Modeling and Restraining Mobile Virus Propagation

Chao Gao and Jiming Liu, *Fellow*, *IEEE*

Abstract—Viruses and malwares can spread from computer networks into mobile networks with the rapid growth of smart cellphone users. In a mobile network, viruses and malwares can cause privacy data leakage, extra charges, and remote listening. Furthermore, they can jam wireless servers by sending thousands of spam messages or track user positions through GPS. Because of the potential damages of mobile viruses, it is important for us to gain a deep understanding of the propagation mechanisms of mobile viruses. In this paper, we propose a two-layer network model for simulating virus propagation through both Bluetooth and SMS. Different from previous work, our work addresses the impacts of human behaviors, i.e., operational behavior and mobile behavior, on virus propagation. Our simulation results provide further insights into the determining factors of virus propagation in mobile networks. Moreover, we examine two strategies for restraining mobile virus propagation, i.e., preimmunization and adaptive dissemination strategies drawing on the methodology of autonomy-oriented computing (AOC). The experimental results show that our strategies can effectively protect large-scale and/or highly dynamic mobile networks.

Index Terms—Mobile networks, phone virus, human mobility, autonomy-oriented computing, preimmunization, adaptive dissemination

1 Introduction

Many studies have reported the damages of mobile viruses in smart phones [1], [2], [3]. For example, an outbreak of mobile viruses occurred in China in 2010. The "Zombie" virus attacked more than 1 million cell phones, and created a loss of $300,000 per day.[1] Among many potential damages, mobile viruses can cause private data leakage and disturb conversation by remote control [3], [4]. In some more serious situations, viruses can even jam wireless services by sending thousands of spam messages, and reduce the quality of voice communication. In view of this situation, there is an urgent need for both users and service providers to further understand the propagation mechanisms of mobile viruses and to deploy efficient countermeasures.

In order to help researchers observe and predict potential damages of a virus, some models have been used to study the dynamic process of virus propagation. Valid propagation models can be used as testbeds to: 1) estimate the scale of a virus outbreak before it occurs in reality [5] and 2) evaluate new and/or improved countermeasures for restraining virus propagation [6]. Recently, there exist some models to characterize and predict the infection dynamics of mobile viruses [5], [7], [8], [9], [10]. However, most of them have considered only one aspect of human behaviors. For example, they apply random walks and/or levy flight processes to characterize human mobility patterns [5]. Other statistical characteristics of mobility patterns revealed from real-world data traces are not incorporated into their models; some examples of such characteristics include moving probability at a given time [7] and revisit probability to an old place (i.e., local bounded mobility areas) [5], [11]. In addition, these models do not consider human operational patterns (e.g., whether or not a user clicks on a suspicious message as shown in [12]).

In this paper, we propose a two-layer network model for characterizing BT-based and SMS-based viruses, which propagate through Bluetooth and Short/Multimedia Message Services, respectively, in order to address the above-mentioned shortcomings. In our proposed model, viruses are triggered as a result of human behaviors, rather than contact probabilities in a homogeneous model [8]. Two types of human behavior, i.e., operational behavior and mobile behavior (mobility), are considered in our individual-based model. Different from existing work that focuses on the effects of network structures on virus propagation, our work is aimed to gain further insights into how human behaviors affect the propagation dynamics of mobile viruses.

Recently, several methods have been proposed to restrain mobile virus propagation based on existing models. Although some straightforward anomaly detection technologies can, to a certain extent, protect infected phones from sending infected messages based on system calls sequences and APIs [3], [4], [13], [14], they will not be able to detect new viruses due to the limitation of antivirus knowledge. In order to make sure that users timely update their own detection databases, service providers or security companies need to disseminate notifications or patches to smart phones. However, it would be impractical to disseminate security notifications or patches to all phones because of the

[1] www.informationweek.com/news/security/attacks/228200648.

- C. Gao is with the Department of Computer Science, Hong Kong Baptist University, RRS734, 224 Waterloo Road, Kowloon Tong, Hong Kong, and the College of Computer and Information Science, Southwest University, Tiansheng Road #2, Beibei District, Chongqing, 400715, China. E-mail: cgao@comp.hkbu.edu.hk.
- J. Liu is with the Department of Computer Science, Hong Kong Baptist University, RRS727, 224 Waterloo Road, Kowloon Tong, Hong Kong. E-mail: jiming@comp.hkbu.edu.hk.

Manuscript received 11 Jan. 2011; revised 15 Dec. 2011; accepted 6 Jan. 2012; published online 23 Jan. 2012.
For information on obtaining reprints of this article, please send e-mail to: tmc@computer.org, and reference IEEECS Log Number TMC-2011-01-0010.
Digital Object Identifier no. 10.1109/TMC.2012.29.

limitation of time and bandwidth. Some strategies attempt to forward security notifications or patches based on the short-range communication capabilities of intermittently connected phones [15], [16], but their impact will be affected by human mobility patterns [7], [17] and intercontact frequencies among phones [18], [19], [20]. It would be difficult to acquire signature files in a timely manner [13]. In the meantime, other dissemination strategies have also been used to distribute patches [21], [22], and the difficulty remains when dealing with a large-scale or highly dynamic network. Thus, it would be desirable for us to propose a new strategy that can efficiently forward patches to as many phones as possible, even in large-scale and/or dynamically evolving networks.

In this paper, we propose a two-layer network propagation model that accounts for the behavior of users (i.e., operational and mobility patterns) in mobile networks. Based on our model, we examine the performance of a preimmunization strategy that draws on the methodology of autonomy-oriented computing (AOC) [23], [24], as reported in [25], in restraining mobile virus propagation. In order to evaluate the effect of patch distribution delay on virus propagation, we deploy the AOC-based preimmunization strategy into a network at different times. Furthermore, we design an adaptive dissemination strategy by extending local reactive behaviors of entities in [25]. Thus, the goal of our work is threefold:

1. To uncover some key factors in determining mobile virus propagation through our two-layer network propagation model;
2. To observe the effects of operational patterns and mobility patterns on mobile virus propagation;
3. To examine two strategies for restraining virus propagation in mobile networks, i.e., preimmunization and adaptive patch dissemination strategies drawing on the methodology of AOC.

The remainder of this paper is organized as follows: Section 2 surveys existing work on propagation models and countermeasures against mobile viruses. Section 3 presents a two-layer network model for simulating virus propagation through different communication channels in mobile networks. Section 4 discusses the effects of operational patterns and mobility patterns on virus propagation. Section 5 examines two AOC-based defense strategies for restraining mobile virus propagation. Section 6 highlights our major contributions.

2 Related Work

In what follows, we first review related work on mobile virus propagation models. Next, we introduce some virus defense methods, including abnormal detection technologies and patch dissemination strategies for restraining virus propagation in mobile networks.

2.1 Virus Propagation through BT and SMS

According to the communication channels of mobile viruses, mobile viruses fall into two categories: BT-based viruses (e.g., Cabir, Lasco) and SMS-based viruses (e.g., TXSBBSpy, Zombie, Commwarrior).

A BT-based virus is a local-contact driven virus [7] since it infects other phones only through Bluetooth and WiFi devices within a short radio range. Similar to other contact-based diseases in humans (e.g., SARS and H1N1) [26], the propagation of a BT-based virus follows a spatially localized spreading pattern. One of the most common approaches to studying such virus propagation is based on epidemic modeling. It assumes that individuals are homogeneous in a host population, each of which has an equal likelihood of contact with others [27], [28]. Some studies have applied epidemic modeling to analyzing the propagation dynamics of a BT-based virus. For example, studies reported in [5], [7] and [16] have characterized the propagation process of a BT-based virus based on the typical SI [27] and SIR [28] models, respectively. Because of the limited transmission range of a Bluetooth device, human mobility plays an important role in BT-based virus propagation [17]. Statistics from mobile service providers that reveal the information about mobility patterns have shown that users' mobility possesses certain social network properties [18], [19], [20], [29], [30], [31]. However, most of the models are, to a certain extent, simplified (e.g., using random walks in [5]) in characterizing human mobility patterns, and do not consider the temporal patterns of human mobility (e.g., moving probability at a given time [7] and intercontact times among phones (i.e., the time elapsed between two consecutive contacts between two phones) [18], [19]). Although Wang et al. have improved the model of a BT-based virus propagation, as reported in [7], by extracting and predicting the characteristics of human mobility from real-world data traces [11], [20], [29], their model do not address the effects of operational patterns (i.e., whether or not a user clicks on an infected message) on virus propagation.

On the other hand, SMS-based viruses can send copies of themselves to all phones that are recorded in address books, by means of forwarding photos, videos, and short messages, etc. The propagation of SMS-based viruses in mobile networks follows a long-range spreading pattern that is similar to the spreading of computer viruses, especially worm propagation in e-mail networks [6], [12]. When a user receives a suspicious message, the user normally has two options: either open or delete it. Thus, the operational behavior of users play a key role in SMS-based virus propagation. Users with certain awareness about the risk of viruses will not likely be infected even if they receive an infected attachment from others. In order to quantitatively study SMS-based virus propagation, we need to consider certain operational patterns, such as whether or not users open a virus attachment. Although existing studies have constructed models of mobile networks based on the call records or address books of phones [21], [22], [32], they do not take into account the effects of human behaviors on virus propagation.

