Modeling and Predicting the Dynamics of Mobile Virus Spread Affected by Human Behavior

Chao Gao and Jiming Liu*
*Department of Computer Science, Hong Kong Baptist University, Kowloon Tong, Hong Kong
Email: jiming@comp.hkbu.edu.hk

***Abstract*—Viruses and malwares can spread from computer networks to mobile networks with the rapid growth of smart cellpone users. In a mobile network, viruses and malwares can cause privacy leakage, extra charges, remote listening and accessing private short messages and call history logs etc. Furthermore, they can jam wireless servers by sending thousands of spam messages or track user positions via GPS. Because of the potential damages of mobile viruses, it is important for us to design a realistic propagation model to observe and understand the propagation mechanisms of mobile viruses. In this paper, we propose a two-layer model to simulate the propagation process of BT-based and SMS-based viruses in mobile networks. Different from previous work, here we focus on the impacts of human behavior, i.e., human operations and mobility patterns, on virus propagation. Through simulations, we aim to gain some insights into how human behavior affects the dynamics of virus spread in mobile networks.**

***Keywords*-human behavior; virus spread dynamics; mobile networks**

I. INTRODUCTION

The report by Nielsen in 2010 shows that 28% of mobile phones in USA are smart phones[1]. And, more and more applications are running on smart phones, such as emails, files transfer and messaging. As smart phones become more popular, users are more vulnerable to mobile viruses.

Generally speaking, there are two communication channels for mobile virus propagation: Bluetooth (BT) and Short / Multimedia Message Service (SMS / MMS). SMS-based viruses (e.g., TXSBBSpy), as embedded in photos, audios, videos and/or short messages, can reproduce themselves to their neighbors based on phones' address books just like worms in email networks. On the other hand, BT-based viruses (e.g., Cabir, Lasco) can automatically search available Bluetooth services within a certain distance and replicate themselves to other phones[2]. Hybird viruses (e.g., Commwarrior and Mabir) can use both BT and SMS communication channels to propagate.

Many studies have reported the damages of mobile viruses [1][2][3][4]. Generally speaking, mobile viruses can attack two types of targets: (1) individuals and (2) wireless services. When targeting individuals, some viruses can automatically send numerous messages that automatically deduct cost and quickly drain batteries [2][3]. Meanwhile some viruses try to infect more phones via BT and / or SMS in order to access users' private emails, short messages and other data. More seriously, some viruses can disturb a conversation by remote control or track users' locations via GPS [3][4]. While targeting wireless services, some viruses try to jam wireless services by sending thousands of spam messages, and reduce the quality of wireless services. Therefore, it has became urgent for both users and network service providers to restrain the propagation of mobile viruses.

In order to help researchers observe and predict the potential damages of a virus, some models have been used to study the dynamic process of virus propagation [5][6][7][8][9][10][11]. Valid propagation models can provide effective test-beds for developing or evaluating new and/or improved security strategies for restraining virus propagation [5][6]. De et al. have used epidemic models to characterize virus propagation in a wireless network [7][8][9]. They focus mainly on the vulnerability analysis of current broadcast protocols against the process of virus propagation in sensor networks. Although the communication mechanism in a wireless sensor network is similar to that in a mobile network, their models just provide the macroscopic understanding of virus propagation, i.e., the final outcome of the infection. Yet, it cannot provide an in-depth understanding of the impacts of human behavior on virus propagation, such as human operations and mobility patterns. Yan and Eidenbenz have chosen Bluetooth-based viruses as their search targets and investigated the effects of mobility patterns on Bluetooth-based virus propagation [10]. However, they only simulates the mobility patterns from the viewpoint of temporal scale, and ignores the spatial scale of human mobility. As a result, the mobility patterns, reported in [10], cannot reflect the real world situations. Wang et al. have proposed a more realistic propagation model to study BT-based viruses through analyzing and predicting the mobility patterns in the real world situations [11]. They have extracted the characteristics of human mobility from the real data traces, and then proposed a model to predict mobility patterns [12]. But, the operational patterns (i.e., whether or not a user opens an infected message) are ignored in their

[1]Http://blog.nielsen.com/nielsenwire/category/online_mobile/

[2]The propagation process of BT-based viruses just like the epidemic diffusion in biological networks from the perspective of propagation range

978-1-4577-0351-5/11/$26.00©2011IEEE

model.

In this work, we provide a two-layer propagation model to overcome the above-mentioned shortcomings, in which viruses are triggered by human behavior, rather than contact probabilities in a homogeneous model. The two-layer propagation model presented in this paper takes into consideration the behavior of users in mobile networks, including human operations and mobility patterns. The contributions of this paper are summarized as follows:

1) Uncovering / mining key factors in determining virus diffusion in terms of propagation speed and scope;
2) Observing the effects of human behavior, i.e., operational patterns and mobility patterns, on mobile virus propagation.

The remainder of this paper is organized as follows. Section II surveys the current work about propagation models for mobile viruses. Section III presents a two-layer model to simulate the propagation process of BT-based and SMS-based viruses in mobile networks. Section IV provides more reasonable depictions about operational patterns and mobility patterns in our model. Section V uses some experiments to uncover key factors in determining virus diffusion in mobile networks.

II. Related Work

In this section, we review some related work on mobile virus propagation models. Generally speaking, the mobile viruses can be categorized into two types, i.e., BT-based viruses and SMS-based viruses, in terms of communication channels.

