full potential. The main goal of our work is to verify the applicability using the cellular automata to characterize the propagation dynamics of Bluetooth worms. We believe that CAs can be useful in simulating this kind of network because the behavior and/or the state of a wireless node are/is capable of modifying all network behaviors. This characteristic is similar to that found in many dynamic systems, which are commonly simulated through CAs.

In this paper, based on cellular automata, we present a detailed analytical model that characterizes the propagation dynamics of Bluetooth worms by considering the following realistic modeling assumptions: 1) the infection factor of an infectious device for susceptibility is different, and 2) the resistance factor of each device for spreading a worm is different. These assumptions are not usually addressed in previous analytical work due to their simplicity. The goal of our work is summarized as follows:

- To characterize the propagation dynamics of Bluetooth worms by exploiting cellular automata and by introducing an infection index to measure the state of transition to susceptible individuals.
- To formulate the impact of individual difference on the propagation dynamics of Bluetooth worm by introducing an infection factor and/or resistance factor of individuals.
- To show the effectiveness and rationality of the proposed approach through extensive simulations and numerical analysis.

The remainder of this paper is structured as follows: In Section 2, we provide an overview of related work and discuss the system model in Section 3. In Section 4, we present a model to characterize the spreading of the epidemic. We show the results of model validation in Section 5, and conclude the paper in Section 6.

2. Related work

In this section, we investigate related work in three dimensions. The first dimension is the Bluetooth-based worm propagation model; the second is related to the SMS/MMS-based worm propagation model; and the last is related to the hybrid worm propagation model.

2.1. Bluetooth-based

With the increasing of inherent convenience and computation and communication power, smartphones are becoming a natural focus of future network applications. However, the smartphone-based mobile networks in turn have become the target of malware. A number of studies have demonstrated the severe threat of Bluetooth-based malware propagation.

Yan and Eidenbenz [17] built a comprehensive analytical model to study the spread of Bluetooth worms and to investigate the impact of mobility patterns on Bluetooth worm propagation. Rhodes and Nekovee [18] investigated the effect of population characteristics and device behavior on the outbreak dynamics of Bluetooth worms. Martin et al. [19] predicted the future spread of cell phone viruses using the SIS model from mathematical epidemiology. Su et al. [20] investigated whether a large-scale Bluetooth worm outbreak is viable in practice and used trace-driven simulations to examine the propagation dynamics of Bluetooth worms. They found that Bluetooth worms can infect a large population, in just a few days. Zheng et al. [21] focused on modeling population distribution density, Bluetooth radius, and node velocity. Their results pointed to a variety of quarantine methods that could greatly reduce the worm potential virulence. Mickens and Noble [22] proposed a probabilistic queuing framework to model the propagation of mobile viruses over short-range wireless interfaces using coupled differential equations. The authors demonstrated the impact of node speed upon the steady state infection level of the network, and provided a preliminary stochastic counterpart for the deterministic model.

2.2. SMS/MMS-based

Some viruses can spread via short/multimedia messaging service (SMS/MMS) messages by attaching a copy of itself to a SMS/MMS message and sending the virus to some other device capable of receiving SMS/MMS. The propagation of SMS/MMS-based viruses in smartphones follows a long-range spreading pattern similar to the spreading of computer viruses.

Van Ruitenbeek et al. [23] proposed response mechanisms to analyze the effects of multimedia messaging system (MMS) viruses that spread by sending infected messages to other phones. Fleizach et al. [24] developed an event-based simulator to evaluate the effects of malware propagation using communication services like VOIP and MMS in mobile phone networks. However, they did not use real traffic data in their worm propagation model.

2.3. Hybrid-based

Specifically, some hybrid viruses can propagate via Bluetooth and SMS/MMS, and have the potential to become more dangerous than the propagation of viruses through a single spreading vector. Investigating Hybrid-based schemes related to the malware of smartphones is now gaining attention, with many malware propagation models for smartphones proposed.

Gao and Liu [25] proposed a two-layer model to simulate the propagation process of Bluetooth-based and SMS-based viruses in mobile networks. The impact of human behavior (i.e., human operations and mobility patterns) on virus propagation were imported into this model. Cheng et al. [26] proposed an analytical model to efficiently analyze the speed and severity for spreading the hybrid malware, such as Commwarrior which could target a multimedia messaging service (MMS) and Bluetooth. Ramachandran and Sikdar [27] presented a comprehensive analytical model to explore the impact of various spreading mechanisms on the dynamics of malware propagation in networks of smart cell phones, such as downloads from the Internet or P2P networks, transfers through Bluetooth, WLAN and infra-red interfaces, and also through MMS or SMS messages. Xia et al. [28] discussed the propagation characteristics of Bluetooth and MMS, and then built the susceptible–exposed–infected–recovered–dormancy (SEIRD) model for the Bluetooth and MMS hybrid spread mode according to Commwarrior. Wang et al. [29] presented a model on mobile malware using the SI model and studied the spreading patterns of both Bluetooth and MMS worms. Mobile phone data was processed to obtain the mobility of devices at a cell-tower resolution. The compartmental model studied here did not represent the heterogeneity that was required to represent realistic network characteristics. Bose and Shin [30] modeled the malware propagation through both MMS/SMS and Bluetooth vectors using a fine-grained agent-based simulator. They emulated the propagation of this virus in a small mobile network representative of a public meeting place such as a stadium or airport using data from a real-world SMS network. Fan et al. [31] built the Susceptible-Exposed-Infected-Recovered (SEIR) model for the Bluetooth and SMS/MMS hybrid spread mode based on the preventive immunity and mutation of a mobile phone virus. They further discussed the influence of the propagation parameter such as preventive immunity of mobile phone users, mutation of virus, immunity structure in the SMS/MMS network and node average degree in the Bluetooth network on the propagation of the virus.