In this work, we incorporate related research on human mobility and operational behavior into our model in order to provide a computational model for characterizing and simulating the propagation dynamics of mobile viruses. The characteristics of mobility patterns described by our model are consistent with statistical results from the real-world traces, i.e., local bounded mobility areas [18], power-law traveling distances [11], and intercontact times [19].

2.2 Defense Strategies against Mobile Viruses

Some countermeasures such as anomaly detection technologies have been proposed to protect users' private information from being revealed to other users. For example, Bose et al. have discriminated some malicious behaviors from normal operations by training a classifier based on the method of support vector machines [14]. Kim et al. have suggested a method of detecting certain malwares by monitoring battery-lifetime, which can find some unknown energy-depletion threats [2]. Cheng et al. have provided an approach to detecting both single-device and system-wide abnormal behaviors by collecting and sending communization data to remote servers in order to reduce the detection burden of phones [33].

Although these abnormal detection technologies can help directly protect phones from being affected by certain viruses, it is difficult for them to detect new viruses. That is because the monitoring technologies must first be trained to recognize normal and abnormal operational behaviors. If a new virus produces some unknown patterns (e.g., a series of system calls), these monitoring technologies cannot detect such a virus. Therefore, it is challenging to detect a worm outbreak at the early stage unless both users and security companies frequently update their detection classifiers. Different from wired networks (e.g., computer networks), it is almost impossible to send patches to all phones simultaneously and timely due to bandwidth constraints. Thus, we need new strategies to efficiently disseminate security notifications or patches to as many phones as possible with a relatively lower communication cost before a new virus spreads to a large population.

In order to reduce communication redundancy, some strategies send patches based on Bluetooth [15], [16]. These strategies select some "important" phones that can divide a Bluetooth-based network into different communities based on the contact time and frequency. Thereafter, they send security signatures to all communities based on the local detection. However, this method cannot ensure that users acquire patches in time [13]. In order to enable the "important" phones (that can amplify virus propagation scope as shown in [6]) to timely acquire patches, some security notifications or patches can be directly sent from a center server to those phones through pre-immunization strategies, as in e-mail networks [6]. For example, Zhu et al. have selected some immunized phones based on clustered graph partitioning and balanced graph partitioning [21]. This is essentially a betweenness-based strategy as applied in email networks [6], [34]. However, this strategy cannot readily be applied to a real-world mobile network due to the unknown and/or highly dynamic topology of the network. In this paper, we examine the performance of an AOC-based preimmunization strategy that selects some highly-connected phones and prevents a virus from turning into an epidemic. Furthermore, we design an AOC-based dissemination strategy that distributes security notifications or patches to smart phones with a low communication redundancy, in order to restrain virus propagation before it causes further infections.

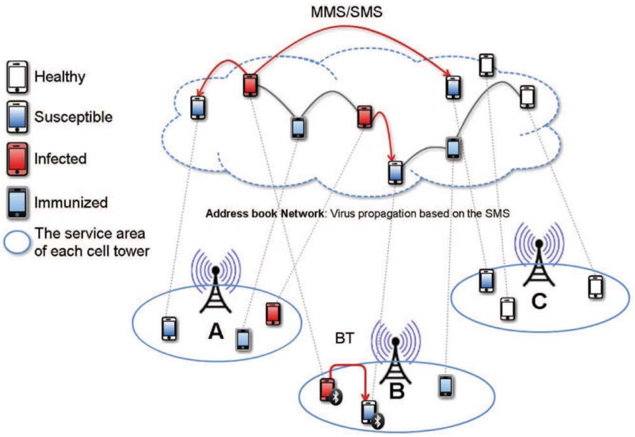

MMS/SMS
Healthy
Susceptible
Infected
Immunized
The service area of each cell tower
Address book Network: Virus propagation based on the SMS
A
B
C
BT

Fig. 1. A two-layer network model for simulating mobile virus propagation. The network of cell towers (e.g., A, B, and C) is built based on geographical information, whereas the social relationship network is constructed from the address books of mobile users.

3 Modeling Mobile Virus Propagation

In this section, we first introduce a two-layer network model for simulating mobile virus spreading through different communication channels in Section 3.1. Next, we present detailed propagation processes of SMS-based and BT-based viruses in Sections 3.2 and 3.3, respectively.

The work presented in this section is an extension of the work in [35]. Different from others, our work addresses the issue of how human behaviors, i.e., operational and mobile behavior, affect virus propagation. Based on the analysis of propagation mechanisms, we note that a primary factor contributing to SMS-based virus propagation lies in users' operations after receiving infected messages. If users have enough knowledge about the risk of mobile viruses (i.e., with a high security awareness), they will not open suspicious messages and their phones will not be easily infected. In addition to operational patterns, mobility patterns play a key role in BT-based virus propagation. This is because BT-based viruses can only infect local neighbors (whether or not they know these neighbors) within a certain range.

With our model, we can evaluate the impact of operational behavior on SMS-based virus propagation in social relationship networks, as well as the effects of mobile behavior on BT-based virus propagation in geographical contact networks, as to be discussed in Section 4.

3.1 Two-Layer Network Propagation Model

The basic ideas behind our two-layer network propagation modeling are shown in Fig. 1. The lower layer represents a geographically based cell tower network. BT-based viruses spread in this layer to various positions of mobile phones [35]. The upper layer corresponds to a logical network constructed from the address books of phones. SMS-based viruses propagate in this layer following the social relationships among mobile users.

3.1.1 The Structure of a Geographical Network

Mobile phones connect with each other through wireless signals provided by cell towers. In our study, we model the geographical network of cell towers using a 2D grid as defined in Definitions 1, 2, and 3. In this grid, the location of

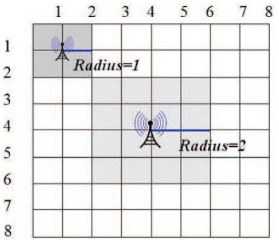


Fig. 2. An illustration of towers and their service areas.

each cell tower is specified using coordinates $p(x, y)$. For example, the location of T_1 is at $p(1, 1)$ and T_2 is at $p(4, 4)$ as shown in Fig. 2. The cell towers may have different service areas. The service area of T_i covers some lattices that are determined from its location coordinates $p(x, y)$ and service radius (r) of T_i. For example, the service area of T_1 in Fig. 2 covers four lattices, i.e., {[1,1], [1,2], [2,1], [2,2]}.

Definition 1. *A* **geographical network** *is represented in a 2D grid, $G[N][N]$. N is the size of the grid. Each lattice corresponds to one service area of a mobile signal. A service area of a tower may consist of many lattices.*

Definition 2. *$T[N_t]$ records information about* **cell towers**. *There are N_t towers in a grid. A tower denoted as T_i is a tuple <id, r, p(x, y), T_{link}, n_{tp}>, where:*

- *id is the identifier of a tower;*
- *r is the service radius of a tower;*
- *there are n_{tp} phones in the service area of T_i;*
- *p(x, y) corresponds to the coordinates of T_i;*
- *T_{link} is a list of the adjacent neighbors of T_i.*

Definition 3. *Each* **lattice**, *[x,y], contains two parts in a grid: $<T_{id}, n_{lp}>$, where T_{id} records the id of a cell tower that sends wireless signals to cover the lattice and n_{lp} records how many phones in this lattice.*

Users with their phones can travel in a geographical network, moving from one lattice to another based on their mobile behavior. The wireless signals in two lattices may be provided by the same or different cell towers. The distribution of towers' service areas, which follows a power-law distribution based on [7] is shown by [36, Fig. 2a]. The number of phones served by cell towers in different service radii is presented by [36, Fig. 3b].

3.1.2 The Structure of a Logical Network

A logical relationship network among mobile users can emerge from the address books of mobile phones. In such a network, nodes correspond to phones and links show the communications among them [37]. Different from virus propagation through Bluetooth that is only capable of affecting nearby phones, some viruses may spread through SMS (e.g., Zombie) and hence attack remote phones [1]. Therefore, SMS-based viruses could potentially spread as fast as worms in email networks.

We construct a synthetic logical relationship network following a power-law distribution in terms of node degrees, according to the observations from the real-world data [7], [38]. Definition 4 specifies a synthetic logical network that has 10^4 phones and $<K> = 8.371$ as in our model. The cumulative degree distribution of such a network and the initial density distribution of mobile phones in cell towers, respectively, is shown in [36, Fig. 3].

Definition 4. *$P[N_p]$ records information about* **mobile phones**. *There are N_p phones in a grid. Each phone v_i contains: $<id, T_{id}, l(x, y), P_{link}, on\text{-}off, t_{on}, p_{click}, status>$,*

- *id, T_{id}, $l(x, y)$ constitute the basic information about a phone in a geographical network. T_{id} is a cell tower that provides the wireless service to this phone. $l(x, y)$ is the coordinate of a phone in a network;*
- *P_{link} corresponds to the address book of a phone;*
- *on-off is a boolean variable indicating whether or not a phone is on. t_{on} corresponds to the time phone is open;*
- *p_{click} is the probability of a user clicking on a suspicious message, which is determined by user's own security awareness. If a user has enough knowledge background about mobile viruses (i.e., higher security awareness), the user will have a lower p_{click} to click on a suspicious message;*
- *$status$ is the state of a phone. Fig. 11 shows the state transition of a phone in the face of SMS-based viruses.*

Based on the above formulation, the propagation processes of BT-based and SMS-based viruses can be simulated in a geographical contact network and a social relationship network, respectively. In our model, two types of human behavior are characterized: operational behavior to be described in Section 3.2 and mobile behavior in Section 3.3.