First, some viruses can infect mobile phones via BT and Wi-Fi devices within a short-range communization, which are local-contact driven viruses. Similar to contact-based diseases (e.g., SARS and H1N1) in social networks [11], the propagation of BT-based viruses follows a spatially localized spreading pattern. Some studies, reported in [7][8], have applied epidemic theories to model the dynamic spreading process of BT-based viruses. For example, studies reported in [8][11] and [7][14] have characterized the process of BT-based virus propagation based on the typical SI [13] and SIR [15] theory, respectively. Based on the mean-filed theory, the SI and SIR models depict population transitions among different states (i.e., Susceptible, Infected and Recoverable). Because of the limited transmission range of a Bluetooth device, human mobility [12][16] plays an important role in BT-based virus propagation. However, traditional models only consider the temporal patterns of human mobility or just use a variety of simplified random mobility patterns to characterize the spatial patterns of human mobility [10]. Statistics, from mobile service providers to databases that record the information about mobility patterns, show that users' mobility possesses certain social network properties [17][18][19][20][21]. In this work, we provide a feasible and operable algorithms for simulating human mobility in a mobile network in order to accurately characterize the spreading process of BT-based viruses. The features of mobility patterns simulated by our model are consistent with the statistical results from real mobile phone traces, i.e., power-law inter-contact times, local bounded mobility areas and power-law traveling distances [17][18].

Second, some viruses can send a copy of itself to all mobile phones, which are stored in the address books of mobile phones, via SMS / MMS. The propagation of SMS-based viruses in mobile networks follows a long-range spreading pattern that is similar to the spreading of computer viruses, such as worm propagation in email networks [6][22]. Thus, human operations (e.g., the security awareness of a user) paly important roles in SMS-based virus propagation. Users, with higher security awareness, can not be infected even if they receive infected attachments from others. In order to quantitatively study SMS-based virus propagation, we need to simulate certain operational patterns, such as whether or not users open virus attachments. Although current studies have constructed mobile networks based on the call records or address books of phones [11][23][24][25], they all ignore the effects of human behavior on virus propagation. In this work, we simulate some operational patterns and transmission statuses of short messages in order to make model more realistic, and to observe the effects of operational patterns on virus propagation.

Specifically, some hybrid viruses can propagate via BT and SMS / MMS, and can become more dangerous than viruses propagate via a single channel [11]. The motivation of this paper is to investigate the effect of human behavior on mobile virus propagation. We take virus propagation via a single channel as an example. And hybrid viruses will be addressed in our future work.

III. Modeling mobile virus propagation

In this section, we first introduce a two-layer model to depict the geographic network composed of cell towers and the logical contact network composed of mobile phones. BT-based and SMS-based viruses can propagate in each layer, respectively. Then, we provide detailed introductions about each layer. With our model, we focus on evaluating the effects of human operations on SMS-based virus propagation in contact networks, and the effects of human mobility on BT-based virus propagation in geographic networks.

The basic ideas behind our two-layer propagation model are shown in Fig. 1. The lower layer is a cell tower network based on geographical information. BT-based viruses can spread in this layer based on the local positions of mobile phones. The upper layer is a logical network based on the address book of each phone. SMS-based viruses propagate in this layer based on the contact relationships among mobile users.

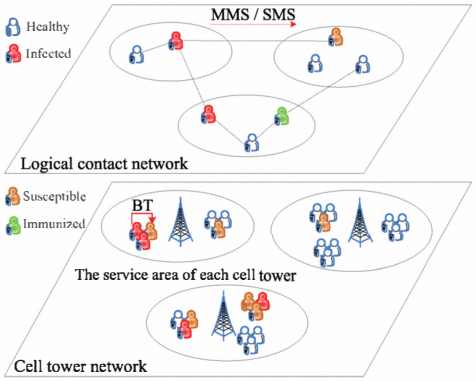

Figure 1. A two-layer model for simulating BT-based and SMS-based viruses in mobile networks. The cell tower network is built based on the information of geographical information, and the contact network is built based on the address book of mobile users.

A. The structure of a geographic network

In this work, a geographical network is represented as a 2-dimension grid, $G[N][N]$. N is the total size of the grid. A cell tower is denoted as T_i, which is a tuple $<r$, $p(x,y)$, n_{tp}, $T_{link}>$, where r is the service radius of a cell tower; $p(x,y)$ records the coordinates of T_i; n_{tp} is the total number of phones in the service area of T_i; T_{link} is the information list about the adjacent neighbors of T_i. Specifically, the service area of T_i is composed of some lattices in the 2-dimension grid, which can be measured based on the position coordinates ($p(x,y)$) and service radius (r) of T_i. For example, $T_1.p(x,y)$=(1,1) and r=1 in Fig. 2. And the service area of T_1 includes four lattices, i.e., {[1,1], [1,2], [2,1], [2,2]}.

Each lattice in a grid includes two parts, $<T_{id}$, $n_{lp}>$, where T_{id} records the id of a cell tower that sends wireless signals to cover the lattice; n_{lp} records how many phones in this lattice.

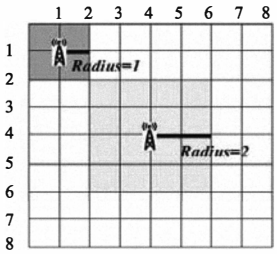

Figure 2. An illustration of cell towers and their service areas.