3. System modeling

According to the spread property of Bluetooth worms, the epidemic state of a node or a cell is divided as follows:

Susceptible state (S): nodes have not been infected by any worm in the network but are prone to infection.

Exposed state (E): nodes have been infected by the worm but have not spread the worm to the susceptible smartphone while transmitting data or controlling the messages sent to the phones for the time being.

Infectious state (I): nodes have been infected by worms in the network and they may infect some nodes in state S.

Diagnosed state (D): nodes have been diagnosed to be infected by some kind of specific worm.

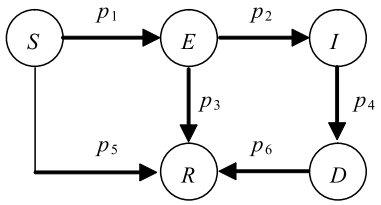


Fig. 1. State transition relationship for worm propagation.

Table 1
Parameters description.

Parameter	Meaning
p_1	Probability with which a node in state S becomes a node in state E
p_2	Probability with which a node in state E becomes a node in state I
p_3	Probability with which a node in state E becomes a node in state R
p_4	Probability with which a node in state I becomes a node in state D
p_5	Probability with which a node in state S becomes a node in state R
p_6	Probability with which a node in state D becomes a node in state R

Recovered state (R): nodes that used to be infected by worms or nodes no longer work as their energy is exhausted. Those nodes are cleaned of worms and immune to the same type of cleaned worms.

The transforming process of states for worm propagation is illustrated in Fig. 1.

Let the number of susceptible, exposed, infectious, diagnosed and recovered nodes at time t be denoted by $S(t)$, $E(t)$, $I(t)$, $D(t)$ and $R(t)$, respectively. Then, $S(t) + E(t) + I(t) + D(t) + R(t) = N$.

We assume that N wireless nodes are randomly deployed in the network where communication radius is r. The description of related parameters is showed in Table 1.

4. Modeling worm propagation

4.1. Overview of Bluetooth

Bluetooth [3,4] is a short-range radio technology that connects different wireless devices at low cost. It has a low power consumption specification that uses an ad-hoc network and uses data and voice communication in any place throughout the world. Bluetooth technology was created by Ericsson in 1994 to provide wireless connection between devices and mobile phones. The given name and logotype came from a Scandinavian king called Harold Bluetooth (Blatand'). Bluetooth technology has a wide range of applications, such as wireless headsets, dial-up networking, and peer-to-peer file sharing. The market for Bluetooth-enabled devices has grown rapidly in recent years, and 272 million Bluetooth-enabled devices were shipped in 2005, twice as many as in 2004. One industry research report [32] estimates that nearly 2.5 billion Bluetooth-enabled devices will be shipped in 2014.

4.2. Overview of cellular automata

Cellular automata [11] were first proposed by Von Neumann and Stan Ulam in the early 1950s to act as a simple model of biological self-reproduction. A CA is a discrete dynamic system, where space, time, and the states of the system are distinct, and it is a spatially and temporally discrete, deterministic mathematical model. A CA contains large numbers of simple identical components with local interactions, and has the ability to simulate the complex system and the spatial–temporal evolution process. It becomes an important tool to study the space–time evolution of self-organization system due to its capability to characterize the characteristics of complex system based on simple local rules.

In general, a CA can be defined by any dimension. One-, two-, and three-dimensional cellular automata are often used by researchers. For example, a one-dimensional CA can be visualized as having a cell at each integral point on the real number line, with a cell Ci having a left and a right neighbor (except edge conditions). A two-dimensional CA is represented as a regular spatial lattice or grid. At time t, each cell stays in one of a finite number of possible discrete states. By interacting with its neighbors, each cell updates its current state following a set of specific transition rules.

According to the above description, a CA can be formally defined as a four-tuple, $\{C, S, V, f\}$ where:

C denotes a cellular space, for a two-dimensional CA, $C = \{(i, j) \mid i, j \in Z,\ 1 \leqslant i \leqslant L,\ 1 \leqslant j \leqslant L\}$.

S denotes a finite state set whose elements are all the possible states of the cells.

V denotes the neighborhood of each cell, for a two-dimensional CA, $V = \{(x_k, y_k),\ 1 \leqslant k \leqslant N\} \subset Z \times Z$.

f denotes a set of local transition rules.

