Worm Propagation Modeling Using 2D Cellular Automata in Bluetooth Networks

Sancheng Peng[1,2], Guojun Wang[1,*]
1. School of Information Science and Engineering, Central South University, Changsha, China, 410083
2. School of Computer Science, Zhaoqing University, Zhaoqing, China, 526061
*Correspondence to: csgjwang@mail.csu.edu.cn

***Abstract*—Bluetooth networks are envisioned to provide many promising services and applications. Meanwhile, Bluetooth networks are also increasingly becoming the target of worms. Many emerging worms can utilize the proximity of devices to propagate in a distributed manner, resulting in modeling on worm propagation substantially more challenging. In this paper, we propose an efficient Worm Propagation Modeling scheme, WPM for short. WPM utilizes the two-dimensional (2D) cellular automata to simulate the dynamics of the worm propagation process from a single node to the entire Bluetooth network. The WPM scheme integrates infection factor, which evaluates the spread degree of infected nodes, and resistance factor, which offers resistance evaluation towards susceptible nodes. Moreover, the epidemic state of each node is classified into five types in the WPM scheme, including susceptible, exposed, infected, diagnosed, and recovered. The effectiveness and rationality of the proposed model are validated through extensive simulations.**

Keywords- worm propagation, Bluetooth, cellular automata

I. INTRODUCTION

In recent years, with the emerging of portable wireless devices such as cellular phones, laptops and PDAs, mobile networks are becoming an important part of our everyday networking facilities. However, the growth of mobile networking is leading to new security challenges due to attraction for attention of virus and worm writers who exploit such features for launching new computer-virus outbreaks.

Bluetooth [1-3] is a short-range radio technology that connects different wireless devices at low cost, low power consumption specification for an ad-hoc network for data and voice communication in any place of the world. Bluetooth technology was created by Ericsson in 1994 to provide wireless connection between devices and mobile phones. The given name and logotype come 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 been growing rapidly in recent years, and 272 million Bluetooth-enabled devices have been shipped in 2005, twice as many as in 2004. One industry research report estimates that nearly 2.4 billion Bluetooth-enabled devices will be shipped in 2014.

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, and are not new to us. The last few years has witnessed the emergence of a new type of worms which specifically target Bluetooth-enabled portable wireless devices, such as smart phones and laptops. The novel feature of Bluetooth worms is that they do not necessarily require Internet connectivity for their propagation. Unlike Internet worms which often scan the entire IP address space for susceptible victims, a Bluetooth-enabled device, due to the limited transmission range, leads to a proximity-based infection mechanism. That is, the Bluetooth-enabled device, close to an infected device within its radio range, may also get infected. The first mobile phone virus named Cabir [4] hit Symbian-based Bluetooth phones. The virus used Bluetooth connectivity channels on devices running the Symbian Operating System to mitigate onto other devices.

Mathematical epidemiology has been developing for over a hundred years. Since Internet worms are similar to biological viruses in their self-replicating and propagation behaviors, epidemiological models for analyzing the propagation of Internet worms are nothing new to us, and there has been tremendous interest in modeling on the propagation of Internet worms over the past decades [5-7].

The security issue regarding to worm propagation that exploits geographic proximity of wireless-enabled devices has raised attentions in recent years. Many efforts have been made to model the propagation behavior of worm in wireless networks, such as wireless sensor networks [8], wireless ad-hoc networks [9], and Bluetooth networks [10-11]. Most epidemic models have focused almost entirely on the technology of differential equations [8-9, 12] and Markov chain [14-15].

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 local characteristics of the spreading process, nor to include interaction behavior among individuals, and the models based on Markov chain are difficult to describe the spatial-temporal process of worm propagation.

Cellular automata (CA for short) can overcome these drawbacks and have been used by several researches as an efficient alternative method to characterize epidemic spreading [16-20]. Generally speaking, cellular automata are simple models of computation capable of characterizing physical,

978-0-7695-4600-1/11 $26.00 © 2011 IEEE
DOI 10.1109/TrustCom.2011.38

IEEE computer society

biological or environmental complex phenomena, such as growth processes, reaction-diffusion systems, epidemic models, and forest fire spreading.