We deploy some cell towers with different service radius into a geographic network. The distribution of cell towers' service radius, as shown in Fig. 3(a), follows a power-law distribution based on [11]. And each lattice contains the different number of users who can travel in a 2-dimension network following different moving patterns. The neighbors

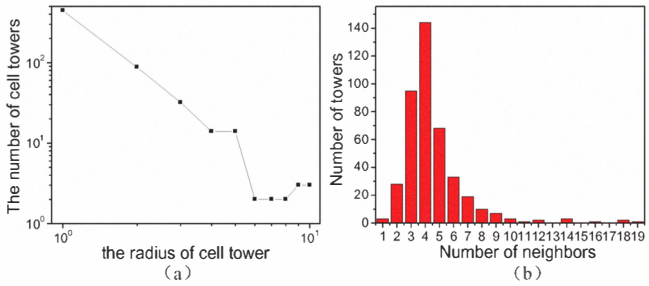

Figure 3. Geographic networks in our model. (a) The distribution of cell towers' service areas. (b) The degree distribution of cell towers in a 2-dimension network.

of a cell tower are defined as those towers whose service areas are adjacent to it. Fig. 3(b) shows the degree distribution of cell towers in the 2-dimension network.

B. The structure of a contact network

Based on the address books of mobile phones, it is possible to build a logical contact network, where nodes denote mobile phone and links denote that there has been a communication between two phones [26]. Different from virus propagation via BT that is only capable of affecting nearby phones, some viruses can spread via SMS (e.g., CommWarrior) and attack remote users in a logical contact network [1]. Therefore, SMS-based viruses could potentially spread as quickly as worms in email networks.

In a logical contact network, each phone v_i is represented as a tuple $<T_{id}, l(x,y), on\text{-}off, t_{on}, p_{click}, P_{link},>$, where: T_{id} is the id of a cell tower that provides wireless service for v_i. $l(x,y)$ records the coordinates of v_i in the geographic network; $on\text{-}off$ is a boolean variable that is used to verify whether or not v_i is open. t_{on} records the time v_i is open; p_{click} is the probability of a user clicking a suspicious message, which is determined by the security awareness of the user; P_{link} records the address book of v_i.

We construct a synthetic contact network, which has 10^4 users and <K>=8.371, following a power-law distribution in terms of node degrees. This is because some observations from the real data traces show that a mobile network follows a heavy-tailed distribution [11][27][28]. Fig. 4(a) shows the cumulative degree distribution of the logical contact network. Fig. 4(b) shows the density distribution of mobile phones in cell towers at the initial stage.

Based on above introductions, we can simulate the propagation process of BT-based and SMS-based viruses in geographic networks and contact networks, respectively. In order to make our model more realistic, we involve certain human behavior into our model in the next section.

IV. Modeling Human Behavior

In this section, we introduce two kinds of human behavior: operational behavior and mobile behavior (mobility), which

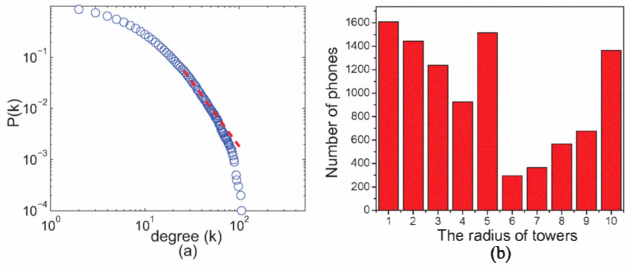

Figure 4. The logical network based on the address books of mobile phones. (a) The cumulative degree distribution of the mobile network in our model. (b) The number of users served by cell towers with the same service radius.

may affect mobile virus propagation. Generally speaking, the prime determinant of SMS-based virus propagation is users' operations after receiving infected messages. If the user of a phone has a higher level of security awareness, they can identify and delete the suspicious messages and the phone could not be infected. Otherwise, the phone could be infected and send virus attachments to other users. Besides operational patterns, mobility patterns play important roles in BT-based virus propagation because BT-based viruses only infect local neighbors (whether or not they know these neighbors) in a certain range.

A. Operational behavior

If users have higher security awareness, they do not open infected messages and could not be infected even if they receive viruses. In our model, we use the probability of clicking a suspicious attachment to reflect and quantify the security awareness of a user. Briefly, once the sample size goes to infinity, the message-clicking probabilities among different users follow a Gaussian distribution [6][22][29], i.e., $v_i.p_{click} \sim (\mu, \sigma^2)$, where $\mu = 0.5$ and $\sigma = 0.3$ in our model. In other words, the larger the $v_i.p_{click}$ is, the lower the security awareness is.

In order to better characterize SMS-based virus propagation, we assume that:

- If a user opens an infected message, the phone of this user is infected and automatically sends viruses to all phones based on its address book;
- When a user does not open an infected message, it is assumed that the user with higher security awareness deletes this infected message;
- An infected phone sends out viruses to other phones only once, after which infected phones do not send out viruses any more;
- If mobile phones are immunized, they never send out viruses even if users open these infected messages.

However, different from SMS-based viruses, some viruses (e.g., Lasco and Cabir) only propagate via Bluetooth service. That is to say, a BT-based virus can only infect their local neighbors with the same OS within a certain distance. A BT-based virus in the real world can connect and infect one neighbor at a time. Therefore, the infected phones, in our model, randomly select a susceptible phone as their targets in each service area of a cell tower. That is to say, mobile phones in each cell tower are homogeneous. Therefore, we can use the typical SIR model [15] to characterize the propagation process of BT-based viruses in each tower. Different from human body, a mobile phone cannot be recovered by itself. Some external intervention or recovery strategies (e.g., individual operations and public security awareness in our model), as shown in [8], are necessary for helping mobile phones recovery.