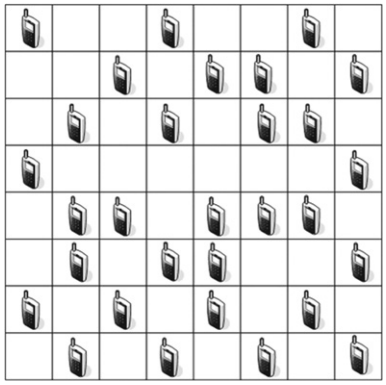


Fig. 2. A networks with N nodes in $L \times L$ areas.

4.3. Worm propagation modeling with cellular automata

(1) Cellular space.

In this paper, we consider that a network (see Fig. 2) is composed of N Bluetooth-enabled smartphones which are randomly deployed on a square 2-D grid composed of $L \times L$ units. Thus, the cellular space is formed by a 2-D array of $L \times L$ cells. Moreover, it is assumed that each cell is occupied by at most one wireless node in the cellular space.

Each wireless node can establish wireless links only with those nodes within a circle of radius r due to the limited transmission range. To simplify the analysis, we assume that the horizontal and vertical coordinates of a wireless node are represented by i and j in the 2-D grid (cellular space). Namely, cell C_{ij} denotes a node located in the position with a 2-D coordinate (i, j).

(2) Cellular state.

The traditional cellular automata paradigm forms the basis of our worm model and incorporates the spatial distribution of the population by use of the Moore neighborhood. The basic unit of cellular automata is a cell. Each cell can be in one of a finite number of distinct states at each discrete time. Moreover, each cell transforms from its current state to a new state (at the next time) based on its current state and the states of its neighbors, according to the transition rules. In our model, a cell represents an individual with a Bluetooth-enabled device. Thus, each cell can be characterized by the state and the likelihood of risks for exposure and infection by a worm.

Similar to the traditional epidemic model, in the susceptible state S, the cell is capable of infecting a worm from its infected neighbors; in the exposed state E, the cell has been infected by the worm but not yet infectious; in the infectious state I, the cell is capable of transmitting the infection to its neighbors; in the diagnosed state D, the cell has been diagnosed to be infected by some kind of specific worm; in the recovery state R, the cell is neither capable of passing on the infection nor capable of contracting the infection.

Let $S_{ij}^{u}(t)$ denote the state of a wireless node u which is located in cell C_{ij} at time t. To simplify the analysis, the epidemic state of u which is located in the cell C_{ij} is defined as follows:

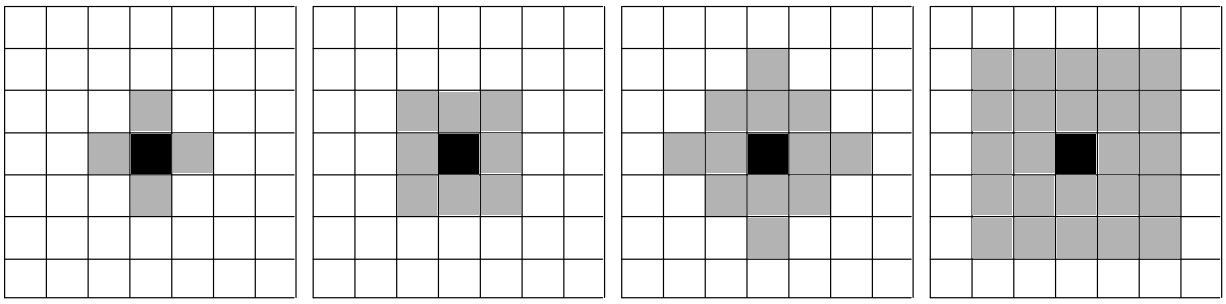
$$S_{ij}^{u}(t) = \begin{cases} 0, & C_{ij} \text{ is susceptible at time } t, \\ 1, & C_{ij} \text{ is exposed at time } t, \\ 2, & C_{ij} \text{ is infected at time } t, \\ 3, & C_{ij} \text{ is diagnosed at time } t, \\ 4, & C_{ij} \text{ is recovered at time } t. \end{cases} \tag{1}$$

(3) Cellular neighbor.

According to the corresponding transmission range r, we define the neighborhood of wireless nodes as shown in Fig. 3. Let the length of a grid be 1. If $r = 1$, each cell or node has no more than 4 cells or nodes as neighbors, that is, the neighborhood of Von Neumann (see Fig. 3 (a)). If $r = 1.414$, each cell or node has no more than 8 cells or nodes as neighbors, that is, the Moore neighborhood (see Fig. 3 (b)). If $r = 2$, each cell or node has no more than 12 cells or nodes as neighbors, that is, the extension for the neighborhood of Von Neumann (see Fig. 3 (c)). If $r = 2.828$, each cell or node has no more than 24 cells or nodes as neighbors, that is, the extension of Moore neighborhood (see Fig. 3 (d)). It is obvious that a cell or node has more neighbors as r increases.

(4) Transition rule.

