RESEARCH ARTICLE OPEN ACCESS

Modeling and Detaining the Mobile Virus Proliferation over Smartphone

Ashwini L. Gour*, Jagdish Pimple**
*(Department of Computer Science Engineering, RTMNU University, India
Email: ashwinigour90@gmail.com)
** (Department of Computer Science Engineering, RTMNU University, India
Email: pimplejagdish@gmail.com)

ABSTRACT
The Android operating system devices have been on the rise and the malware threat is expected to increase with the functionality enhancement of mobile phones. In a mobile network, viruses can cause privacy leakage, extra charges, battery power depletion, remote listening and accessing private short message and call history logs etc. Because of the potential damages of mobile viruses, it is important 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 installation of apps on a device. It addresses on the behaviors of virus propagation and restraining it and determining factors of virus propagation in mobile networks and analyzing the virus in the device. The presence of viruses in an application will be reported and hence, avoided by further users of the same app. Network immunization are the most effective techniques to restrain virus propagation in complex networks. We observe two strategies for avoid mobile virus propagation, i.e., Preimmunization and Adaptive Dissemination strategies represent on the methodology of Autonomy-Oriented Computing (AOC). By using the method it can automatically detect and delete virus before enter into the Smartphone operating system.

Keywords – Autonomy-oriented computing, human mobility, malwares, mobile networks, preimmunization.

I. Introduction

In recent years, the smart phones worldwide market has grown dramatically. Smartphone users perform many online tasks, including web browsing, document editing, multimedia streaming, Internet banking, and share the documents from one mobile to another through Bluetooth, SMS services and through social applications like whatsapp, facebook. Simultaneously, the increasing use of smartphones in life and business has been attracting the attention of malware writers, who aims to theft data confidentiality, integrity, and the ability to use handheld services. Examples of the most infamous threats to mobile phones include the Skull and Mabir worms, targeting at android phone applications. These are malware or viruses or cell-phone worms, which are malicious codes that act susceptibility in cell-phone software and spread in networks through current services such as Bluetooth and Short / Multimedia Messaging Service (SMS/MMS). A user can be automatically exciting for numerous SPAM messages generated by the worm and the phone battery will be quickly exhausted. Many studies reported the damages of mobile viruses [7], [8]. Other reported worm damages extend from robbery user data and privacy to destroying hardware.

This Malware can also be termed as all kind of intrusions that is disastrous to the computer software and hardware system. The malware is created by malware writers for different reasons and purposes ranging from challenges to productive commercial gain, destruction to punishment among others. Hence, its growth is tremendously alarming in volume and its expansion rate is also cannot be overlooked due to its damages. Through different media if once malware gets itself into the system like copying of files from external devices onto the system and mostly by downloading files from the internet, it checks the susceptibilities of the system and infects the system if the system is terrifically vulnerable. The involvement for the rate of malware spread today is a global paradox, especially as its spreading capacity is twice over the internet which is a means of global communication. Today's malware is capable of doing numerous things, such as: stealing and transmitting the contact list and other data, locking the device completely, giving criminals to access the system remotely, sending other devices unwanted SMS and MMS messages etc.

From year 2004 to 2008, the types of mobile malware have increased significantly in numbers. As of March 2008, FSecure has counted 401 varieties of mobile malware in the world, and McAfee has counted 475 kinds of mobile malware. Overall, in 2012 the number of known malicious samples for Android is more than eight times. Hence, the mobile malware various includes leaking of user privacy, extra service charges by automatically sending expensive multimedia messages or making long-distance calls, and battery power depletion.

Valid proliferation models can be used as test beds to:

1) Measure the scale of a malware outbreak before its occurrence in reality and

2) Check out new and/or improved remedies for governing virus propagation.

In this paper, we propose a two-layer network model for characterizing viruses, for which Bluetooth , installing apps and SMS Services, is the propagating medium in order to address the above mentioned shortcomings. In our proposed model, viruses are triggered as a result of human behaviors, instead of the contact probabilities in a uniform model. Here, the two operational behavior and mobile behavior (mobility) are focused in our individual-based model. Different from existing work that focuses 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 and to avoid further misuse of the same.