The population in a SIR model is divided into disjoint classes whose size change in time. The population of each class depends on the possible states of an infection. There are three states in a SIR model, i.e., **S**usceptible (phones are prone to be infected), **I**nfected (phones have been infected) and **R**ecoverable (phones are recovered by anti-softwares or human interventions). Core parameters in a SIR model is the effective infection rate β and recoverable rate γ. The dynamic process of viruses evolved in times is shown in Fig. 5.

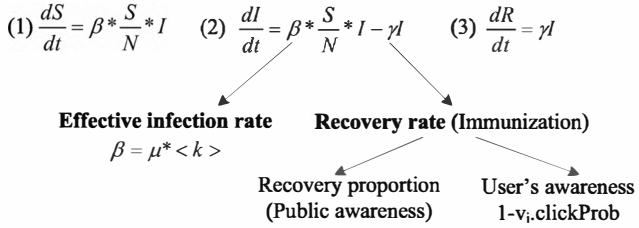

Figure 5. A SIR model in each tower for BT-based virus propagation.

The states S, I and R represent the total number of phones with different states in each tower, respectively. And N=n_{tp} is the total number of phones in each cell tower.

The effective infection rate β in our model is the same as in [11], i.e., $\beta = u * <k>$, where u is the inverse of time that a virus takes to infect a susceptible phone, and $<k>$ is the average number of phones that can contact with each others. Specifically, $<k>$ is decided by Bluetooth communication area and population density inside a tower's service area. In our model, $u = 2$ based on [11] and $<k> = T_i.n_{tp} / (2 * T_i.r)^2$.

The recovery rate (γ) depends on user's own security awareness that can be quantified by $v_i.p_{click}$, and the recovery proportion that depends on the public security awareness. If users have higher individual security awareness (i.e., a small $v_i.p_{click}$), they have a less probability to open infected messages received from SMS, and have larger probability to recover their smart phones. Meanwhile, the higher the public security awareness is, the larger the recovery proportion is. Some experiments in Section V are used to evaluate the effects of individual and public security awareness on BT-

based virus propagation.

B. Mobile behavior

Through analyzing the characteristics of BT-based viruses, we can find that user travel patterns [12] play important roles in virus propagation, just like the impacts of people traveling on the epidemic diffusion in social networks (e.g., SARS, H1N1) [16][30][31]. Fig. 6 shows three mobility patterns of users. Therefore, a propagation model should be accurate in predicting the human mobility in the real world situations. And, the more accurate the mobility pattern is, the more realistic the propagation model is. Based on current studies in [11][12][17][18][19][32][33], some features of mobility are observed from the real data traces:

- The lengths / distances of human travels has a truncated power-law distribution [12][18][19][32];
- People move with a probability at each time [11];
- People devote the most of time to only a few locations where they can meet a lot of other people [12][17];
- Two successive contacts (inter-contact times) of the same persons follows a power law distribution [18][33].

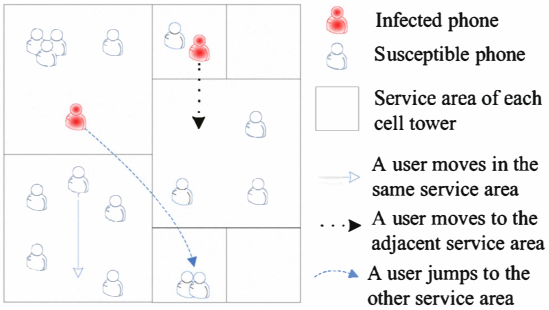

Figure 6. The mobility patterns of users in a geographic network, which can affect virus propagation via the Bluetooth device.

In our work, in addition to traveling distance patterns, some characteristics of human mobility patterns are taken into account as follows:

1) **Whether or not users move**.
   Users are not moving all the time. Wang et al. have proposed a moving probability, $P(t)$, through analyzing the real mobile data traces [11]. Thus, in our model, the moving probability of each user in a given hour follows $P(t)$ based on [11], which is shown in Fig. 7(a).
2) **When users return to old places**.
   In our model, each user could return to some fixed positions (home and/or workplace), where they can be found the most of time. The probability of finding a user at a location with a given rank L is well approximated by $P(L)\sim 1/L$, which is independent of the number of locations visited by the user [12].
3) **How far users move in the next time**.
   Gonzalez et al. have found that the distribution of displacements over all users is well approximated by a power-law with exponent 1.75 ± 0.15 [12]. Two different distance patterns are used in our model: power-law and levy flight with exponent 1.75 ± 0.15 that is the same with [12]. The distributions of distances exponents over all uses are shown in Fig. 8.

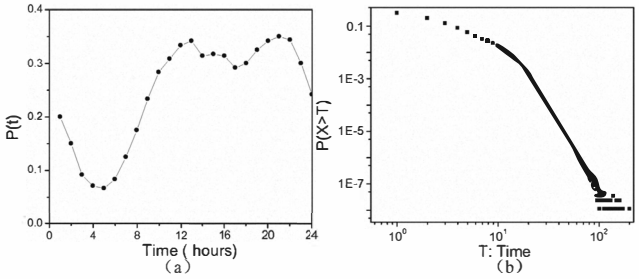

Figure 7. (a) The moving probability of a user based on the supplementary file of [11]. (b) The distribution of inter-contact time of users in our model.

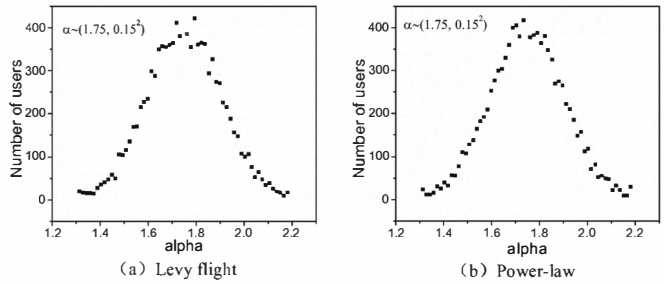

Figure 8. The distributions of distances exponents. The values of exponent are based on [12].