3.2 SMS-Based Propagation Process

Social relationships are embodied in mobile networks based on the address books of smart phones. If a phone is infected by an SMS-based virus, the virus automatically sends its copies to other phones based on the address book of the infected phone. When users receive a suspicious message from others, they may open or delete it based on their own security awareness and knowledge about the risks of mobile viruses. Therefore, the security awareness of mobile users is one of the dominant factors that determine SMS-based virus propagation.

In our model, we simulate one type of operational behavior, i.e., whether or not a user opens a suspicious message. The probability of clicking on a suspicious attachment can be used to reflect and quantify the security awareness of a user. Analogous behavior has been used to simulate email virus propagation [6], [12]. Briefly, once the sample size goes to infinity, the message-clicking probabilities among different users will follow a Gaussian distribution [12], [39], i.e., $v_i.p_{click} \sim (\mu, \sigma^2)$, where $\mu = 0.5$ and $\sigma = 0.3$ as in our model. If users have higher security awareness, they would not be infected even if they receive infected messages. In order words, the lower the $v_i.p_{click}$ is, the higher the security awareness will be. In order to better characterize the SMS-based virus propagation, we assume that [35]:

- 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;
- If 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 the infected phone will not send out viruses any more;
- If a phone is patched (immunized), it will not send out viruses even if a user opens an infected message.

In order to reflect the real transmission of short messages, we add some parameters to simulate the states of short messages and smart phones in our model [35].

1. **The message delivery latency and failure.** Statistical results in [40] have shown that 91 percent of delivered messages have a latency period less than 5 minutes (95 percent of messages have a latency less than 1 hour from [40, Fig. 2]), and 5 percent of delivered messages have a latency longer than 1 hour. Meanwhile, 5.1 percent of messages fail to reach their destinations. Internet service providers can apply the throttling technology, which has been used in computer networks [41], to slow down the speed of virus propagation by increasing the delivery latency of messages. By doing so, we can gain some time to disseminate security patches to subscribers, hence to restrain mobile virus propagation.
2. **Power on or off.** Mobile phones may be turned off when users sleep. Here, we simulate the power on or off period based on the awake or sleep time of a user, respectively, as reported in the existing studies[2]; that is, the period of power on (awake time) is between 14 and 18 hours, whereas the period of power off (sleep time) is between 6 and 10 hours.

The propagation process of an SMS-based virus is shown in Algorithm 1 and [36, Algorithm 1]. Section 4 presents some experimental results to demonstrate how users' security awareness affects mobile virus propagation.

Algorithm 1. Mobile virus propagation
Input: $G[N][N]$, $T[N_t]$, $P[N_p]$
Output: SMSnum[*step*][k] and BTnum[*step*][k] store the total numbers of phones infected by SMS-based and BT-based viruses, respectively, at the k^{th} time

```
Propagation_initPhone( );
for $k = 1$ to $Runtime$ do//average results over $Runtime$ times
  for $step = 1$ to $Endsimul$ do //simulation steps is 500
    for $i = 1$ to $N_p$ do            //SMS-based propagation
      if($v_i.on\text{-}off == True$);    //the phone is open
        if $v_i.status == Dangerous$ && $v_i.p_{click} >$ rand() then
          $v_i$ is infected and send viruses to its friends;
          $sum_I$++;
    SMSnum[$step$][$k$] = $sum_I$;
    for each cell tower $T_i$ do // BT-based propagation
      $v_{it} = v_{it}$+BT_SIR($T_i$); // SIR model in each tower
  BTnum[$step$][$k$] = $v_{it}$;
  Human_Mobility($step$);   // Based on Alg. 2
```

3.3 BT-Based Propagation Process

Different from SMS-based viruses, if a phone is infected by a BT-based virus, it automatically searches another phone through available Bluetooth services within a certain range, and then replicates the BT-based virus to that phone. Therefore, users' contact frequency and mobility patterns play key roles in BT-based virus propagation. In our model, we integrate a stochastic local infection dynamics among phones with the mobile behavior of each user in a geographical network, taking into account prior research on human mobility [11], [20], [29], [30].

3.3.1 SIR Model in Each Cell Tower

A BT-based virus can only infect its geographically local neighbors with the same OS within a certain range. These geographically local neighbors are homogeneous for a BT-based virus since an infected phone randomly selects a susceptible phone as its target at a time. Therefore, the deterministic differential equations are applicable to capturing the propagation dynamics. We utilize an SIR model to characterize the propagation dynamics of a BT-based virus in a certain range for evaluating the effect of an immunization strategy on virus propagation. Similar models have been used to describe computer virus propagation on the internet and on e-mail networks [28], [41]. Since mobile phones cannot be recovered by themselves, some external intervention strategies (e.g., individual operations and public security awareness as in our model), as shown in [10], are necessary for helping them recover.

The population in an SIR model is divided into disjoint compartments whose sizes change with time. Each compartment is labeled with one of three states: Susceptible (**S**: phones are prone to be infected), Infectious (**I**: phones have been infected), and Recovered (**R**: phones are recovered through antisoftware or human interventions). The dynamic process of viruses evolving in each tower is modeled in

$$\begin{cases} \dfrac{dS}{dt} = \beta * \dfrac{S}{N} * I \\ \dfrac{dI}{dt} = \beta * \dfrac{S}{N} * I - \gamma * I \\ \dfrac{dR}{dt} = \gamma * I, \end{cases} \tag{1}$$

where S, I, and R represent the numbers of phones with different states in each tower, respectively. $N = N_{tp}$ is the number of phones in each tower. Key parameters in an SIR model are the effective infection rate β and the recovery rate γ [35], where:

- The effective infection rate β as in our model is the same as in [7], 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 have a contact with each other. Specifically, ${<}K{>}$ is decided by the Bluetooth communication area and the population density inside a tower's service area. Briefly, we assume that phones in the same cell tower are homogeneous and can potentially contact each other (which may overestimate the damages of a BT-based virus). In our model, $u = 2$ based on [7] and ${<}K{>} = T_i.n_{tp}/(2 * T_i.r)^2$.
- The recovery rate (γ) depends on individual security awareness (represented as $1 - v_i.p_{click}$) and public security awareness (quantified by the recovery proportion η). If users have higher individual

[2] http://www.sleepfoundation.org/.

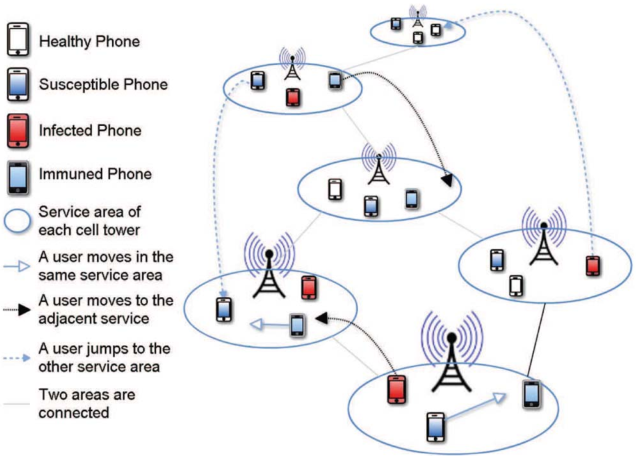

Healthy Phone
Susceptible Phone
Infected Phone
Immuned Phone
Service area of each cell tower
A user moves in the same service area
A user moves to the adjacent service
A user jumps to the other service area
Two areas are connected

Fig. 3. The mobility patterns of users in a geographical network, which can affect BT-based virus propagation.

security awareness (i.e., a small $v_i.p_{click}$), they will less likely open infected messages, and more likely recover their phones. Meanwhile, the higher the public security awareness, the larger the recovery proportion will become.

We can now measure the propagation dynamics of a BT-based virus in a mobile network. More importantly, given the different initial conditions (e.g., individual and public security awareness on BT-based viruses), we can estimate different evolution scenarios. Fig. 8 in Section 4 and [36, Fig. 7] show some experimental results.

3.3.2 Human Mobility

Although we have used a homogenous model to simulate BT-based virus propagation in each tower, users' different traveling patterns will cause different dynamic spreading processes. Several studies have found that users' traveling patterns play a key role in virus propagation [42], [43], similar to contact-based epidemics (e.g., SARS) in humans [26], [44]. Fig. 3 shows three mobility patterns of users. The more accurate the mobility patterns of users are, the better predicting results about virus propagation will be. Based on existing studies, four characteristics of mobility have been observed from the real-world data:

- The traveling distances of a user follow a truncated power-law distribution [11], [19], [30], [45];
- People move with a probability at each time [7];
- People trend to devote most of the time to only a few locations in their daily life where they can meet a lot of other people [11], [18];
- Intercontact times (i.e., the time elapsed between two consecutive contacts of the same two phones) follow a power-law distribution [19], [46].