In several existing methods some will not be able to detect new viruses due to the limitation of antivirus knowledge. Our work focuses that if so happens the device initially affording the application can provide the feedback to the server which enhances further devices not installing that particular app. In order to make sure that users timely update their own detection databases, the smart phones are disseminated with the notifications or patches by the service providers or security companies. Some strategies attempt to forward security notifications or patches based on the short-range communication capabilities of intermittently connected phones but their impact will be affected by human mobility patterns and inter contact frequencies among phones. It would be difficult to acquire signature files in a timely manner. In the meantime, other dissemination strategies have also been used to distribute patches and the difficulty remains when dealing with a large-scale or highly dynamic network. Thus, we propose a new strategy that can efficiently forward patches to as many phones as possible, even in large-scale and/or dynamically evolving networks.

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) in restraining mobile virus propagation. We design an adaptive dissemination strategy by extending local reactive behaviors of entities.

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

II. The Literature Survey

In what follows, the related work on mobile virus propagation models is reviewed first. Next, some virus defense methods that contain abnormal detection technologies for restraining virus propagation in mobile networks are introduced here.

1.1 Smartphone Malwares

The Smartphone virus, Cabir, was developed in 2004 by the virus writing group. It can self-replicate but does no damage to the phones. Now a day more than a hundred mobile viruses have come into existence, many of which contain susceptible codes and cause various damages to the smart phones. The smart phones virus growth is very fast, as compared to the virus from the computer and Internet world. Such suddenly growth of smart phones will provide a productive ground for the malware to spread. An affected smart phone can cause severe compensation for both the users and the cellular service provider. In case of users, the damage may contain the loss or theft of private data, the interference of normal smart phone usage and also economic losses (e.g., the virus may secretly use the SMS/MMS services).In the cellular infrastructure side, the mobile viruses present a serious effect of Denial of Server.

1.2 Types of Viruses

There are many ways to categorize Smartphone viruses. These Smartphone viruses are categorized based on the targets that the virus attacks (e.g. the call center, the cellular base station) [10]. Instead of focusing on what the viruses seek to attack or achieve, we choose to categorize the Smartphone viruses based on the multiple infection vectors that the virus enters and/or exits the device. The benefit of our approach is that it provides a generic view on how a virus penetrates into a Smartphone and how easily it can spread in the Smartphone population. We have identified the categories of infection vectors for Smartphone virus, which are listed in Table below [10] gives some descriptive viruses at present in existence for each infection vector. Below, we will describe these infection vectors in more detail.

Types of Smartphone Viruses Based on Infection Vector

Infection Vector	**Examples**
Cellular Network	CommWarriors, Mabir
Bluetooth	CommWarriors
Internet	Skulls, Doomboot
USB	Mobler, Crossover
Peripherals	Cardtrap

1.3 Virus Propagation through BT and SMS

According to the communication channels of mobile viruses, the viruses fall into two categories namely: BT-based viruses (e.g., Cabir, Lasco) and SMS-based viruses (e.g., TXSBBSpy, Zombie, and Commwarrior). A BT-based virus is a local-contact driven virus since it infects other phones only through Bluetooth and WiFi devices within a given radio range. Similar to contact based diseases as in humans (e.g., SARS and H1N1), the propagation of a BT-based virus follows a spatially localized spreading pattern. Epidemic modeling is one of the most common approaches for studying such virus propagation. It assumes that individuals are homogeneous in a host community, each having an equal likelihood contact with others. Also, epidemic modeling is applied on some studies to analyze the propagation dynamics of a BT-based virus. SMS-based viruses can send copies of themselves to all phones that are recorded in address books, by means of photos forwarding, videos, and short messages, etc. The propagation of SMS-based malwares follows a long-range spreading pattern that is similar to the spreading of viruses in computer, especially like worm propagation in e-mail networks thus, the operational behavior of users is important in SMS-based virus propagation. Users with awareness about the viruses risk will not likely be infected even if they receive attachment. In order to study SMS-based virus propagation, we consider certain the operational patterns, such as if the users open a virus attachment or not.