Despite that 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 of using the cellular automata concept as a tool to characterize the propagation dynamics of Bluetooth worms. We believe that CAs can be useful to simulate this kind of network because the behavior and/or the state of a wireless node are/is capable of modifying all network behavior. 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 an efficient Worm Propagation Modeling scheme (WPM for short). It characterizes the propagation dynamics of Bluetooth worms by introducing the following realistic modeling assumptions: 1) the infected factor of infectious device for the susceptible is different, and 2) the resisted factor of each device for the worm spread is different. These assumptions are usually not addressed in previous analytical work for reasons of simplicity. Our contributions are summarized as follows:

- We formulate the problem of Bluetooth worm propagation by introducing infected factor and/or resisted factor of individuals.
- Based on epidemic theory, we introduce infection index to measure the state transition of susceptible individuals, which characterizes the propagation dynamics of Bluetooth worms exploiting cellular automata.
- Through extensive numerical simulations and analysis, the analytical results show the effectiveness and rationality of the proposed approach.

The remainder of this paper is structured as follows: Section 2 gives an overview of related work. Section 3 discusses the system model. Section 4 presents a model to characterize the epidemic spreading. Section 5 gives results of model validation. Finally, Section 6 concludes this paper.

II. Related Work

The study of computer worms in general and Internet worms in particular is quite familiar. Kephart and White [5] conducted a study of viral infections in computers using epidemiological models. Zou et al. [6] proposed a two-factor worm model to characterize the epidemic spreading of Internet worms. Staniford et al. [7] used the classical logistic function to fit the propagation curve of the Code Red I worm. Although these models can model the propagation process of Internet worms, they are not directly adapted to the wireless networks for modeling worm spreading process.

Investigation of worms spreading in wireless networks, such as Bluetooth networks, wireless sensor networks, and mobile ad-hoc networks, has attracted many researchers. Tang and Mark [8] proposed a Susceptible-Infective-Recovered with Maintenance (SIR-M for short) model by using epidemic theory to characterize the dynamics of the virus spreading process from a single node to the entire network. Nekovee [9] developed a model for the spreading of worms in Wi-Fi-based wireless ad hoc networks and investigated the properties of worm epidemics in these networks via extensive Monte Carlo simulations. Yan and Eidenbenz [10] 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 [11] investigated the effect of population characteristics and device behavior on the outbreak dynamics of Bluetooth worms.

Khouzani et al. [12] modeled the malware propagation as a deterministic epidemic and introduced a defense strategy to quarantine the malware by reducing the communication range. Li et al. [13] proposed a proximity malware coping scheme based on the social relationships and community structure of the smartphone-based mobile networks. The proposed scheme integrates short-term coping components, which deal with individual malware, and long-term evaluation components, which offer vulnerability evaluation towards individual nodes. Karyotis et al. [14] proposed a malware-propagative model in mobile ad hoc networks, using the Norton equivalent of the closed queuing network. Gu and Wang [15] developed a model called the discrete probability susceptible infectious (short for DP-SI for short) using homogeneous Markov chain. Song and Jiang [16] proposed a malware propagation model for complex networks based on 1-D cellular automata.

Furthermore, on the basis of cellular automata, many epidemic spreading models are presented in [17-20]. White et al. [17] presented a theoretical model to simulate the epidemic spreading using a two-dimensional cellular automata endowed with a suitable local transition function. The population is divided into three classes: susceptible, infected and recovered individuals in the proposed model. Li et al. and Gao et al. presented a analytical model for SARS (short for severe acute respiratory syndrome) spreading based on the cellular automata in [18-19], respectively. Mikler at al. [20] proposed a global stochastic cellular automata paradigm (GSCA for short) to model and simulate epidemics of an infectious disease. GSCA incorporates geographic and demographic based on interactions.