Based on the above statistical findings, a user will have three basic characteristics at a given time in our model:

1. **Whether or not a user moves at a given hour.** Users do not always move. Recurrent mobile behaviors are unique to human mobility. Wang et al. have proposed a moving probability, $P(t)$, by analyzing the real mobile data traces [7]. Thus, in our model, the moving probability of each user at a given hour follows $P(t)$ based on [7], as shown in [36, Fig. 5].

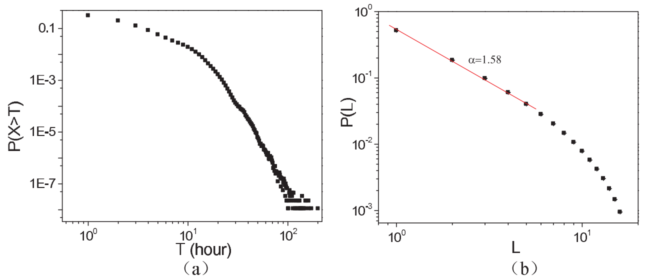


Fig. 4. (a) The distribution of intercontact times of over all users in our model. (b) The average frequency of visited Lth places in our model.

2. **Users' return to visited places at the next time.** Users would return to some fixed positions (home or workplace), where they can be found most of the time. The probability of finding a user at the Lth location with a given rank L is well approximated by $P(L) \sim 1/L$ [11], which is independent of the number of locations visited by the user.
3. **Traveling distances of a user at the next time.** Gonzalez et al. have found that the distribution of traveling distances over all users is well approximated by a power-law distribution [11]. Two functions are used in our model to generate the distribution of traveling distances; they are: a levy flight process and a power function. The distribution exponent of the two functions is 1.75 ± 0.15 based on [11]. The distributions of distance exponents over all users are shown in [36, Fig. 4].

Based on the above analysis, a user in our model can: 1) stay at the current place and not move at the time t based on $P(t)$; 2) return to the Lth visited place based on $P(L)$; 3) go to a new place based on different traveling distances. Algorithm 2 characterizes user's mobility behavior in a geographical network. More details are given in [36, Section II-C]. Based on this algorithm, the fourth characteristic of mobility, i.e., the intercontact times among phones in the real-world data traces follow a power-law distribution [18], [19], can be observed in Fig. 4a. Fig. 4b and [36, Fig. 6] show the average frequencies of visited Lth places. The results indicate that average frequencies are independent of traveling distances and the number of locations visited by users.

Algorithm 2. Human_Mobility($step$)
Input: The position of users in Grid
Output: A new position at the next time step

```
for each phone $v_i$ do
  if rand()< $MovingProb[step]$ then
    $visited\_place = int(1/rand())$;
    if $v_i.PosFrequency[visited\_place][0] > 0$ then
      $v_i$ returns to a visited place based on $P(L)$in [7];
      $v_i$. $PosFrequency\ [visited\_place][0]$++;
    else
      $v_i$ goes to a new place;
      $v_i.PosFrequency\ [newplace][0]$++;
  else
    $v_i$ stays at the current place;
    $v_i$. $PosFrequency\ [visited\_place][0]$++;
  Sort_PosFrequency($v_i$);
```

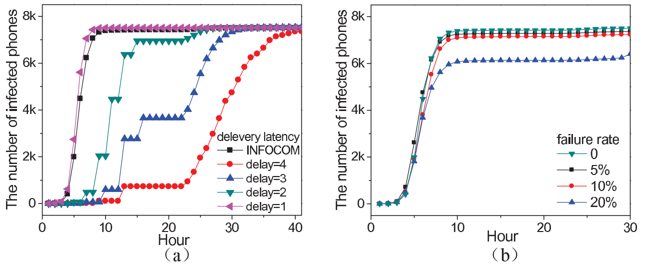


Fig. 5. The effects of (a) message delivery latency and (b) delivery failure rate on SMS-based virus propagation.

Algorithm 1 outlines the process of virus propagation. More details are presented in [36, Section II-C]. In our model, we integrate the traditional population-based epidemic model (i.e., SIR model) with the individual-based simulation to observe the effects of human mobility and operational behavior on the virus propagation dynamics.

4 Simulation Results

In this section, we describe several experiments that are aimed to uncover some key factors that affect virus propagation. Initially, we randomly select two phones from a network as the infected phones in order to simulate a multiple-seed attack that is likely to occur in the real world. All experimental results are average values over 10 simulation runs.

Section 4.1 presents two experiments to analyze the effects of short messages states (i.e., the delivery latency and failure rate) and users' own security awareness on SMS-based virus propagation. Section 4.2 evaluates the effects of users' operational patterns and mobility patterns on BT-based virus propagation.

4.1 SMS-Based Virus Propagation

Fig. 5 shows the effects of message delivery latency and failure rate (as mentioned in Section 3.2) on SMS-based virus propagation. The parameter of "INFOCOM" in Fig. 5a means that 5 percent of delivered messages have a latency longer than 1 hour [40]. While, other delay times in Fig. 5a are constant. The results show that a long delivery latency can affect the propagation *speed* (i.e., postpone the outbreak of virus propagation, just as the throttling technique [41] in computer networks), but cannot restrain the propagation *scope* (i.e., reduce the final number of infected phones). However, appropriately increasing the delivery failure rate, as shown in Fig. 5b, can restrain virus propagation in terms of both propagation speed and scope.

Fig. 6 shows the effect of users' security awareness on SMS-based virus propagation. The results indicate that if users' security awareness is higher (i.e., μ is smaller), the propagation scope will become smaller (i.e., the number of infected phones are smaller). Therefore, it will be useful to send security notifications to more users in order to improve their security awareness about mobile viruses. At the moment, there are two approaches to improving users' security awareness: one is to provide more public campaigns on the risks of mobile viruses to users, and the other is to provide pop-up warning messages when users are about to open or install some new files [22].

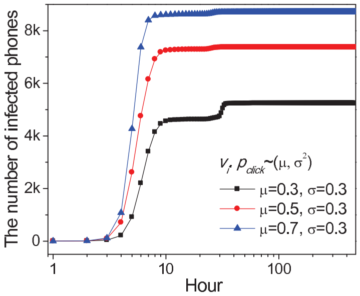


Fig. 6. The effect of individual security awareness on SMS-based virus propagation (semilog scale).

In this work, we do not consider the effect of network topology on SMS-based virus propagation. That is because the propagation process of SMS-based viruses is similar to the spreading of e-mail worms. We have provided additional comparative results and explanations about the topological effects on the e-mail worm propagation in [6].

4.2 BT-Based Virus Propagation

Human mobility patterns, as analyzed in Section 3.3, play a key role in BT-based virus propagation. In order to observe the effects of mobility patterns on BT-based virus propagation, we first utilize an SI model [27] to depict the propagation dynamics of a BT-based virus. Fig. 7a compares the effect of traveling distances on BT-based virus propagation. The traveling distances of a user are generated by a power function, a levy flight process and a random walk, respectively. Besides traveling distances, Fig. 7b incorporates more mobility patterns (such as the moving probability at a given hour, the probability of a user returning to a visited place) into our model.

Comparing Figs. 7a and 7b, it is interesting to find that the power-law traveling distances can accelerate BT-based virus propagation under the scenario that users are only different from each other in their traveling distances. However, if other three mobility characteristics, as introduced in Section 3.3.2, are incorporated into the human mobility pattern, more phones will be infected by BT-based viruses. That is because an infected phone can contact only one geographical neighbor within the service area through Bluetooth at a time. Therefore, the longer the intercontact time users have, the more viruses will spread. Although the traveling distances of a levy flight pattern also follow a heavy-tail distribution, users can frequently visit more

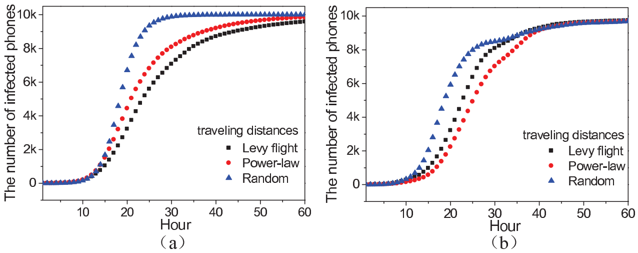


Fig. 7. The effects of mobility patterns on BT-based virus propagation. (a) The traveling distances follow different patterns. (b) Four characteristics (as shown in Section 3.3.2) are used to characterize human mobility patterns.

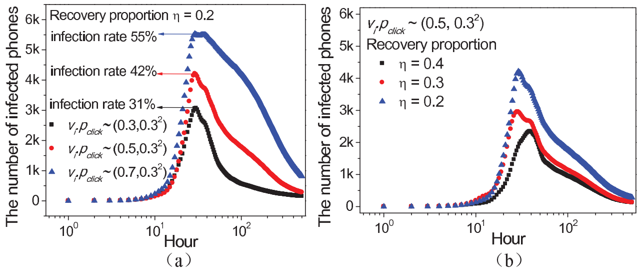


Fig. 8. The effects of recovery rate (γ) on BT-based virus propagation (semilog scale). The traveling distances are generated by the levy flight process.

places near their homes or workplaces where they can meet a lot of other people.