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 traits of mobility patterns described by our model are consistent with statistical results from the real-world traces, i.e., local bounded mobility areas; power-law traveling distances, and inters contact times.

1.4 Defense Strategies against Mobile Viruses

Some countermeasures such as anomaly detection technologies have been proposed to protect users' private information from being revealed to different users. Like, Bose et al. discriminated some of the malicious behaviors from normal operations by training a classifier based on the method of support vector machines. 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.

Although these abnormal detection technologies can help directly protect phones from being affected by certain viruses, it is not easy to detect new viruses because the monitoring technologies must first be trained to recognize normal and abnormal operational behaviors. If any new virus produces some patterns (e.g., a series of system calls), these monitoring technologies cannot detect such virus. Hence, 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. 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, strategies that send patches based on Bluetooth is utilized. After which they send security signatures to all communities based on the local detection. However, this method cannot ensure that

users acquire patches in time. 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, AOC-based dissemination strategy is designed 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.

III. Problem Statement

The motivation for writing mobile malware is as follows.

1.5 Novelty Changes

Some malware can cause mischief or damage in such a way that appears to amuse the author. For example, the wallpaper of infected devices are changed by Ikee, and sent anti religion text messages from Android phones. Number of malware fall into this category and no other.

1.6 Selling User Information

Mobile operating system APIs provide apps with large amounts of user's data. The applications can also query the device APIs for the user's location, list of contacts, browser and downloaded history, installed applications, and IMEI number (the unique device identifier). We still cannot know for sure why malware collects this data; we contemplate that for financial gain this type of data is being sold by malware distributors. Advertising or marketing companies might be willing to purchase users' locations, browsing histories, and lists of installed applications to improve their behavioral profiling and product targeting.

1.7 Stealing User Credentials

Credentials could be used directly by malware authors for greater financial gain, but financial fraud can be difficult to perpetrate and requires specialization. People use Smartphone for shopping, banking, e-mail, and other activities that require passwords and payment information. Banks rely on cell phones for two-factor authentication. Users may also save payment credentials and authentication in text documents on their devices (for example, to use phone as a password manager), which in turn makes the device a target for credential theft.

1.8 Premium-Rate Calls and SMS

Premium-rate cost call or SMS is charged to the sender's phone bill. Calls of premium rate can cost several dollars per time, and SMS messages of premium-rate can cost several dollars per SMS. In Android and Symbian devices, malware tries to completely hide premium-rate SMS messages from the user. Premium-rate SMS attacks could in turn is feasibly go unnoticed until the user's next phone bill.

1.9 SMS Spam

SMS spam is used for commercial advertising and spreading phishing links. Commercial spammers are incentivized to use malware to send SMS spam because sending SMS spam is illegal in most countries. Furthermore, the use of SMS may lend more authenticity to spam than e-mail because phone contacts are often more intimately acquainted than e-mail contacts. 8 of the malicious Symbian and Android applications send SMS spam.

1.10 Search Engine Optimization

Many web sites rely on search engines for traffic congestions, which makes web site owners desire high visibility in search engine results. Search engines rank the web sites as per how relevant each web site is to a given search term. An engine's perception of relevance is announced by the rate at which users click on the web sites for a search term.

1.11 Ransom

Malware can be a tool for blackmail. For example, the desktop Trojan Kenzero stole the user's browser history, published it publicly on the Internet alongside the person's name, and then demanded 1500 yen to take down the person's browser history. There has not yet been any mobile malware that seriously threatens or publicly embarrasses the user for profit, but one piece of mobile malware has sought a ransom.