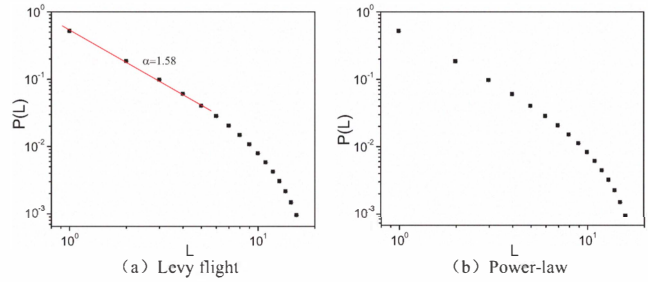

Figure 9. The average frequency of visited L^{th} places in our model. The moving distances follows the Levy flight and power law distribution. The results show that average frequencies are independent of moving distances and the number of locations visited by users.

Based on the above analysis, we provide a feasible algorithm for simulating human mobility in a mobile network in order to observe the spreading process of BT-based viruses. In our model, a user can (1) stay at the old place and do not move at the time t based on $P(t)$, (2) return to a visited place based on $P(L)$, and (3) go to a new place based on different

distance patterns. We carry out some experiments to evaluate users' mobility patters. Fig. 9 shows the average frequencies of visited L^{th} places. Fig. 7(b) shows the distribution of inter-contact times (i.e., the times elapsed between two successive contacts of the same persons), which is consistent with the observed results from the real data in [17][18].

C. Other factors

We consider some other parameters in our model in order to reflect the real transmission of short messages.

1) **The message delivery latency and failure.** Some statistical results in [34] show that 91% of delivered messages have latency less than 5 minutes (95% of messages have latency less than 1 hour from Fig. 2 in [34]), and 5% of delivered messages have latency larger than 1 hour. Meanwhile, the statistical results in [34] also show that 5.1% of messages fail to reach their destinations. Internet service providers can apply the throttling technology [35], which has been applied in computer networks, to slow down the speed of virus propagation through increasing the delivery latency of messages. By doing so, we can gain some time to disseminate security patches to subscribers, hence to restrain virus propagation in mobile networks.
2) **Power on or off.** Mobile phones can be turned off when users fall asleep or batteries run out. We simulate the sleeping time of a user, i.e., the time of power off is 6-10, and power on is 18-14, respectively.

V. Simulation-based Experimentation

In this section, we carry out some experiments to evaluate the dynamics of virus propagation and uncover some key factors that determine virus diffusion. At the beginning, we randomly select two nodes from a network as the initial infected nodes. All numerical results are average values over 10 simulation runs.

A. SMS-based virus propagation

We carry out some experiments to observe the dynamic process of SMS-based virus propagation. Fig. 10 shows the effects of message delivery latency and failure on SMS-based virus propagation. The parameters of "INFOCOM" in Fig. 10(a) are consistent with the setting in Section IV-C, i.e., 5% of delivered messages have latency larger than 1 hour. While, other delay times in Fig. 10(a) are constant as shown in the figure. From these results, we know that the larger delivery latency can restrain the speed of virus propagation, just as the throttling technique [35] in computer networks. But, the final number of infected phones (i.e., the propagation scope) is independent of the message latency. However, The larger delivery failure rate, as shown in Fig. 10(b), can restrain virus propagation in terms of the speed and scope.

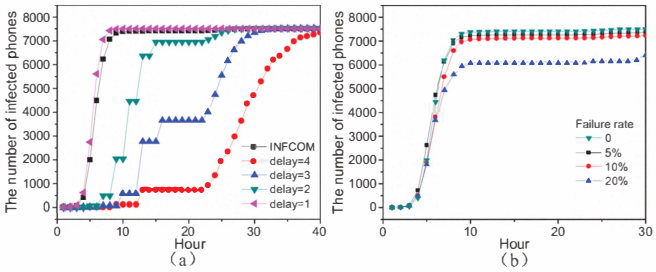

Figure 10. The effects of message delivery latency (a) and message delivery failure rate (b) on SMS-based virus propagation.

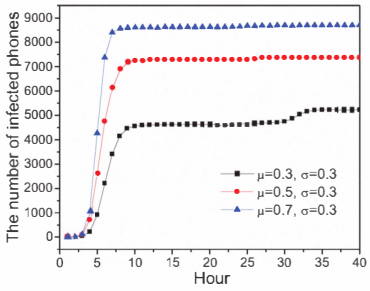

Figure 11. The effects of user awareness on SMS-based virus propagation.

Figure 11 shows the effects of users' security awareness on SMS-based virus propagation. Viruses propagation can be restricted by the security awareness of users. That is to say, if users have the higher security awareness (i.e., μ is smaller), the propagation scope becomes smaller (i.e., the number of infected phones are less). Therefore, it is helpful and valuable to send security notifications to more users in order to improve the individual security awareness for mobile viruses.

In this work, we do not compare the effects of the mobile network topology on SMS-based virus propagation. This is because the propagation process of SMS-based viruses is similar to the spreading of email worms. We have provided more comparing results about the effects of network structures on the e-mail worm propagation in [6].