The recovery rate (γ) in the BT-based propagation model depends on the individual and public security awareness. Here, the individual security awareness is quantified by $1 - v_i{\cdot}p_{click}$, i.e., a user v_i with higher security awareness will have a smaller $v_i{\cdot}p_{click}$. On the other hand, the public security awareness is quantified by the recovery proportion η. With the same public security awareness (i.e., the same η in Fig. 8a), users with higher 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, as shown in [36, Fig. 7]). When the public security awareness (i.e., η) is improved in Fig. 8b, the resilience of the whole network for virus propagation can be strengthened. Therefore, it is important to improve users' risk awareness about viruses through public security education or warning messages as shown in [22].

The spatial pattern of mobile virus propagation is shown by [36, Fig. 8]. The propagation scope and speed of an SMS-based virus in a geographical network is larger and higher than that of a BT-based virus. That is because a BT-based virus can ripple out and infect one geographical neighbor at a time, whereas an SMS-based virus can simultaneously send its copies to all friends' phones (that may geographically locate at anywhere) based on the address book of the infected phone. For example, when $T = 10$ in [36, Fig. 8], SMS-based viruses have already spread all over a geographical network; whereas BT-based viruses only propagate in two local regions. Therefore, the security patch should be immediately sent through SMS in order to efficiently restrain mobile virus propagation.

The above sections have analyzed the propagation dynamics of SMS-based and BT-based viruses in a two-layer network propagation model. Based on this model, the next section will describe two strategies to restrain virus propagation.

5 Countermeasures against Mobile Viruses

Based on our analysis, a smart phone can avoid a BT-based attack by turning off the Bluetooth service. However, SMS-based viruses often propagate through the trust relationships among friends. Previous experiments also show that SMS-based viruses are more dangerous than BT-based viruses in terms of propagation speed and scope. In this section, we describe two strategies to restrain SMS-based virus propagation. Section 5.1 describes a preimmunization strategy based on the methodology of AOC [23], [24], which can effectively reduce the number of infected users in e-mail networks [25]. Section 5.2 presents an adaptive dissemination strategy by adjusting the search behavior of *autonomous entities* in the preimmunization strategy, which can disseminate security notifications or patches to as many phones as possible in mobile networks with a relatively lower communication redundancy.

All experiments in this section are based on the SMS-based propagation model as shown in Section 3.2. The message-clicking probabilities among users follow $v_i{\cdot}p_{click} \sim (0.5, 0.3^2)$. The parameters of message delivery latency and failure are the same as the settings in [40].

5.1 Preimmunization Strategy

Recently, one of the commonly adopted methods for restraining virus propagation is network immunization, which cuts epidemic paths by preimmunizing a set of nodes from a network following some defined rules. The immunized nodes are selected to protect computers or social networks based on the measurements of degree [47], [48] or betweenness [6], [34]. Some strategies have been proposed to restrain virus propagation by dividing a mobile network into small clusters [15], [21]. However, it would be difficult for these strategies to deal with large-scale, decentralized and/or highly dynamic networks [25].

This section examines the performance of the AOC-based preimmunization strategy, which has been described earlier in [25], in restraining SMS-based virus propagation. In order to cut the epidemic path and reduce the infection rate as low as possible, the AOC-based preimmunization strategy selects a group of phones, with the highest degrees and larger transmission capabilities in a mobile network, for protection (e.g., patching). Furthermore, we evaluate the robustness and scalability of the AOC-based preimmunization strategy in [25] and show how it works with large-scale and/or highly dynamic mobile networks.

In the real world, different companies may release security patches at different time because of the response delays for new viruses. Therefore, different from our previous work in [25], the AOC-based preimmunization strategy will be deployed into a network at different times. The deployment delay determines when security patches are distributed to the selected phones based on our strategy. Fig. 9 shows that the shorter the deployment delay, the smaller the number of infected phones will be. This result suggests that security software companies should improve their abilities to detect viruses and release patches as fast as possible. Fig. 10 compares the number of immunized phones with respect to the total number of infected phones. The experimental results show that the propagation of mobile viruses can be restrained by patching a small set of phones. Furthermore, Fig. 10b shows that there exists a critical number of immunized phones, at which viruses almost cannot spread. That is because a certain number of immunized phones can divide the whole network into small blocks and cut the epidemic paths, and then restrain virus propagation. However, if the preimmunization is deployed into a network later (e.g., H = 10), it would not be

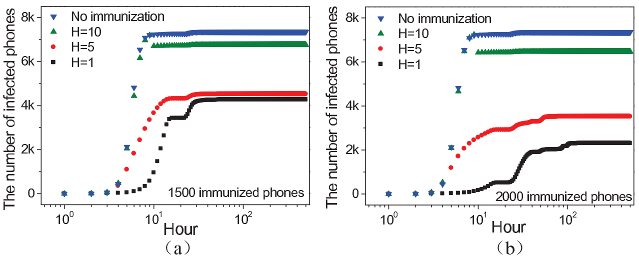


Fig. 9. The effect of the AOC-based preimmunization deployment time (H) on virus propagation.

able to protect the whole network. In view of this, we present a new dissemination strategy in the next section that further mitigates the damages of viruses in a mobile network where virus outbreaks occur.

5.2 Patch Dissemination Strategy

Section 5.1 has introduced a preimmunization to protect networks before virus propagation. However, in reality, we detect certain viruses and then allocate patches or antivirus programs into networks only after these viruses have already propagated (e.g., Melissa). Due to the network bandwidth constrains, the security notifications or patches cannot be sent to all users simultaneously. Therefore, we propose an adaptive dissemination strategy based on the methodology of AOC in order to efficiently send security notifications or patches to most of phones with a relatively lower communication cost.

5.2.1 A Description of Our Strategy

The AOC-based preimmunization strategy that we have described in the preceding section is to search a set of the highly connected phones with large communication capacities in a mobile network (i.e., a **distributed constraint search problem**). On the other hand, the AOC-based dissemination strategy that we will discuss below is concerned with how to route security notifications or patches to as many phones as possible with a relatively lower communication cost and a higher coverage rate (i.e., a **route selection problem**). Initially, we only deploy a few dissemination entities into a mobile network. Each entity with the security patch will be first routed to the highly connected phones based on the local information in order to efficiently disseminate the security notification to other phones. Additional definitions to expatiate our strategy is provided by [36, Section III-A].

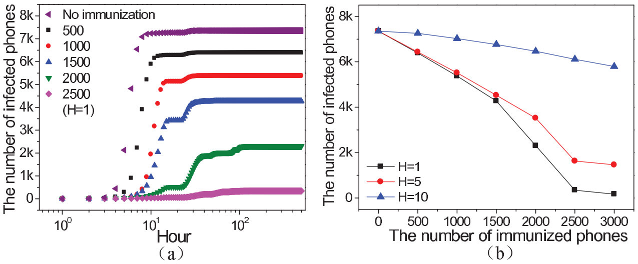


Fig. 10. (a) The number of immunized phones with respect to virus propagation when the AOC-based preimmunization is deployed into the network at H = 1. (b) The relationship between the number of immunized phones and the number of infected phones.

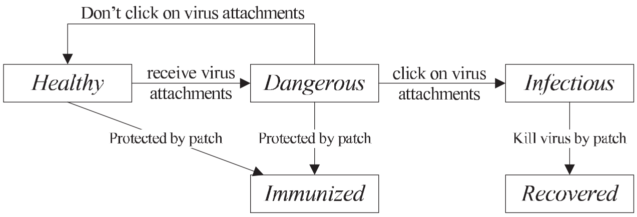


Fig. 11. The state transition of smart phones in the AOC-based dissemination strategy.

Different from the moving behavior of immunization entities in [25], a dissemination entity will still move to another nonresided highly connected neighbor (i.e., this neighbor is not resided before) at the next time step even though it has already resided in the highest degree phone in a network. Fig. 11 introduces the state transition of phones in the face of SMS-based viruses:

- If a phone receives a message with a virus-embedded attachment, it is likely to be infected, i.e., *Healthy* → *Dangerous*;
- If a phone has received an infected message, there are two types of operational behavior: the user of this phone does not open the infected message, *Dangerous* → *Healthy*; or open it, *Dangerous* → *Infectious*;
- The autonomous entities are deployed into a network for distributing patches to phones. If an infected phone receives the patch, it will recover from the infected state, i.e., *Infectious* → *Recovered*. If a phone is in *Healthy* or *Dangerous* state, the patch will protect the phone from the attacks of viruses, i.e., *Dangerous* → *Immunized*, *Healthy* → *Immunized*.

Fig. 12 shows the dissemination process of autonomous entities in our strategy. The AOC-based dissemination strategy can forward the security patch to more phones with a few forward requests. The detailed formulation of the AOC-based dissemination strategy, including the notions of autonomous entities, local environments, and behaviors is presented by [36, Section III-B]. The main behaviors of entities in the AOC-based dissemination strategy are as follows:

1. *Rational_move*: An entity moves to a nonresided phone with the highest degree in its local environment. In the previous AOC-based preimmunization strategy, if an immunizing entity resides in the highest degree phone in its local environment, it will not move any more [25]. However, even if a dissemination entity has found and resided in the highest degree phone in its local environment, it will continue to move to the nonresided highest degree neighbor at the next time step. If there exist more than one nonresided highestdegree neighbors, the entity will choose the first one from its friend list.
2. *Random_jump*: An entity moves along the edges with a randomly determined number of steps in order to avoid getting stuck in local optima.
3. *Wait*: If an entity does not find any available phone for residing in, it will stay at the current position.