IV. PROPOSED APPROACH

In the system we are implementing a two layer network model for spreading virus through Bluetooth and SMS/MMS channel. The operation of human behaviors such as mobile behavior and operational behavior [3] addresses the spreading of viruses. Moreover we examine two strategies to avoid virus in mobile phones. i.e., Preimmunization and Adaptive Dissemination strategies through the methodology of Autonomy-Oriented Computing

(AOC) [1].In this method it can automatically detect the virus before when virus enter into the Smartphone and delete it.

1.12 Autonomy-Oriented Computing

Autonomic computing alludes to the self-managing physical appearance of distributed computing resources, adapting to irregular changes while beating intrinsic difficulty to operators and users [6]. Started by IBM in 2001, this enterprise finally aims to develop computer systems capable of self-management, to overcome the quickly growing difficulty of computing managements of system, and to reduce the obstacle that complexity indicates to further growth. Using high-level policies the system makes conclusion on its own and it will frequently check and enhance its status automatically so that it can modify itself to changing conditions. An autonomic computing framework is collected of autonomic components (AC) interacting with each other.

1.13 Modeling Mobile Virus Propagation

In this section, first a two-layer network model for simulating mobile virus spreading through different communication channels is introduced. Next, we present detailed propagation processes on mobile application viruses. The work presented in this section is an extension of the work in Modeling and Restraining the Propagation of Mobile Viruses. Based on the analysis of propagation mechanisms, a primary factor contributing to virus propagation lies in operations of users after infected messages are received from the network through the applications being installed on the device. If users have enough knowledge they will not open suspicious messages and their phones will not be easily infected. Mobility patterns play a key role in virus propagation because as these viruses can only infect local neighbors (whether or not they know these neighbors) within a certain range. This can evaluate the impact of operational behavior on mobile virus proliferation in social related networks, and also the effects of mobile behavior on the virus and other virus propagation in geographical contact networks.

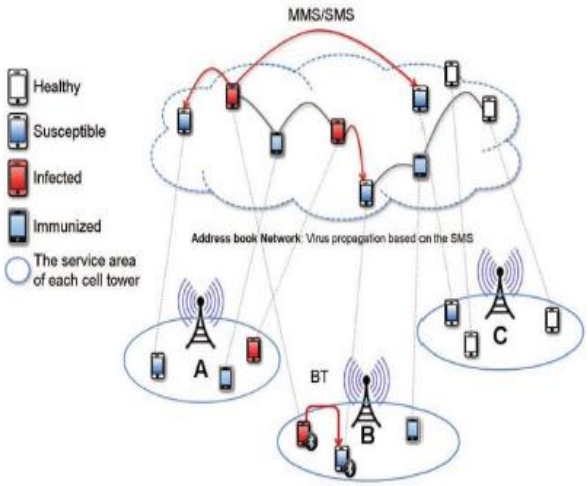


Fig 1: a two-layer network model for simulating mobile virus propagation. the network of cell towers (e.g., a, b, and c) is built based on geographical information, whereas the social relationship network is constructed from the address books of mobile users [1].

1.14 Two-Layer Network Propagation Model

The basic ideas behind our two-layer network proliferation designing are shown in Fig1. The lower layer represents a geographically based cell tower network. In this layer BT-based viruses spreads to various positions of mobile phones as shown. 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 and interaction proceeds.

1.15 The Structure of Geographical Network

Mobile phones connect with each other through wireless signals provided by cell towers. Users with their phones can travel in a geographical network, moving from lattice to another based on their mobile behavior. The same or different towers provide the basic wireless signals in these two lattices. The propagation processes of BT-based and SMS-based viruses can be simulated in a geographical contact network and a social related network, respectively.

1.16 The Structure of Logical Network

A logical relationship network among mobile users can emerge from the address books of mobile phones. In such a network, the various nodes correspond to phones and links and shows the communications

among them. Different from virus propagation through Bluetooth that is only capable of affecting nearby phones, some viruses may spread through SMS (e.g., Zombie). Hence, they can also attack remote phones. Therefore, SMS-based viruses potentially spread as fast as consider to worms in email networks.

