2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications

Modeling Malware Propagation in Smartphone Social Networks

Sancheng Peng[†‡], Guojun Wang[†*], Shui Yu[§]
[†]School of Information Science and Engineering, Central South University, Changsha, 410083, P. R. China
[‡]School of Computer Science, Zhaoqing University, Zhaoqing, 526061, P. R. China
[§]School of Information Technology, Deakin University, 221 Burwood HWY, Burwood, VIC 3125, Australia
[*]Corresponding author: csgjwang@csu.edu.cn

***Abstract*—Smartphones have become an integral part of our everyday lives, such as online information accessing, SMS/MMS, social networking, online banking, and other applications. The pervasive usage of smartphones also results them in enticing targets of hackers and malware writers. This is a desperate threat to legitimate users and poses considerable challenges to network security community. In this paper, we model smartphone malware propagation through combining mathematical epidemics and social relationship graph of smartphones. Moreover, we design a strategy to simulate the dynamic of SMS/MMS-based worm propagation process from one node to an entire network. The strategy integrates infection factor that evaluates the propagation degree of infected nodes, and resistance factor that offers resistance evaluation towards susceptible nodes. Extensive simulations have demonstrated that the proposed malware propagation model is effective and efficient.**

Keywords*—smartphones; mobile malware; propagation model; SMS/MMS; social relationship graph

I. Introduction

Smartphones combine the functions of PDA (personal digital assistant) with the communication capabilities of cellphones, which enables users to access a large variety of ubiquitous services, such as surfing the web, simple messaging service/multimedia messaging service (SMS/MMS), sending or receiving emails, and online shopping [1], [2]. Moreover, an application-based interface is used in most smartphones, which enables mobile users to download individual programs that can perform a variety of tasks. However, the availability of these ubiquitous and mobile services provided by smartphones increases chances to malware [3].

According to the recent security reports [4]–[6], the executed attacks have gone through a surge in the past few years. In 2010, more than 1 million cell phone users in China have been infected by the 'Zombie' virus which can automatically send text messages, and the attack costs users about 300,000 US dollars per day. Juniper Networks Mobile Threat Center (MTC) released its 2011 Mobile Threats Report, which showed that the number of mobile malwares increases 155% across all platforms compared with that of the previous year, and provided the evidence of a new level of maturity in security threats targeting mobile devices.

However, fewer smartphones have been designed to guard against malware attacks, making them an enticing target for hackers and malware writers. If smartphones have been compromised by malware, it could cause their users' services interrupted, such as system damage, financial loss, data loss, and privacy information leakage.

Bluetooth and SMS/MMS are the attack vectors for mobile worms to propagate in cellular networks. The first Bluetooth-based worm is Cabir [7], which can propagate through Bluetooth connection to other Bluetooth-enabled devices that it can find. The first SMS/MMS-based worm is Commwarrior [8], which can spread via SMS/MMS. It searches a user's local address book for phone numbers and sends SMS/MMS messages containing infected files to users in the address book.

In recent years, many efforts have been made to model propagation dynamics of malware for smartphones. Worm propagation models include Bluetooth-based [9]–[15], SMS/MMS-based [16], [17], and hybrid-based [8], [18]–[23]. However, most models have focused almost entirely on the technology of differential equations, they failed to consider the impact of social relationships [24] between any two users on malware propagation in smartphones, and did not consider the impact of individual difference on propagation dynamics of malware. Thus, it poses considerable challenges for modeling on propagation dynamics of malware.

The main goal of our work is to verify the applicability by using smartphone social networks as a tool to characterize the propagation dynamics of SMS/MMS-based worms. We believe that social network theory can be useful to simulate this kind of networks, because the relationships between any two nodes could be capable of modifying all network relationships. This characteristic is similar to that found in many dynamic systems, which are commonly simulated through social network graphs.

In this paper, based on the previous work [24], we propose a new approach to characterize propagation dynamics of SMS/MMS-based worms. We introduce social network theory to characterize mobile worms that spread using MMS or SMS, and typically exploit the social network of users to propagate from one mobile device to another. Moreover, we consider the impact of individual difference on malware propagation. Our contributions are summarized as follows:

- We construct a social relationship graph of mobile devices by extracting their communication patterns based on message records. This graph describes the social relationships between any two smartphones, which are exploited by SMS/MMS-based worms for propagating.
- We present a detailed analytical model for character-

978-0-7695-5022-0/13 $26.00 © 2013 IEEE
DOI 10.1109/TrustCom.2013.28

izing the propagation dynamics of SMS/MMS-based worms using the social relationship graph. Moreover, we consider 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.