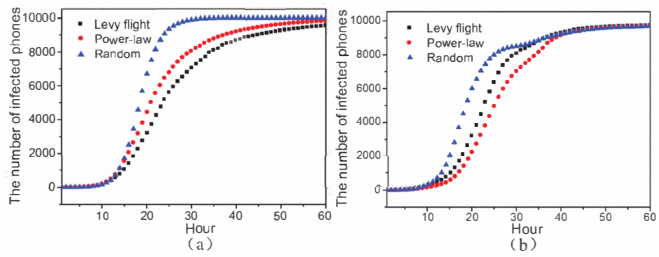

Figure 12. The effects of human mobility patterns on BT-based virus propagation. (a) Different distance patterns. (b) More features are used to characterize human mobility patten.

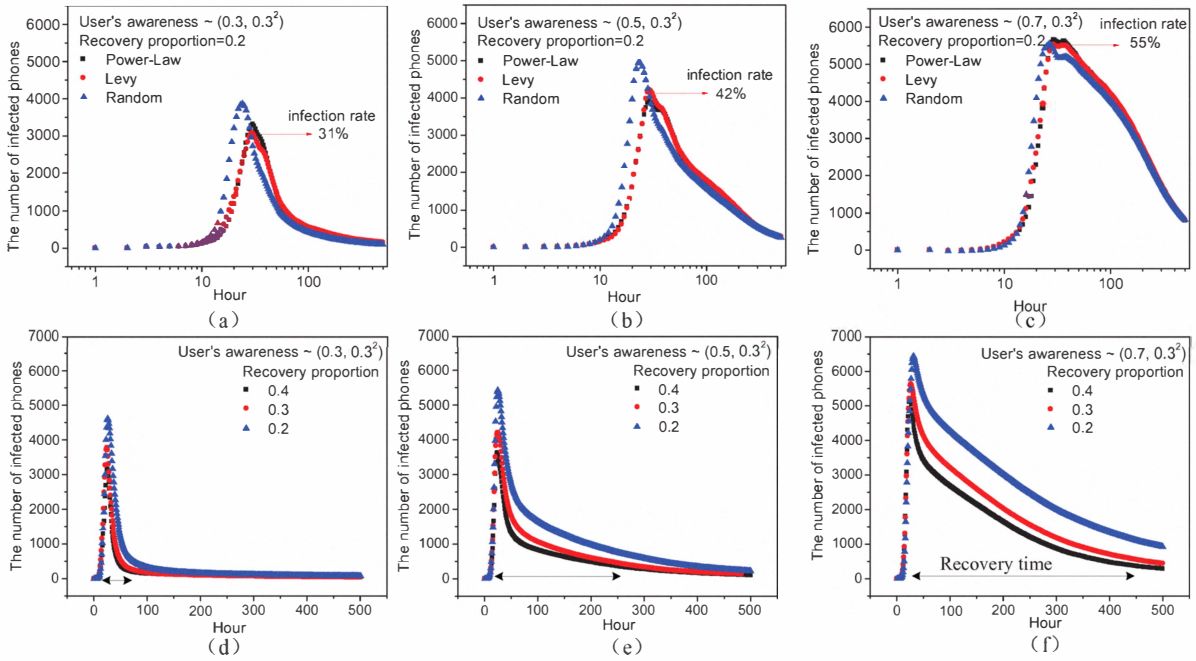

Figure 13. The effects of recovery rate (α) on BT-based virus propagation. (a-c) are semilog figures. (d-f) are linear figures.

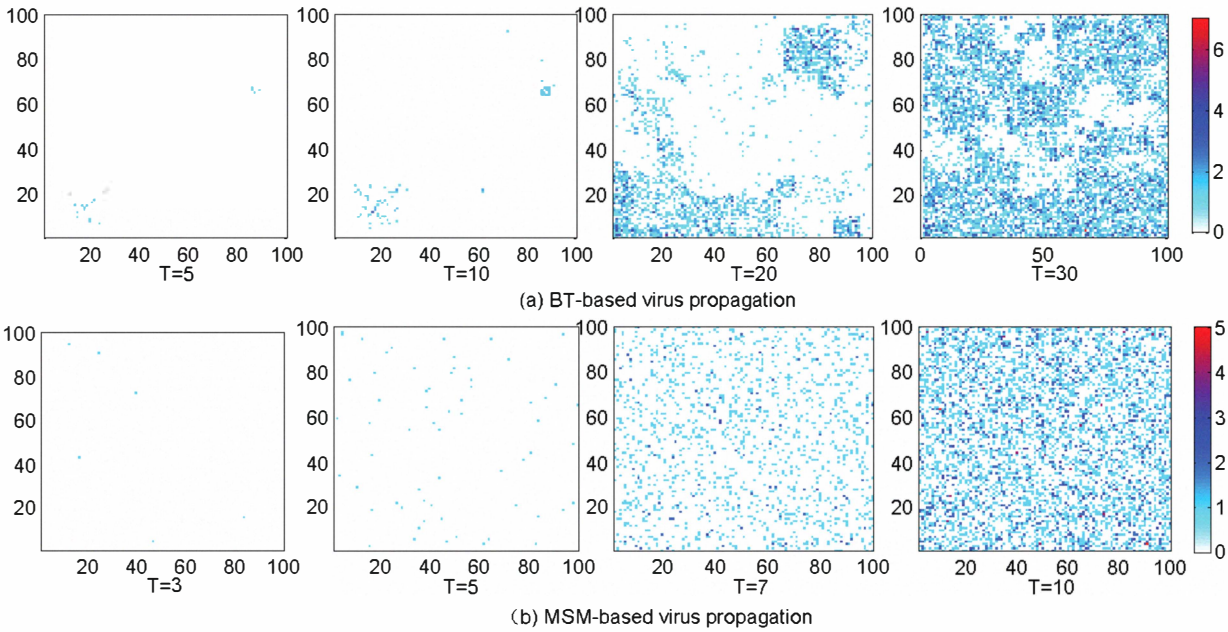

Figure 14. Spatial patterns in the spread of virus propagation via different communication channels. The color represents the number of infected phones in each lattice.