1.17 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 this type of virus, it automatically sends its copies to other phones as per the address book of the infected phone. When users gets a suspicious message from other devices, based on their own security awareness they opens or delete according to the knowledge about the risks of mobile viruses. Therefore, the security awareness of mobile users is one of the dominant factors that describe SMS based virus propagation. In our model, one type of operational behavior is simulated, i.e., whether or not a user opens a suspicious message. In order to better characterize the SMS based virus propagation, following is assumed:

- 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, its assume that the one with higher security awareness can deletes this infected message;
- An infected phone sends out viruses to other phones only once, and the infected phone cannot send out viruses anymore;
- If a phone is patched (immunized), it will not send out any viruses even if a user opens an infected message.

1.18 BT- Based Propagation Process

Different from SMS-based viruses, if a phone is infected with BT-based virus, then it automatically searches another device 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 which 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.

V. Methodology

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, similar to contact-based epidemics (e.g., SARS) in humans. Fig. 2 shows three mobility patterns of users. The more accurate the mobility patterns of users are, the better predicting results about virus propagation will be.

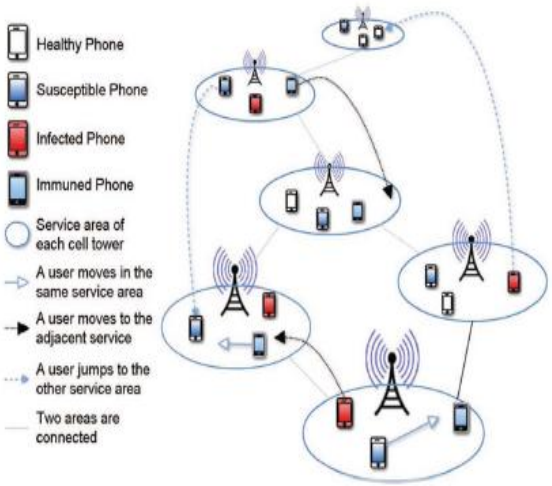


Fig 2 : the mobility patterns of users in a geographical network, which can be affected by bt virus propagation[1].

Based on existing studies, characteristics of mobility observed from the real-world data are:

- The traveling distances of a user follow a truncated power-law distribution;
- People move with a probability at each time;
- 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;

1.19 Goals and Modeling Process of Autonomy-Oriented Computing

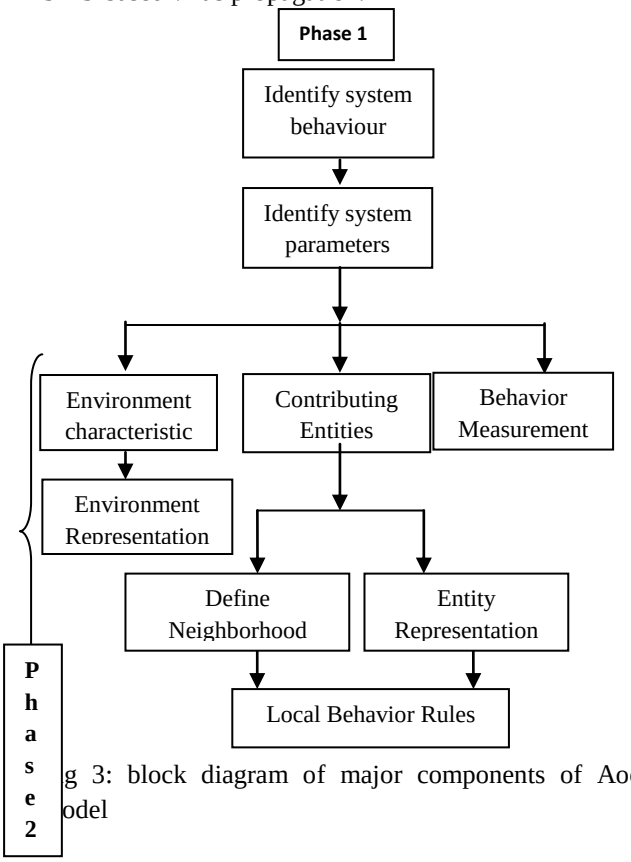
AOC has three goals [10], the first goal is to reproduce life-like behavior in computation. With complete knowledge of the fundamental mechanism, simplified life-like behavior can be used as model for a general-purpose problem solving technique. Replication of behavior is not the end, but rather the means, of these computational algorithms; the second goal is to understand the essential mechanism of a real-world complex system by hypothesizing and