III. System Model

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 they are prone to infection.
- Exposed state (*E*): nodes have been infected by the worm, but they are not to spread the worm to the susceptible while transmitting data or controlling messages to them 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.
- Recovered state (*R*): nodes used to be infected by worms or nodes will never work as their energy is exhausted; they are cleaned of worms and/or are immune to the same type of cleaned worms.

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

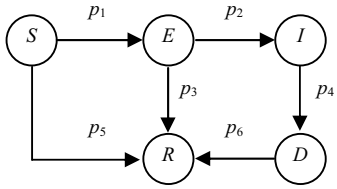


Fig. 1. State transition relationship for worm propagation

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

TABLE 1 Parameters description

Symbol	Explanation
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 *S*
P_6	Probability with which a node in state *D* becomes a node in state *R*

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, $S(t) + E(t) + I(t) + D(t) + R(t) = N$.

IV. MODELING WORM PROPAGATION

A. Overview of cellular automata

Cellular automata were first proposed by Von Neumann in 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. CAs contain large numbers of simple identical components with local interactions. CAs have 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 many researchers. For example, an one-dimensional CA can be visualized as having a cell at each integral point on the real number line, and cell C_i has 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, $C = \{(i, j) \mid i, j \in Z, 0 \le i \le L, 0 \le j \le L\}$

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

V denotes the neighborhood of each cell.

f denotes a set of local transition rules.

B. Worm propagation modeling with cellular automata

(1) Cellular space

In this paper, we consider that a Bluetooth network is composed of *N* Bluetooth-enabled devices, which are randomly deployed on 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. We assume that each cell is occupied by at most one wireless node, which is deployed in the center of the cell.

Each wireless node can establish wireless links with those nodes only within a circle of radius *r* due to the limited transmission range. To simplify 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 Bluetooth-enabled device. Thus, each cell can be characterized by state and likelihood risks for exposure and infecting the worm.

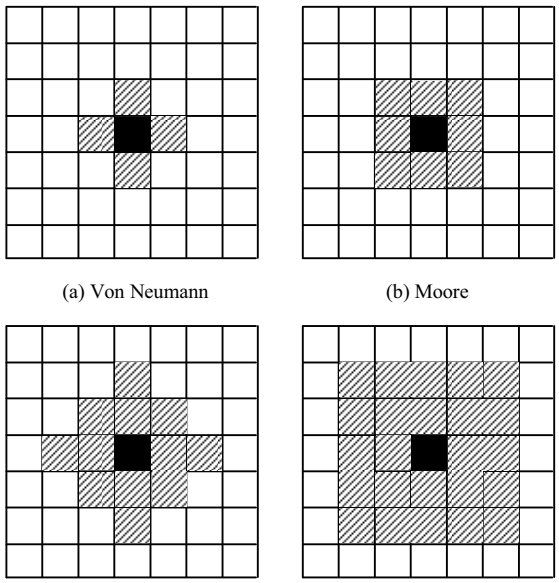
Similar to the traditional epidemic model, in the susceptible state *S*, the cell is capable of infecting worm from its infected neighbors; in the exposed state *E*, the cell has been infected by the worm but not yet infectious; in the infectious state *I*, the cell is capable of transmitting the infection 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 locates in the cell C_{ij} at time t. To simplify the analysis, the epidemic state of u which locates in the cell C_{ij} is defined as follows:

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

(3) Cellular neighbor

According to the corresponding transmission range r, we define the neighborhood of wireless nodes as shown in Fig. 2. 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. 2 (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. 2 (b)). If r=2, each cell or node has no more than 12 cells or nodes as neighbors, that is, the extension for neighborhood of Von Neumann (see Fig. 2 (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. 2 (d)). It is obvious that a cell or node has more neighbors as r increases.



(a) Von Neumann (b) Moore

(c) Extension of Von Neumann (d) Extension of Moore

Fig. 2. Neighborhood of Von Neumann and Moore

(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 infection from one cell to another cell. Let δ denote 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 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.