B. BT-based virus propagation

We carry out some experiments to study BT-based virus propagation. Based on the analysis in Sec. IV-B, human mobility plays an important role in BT-based virus propagation. Fig. 12(a) compares the effects of different travel distance patterns on BT-based virus propagation. The travel distance patterns of users follow the power-law, levey flight and random walk (i.e.,a user randomly moves in a network), respectively. And, Fig. 12(b) provides a more realistic model in which mobility does not only follow the power-law distance patterns, but also follow some patterns similar to the real world situations. For example, users may not move in each given hour, or return to a visited place that are introduced in Sec. IV-B.

Comparing Fig. 12(a) and Fig. 12(b), it is interesting to find that the power-law traveling distance can accelerate BT-based virus propagation if there are no other mobility features in our model. However, users with a levy flight traveling pattern can infect more neighbors if more mobility features are involved into our model, which are introduced in Sec. IV-B. This is because BT-based viruses propagate with a probability pattern. Each infected user can only infect one local neighbor at a time. Therefore, the more inter-contact time users have, the more infected chance viruses have. Although the traveling distances of a levy flight pattern also follows a power-law distribution with a heavy tail, users with the levy flight pattern can frequently visit more places near their homes or workplaces where they can meet a lot of other people.

Figure 13 compares the effects of user security awareness and recovery proportion on BT-based virus propagation. The security awareness of a user v_i is quantified by the $v_i.p_{click}$, i.e., a user with higher security awareness can have a smaller $v_i.p_{click}$. With the same public security awareness (i.e., the same recovery proportion), users with a higher individual security awareness can quickly recover their phones and effectively restrain BT-based virus propagation (i.e., the recovery time is the shortest and the infection rate is the least). When the public security awareness (i.e., the recovery proportion) is improved, the coping ability of the whole mobile network for mobile virus can be strengthened. From these results, we find that it is important and valuable to improve users' defense awareness through security notifications or public security education.

Figure 14 shows the spatial patterns of BT-based and SMS-based virus propagation. A BT-based virus can spread from one location to nearby neighbors that is kind of in waves. Whereas a SMS-based virus can spread all over a network. From this figure, we know that SMS-based virus is more dangerous than BT-based virus in terms of propagation speed and scope. Therefore, security patches should be quickly sent via SMS in order to efficiently restrain virus propagation in mobile networks.

VI. Conclusion

In this work, we have proposed a two-layer propagation model to study the propagation characteristics of BT-based and SMS-based viruses. Different from other existing work, here our work focuses on the impacts of human behavior on mobile virus propagation. In order to make our model more reasonable, we have simulated two kinds of human behavior: operational behavior and mobile behavior (mobility). Specifically, we have provided a mobility algorithm by which more mobility features, observed from the real data traces, are characterized. According to experimental results, we have compared and observed the dynamic diffusion processes of BT-based and SMS-based viruses in terms of propagation speed and scope. Importantly, we have provided more experiments to analyze the effects of human behavior, especially human operations and mobility patterns, on mobile virus propagation. Based on our model, we can design and evaluate some defense strategies to restrain mobile virus propagation in the future. Meanwhile, we will further analyze the spreading characteristics of hybrid viruses and internet-based viruses in our future work.

References

[1] D.-H. Shi, B. Lin, H.-S. Chiang, and M.-H. Shih, "Security aspects of mobile phone virus: A critical survey," *Industrial Management and Data System*, 2008, 108(4): 478–494.

[2] H. Kim, J. Smith, and K. G. Shin, "Detecting energy-greedy anomalies and mobile malware variants," in *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services (MobiSys08)*, 2008: 239–252.

[3] L. Xie, H. Song, T. Jaeger, and S. Zhu, "A systematic approach for cell-phone worm containment," in *Proceedings of the 17th International World Wide Web Conference (WWW08)*, 2008: 1083–1084.

[4] N. Xu, F. Zhang, Y. Luo, W. Jia, D. Xuan, and J. Teng, "Stealthy video capturer a new video-based spyware in 3G smartphones," in *Proceedings of the 2nd ACM conference on Wireless Network Security (WiSec09)*, 2009: 69–78.

[5] I. Whalley, B. Arnold, D. Chess, J. Morar, A. Segal, and M. Swimmer, "An environment for controlled worm replication and analysis," *Virus Bulletin*, 2000: 1–20.

[6] C. Gao, J. Liu, and N. Zhong, "Network immunization and virus propagation in email networks: Experimental evaluation and analysis," *Knowledge and Information Systems*, 2011, 27(2): 253–279.

[7] P. De, Y. Liu, and S. K. Das, "An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks," *IEEE Transactions on Mobile Computing*, 2009, 8(3): 413–425.

[8] P. De, Y. Liu, and S. K. Das, "Deployment aware modeling of node compromise spread in wireless sensor networks using epidemic theory," *ACM Transactions on Sensor Networks*, 2009, 5(3): Article 23, 1–33.

[9] P. De, Y. Liu, and S. K. Das, "Modeling node compromise spread in wireless sensor networks using epidemic theory," in *Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM06)*, 2006: 237–243.