Taking Fig. 12a as an example, two entities e_1 and e_2 are randomly deployed into a mobile network. They initially

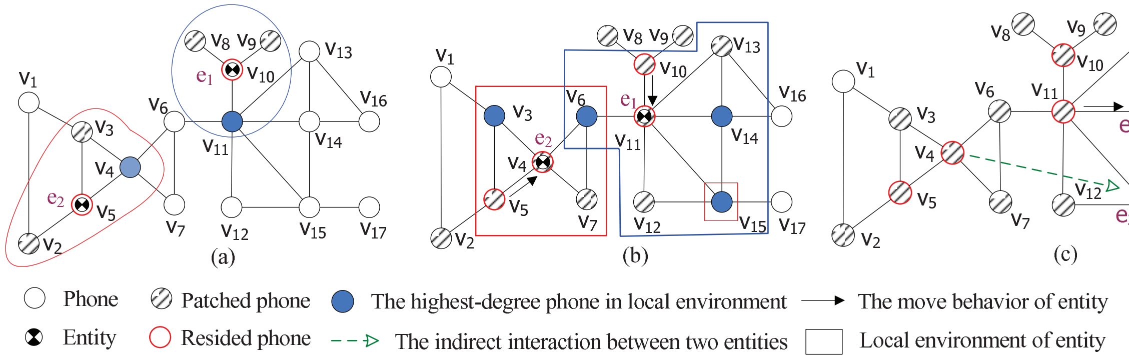

v1
v2
v3
v4
v5
v6
v7
v8
v9
v10
v11
v12
v13
v14
v15
v16
v17
e1
e2
(a)
(b)
(c)
○ Phone
▨ Patched phone
● The highest-degree phone in local environment
→ The move behavior of entity
Entity
○ Resided phone
- - ▷ The indirect interaction between two entities
□ Local environment of entity

Fig. 12. An example of the AOC-based dissemination strategy. The aim of the AOC-based dissemination strategy is to route security notifications to more phones in order to protect them from virus attacks or help them recover.

reside in v_{10} and v_5, respectively. Entities first send security patches to their neighbors (i.e., $\{v_8, v_9, v_{11}\}$ and $\{v_2, v_3, v_4\}$). Then, the entities will move to the highest degree phones, which have not been resided before (i.e., the nonresided highest degree phones), in their own local environments, i.e., e_1 and e_2 move from v_{10} and v_5 to v_{11} and v_4, respectively. After that, although e_1 resides in the highest degree phone (i.e., v_{11}) in a network, it will continue to move to the first nonresided highest degree phone in its local environment (i.e., v_{14}) as shown in Fig. 12c. We define an indirect interaction among autonomous entities in [25]. More importantly, the nonlinear self-organized computing emerges from indirect interactions among entities based on their shared local environment. For example, e_2 can search remote phones (i.e., v_{15}) based on the shared environment (i.e., v_6) with e_1 in Fig. 12b. Finally, autonomous entities can move to other nonresided highly connected phones and send patches to more neighboring phones with a lower communication redundancy. We provide additional explanations and examples in [36, Section III-B] and [25].

In order to evaluate the efficiency of the AOC-based dissemination strategy, some measurements are defined as follows:

Coverage rate is defined as $N_{patched}/N$, where $N_{patched}$ represents the total number of visited phones that are patched by autonomous entities, and N represents the total number of phones in a network.

Communication cost is defined as $M_{packets}/R_{num}$, where $M_{packets}$ is the total number of security notifications or patches that are forwarded by entities. R_{num} is the number of resided phones. Autonomous entities can send notifications or patches from resided phones to their direct neighbors.

Entity steps are the average moving steps of an entity, as defined in [25].

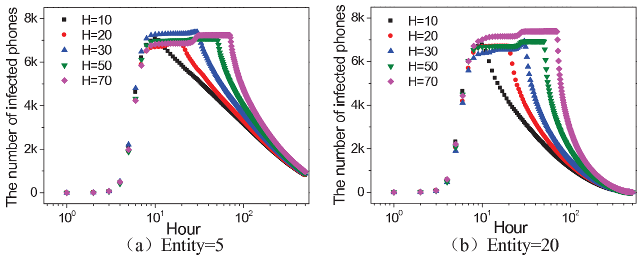
5.2.2 Static Networks

An effective dissemination strategy can forward security notifications or patches to more phones with a lower computational redundancy (i.e., a higher *coverage rate* and a lower *communication cost* defined in the last section). In this section, we utilize some static networks, including synthetic and benchmark networks, to evaluate the efficiency of the AOC-based dissemination strategy.

We first use the previous synthetic network, as shown in [36, Fig. 3a], to evaluate whether our strategy can efficiently disseminate patches to phones and restrain virus propagation. We deploy five and 20 entities into this network at different times ($\mathrm{H} = 10, 20,$ etc.). Fig. 13 shows that the earlier the patch is disseminated, the shorter the propagation duration will be. Meanwhile, we deploy different numbers of dissemination entities at the same time. Fig. 14 shows that the more dissemination entities are deployed, the more efficiently the virus propagation will be restrained.

In the following, we use some benchmark networks (i.e., the coauthorship network,[3] university e-mail network,[4] and autonomous system network[5]) to reflect the topological structures of social relationships in the real world. The cumulative degree distribution of three benchmark networks and the structure of a synthetic community-based network is shown by [36, Fig. 10]. Fig. 15 and [36, Fig. 11] show that the AOC-based dissemination can overcome the network topological challenges and distribute security patches to smart phones, and thus efficiently restrain SMS-based virus propagation.

When an autonomous entity arrives at a phone, it will disseminate security patches to all neighbors of this phone. Therefore, a phone may receive the same patch from different neighbors more than once. A good dissemination strategy would reduce such dissemination redundancy, and thus mitigate the burden of network communications. In the following, we compare the efficiency of our AOC-based dissemination strategy with one typical search strategy, i.e., flooding, with respect to the measurements of *coverage rate* and *communication cost*.

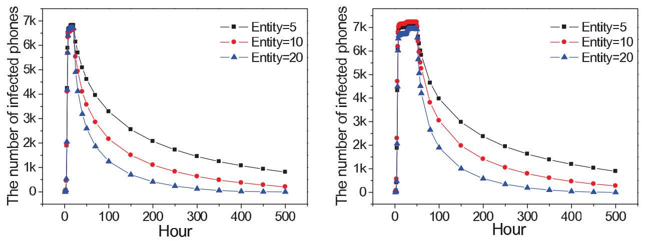


(a) Entity=5

(b) Entity=20

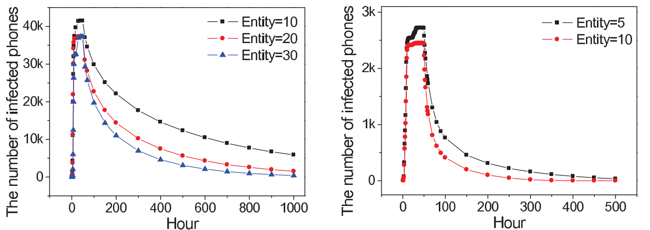
Fig. 13. The effect of deployment time on SMS-based virus propagation.

[3] http://www-personal.umich.edu/mejn/netdata/astro-ph.zip.
[4] http://deim.urv.cat/~aarenas/data/welcome.htm.
[5] http://routeviews.org/.



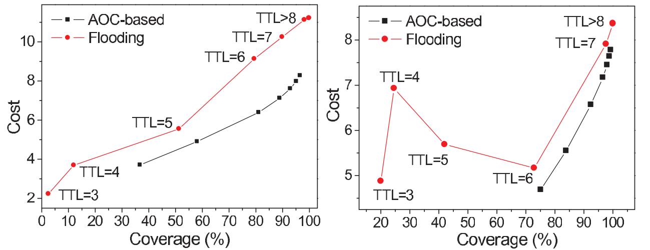
(a) H=20 (b) H=50

Fig. 14. The number of dissemination entities with respect to SMS-based virus propagation.



(a) Coauthorship network structure (b) Community-based network structure

Fig. 15. The effect of dissemination entities on SMS-based virus propagation in the coauthorship network and the synthetic community-based network (H = 50).

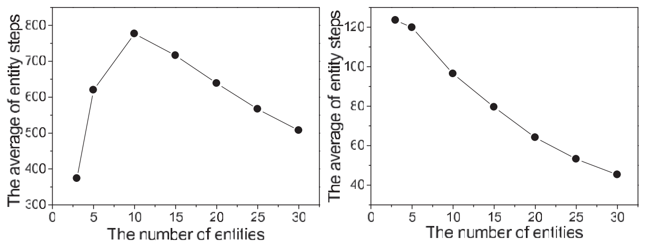


(a) Coauthorship network structure (b) Community-based network structure

Fig. 16. The change of computational cost with respect to coverage rate in the coauthorship network and the synthetic community-based network.