- We design and implement a simulator using C++. Furthermore, we show the effectiveness and rationality of the proposed approach through extensive numerical simulations and analysis.

The remainder of this paper is structured as follows: In Section II, we present an overview of related work, and discuss the construction of social relationship graph in Section III. In Section IV, we present a worm propagation modeling scheme with social relationship graph, and provide the results of model validation in Section V. Finally, we conclude this paper in Section VI.

II. Related Work

In this section, we make a survey on the related work in three dimensions. The first dimension is the Bluetooth-based malware propagation model; the second one is related to the SMS/MMS-based malware propagation model; and the last one is the hybrid malware propagation model.

A. Bluetooth-based

Yan and Eidenbenz [9], [10] built an analytical model to study the propagation of Bluetooth worms. In the model, the impact of mobility patterns on Bluetooth worm propagation can be investigated by introducing the input parameters, such as average node meeting rate, average node degree, and the link duration distribution. Rhodes and Nekovee [11] analyzed the effect of population characteristics and device behavior on the outbreak dynamics of Bluetooth worms using the SIP model.

Martin et al. [12] predicted the future propagation of cell phone viruses using the SIS model from mathematical epidemiology. Su et al. [13] investigated whether a large-scale Bluetooth worm outbreak was viable in practice and used trace-driven simulations to examine the propagation dynamics of Bluetooth worms. They found that Bluetooth worms could infect a large population in just a few days.

Zheng et al. [14] focused on analyzing the effect of population distribution density, Bluetooth radius, and node velocity on virus propagation. Their results pointed to a variety of quarantine methods that could greatly reduce the potential virulence.

Peng and Wang [15] presented a worm propagation modeling scheme (WPM). WPM utilized a 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 combined infection factor, which evaluates the spread degree of infected nodes, with resistance factor, which offers resistance evaluation towards susceptible nodes.

B. SMS/MMS-based

Van Ruitenbeek et al. [16] presented response mechanisms to analyze the effects of multimedia messaging system (MMS) viruses that propagate by sending infected messages to other phones. Fleizach et al. [17] proposed an event-based simulator to evaluate the effects of malware propagating using communication services like MMS and VOIP in mobile phone networks. It is only based on US census data and estimated address book degree distribution. However, they did not use real traffic data in their worm propagation study.

C. Hybrid-based

Gao and Liu [18] presented a two-layer model to simulate the propagation process of SMS-based and Bluetooth-based viruses in the geographic network composed of cell towers and the logical contact network composed of mobile phones, respectively. The lower layer is a cell tower network based on geographical information. Bluetooth-based viruses can propagate in this layer based on local positions of mobile phones. The upper layer is a logical network based on the address book of each phone. SMS-based viruses spread in this layer based on the contact relationships among mobile users. The impact of human behavior (i.e., human operations and mobility patterns) on virus propagation was imported into this model.

Cheng et al. [19] presented an analytical model to analyze the speed and severity for spreading the hybrid malware, such as Commwarrior that could target multimedia messaging service (MMS) and Bluetooth. Ramachandran and Sikdar [20] proposed a comprehensive analytical model to explore the impact of various spreading mechanisms such as downloads from the Internet or P2P networks, transfers through Bluetooth, WLAN and infra red interfaces and through SMS or MMS messages on the dynamics of malware propagation in networks of smart cell phones.

Xia et al. [8] investigated the propagation characteristics of Bluetooth and MMS, and then presented the susceptible-exposed-infected-recovered-dormancy (SEIRD) model for the Bluetooth and MMS hybrid spread mode according to Commwarrior. They divided phone nodes into five states, such as S, E, I, R, and D, and 11 kinds of state conversions, such as (i) $S \rightarrow I$, $I \rightarrow D$, $D \rightarrow I$, and $E \rightarrow I(\beta)$ are related to Bluetooth spread mode; (ii) $S \rightarrow E$, $E \rightarrow S$, $E \rightarrow R$, and $E \rightarrow I(\mu)$ are related to SMS/MMS spread mode; (iii) $S \rightarrow R$, $I \rightarrow S$, and $I \rightarrow R$ are related to the combination of both Bluetooth and SMS/MMS modes.