Let $\Phi_{C_{ij},C_{kl}}$ denote the interaction coefficient between cell C_{ij} and its neighbors, which is defined as the strength or likelihood of an infection from one cell to another. Let δ denote an infection index, which is calculated as a ratio of the interaction coefficient between cell C_{ij} and its neighbors to its resisted factor. Let T denote the transmission threshold



(a) Von Neumann neighborhoods (b) Moore neighborhoods (c) Extension of Von Neumann neighborhoods (d) Extension of Moore neighborhoods

Fig. 3. Neighborhoods of Von Neumann and Moore.

through which a wireless node u transforms from state S to other states. Let N_u denote the number of each node's neighbor nodes. Thus, $\Phi_{C_{ij},C_{kl}}$ and δ are described as follows

$$\Phi_{C_{ij},C_{kl}} = \sum_{m=1}^{m=N_u} \frac{IF_{vu}}{\sqrt{(i-k)^2+(j-l)^2}}, \tag{2}$$

$$\delta = \frac{\Phi_{C_{ij},C_{kl}}}{RF}. \tag{3}$$

Where: IF_{vu} is the infected factor, which denotes the infection degree from node v to node u ($0 \leqslant IF \leqslant 1$). If IF equals to 0, it denotes the node has no infection to other nodes. If IF equals to 1, it denotes that the node has a stronger infection with other nodes. RF is the resisted factor, which denotes the resistance degree of a node on infection from other nodes ($0 < RF \leqslant 1$). If RF equals to 1, it denotes that the node has a strong ability to resist infection.

Step 1: Network initialization. All nodes are randomly distributed in a two-dimensional plane (e.g. an $L \times L$ area), and they communicate with each other through short-range radio transmissions.

Step 2: Node state initialization. Node i is randomly selected and its state is set to be state I, and the states of other nodes are set to be state S.

Step 3: Each node collects the information of its neighbors.

Step 4: Node u is accessed at time t, thus:

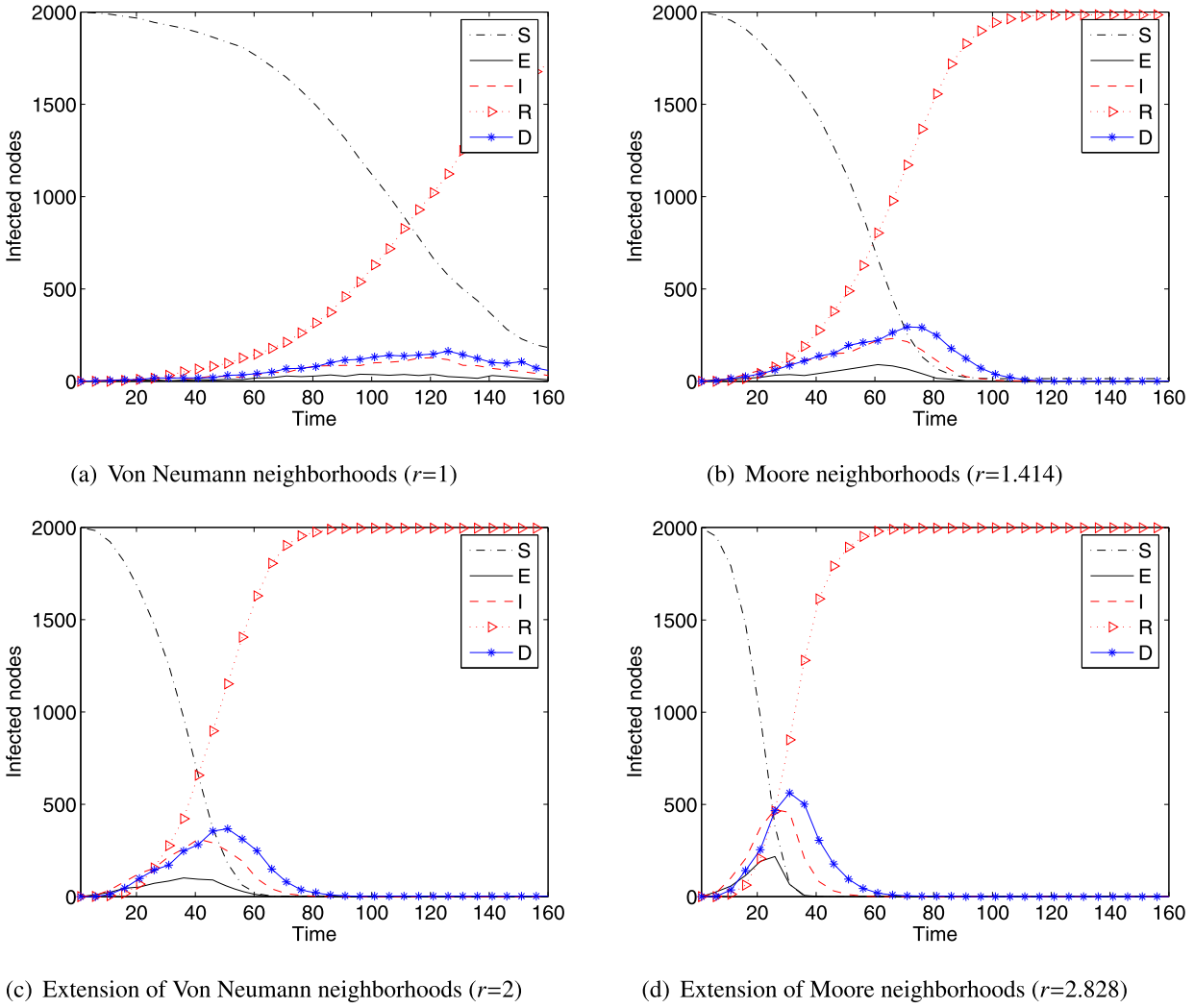
- Case 1: As to node u, if its state is I (e.g. $S_u(t) = 2$), its neighbor nodes are accessed. If the state of its neighbor node v is S (e.g. $S_u(t) = 0$), and if δ is not smaller than T, node v changes its state from S to E with probability p_1. Otherwise, node v remains in the previous state. If IF_{vu} equals to 0 or RF equals to 1, node v changes its state from S to R with probability p_5. At the same time, node u changes its state from I to D with probability p_4.
- Case 2: As to node u, if its state is E (e.g. $S_u(t) = 1$), node u changes its state from E to R with probability p_3, or node u changes its state from E to I with probability p_2.
- Case 3: As to node u, if its state is D (e.g. $S_u(t) = 3$), node u changes its state from D to R with probability p_6.
- Case 4: As to the above process, any node has a probability α to establish a connection with its neighbor nodes.
- Case 5: Repeat the beginning of Step 4 until all nodes in the network are accessed.