[10] G. Yan and S. Eidenbenz, "Modeling propagation dynamics of bluetooth worms (extended version)," *IEEE Transactions on Mobile Computing*, 2009, 8(3): 353–367.

[11] P. Wang, M. C. Gonzalez, C. A. Hidalgo, and A.-L. Barabasi, "Understanding the spreading patterns of mobile phone viruses," *Science*, 2009, 324(5930): 1071–1076.

[12] M. C. Gonzalez, C. A. Hidalgo, and A. L. Barabasi, "Understanding individual human mobility patterns," *Nature*, 2008, 453(7196): 779–782.

[13] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Physical Review Letters*, 2001, 86(14): 3200–3203.

[14] G. Zyba, G. M. Voelker, M. Liljenstam, A. Mehes, and P. Johansson, "Defending mobile phones from proximity malware," in *Proceedings of the 28th IEEE International Conference on Computer Communication (INFOCOM09)*, 2009: 1503–1511.

[15] M. E. J. Newman, "The spread of epidemic disease on networks," *Physical Review E*, 2002, 66(1): 016128.

[16] S. Funk, M. Salath, and V. A. A. Jansen, "Modelling the influence of human behaviour on the spread of infectious diseases: A review," *Journal of The Royal Society Interface*, 2010, 7(50): 1247–1256.

[17] A. Mei and J. Stefa, "SWIM: A simple model to generate small mobile worlds," in *Proceedings of the 29th IEEE International Conference on Computer Communication (INFOCOM10)*, 2010: 2106–2113.

[18] K. Lee, S. Hong, S. J. Kim, I. Rhee, and S. Chong, "SLAW: A mobility model for human walks," in *Proceedings of the 28th IEEE International Conference on Computer Communication (INFOCOM09)*, 2009: 855–863.

[19] I. Rhee, M. Shin, S. Hong, K. Lee, and S. Chong, "On the levy walk nature of human mobility," in *Proceedings of the 27th IEEE International Conference on Computer Communication (INFOCOM08)*, 2008: 924–932.

[20] E. Daly and M. Haahr, "Social network analysis for routing in disconnected delay-tolerant manets," in *Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc07)*, 2007: 32–40.

[21] W. Hsu, T. Spyropoulos, K. Psounis, and A. Helmy, "Modeling time-variant user mobility in wireless mobile networks," in *Proceedings of the 26th IEEE International Conference on Computer Communication (INFOCOM07)*, 2007: 758–766.

[22] C. C. Zou, D. Towsley, and W. Gong, "Modeling and simulation study of the propagation and defense of internet e-mail worms," *IEEE Transaction on dependable and secure computing*, 2007, 4(2): 105–118.

[23] C. Fleizach, M. Liljenstam, and P. Johansson, "Can you infect me now? Malware propagation in mobile phone networks," in *Proceedings of the 2007 ACM Workshop on Recurring Malcode (WORM07)*, 2007: 61–68.

[24] E. V. Ruitenbeek 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 (DSN07)*, 2007: 790–800.

[25] Z. Zhu, G. Cao, S. Zhu, S. Ranjan, and A. Nucci, "A social network based patching scheme for worm containment in cellular networks," in *Proceedings of the 28th IEEE International Conference on Computer Communication (INFOCOM09)*, 2009: 1476–1484.

[26] M. Seshadri, S. Machiraju, A. Sridharan, J. Bolot, C. Faloutsos, and J. Leskovec, "Mobile call graphs: Beyond power-law and lognormal distributions," in *Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD08)*, 2008: 596–604.

[27] A. A. Nanavati, R. Singh, D. Chakraborty, K. Dasgupta, S. Mukherjea, G. Das, S. Gurumurthy, and A. Joshi, "Analyzing the structure and evolution of massive telecom graphs," *IEEE Transactions on Knowledge and Data Engineering*, 2008, 20(5): 703–718.

[28] J. P. Onnela, J. Saramaki, J. Hyvonen, G. Szabo, D. Lazer, K. Kaski, J. Kertesz, and A. L. Barabasi, "Structure and tie strengths in mobile communication networks," *Proceedings of the National Academy of Sciences of the United States of America*, 2007, 104(18): 7332–7336.

[29] R. J. Herrnstein and C. Murray, *The Bell Curve*. The free press, 1994.

[30] L. Hufnagel, D. Brockmann and T. Geisel, "Forecast and control of epidemics in a globalized world," *Proceedings of the National Academy of Sciences of the United States of America*, 2004, 101(42): 15124–15129.

[31] V. Colizza, A. Barrat, M. Barthelemy and A. Vespignani, "The role of the airline transportation network in the prediction and predictability of global epidemics," *Proceedings of the National Academy of Sciences of the United States of America*, 2006, 103(7): 2015–2020.

[32] D. Brockmann, L. Hufnagel, and T. Geisel, "The scaling laws of human travel," *Natue*, 2006, 439(7075): 462–465.

[33] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, "Impact of human mobility on the design of opportunistic forwarding algorithms," in *Proceedings of the 26th IEEE International Conference on Computer Communication (INFOCOM06)*, 2006: 606–620.

[34] X. Meng, P. Zerfos, V. Samanta, S. H. Wong, and S. Lu, "Analysis of the reliability of a nationwide short message service," in *Proceedings of the 26th IEEE International Conference on Computer Communication (INFOCOM07)*, 2007: 1811–1819.

[35] J. Balthrop, S. Forrest, M. E. J. Newman, and M. M. Williamson, "Technological networks and the spread of computer viruses," *Science*, 2004, 304(5670): 527–529.