Wang et al. [21] proposed a model on mobile malware using SI model and studied spreading patterns of both Bluetooth and MMS worms. Mobile phone data was processed to obtain mobility of devices at a cell-tower resolution. The compartmental model studied here failed to represent the heterogeneity that was required to represent realistic network characteristics.

Bose and Shin [22] modeled the malware propagation through both Bluetooth and SMS/MMS vectors using a fine-grained agent-based simulator, and 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. [23] presented a Susceptible-Exposed-Infected-Recovered (SEIR) model for the Bluetooth and SMS/MMS hybrid spread mode, based on the preventive immunity and mutation of mobile phone virus. In this model, the phone nodes are divided into 4 states and 8 kinds of state conversions among them: $S \rightarrow I$ and $E \rightarrow I(\beta_1)$ are Bluetooth spread mode; $S \rightarrow E$, $E \rightarrow I(\beta_2)$, and $E \rightarrow R$ are SMS/MMS spread mode; $S \rightarrow R$, $R \rightarrow S$, and $I \rightarrow R$ are the combination of both Bluetooth and SMS/MMS modes. They further discussed the influence of the propagation parameter such as mutation of virus, preventive immunity of mobile phone users, immunity structure in SMS/MMS network and node average degree in Bluetooth network on the propagation of the virus.

III. Construction of Social Relationship Graph

The popularity and unique property of SMS/MMS-based worms increase, drawing our focus on dealing with SMS/MMS-based worms in this paper. Cellular services, such as SMS and MMS, can be used as attack vectors for smartphones. For example, SMS and MMS messages can be used to deliver malicious content and to maintain the communication with the attacker. As to SMS, the attacker uses SMS to send URL link, then the user would be lured to open a browser window using this URL. As to MMS, the message itself could be the malicious payload. A victim receiving this message will most likely open and download the message since he/she believes it comes from someone he/she knows and trusts. Thus, an effective SMS/MMS-based worm propagation approach should take into account the social relationship graph between mobile devices in a cellular network. By figuring out the social interactions between smartphones, i.e., which smartphones are more likely to exchange messages with each other, the propagation path of such mobile malware can be predicted.

If user A and user B exchange messages with each other on a regular basis, user A would in a higher probability to download and open the messages from user B, because they have trust in each other and they wouldn't doubt the credibility of the messages. However, if user A's smartphone has been infected by SMS/MMS-based worm and he accidentally send this message to user B, user B's smartphone is very likely to get infected by this worm. The fact is that if the two smartphone users have never sent messages to each other, user B's phone would never get infected despite the fact that A's smartphone has been infected. In this paper, we make use of SMS and MMS records between two smartphones to predict whether they would get involved in a malware's propagation path, and the proposed propagation model presents the propagation process of a malware based on the message records of infected hosts.

We investigate how a social relationship graph is constructed by using message records collected at one of the largest cellular networks in China. The message records contains information about 0.4 million users in this network exchange about 20 million SMS/MMS messages over a three week period in October 2012. The content of message records were deleted, while the uniqueness of the identifiers of involved phone numbers are preserved.

Social relationship graph is represented by an undirected weighted graph $G = (V, E)$, where the set V of vertices corresponds to the smartphones in cellular networks, and the set E of edges corresponds to the traffic flow exchanged between any two smartphones, i and j. The degree of vertex i, denoted by d_i, which is the number of smartphones (representing the number of links or representing that smartphone's owner has d_i friends). The amount of message records initiated from i to j is denoted by C_{ij}.

We introduce two functions $f(i)$ and $f(i, j)$ to map each vertex $i \in V$ and each edge $(i, j) \in E$, respectively. Thus, the graph can be weighted with $f(i)$ and $f(i, j)$ determining the weights of vertex and edge, respectively. The mapping functions of the weights of vertex and edge are described as follows.

$$f(i) = d_i \tag{1}$$

$$f(i, j) = C_{ij} + C_{ji} \tag{2}$$

The weights of vertices and edges together contribute to a significant level which represents the probability of being infected by malware. As can be seen from Equation (1), the weights of vertices depend on d_i. For SMS/MMS-based malware, a smartphone with a higher in-degree means that it is more likely to be infected, while a smartphone with a higher out-degree is more likely to infect other smartphones. Thus, those high-degree smartphones, either in-degree or out-degree, should be assigned a higher vertex weight.