Step 5: t equals to t plus 1. This completes the algorithm.

5. Performance evaluation

To evaluate the feasibility of the proposed scheme using cellular automata to simulate the dynamics of Bluetooth worm propagation in smartphones, and to verify the effectiveness and rationality of the proposed model on worm propagation in Bluetooth networks, a C++ simulator has been implemented. In the simulator, the wireless nodes are deployed into a 50×50 regular grid, and the length of each grid is 1; the total number of nodes N is 2000; the transmission radius r is 1.414. The other parameters are set as follows, otherwise indicated in the figures: $p_1 = 0.5$, $p_2 = 0.6$, $p_3 = 0$, $p_4 = 0.2$, $p_5 = 0$, $p_6 = 0.15$ (all parameters are given in dimensionless units).

Fig. 4 shows the evolutions on the number of susceptible, exposed, infected, diagnosed and recovered nodes. We find that the number of infected nodes increases from $t = 1$ to $t = 123$ with Von Neumann neighborhoods ($r = 1$), from $t = 1$ to $t = 63$ with Moore neighborhoods ($r = 1.414$), from $t = 1$ to $t = 41$ with extension of Von Neumann neighborhoods



(a) Von Neumann neighborhoods (r=1)

(b) Moore neighborhoods (r=1.414)

(c) Extension of Von Neumann neighborhoods (r=2)

(d) Extension of Moore neighborhoods (r=2.828)

Fig. 4. The number of susceptible, exposed, infected, diagnosed and recovered nodes for Von Neumann neighborhoods, Moore neighborhoods, the extension of Von Neumann neighborhoods, and the extension of Moore neighborhoods.

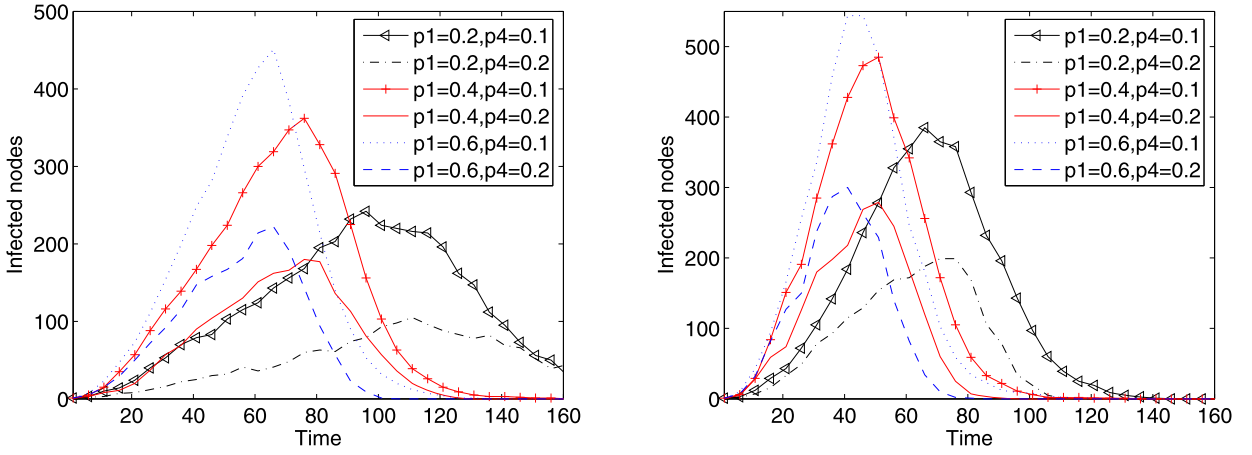
($r = 2$), and from $t = 1$ to $t = 25$ with the extension of Moore neighborhoods ($r = 2.828$). It is evident that the number of susceptible nodes decreases as the number of recovered nodes increases. Furthermore, it can be found that the outbreak point is achieved earlier when r increases.