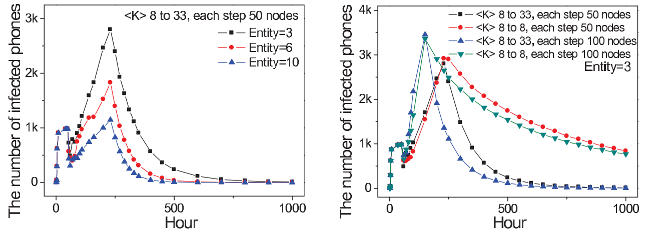
Flooding is a typical technology in the field of network search. It forwards patches from a source phone to all its direct neighbors. Then, these neighbors forward patches to all of their direct neighbors. Therefore, flooding will cause overloaded traffic in a network. In order to overcome this shortcoming, the time-to-live (TTL) is used to reduce the network traffic. However, this strategy is sensitive to the initial setting (i.e., the length of TTL). That is, the longer TTL will result in communication redundancy, whereas the shorter TTL will reduce *coverage rate* and be not suitable for large-scale networks.

We have conducted some experiments to compare the *coverage rate* and *communication cost* of the AOC-based dissemination strategy and flooding in static networks. The experimental results are shown in Fig. 16 and [36, Fig. 12]. From these results, we find that the AOC-based dissemination strategy can reach the same *coverage rate* with a lower *communication cost*. Furthermore, entities in our strategy can disseminate security patches to more phones with a few steps. The explanations about the *infection point* in Fig. 17 (including [36, Fig. 13]) are given in [25]. That is, when an adequate number of entities is reached, the efficiency of the AOC-based dissemination strategy can nonlinearly grow based on the indirect interactions among entities.



(a) Coauthorship network structure (b) Community-based network structure

Fig. 17. The number of moving steps of entities with respect to the number of entities.



(a) (b)

Fig. 18. The effect of the AOC-based dissemination entities on virus propagation in dynamically-evolving networks. The network scale increases from 10^3 to 10^4. (a) the average degree grows from 8 to 33 and 50 phones are added into the network at each step. (b) there are three entities in the network.

From the above results and the extended experiments (as shown in Fig. 12 and [36, Fig. 13]), we conclude that the AOC-based dissemination strategy can improve the search coverage with a relatively lower communication cost through the emergent computing ability, as realized by the mechanisms of self-organization and positive feedback [25].

5.2.3 Dynamically Evolving Networks

In the real world, the structure of a network can dynamically change all the time. In order to evaluate whether the AOC-based dissemination strategy can restrain virus propagation in such a network, we construct some dynamically evolving networks based on GLP algorithm [49]. The initial network has 10^3 phones with $\alpha_{CDF} = 2.20$ and $<K> = 8$. As shown in [36, Table 1], a network could have different patterns of evolving: 1) the network scale will grow to 10^4 or $3 * 10^4$; 2) 50 or 100 phones are added into the network at each step from 50 hours; 3) the network degree, $<K>$, will remain unchanged or change from 8 to 33, respectively. The cumulative degree distribution of evolving networks at different times is shown by [36, Fig. 14].

We have carried out further experiments to analyze how network evolution affects the propagation dynamics of a mobile virus. Fig. 18 (including Fig. 15 and [36, Fig. 16]) compares the impact of the number of entities on virus propagation. From these figures, we find that the AOC-based strategy can efficiently protect mobile networks from the potential damages of SMS-based viruses no matter how a network evolves. If an evolving network generate more links (i.e., increasing $<K>$), the AOC-based dissemination strategy will more efficiently restrain virus propagation. In reality, a social contact network may change during the outbreak of a virus or an epidemic [50]. If more people are informed about the risk of viruses through public campaigns, virus propagation will more likely be suppressed.

6 Conclusion

In this paper, we have presented a two-layer network model for simulating and analyzing the propagation dynamics of SMS-based and BT-based viruses. Our model characterizes two types of human behavior, i.e., operational behavior and mobile behavior, in order to observe and uncover the propagation mechanisms of mobile viruses. Our simulation-based studies have contributed to the understanding of interactions between human behaviors and the propagation dynamics of mobile viruses. As has been shown in our experimental results, it would be helpful to send security notifications to as many users as possible in order to improve their security awareness, which can in turn play a key role in restraining virus propagation. Meanwhile, our simulation results have shed light on the effects of human mobility on BT-based virus spreading, in terms of infection dynamics and spatially localized spreading patterns.

Based on our proposed two-layer network model, we have examined two strategies for controlling SMS-based virus propagation that are based on the methodology of AOC. As revealed in our experimental results, the AOC-based preimmunization strategy is capable of restraining mobile virus propagation by protecting some highly connected phones, whereas the AOC-based dissemination strategy can forward security notifications or patches to as many phones as possible with a low communication cost in order to help them recover or avoid the potential damages of mobile viruses. Our experimental results have also indicated that our strategies can restrain virus propagation in a large-scale, dynamically evolving, and/or community-based network.

As for our future work, we will investigate the hybrid viruses that propagate through both BT and SMS channels [8]. Some assumptions about human mobility and operational patterns in this paper have been based on some empirical studies and statistical data. In our next step, we will extend our model to incorporate additional characteristics of human mobility and operations. In particular, our future computational model will consider the dynamic changes of users' behaviors in the course of mobile virus propagation.

Acknowledgments

The authors would like to thank the Associate Editor and the anonymous reviewers for their constructive comments and suggestions. The research reported in this paper was supported by a Hong Kong Research Grants Council (RGC) grant (210508), Hong Kong Baptist University (HKBU) faculty research grants (FRG2/09-10/036 and FRG2/10-11/110), and in part by the Natural Science Foundation of CQ CSTC (cstc2012jjA40013 and cstc2012jjB40012). Prof. Jiming Liu is the corresponding author of this paper.

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,* vol. 108, no. 4, pp. 478-494, 2008.

[2] H. Kim, J. Smith, and K.G. Shin, "Detecting Energy-Greedy Anomalies and Mobile Malware Variants," *Proc. Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys 08),* pp. 239-252, 2008.

[3] L. Xie, H. Song, T. Jaeger, and S. Zhu, "A Systematic Approach for Cell-Phone Worm Containment," *Proc. 17th Int'l World Wide Web Conf. (WWW '08),* pp. 1083-1084, 2008.

[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," *Proc. Second ACM Conf. Wireless Network Security (WiSec '09),* pp. 69-78, 2009.

[5] G. Yan and S. Eidenbenz, "Modeling Propagation Dynamics of Bluetooth Worms (Extended Version)," *IEEE Trans. Mobile Computing,* vol. 8, no. 3, pp. 353-368, Mar. 2009.

[6] C. Gao, J. Liu, and N. Zhong, "Network Immunization and Virus Propagation in Email Networks: Experimental Evaluation and Analysis," *Knowledge and Information Systems,* vol. 27, no. 2, pp. 253-279, 2011.

[7] 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, 2009.

[8] S. Cheng, W.C. Ao, P. Chen, and K. Chen, "On Modeling Malware Propagation in Generalized Social Networks," *IEEE Comm. Letters,* vol. 15, no. 1, pp. 25-27, Jan. 2011.

[9] P. De, Y. Liu, and S.K. Das, "An Epidemic Theoretic Framework for Vulnerability Analysis of Broadcast Protocols in Wireless Sensor Networks," *IEEE Trans. Mobile Computing,* vol. 8, no. 3, pp. 413-425, Mar. 2009.

[10] P. De, Y. Liu, and S.K. Das, "Deployment Aware Modeling of Node Compromise Spread in Wireless Sensor Networks Using Epidemic Theory," *ACM Trans. Sensor Networks,* vol. 5, no. 3, pp. 1-33, 2009.

[11] M.C. Gonzalez, C.A. Hidalgo, and A.L. Barabasi, "Understanding Individual Human Mobility Patterns," *Nature,* vol. 453, no. 7196, pp. 779-782, 2008.

[12] C.C. Zou, D. Towsley, and W. Gong, "Modeling and Simulation Study of the Propagation and Defense of Internet E-Mail Worms," *IEEE Trans. Dependable and Secure Computing,* vol. 4, no. 2, pp. 105-118, Apr.-June 2007.

[13] L. Xie, X. Zhang, A. Chaugule, T. Jaeger, and S. Zhu, "Designing System-Level Defenses against Cellphone Malware," *Proc. IEEE 28th Int'l Symp. Reliable Distributed Systems (SRDS '09),* pp. 83-90, 2009.

[14] A. Bose, X. Hu, K.G. Shin, and T. Park, "Behavioral Detection of Malware on Mobile Handsets," *Proc. Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '08),* pp. 225-238, 2008.

[15] F. Li, Y. Yang, and J. Wu, "CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-Based Mobile Networks," *Proc. IEEE INFOCOM,* pp. 2811-2819, 2010.

[16] G. Zyba, G.M. Voelker, M. Liljenstam, A. Mehes, and P. Johansson, "Defending Mobile Phones from Proximity Malware," *Proc. IEEE INFOCOM,* pp. 1503-1511, 2009.