The interactions between any two smartphones can be expressed by Equation (2). If two smartphones have communicated through SMS or MMS, they are more likely to open and activate a worm-infected message from each other. This social relationship graph presents how smartphones connect with each other and how worms propagate by exploiting this relationship.

An example for social relationship graph is shown in Table I. We use the number of message records exchanged between two smartphones i and j over one week as the weight C_{ji}. Each entry in Table I shows how many times any two smartphones communicate with each other every week on an average. According to what we have analyzed from message records, although the number of interactions between two smartphones behaves differently for weekday and weekend, the number of interactions across the three weeks remains similar. Furthermore, the rationality for use of weekly averaged traffic (WAT) is confirmed by [25]. Therefore, we use WAT to measure the relationship between any two smartphones in our paper.

According to Table I, we abstract each smartphone as a vertex, and normalize WAT between any two smartphones by dividing the maximum WAT over the week, a relationship graph can be obtained as Figure 1.

An accurate social relationship graph can be built through the analysis of messaging records. The graph can be reflective of the propagation path of the worm which spreads by exploiting the host's infected address book.

TABLE I. TRAFFIC OF MESSAGING RECORDS BETWEEN ANY TWO SMARTPHONES

$Betweentwosmartphones$	WAT
A and B	2
A and D	6
A and E	3
B and E	20
B and C	6
B and F	4
C and F	8
C and G	9
D and E	6
D and H	4
E and F	6
E and H	14
F and G	6
F and I	12
G and I	8
G and J	10
H and I	4
H and J	12

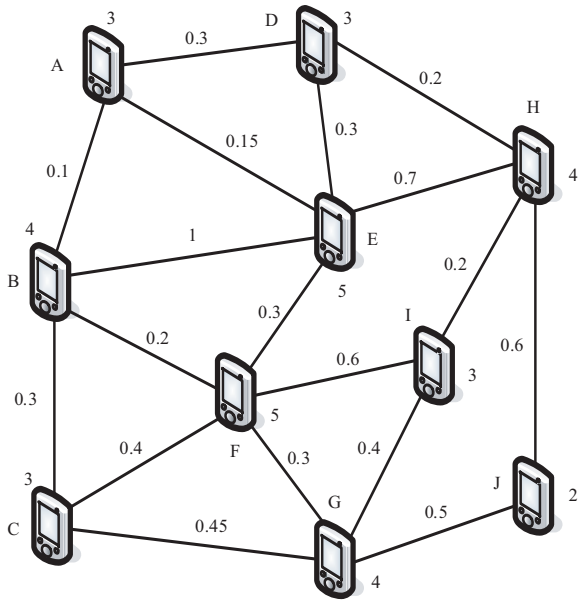

Fig. 1. Social Relationships Graph based on the total number of SMS/MMS messages of each node in a week

IV. MALWARE PROPAGATION MODELING WITH SOCIAL NETWORK GRAPH

In this section, we discuss how a SMS/MMS-based worm propagation model is constructed with social network graph. It is supposed that worms are able to exploit the social relationship information for propagating.

A. State transition relationship

According to the spread property of SMS/MMS-based worms, three classes of epidemic state are considered: susceptible (S), infected (I), and recovered (R). We assume that the number of susceptible, infectious, and recovered nodes at time t are denoted by $S(t)$, $I(t)$, and $R(t)$, respectively. The transforming process of states for worm propagation is illustrated in Figure 2.

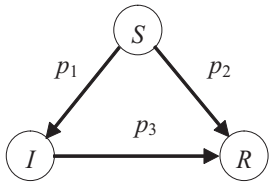

Fig. 2. State transition relationship for SMS/MMS-based worm propagation in smartphones

Some terms of the model are explained as follows:

- $S(t)$ is used to represent the number of individuals not yet infected by malware at time t, or they are susceptible to the malware.
- $I(t)$ denotes the number of individuals who have been infected by malware at time t and are capable of spreading malware to those in the susceptible category.
- $R(t)$ is the compartment used for those individuals who have been infected and then recovered from malware at time t. Those in this category are not able to be infected again or to transmit the infection to others.
- N denotes the total number of susceptible, infectious, and recovered individuals. Let the birth rate be equal to the death rate, the total population size is a constant. Thus, $S(t) + I(t) + R(t) = N$.
- p_1 denotes the probability with which a node in state S becomes a node in state I.
- p_2 denotes the probability with which a node in state S becomes a node in state R.
- p_3 denotes the probability with which a node in state I becomes a node in state R.