Fig. 5 shows the transient response on the number of infected nodes $I(t)$. As time passes, $I(t)$ first increases gradually, reaches the maximum point, and then decreases gradually. It is seen that as the probability p_1 increases, the number of infection nodes $I(t)$ increases, and the outbreak point is achieved ahead of time. However, as the infection probability p_4 increases, the results change in an inverse way.

Fig. 6 shows the transient response on the number of susceptible nodes $S(t)$. $S(t)$ decreases gradually to zero as time passes. We find that as the probability p_1 increases, $S(t)$ decreases quicker, and more susceptible nodes will be infected. We also find that as probability p_4 changes, $S(t)$ does not change.

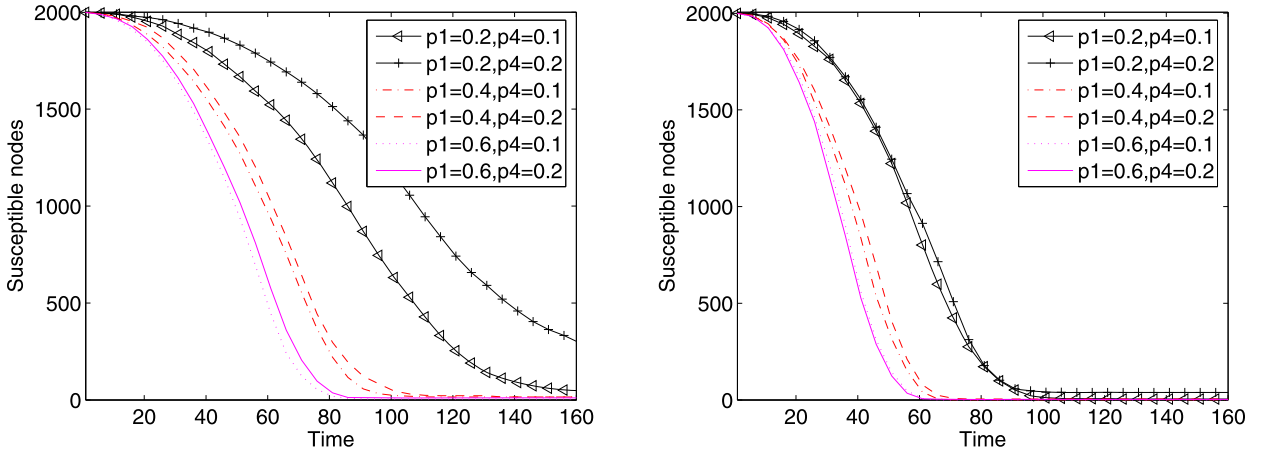
Fig. 7 shows the effects of the transmission range r on the worm propagation. The maximum value of $I(t)$ increases as the node's transmission range increases. That is to say, a greater transmission range r means that every node becomes infected easier. It can be found that the outbreak point is achieved earlier when r is increased. The reason is that a greater transmission radius results in more neighbors for a single node, and thus increased the probability of potential infections as the number of transmission links associated with infected nodes increases.

Fig. 8 shows the effects of the network's density d on the worm propagation. Worms propagation can be enlarged by the network's density. That is to say, if there are more nodes in a certain filed (i.e. d is larger), the propagation scope becomes larger (i.e. the number of infected nodes are more). As observed in Fig. 8, higher network's density leads with higher probability to the worm pandemic state.



(a) Moore neighborhoods (r=1.414) (b) Extension of Von Neumann neighborhoods (r = 2)

Fig. 5. The number of infected nodes with different rates of infection rates for Moore neighborhoods and the extension of Von Neumann neighborhoods.



(a) Moore neighborhoods (r=1.414) (b) Extension of Von Neumann neighborhoods (r = 2)

Fig. 6. The number of susceptible nodes with different rates of infection for Moore neighborhoods and the extension of Von Neumann neighborhoods.