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

$$\delta=\frac{\Phi_{C_{ij},C_{kl}}}{RF} \quad (3)$$

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

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 using 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 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 neighbor nodes.

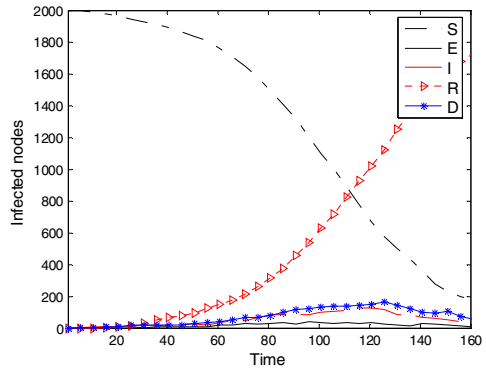
Case 5: Repeat the beginning of Step 4 until all the nodes in the network are accessed.

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

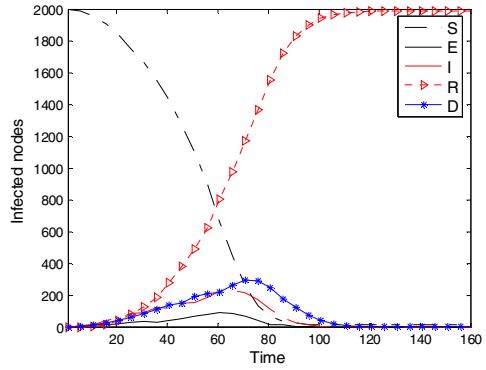
V. SIMULATIONS

To evaluate the feasibility of using cellular automata to simulate Bluetooth networks, and to verify the effectiveness and rationality of the proposed model on worm propagation in Bluetooth networks, a C++ simulator has been implemented. In

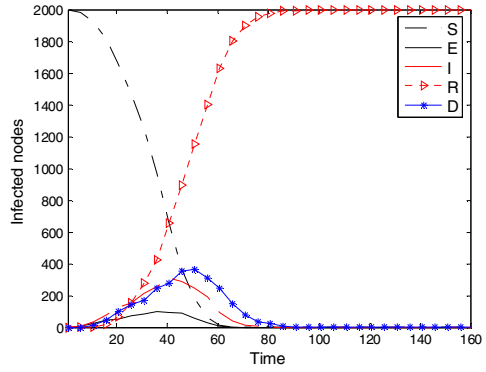
the simulator, the wireless nodes are deployed into a 50×50 regular grid, and the length of each grid is 1; the total number of nodes N is 2000; the transmission radius r is 1.414. The other parameters are set as follows, otherwise indicated in the figures: p_1=0.5, p_2=0.6, p_3=0, p_4=0.2, p_5=0, p_6=0.15, $\alpha = 0.9$ (all parameters are given in dimensionless units).



(a) Von Neumann neighborhoods (r=1)



(b) Moore Neighborhoods (r=1.414)



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

Fig. 3. The evolution on the number of susceptible, exposed, infected, diagnosed and recovered nodes for Von Neumann neighborhoods, Moore Neighborhoods, and extension of Von Neumann neighborhoods

Fig. 3 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), and from t = 1 to t = 41 with extension of Von Neumann neighborhoods (r=2). Furthermore, the number of susceptible nodes decreases as the number of recovered nodes increases.

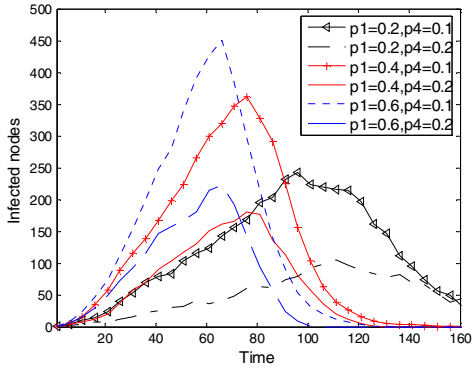


Fig. 4. The number of infected nodes with different infected rates

Fig. 4 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. We also find that as the probability p_4 increases, the outbreak of the infection becomes smaller, and the outbreak point is achieved ahead of time. However, as the infection probability p_1 increases, the results change in an inverse way.