[17] P. Wang and M.C. Gonzalez, "Understanding Spatial Connectivity of Individuals with Non Uniform Population Density," *Philosophical Trans. Royal Soc. A,* vol. 367, no. 1901, pp. 3321-3329, 2009.

[18] A. Mei and J. Stefa, "SWIM: A Simple Model to Generate Small Mobile Worlds," *Proc. IEEE INFOCOM,* pp. 2106-2113, 2010.

[19] K. Lee, S. Hong, S.J. Kim, I. Rhee, and S. Chong, "SLAW: A Mobility Model for Human Walks," *Proc. IEEE INFOCOM,* pp. 855-863, 2009.

[20] C. Song, T. Koren, P. Wang, and A.-L. Barabasi, "Modelling the Scaling Properties of Human Mobility," *Nature Physics,* vol. 6, no. 10, pp. 818-823, 2010.

[21] Z. Zhu, G. Cao, S. Zhu, S. Ranjan, and A. Nucci, "A Social Network Based Patching Scheme for Worm Containment in Cellular Networks," *Proc. IEEE INFOCOM,* pp. 1476-1484, 2009.

[22] E.V. Ruitenbeek and F. Stevens, "Quantifying the Effectiveness of Mobile Phone Virus Response Mechanisms," *Proc. 37th Ann. IEEE/IFIP Int'l Conf. Dependable Systems and Networks (DSN '07),* pp. 790-800, 2007.

[23] J. Liu, "Autonomy-Oriented Computing (AOC): The Nature and Implications of a Paradigm for Self-Organized Computing," *Proc. Fourth Int'l Conf. Natural Computation (ICNC '08),* pp. 3-11, 2008.

[24] J. Liu, X. Jin, and K.C. Tsui, *Autonomy Oriented Computing (AOC): From Problem Solving to Complex Systems Modeling.* Kluwer, 2005.

[25] C. Gao, J. Liu, and N. Zhong, "Network Immunization with Distributed Autonomy-Oriented Entities," *IEEE Trans. Parallel and Distributed Systems,* vol. 22, no. 7, pp. 1222-1229, July 2011.
[26] P. Bajardi, C. Poletto, J. Ramasco, M. Tizzoni, V. Colizza, and A. Vespignani, "Human Mobility Networks, Travel Restrictions, and the Global Spread of 2009 H1N1 Pandemic," *PLos One,* vol. 6, no. 1, p. e16591, 2011.
[27] R. Pastor-Satorras and A. Vespignani, "Epidemic Spreading in Scale-Free Networks," *Physical Rev. Letters,* vol. 86, no. 14, pp. 3200-3203, 2001.
[28] M.E.J. Newman, "The Spread of Epidemic Disease on Networks," *Physical Rev. E,* vol. 66, no. 1, p. 016128, 2002.
[29] C. Song, Z. Qu, N. Blumm, and A.-L. Barabasi, "Limits of Predictability in Human Mobility," *Science,* vol. 327, no. 5968, pp. 1018-1021, 2010.
[30] I. Rhee, M. Shin, S. Hong, K. Lee, and S. Chong, "On the Levy Walk Nature of Human Mobility," *Proc. IEEE INFOCOM,* pp. 924-932, 2008.
[31] W. Hsu, T. Spyropoulos, K. Psounis, and A. Helmy, "Modeling Time-Variant User Mobility in Wireless Mobile Networks," *Proc. IEEE INFOCOM,* pp. 758-766, 2007.
[32] C. Fleizach, M. Liljenstam, and P. Johansson, "Can You Infect Me Now? Malware Propagation in Mobile Phone Networks," *Proc. ACM Workshop Recurring Malcode (WORM '07),* pp. 61-68, 2007.
[33] J. Cheng, S.H.Y. Wong, H. Yang, and S. Lu, "Smartsiren Virus Detection and Alert for Smartphones," *Proc. Fifth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '07),* pp. 258-271, 2007.
[34] P. Holme, B.J. Kim, C.N. Yoon, and S.K. Han, "Attack Vulnerability of Complex Networks," *Physical Rev. E,* vol. 65, no. 5, p. 056109, 2002.
[35] C. Gao and J. Liu, "Modeling and Predicting the Dynamics of Mobile Virus Spread Affected by Human Behavior," *Proc. IEEE 12th Int'l Symp. a World of Wireless, Mobile and Multimedia Networks (WoWMoM '11),* pp. 1-9, 2011.
[36] C. Gao and J. Liu, "Modeling and Restraining Mobile Virus Propagation (Supplementary File)," *IEEE Trans. Mobile Computing,* 2013.
[37] M. Seshadri, S. Machiraju, A. Sridharan, J. Bolot, C. Faloutsos, and J. Leskovec, "Mobile Call Graphs: Beyond Power-Law and Lognormal Distributions," *Proc. 14th ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD '08),* pp. 596-604, 2008.
[38] 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 Comm. Networks," *Proc. Nat'l Academy of Sciences of USA,* vol. 104, no. 18, pp. 7332-7336, 2007.
[39] R.J. Herrnsteind and C. Murray, *The Bell Curve.* The Free Press, 1994.
[40] X. Meng, P. Zerfos, V. Samanta, S.H. Wong, and S. Lu, "Analysis of the Reliability of a Nationwide Short Message Service," *Proc. IEEE INFOCOM,* pp. 1811-1819, 2007.
[41] J. Balthrop, S. Forrest, M.E.J. Newman, and M.M. Williamson, "Technological Networks and the Spread of Computer Viruses," *Science,* vol. 304, no. 5670, pp. 527-529, 2004.
[42] L. Hufnagel, D. Brockmann, and T. Geisel, "Forecast and Control of Epidemics in a Globalized World," *Proc. Nat'l Academy of Sciences of USA,* vol. 101, no. 42, pp. 15124-15129, 2004.
[43] D. Balcan, V. Colizza, B. Goncalves, H. Hu, J. Ramasco, and A. Vespignani, "Multiscale Mobility Networks and the Spatial Spreading of Infectious Diseases," *Proc. Nat'l Academy of Sciences of USA,* vol. 106, no. 51, pp. 21484-21489, 2009.
[44] D. Balcan and A. Vespignani, "Phase Transitions in Contagion Processes Mediated by Recurrent Mobility Patterns," *Nature Physics,* vol. 7, no. 7, pp. 581-586, 2011.
[45] D. Brockmann, L. Hufnagel, and T. Geisel, "The scaling Laws of Human Travel," *Nature,* vol. 439, no. 7075, pp. 462-465, 2006.
[46] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, "Impact of Human Mobility on the Design of Opportunistic Forwarding Algorithms," *Proc. IEEE INFOCOM,* pp. 606-620, 2006.
[47] Y. Chen, G. Paul, S. Havlin, F. Liljeros, and H.E. Stanley, "Finding a Better Immunization Strategy," *Physical Rev. Letters,* vol. 101, no. 5, p. 058701, 2008.
[48] R. Cohen, S. Havlin, and D. Ben-Averaham, "Efficient Immunization Strategies for Computer Networks and Populations," *Physical Rev. Letters,* vol. 91, no. 24, p. 247901, 2003.
[49] T. Bu and D. Towsley, "On Distinguishing Between Internet Power Law Topology Generators," *Proc. IEEE INFOCOM,* pp. 638-647, 2002.
[50] S. Bansal, J. Read, B. Pourbohloul, and L.A. Meyers, "The Dynamic Nature of Contact Networks in Infectious Disease Epidemilogy," *J. Biological Dynamics,* vol. 4, no. 5, pp. 478-489, 2010.

Chao Gao received the PhD degree in computer science from the Beijing University of Technology in 2010. He is an associate professor with the College of Computer and Information Science, Southwest University, Chongqing, China. He is currently a postdoctoral research fellow in the Computer Science Department at Hong Kong Baptist University. His main research interests include autonomy-oriented computing, complex/social networks with applications to web intelligence, and social computing.

Jiming Liu received the BSc degree from East China Normal University, Shanghai, the MA degree from Concordia University, and the MEng and PhD degrees in electrical engineering from McGill University, Montreal. He is an associate dean (research) of science and chair professor of computer science at Hong Kong Baptist University. He was a professor and the director of School of Computer Science at the University of Windsor, Canada. Before 1994, he held full-time R&D positions at the Computer Research Institute of Montreal (CRIM), Virtual Prototypes, Inc. (VPI), and Knowledge Engineering Tech., Inc., in Canada. His current research focuses on complex systems modeling, complex networks, web intelligence, and multi-agent autonomy-oriented computing. He has contributed to the scientific literature in those areas. He received the President's Award for Outstanding Performance in Scholarly Work at HKBU in 2007 and was named an 2011 IEEE fellow for contributions to web intelligence and multi-agent autonomy-oriented computing. He has served as editor-in-chief of *Web Intelligence and Agent Systems*, associate editor of *IEEE Transactions on Knowledge and Data Engineering*, *IEEE Transactions on Systems*, *Man, and Cybernetics*, *Part B*, and *Computational Intelligence*, and editorial board member of several international journals. He is a chair of the IEEE Computer Society Technical Committee on Intelligent Informatics (TCII) and codirector of the Web Intelligence Consortium (WIC).