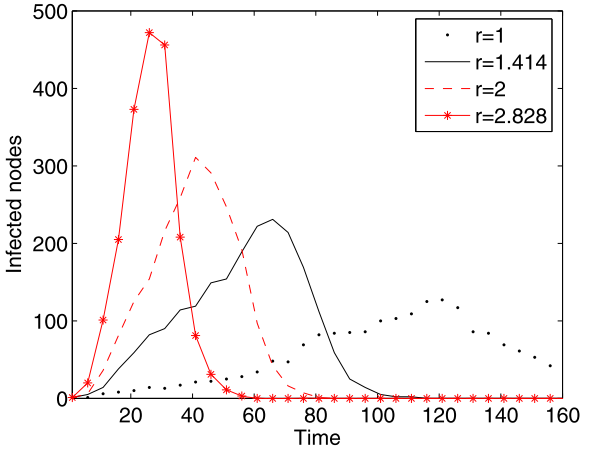
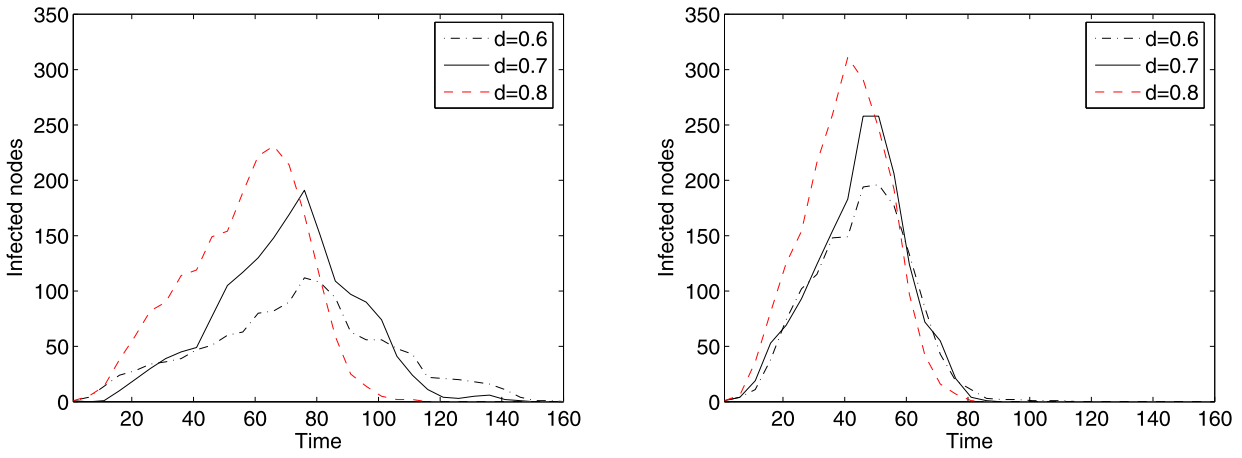


Fig. 7. The number of infected nodes with different transmission range r for Von Neumann neighborhoods, Moore neighborhoods, the extension of Von Neumann neighborhoods, and the extension of Moore neighborhoods.



(a) Moore neighborhoods (r=1.414) (b) Extension of Von Neumann neighborhoods (r = 2)

Fig. 8. Evolution of the infected nodes with different densities for Moore neighborhoods and the extension of Von Neumann neighborhoods.

6. Summary and future work

In this work, we present a theoretical model to characterize the dynamics of worm propagation in smartphones using a two-dimensional cellular automata. We consider two important factors in the proposed model. One is the infection factor, which is used to evaluate the degree of the spread of infected nodes. Another is the resistance factor, which is used to offer a resistance evaluation towards susceptible nodes. The simulation results are obtained through many artificially chosen parameters, which further illustrates the efficiency of the proposed model, and also demonstrates that the proposed model can be used to serve as a basis for the development of new algorithms to simulate propagation dynamics.

However, the proposed model does not characterize the dynamics of hybrid viruses' propagation and the impact of node mobility on worm propagation. As for our future work, we will focus on testing the performance of the proposed model on real data sets. To obtain effective simulation results, the scale and appropriate size of the cells should be considered for a more practical simulation process. Meanwhile, we will further analyze the propagating characteristics of hybrid viruses. In addition, the impact of node mobility on worm propagation should be considered.

Acknowledgments

This work is supported in part by the National Natural Science Foundation of China under Grant Nos. 61073037, 61272151 and 61103035, the Postdoctoral Science Foundation of China under Grant No. 2012M511757, the Ministry of Education Fund for Doctoral Disciplines in Higher Education under Grant No. 20110162110043, the Natural Science Foundation of Guangdong Province under Grant No. S2011040002356, and the Science Project of Zhaoqing University under Grant No. 201101.

References

[1] http://www.canalys.com/newsroom/android-takes-almost-50-share-worldwide-smart-phone-market, 2011, [EB/OL].
[2] http://www.f-secure.com/en/web/labs_global/2004-threat-summary, 2004, [EB/OL].
[3] http://www.developer.nokia.com/Community/Wiki/Bluetooth-Overview, 2005, [EB/OL].
[4] M. Tan, K.A. Masagca, An investigation of Bluetooth security threats, in: Proceedings of the International Conference on Information Science and Applications (ICISA 2011), Jeju Island, Jeju-do, Korea, 2011, pp. 1–7.
[5] S. Peng, G. Wang, Worm propagation modeling using 2D cellular automata in Bluetooth networks, in: Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2011), Changsha, China, 2011, pp. 282–287.
[6] J. Kephart, S. White, Directed-graph epidemiological models of computer viruses, in: Proceedings of the IEEE Computer Symposium on Research in Security and Privacy, 1991, pp. 343–359.
[7] C.C. Zou, W. Gong, D. Towsley, Code red worm propagation modeling and analysis, in: Proceedings of the ACM Conference on Computer and Communication Security (CCS 2002), ACM Press, Washington, DC, USA, 2002, pp. 138–147.
[8] S. Staniford, V. Paxson, N. Weaver, How to own the Internet in your spare time, in: Proceedings of the 11th USENIX Security Symposium, ACM Press, San Francisco, USA, 2002, pp. 149–167.
[9] S. Tang, B.L. Mark, Analysis of virus spread in wireless sensor networks: an epidemic model, in: Proceedings of the 7th International Workshop on Design of Reliable Communication Networks (DRCN 2009), Washington, DC, USA, 2009, pp. 86–91.
[10] V. Karyotis, A. Kakalis, S. Papavassiliou, Malware-propagative mobile ad hoc networks: asymptotic behavior analysis, J. Comput. Sci. Tech. 23 (3) (2008) 389–399.
[11] N. Ganguly, B.K. Sikdar, A. Deutsch, G. Canright, P.P. Chaudhuri, A survey on cellular automata, Tech. Rep., Centre for High Performance Computing, Dresden University of Technology, December 2003.