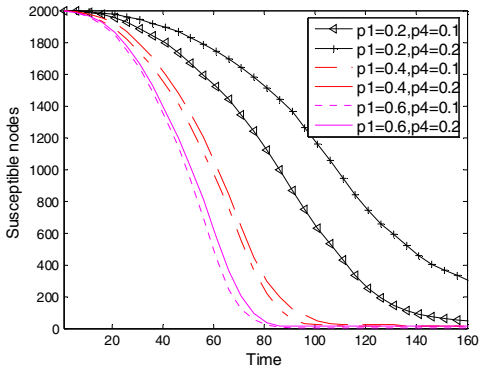


Fig. 5. The number of susceptible nodes with different infected rates

Fig. 5 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 more quickly, since more susceptible nodes will be infected. We also find that as probability p_4 changes, the change of $S(t)$ is not obvious, especially, as the probability p_1 equals to 0.4 and 0.6.

Fig. 6 shows the transient response on the number of infective nodes $I(t)$ over different values of the transmission range r. The maximum value of $I(t)$ increases as the node's

transmission range increases. It can be found that the outbreak point is achieved earlier when r is increased.

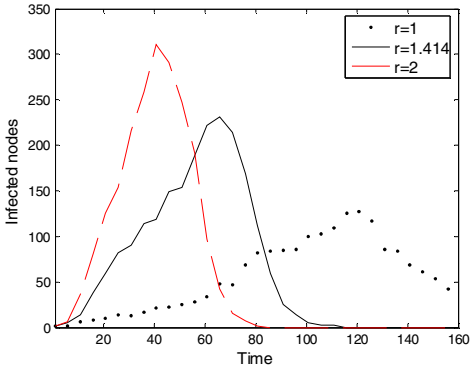


Fig. 6. The number of infected nodes with different transmission range r

VI. CONCLUSIONS

In this work, a detailed analytical model to characterize the dynamics propagation of Bluetooth worm is presented. It is based on the use of a two-dimensional cellular automata with a set of suitable local transition rules. The main features of the proposed model are as follows:

- The total amount of nodes in the cellular space is constant, and they are uniformly distributed in the centre of the cells. The local transition rule is very simple, and many epidemiological and environmental parameters are considered in the proposed model.
- Two important factors are considered in the proposed model. One is the infection factor, which is used to evaluate the spread degree of infected nodes. The other is the resistance factor, which is used to offer resistance evaluation towards susceptible nodes.
- The definition of each cell's state is described as a five-tuple formed by a suitable portion of its population which is susceptible, exposed, infected, diagnosed, and recovered, at each time step, together with the definition of the local transition rule involving these parameters.

The simulation results are obtained through many artificially chosen parameters, which seem to be in agreement with a real worm propagation process. The proposed model can be used to serve as a basis for the development of other algorithms to simulate propagation dynamics.

As our further work, we will focus on testing the performance of the proposed model against real data. To obtain efficient simulation results, the scale and an appropriate size of the cells should be considered for real simulation process. Moreover, the effect of vaccination process on the evolution of infected individuals should also be considered.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China under Grant No. 61073037, the Natural Science Foundation of Guangdong Province under Grant No. S2011040002356, the Science Project of Zhaoqing University under Grant No. 201101, and the Postdoctoral Program of Central South University.

REFERENCES

[1] Bluetooth Overview [EB/OL]. http://www.developer.nokia.com /Community/Wiki/Bluetooth_Overview.

[2] A. Bose and K. G. Shin, "On Mobile Viruses Exploiting Messaging and Bluetooth Services," Proc. of the Second International Conference on Security and Privacy in Communication Networks, Baltimore, MD, pp. 1-10. August 2006.