B. State transition algorithm

To reasonably describe the infection ability of mobile malware in smartphones based on social network graph, we introduce infection degree of node i, denoted by ID_i, which is used to measure the dangerous level from the infected smartphones to a susceptible smartphone.

Moreover, we introduce two important factors to characterize the impact of individual difference on the propagation dynamics of SMS/MMS-based worm.

One is the infected factor, denoted by IF_{ji}, which denotes infection degree from node j to node i ($0 \leq IF_{ji} \leq 1$). If IF_{ji} equals to 0, it denotes that node j has no infection to node i. If IF_{ji} equals to 1, it denotes that the node j has strong infection to node i.

The other is the resisted factor, denoted by RF_{ij}, which denotes resistance degree of node i on infection from a certain worm ($0 < RF_{ij} \leq 1$). If RF_{ij} equals to 1, it denotes that the node i has strong ability to resist infection from node j. Let T denote the transmission threshold through which a wireless node transforms from state S to other states. Let N_i denote the number of infectious friend nodes for node i. ID_i, RF_{ij}, and IF_{ji} can be described as follows.

$$ID_i = \frac{1}{N_i} \sum_{j=1}^{j=N_i} \left(\frac{C_{ji}}{C_{max}} \times \frac{IF_{ji}}{RF_{ij}} \right) \quad (3)$$

$$RF_{ij} = \omega_1 \frac{1 - \lambda_2 e^{-\beta t}}{1 + \lambda_2 e^{-\beta t}} + \omega_2 \frac{1 - \lambda_2 e^{-\beta C_{ji}}}{1 + \lambda_2 e^{-\beta C_{ji}}} \quad (4)$$

$$IF_{ji} = \omega_1 \frac{\lambda_1 e^{\alpha t} - 1}{\lambda_1 e^{\alpha t} + 1} + \omega_2 \frac{\lambda_1 e^{\alpha C_{ji}} - 1}{\lambda_1 e^{\alpha C_{ji}} + 1} \quad (5)$$

where C_{ji} is the number of message records sent from j to i in a week. C_{max} is the largest number of message records sent between any two smartphones in a week. λ_1 and λ_2 are constants, which can be determined according to the practical requirement. α and β are adjusted factors for IF_{ji} and RF_{ij}, respectively. ω_1, ω_2, ω_3, and ω_4 denote weighting factors, $\omega_1 + \omega_2 = 1$, $\omega_3 + \omega_4 = 1$.

The state transition process is formulated as follows.

Step 1: Network initialization. All nodes communicate with each other using SMS/MMS.

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

Step 3: The information of its/theirs friends can be collected by analyzing the message records.

Step 4: Node i is accessed at time t. When node i has communicated with his/her friends via SMS/MMS at time period Δt, thus

- Case 1: As to node i, if its state is I, its friend nodes are accessed. If the state of its friend node j is S, and if ID of node j is not smaller than T, node j changes its state from S to I with probability p_1. Otherwise, node j remains in the previous state. If IF_{ij} equals to 0 or RF_{ji} equals to 1, node j changes its state from S to R with probability p_2. At the same time, node i changes its state from I to R with probability p_3.
- Case 2: Repeat the beginning of Step 4 until all the nodes in the network are accessed.

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

V. Simulations

To evaluate the feasibility of using social relationship graph to simulate SMS/MMS-based human contact network, and to verify the effectiveness and rationality of the proposed model on worm propagation in smartphons, our experiments are based on the social relationship graph generated from a real network traffic tracing from one of the largest cellular networks in China, and our trace analysis includes MMS and SMS messaging service. Moreover, a C++ simulator has been designed and implemented. In the simulator, the total number of nodes N is 5114, and the other parameters are set as follows, otherwise indicated in the figures: p_2=0, p_3=0.5, λ_1=1, λ_2=1, α=0.24, β=0.36, ω_1=0.4, ω_2=0.6, ω_3=0.4, ω_4=0.6.