[12] S.H. White, A.M. del Rey, G.R. Sánchez, Modeling epidemics using cellular automata, Appl. Math. Comput. 186 (1) (2007) 193–202.
[13] B. Li, H. Xu, J. Guo, Modeling the SARS epidemic considering self-cure, Chinese J. Engrg. Math. 20 (7) (2003) 20–28.
[14] B. Gao, T. Zhang, H. Xuan, J. Yang, A heterogeneous cellular automata model for SARS transmission, Systems Engrg. Theory Methodol. Appl. 15 (3) (2006) 205–209.
[15] A.R. Mikler, S. Venkatachalam, K. Abbas, Modeling infectious diseases using global stochastic cellular automata, J. Biol. Systems 13 (4) (2005) 421–439.
[16] Y. Song, G. Jiang, Research of malware propagation in complex networks based on 1-D cellular automata, Acta Phys. Sinica 58 (9) (2009) 5901–5908.
[17] G. Yan, S. Eidenbenz, Modeling propagation dynamics of Bluetooth worms (extended version), IEEE Trans. Mobile Comput. 8 (3) (2009) 353–367.
[18] C.J. Rhodes, M. Nekovee, The opportunistic transmission of wireless worms between mobile devices, Phys. A 387 (27) (2008) 6837–6844.
[19] J.C. Martin, L.L.I. Burge, J.I. Gill, A.N. Washington, M. Alfred, Modelling the spread of mobile malware, Internat. J. Comput. Aided Eng. Technol. 2 (2) (2010) 3–14.
[20] J. Su, K. Chan, A. Miklas, K. Po, A. Akhavan, S. Saroiu, E. Lara, A. Goel, A preliminary investigation of worm infections in a Bluetooth environment, in: Proceedings of the 4th ACM Workshop on Recurring Malcode (WORM 2006), New York, USA, 2006, pp. 9–16.
[21] H. Zheng, D. Li, Z. Gao, An epidemic model of mobile phone virus, in: Proceedings of the 1st IEEE International Symposium on Pervasive Computing and Applications (SPCA 2006), Urumqi, China, 2006, pp. 1–5.
[22] J.W. Mickens, B.D. Noble, Modeling epidemic spreading in mobile environments, in: Proceedings of the 4th ACM Workshop on Wireless Security (WiSe 2005), Cologne, Germany, 2005, pp. 77–86.
[23] E.V. Ruitenbeek, T. Courtney, W.H. Sanders, 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 2007), Edinburgh, UK, 2007, pp. 791–800.
[24] C. Fleizach, M. Liljenstam, P. Johansson, G.M. Voelkery, A. Méhes, Can you infect me now? Malware propagation in mobile phone networks, in: Proceedings of the 5th ACM Workshop on Recurring Malcode (WORM 2007), Alexandria, VA, USA, 2007, pp. 61–68.
[25] C. Gao, J. Liu, Modeling and predicting the dynamics of mobile virus spread affected by human behavior, in: Proceedings of the 12th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM 2011), Lucca, Italy, 2011, pp. 1–9.
[26] S. Cheng, W.C. Ao, P. Chen, K. Chen, On modeling malware propagation in generalized social networks, IEEE Commun. Lett. 15 (1) (2011) 25–27.
[27] K. Ramachandran, B. Sikdar, Modeling malware propagation in networks of smart cell phones with spatial dynamics, in: Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM 2007), Anchorage, Alaska, USA, 2007, pp. 2516–2520.
[28] W. Xia, Z. Li, Z. Chen, Z. Yuan, Commwarrior worm propagation model for smart phone metworks, J. China Univ. Posts Telecomm. 15 (2) (2008) 60–66.
[29] P. Wang, M.C. Gonzalez, C.A. Hidalgo, A.-L. Barabasi, Understanding the spreading patterns of mobile phone viruses, Science 324 (5930) (2009) 1071–1076.
[30] A. Bose, K.G. Shin, On mobile viruses exploiting messaging and Bluetooth services, in: Proceedings of the 2nd International Conference on Security and Privacy in Communication Networks, Baltimore, MD, 2006, pp. 1–10.
[31] Y. Fan, K. Zheng, Y. Yang, Epidemic model of mobile phone virus for hybrid spread mode with preventive immunity and mutation, in: Proceedings of the 6th IEEE International Conference on Wireless Communications Networking and Mobile Computing (WiCOM 2010), Chengdu, China, 2010, pp. 1–5.
[32] http://www.nordicsemi.com/content/download/2076/24025, 2009, [EB/OL].