[3] M. Tan, K. A. Masagca, "An Investigation of Bluetooth Security Threats," Proc. of the International Conference on Information Science and Applications, Jeju Island, South Korea, pp. 1-7, April 2011.

[4] 2004 Security Threat Summary [EB/OL]. http://www.f-secure.com /en_EMEA-Labs/news-info/threat-summaries/2004/index.html#mobile.

[5] J. Kephart and S. White, "Directed-Graph Epidemiological Models of Computer Viruses," Proc. of the IEEE Computer Symposium on Research in Security and Privacy, pp. 343-359, May 1991.

[6] C. C. Zou, W. Gong, and D. Towsley, "Code Red Worm Propagation Modeling and Analysis," Proc. of the ACM Conference on Computer and Communication Security (CCS 2002), Washington DC, USA: ACM press, 2002, pp. 138-147.

[7] S. Staniford, V. Paxson, and N. Weaver, "How to Own the Internet in Your Spare Time," Proc. of the 11th USENIX Security Symposium. San Francisco, USA: ACM Press, pp. 149-167, August 2002.

[8] S. Tang and B. L. Mark, "Analysis of Virus Spread in Wireless Sensor Networks: An Epidemic Model," Proc. of the 7th International Workshop on Design of Reliable Communication Networks (DRCN 2009), Washington, D. C., USA, pp. 86-91, October 2009.

[9] M. Nekovee, "Worm Epidemics in Wireless Ad Hoc Networks," New Journal of Physics, Vol. 9, No. 189, pp. 1-13, June 2007.

[10] G. Yan and S. Eidenbenz, "Modeling Propagation Dynamics of Bluetooth Worms (Extended Version)," IEEE Transactions on Mobile Computing, Vol. 8, No. 3, pp. 353-367, March 2009.

[11] C. J. Rhodes and M. Nekovee, "The Opportunistic Transmission of Wireless Worms between Mobile Devices," Physica A: Statistical Mechanics and its Applications, Vol. 387, pp. 6837-6844, Dec. 2008.

[12] M. Khouzani, E. Altman, S. Sarkar, "Optimal Quarantining of Wireless Malware Through Reception Gain Control," IEEE Transactions on Automatic Control, Volume: PP, Issue: 99, pp. 1-13, April 2011.

[13] F. Li, Y. Yang, and J. Wu, "CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-based Mobile Networks," Proc. of the 29th IEEE Conference on Computer Communications (INFOCOM 2010), San Diego, CA, USA, pp. 1-9, March 2010.

[14] V. Karyotis, A. Kakalis, S. Papavassiliou, "Malware-Propagative Mobile Ad Hoc Networks: Asymptotic Behavior Analysis," Journal of Computer Science and Technology, 23(3): 389-399, May 2008.

[15] Y. Gu and S. Wang, "A Discrete Probabilistic Model of Malware Propagation," Acta Electronica Sinica, 38(4): 894-898, April 2010.

[16] S. H. White, A. Martín del Rey, and G. Rodríguez Sánchez, "Modeling Epidemics Using Cellular Automata," Applied Mathematics and Computation, Vol. 186, Issue 1, pp. 193-202, March 2007.

[17] B. Li, H. Xu, and J. Guo, "Modeling the SARS Epidemic Considering Self-cure," Chinese Journal of Engineering Mathematics, 20(7): 20-28, December 2003.

[18] B. Gao, T. Zhang, H. Xuan, and J. Yang, "A Heterogeneous Cellular Automata Model for SARS Transmission," Systems Engineering-Theory Methodology Application, 15(3): 205-209, June 2006.

[19] A. R. Mikler, S. Venkatachalam, and K. Abbas, "Modeling Infectious Diseases Using Global Stochastic Cellular Automata," Journal of Biological Systems, Vol. 13, No. 4, pp. 421-439, 2005.

[20] Y. Song and G. Jiang, "Research of Malware Propagation in Complex Networks Based on 1-D Cellular Automata," Acta Physica Sinica, 58 (9): 5901-5908, September 2009.