Fig. 3 shows the continuous response on the total number of infected nodes with different infected rates. As time passes, the total number of infected nodes first increases gradually from t=0 to t=20, reaches the maximum point about t=70, and then decreases gradually. It is seen that as the probability p_1 increases, the total number of infected nodes increases.

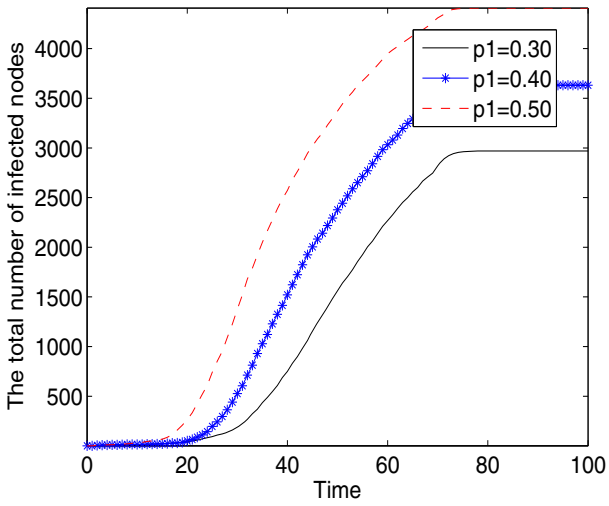

Fig. 3. The total number of infected nodes over the time with different infection rates

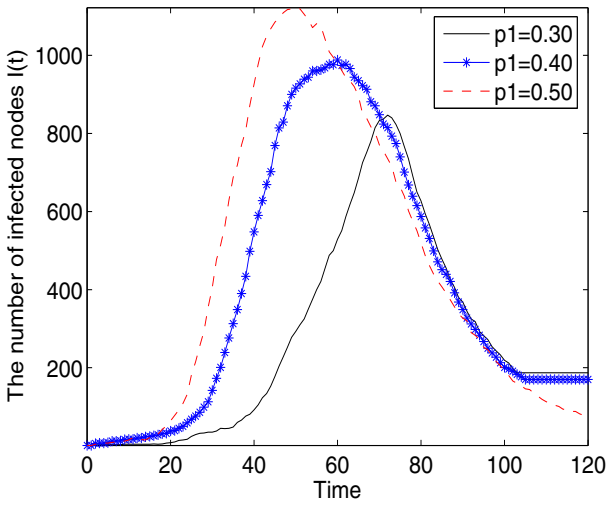

Fig. 4. The number of infected nodes over the time with different infection rates

Fig. 4 shows the transient response on the number of infected nodes $I(t)$. $I(t)$ decreases gradually to zero as time passes. We find that as the probability p_1 increases, $I(t)$ increases quicker, and more susceptible nodes will be infected. It is seen that as the probability p_1 increases, the number of infected nodes increases, and the outbreak point is achieved ahead of time.

VI. Conclusion

In this paper, we proposed a methodology to effectively characterize the propagation of SMS/MMS-based worms via the smartphone social networks. In our solution, three classes of epidemic states are considered: susceptible, infected, and recovered. Moreover, the dynamics of worm propagation process is simulated with social network graph, and its performance is evaluated using simulations based on messaging records collected from real cellular networks. Through extensive evaluations, we demonstrated that our strategies could characterize the propagation of mobile worms effectively. As for our further work, we will focus on analyzing the propagating characteristics of hybrid worms and designing a node misbehavior model using Semi-Markov process [26], which is used to describe the complexity and uncertainty of virus propagation. In addition, the effect of vaccination process on the evolution of infected individuals should also be taken into account.

Acknowledgment

This work is supported by the National Natural Science Foundation of China under Grant Nos. 61272151 and 61073037, 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, the Postdoctoral Program of Central South University, and the Science Project of Zhaoqing University under Grant No. 201101.

References

[1] S. Peng, G. Wang, and S. Yu, "Modeling the dynamics of worm propagation using two-dimensional cellular automata in smartphones," *Journal of Computer and System Sciences*, vol. 79, no. 5, pp. 586–595, August 2013.

[2] S. Peng, "A Survey on Malware Containment Models in Smartphones," *Applied Mechanics and Materials*, vol. 263-266, pp. 3005–3011, 2013.

[3] J. Jamaluddin, N. Zotou, and P. Coulton, " Mobile phone vulnerabilities: a new generation of malware ," in *Proceedings of the IEEE International Symposium on Consumer Electronics*, Jeju Island, Jeju-do, Korea, 2004, pp. 199–202.

[4] C. Gao and 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, June 2011, pp. 1–9.

[5] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (SPSM 2011)*, Chicago, Illinois, USA, October 2011, pp. 3–14.

[6] D. Shih, B. Lin, H. Chiang, and M. Shih, "Security aspects of mobile phone virus: a critical survey," *Industrial Management & Data Systems*, vol. 108, no. 4, pp. 478–494, 2008.

[7] M. L. Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *Accepted by IEEE Communications Survey & Tutorials*, Digital Object Identifier: 10.1109/SURV.2012.013012.00028, 2012.

[8] W. Xia, Z. li, Z. Chen, and Z. Yuan, "Commwarrior worm propagation model for smart phone metworks," *The Journal of China Universities of Posts and Telecommunications*, vol. 15, no. 2, pp. 60–66, 2008.

[9] 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.

[10] ——, "Modeling propagation dynamics of bluetooth worms," in *Proceedings of the 27th International Conference on Distributed Computing Systems (ICDCS 2007)*, Toronto, Ontario, Canada, June 2007, pp. 42–51.

[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, no. 27, pp. 6837–6844, December 2008.

[12] J. C. Martin, L. L. I. Burge, J. I. Gill, A. N. Washington, and M. Alfred, "Modelling the spread of mobile malware," *International Journal of Computer Aided Engineering and Technology*, vol. 2, no. 1, pp. 3–14, 2010.

[13] J. Su, K. Chan, A. Miklas, K. Po, A. Akhavan, S. Saroiu, E. Lara, and 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, November 2006, pp. 9–16.

[14] H. Zheng, D. Li, and 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, August 2006, pp. 1–5.

[15] S. Peng and 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, November 2011, pp. 282–287.

[16] E. V. Ruitenbeek, T. Courtney, W. H. Sanders, and F. Stevens, "Quantifying the effectiveness of mobile phone virus response mechanisms," in *Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2007)*, Edinburgh, UK, June 2007, pp. 791–800.

[17] C. Fleizach, M. Liljenstam, P. Johansson, G. M. Voelkery, and A. Mhes, "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, November 2007, pp. 61–68.

[18] C. Gao and J. Liu, "Modeling and restraining mobile virus propagation," *IEEE Transactions on Mobile Computing*, no. Digital Object Identifier: 10.1109/TMC.2012.29, 2012.

[19] S. Cheng, W. C. Ao, P. Chen, and K. Chen, "On modeling malware propagation in generalized social networks," *IEEE Communications Letters*, vol. 15, no. 1, pp. 25–27, January 2011.

[20] K. Ramachandran and 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, May 2007, pp. 2516–2520.

[21] P. Wang, M. C. Gonzalez, C. A. Hidalgo, and A.-L. Barabasi, "Understanding the spreading patterns of mobile phone viruses," *Science*, vol. 324, no. 5930, pp. 1071–1076, April 2009.

[22] A. Bose and 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, August 2006, pp. 1–10.

[23] Y. Fan, K. Zheng, and 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, September 2010, pp. 1–5.

[24] Z. Zhu, G. Cao, S. Zhu, S. Ranjany, and A. Nucciy, "A social network based patching scheme for worm containment in cellular networks," in *Proceedings of the 28th IEEE Conference on Computer Communications (INFOCOM 2009)*, Rio de Janeiro, Brazil, April 2009, pp. 1476–1484.

[25] A. G. Miklas, K. K. Gollu, K. K. W. Chan, S. Saroiu, K. P. Gummadi, and E. de Lara, "Exploiting social interactions in mobile systems," in *Proceedings of the 9th International Conference on Ubiquitous Computing (UbiComp 2007)*, Innsbruck, Austria, September 2007, pp. 409–428.

[26] S. Peng, G. Wang, Z. Hu, and J. Chen, "Survivability modeling and analysis on 3D mobile ad-hoc networks," *Journal of Central South University of Technology*, vol. 18, no. 4, pp. 1144–1152, August 2011.