frequent experimentation. The conclude product of these simulations is a progress understanding of or explanations to the real working mechanism of the modeled system; the third goal affairs the rise of a problem solver in the absence of human intervention. To build an AOC-based model, the following is a list of common steps:

- Observe macroscopic behaviors of a natural system;
- Design entities with desired synthetic behaviors as well as an environment where entities reside;
- Observe macroscopic behaviors of the artificial system;
- Validate the behaviors of the artificial system against the natural counterpart;
- modify (ii) in view of (iv);
- Repeat (iii)-(v) until satisfactory;
- Find out a model/origin of (i) in terms of (ii) or apply.

From the above steps, we note that an AOC system mainly contains a population of autonomous entities and the rest of the system is referred to as the environment. Concentrating on entity and environment, the construction of an AOC model involves three phases (see Fig. 3). The first phase, natural system identification, can be viewed as the precursor to actual systems modeling and concerns the selection of an appropriate analogy from the natural and physical world. There are two tasks involved: identify desired system behaviors and identify system parameters. Choosing the right analogy is the key to the success of the AOC-based system and the right system usually presents itself through its behaviors. Once an appropriate analogy is chosen, details such as the number of entities to run and the length of time to run the simulation need to be decided. The second phase, artificial system construction, involves all elements in the AOC-based system. This phase is divided into two major sub-phases: autonomous entity modeling and environment modeling. The identify contributing entities task is the first and the most important task in this phase. Designers are required to choose the level of detail to be modeled that is appropriate to the problem at hand. The define neighborhood task defines a certain measurement (e.g., distance) in the solution space within which local interactions can occur and local information can be collected. The define entity representation task handles how to characterize an entity, including its states and goals etc. The last task concerning the entities, define local behaviors and behavioral rules, defines the ways in which an autonomous entity reacts to various information it has collected within its neighborhood and the ways in which it adapts its local behaviors and behavioral rules. The tasks that concern the environment are identifying environment characteristics and define environment representation. The former task concerns the role the environment plays in conveying the knowledge shared between the autonomous entities. The latter task addresses the characterization of the environment. The third phase, performance measurement, concerns the evaluation criteria for comparing the artificial system manifested by the AOC-based system with its natural counterpart. This relates to problem-solving and provides an indication to modify the current set of individual behaviors and behavioral rules.

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.



g 3: block diagram of major components of Aoc odel

2. Countermeasures Against Mobile Viruses

2.1 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. Some strategies have been proposed to restrain virus propagation by dividing a mobile network into small clusters. However, it would be difficult for these strategies to deal with large-scale, decentralized and/or highly dynamic networks.

This section examines the performance of the AOC based preimmunization strategy, 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 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, 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. This result suggests that security software companies should improve their abilities to detect viruses and release patches as fast as possible.

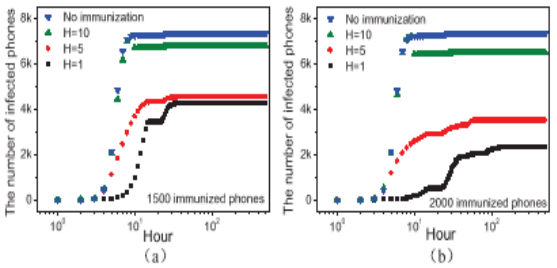


Fig 4: the effect of the AOC-based preimmunization deployment time (h) on virus propagation.

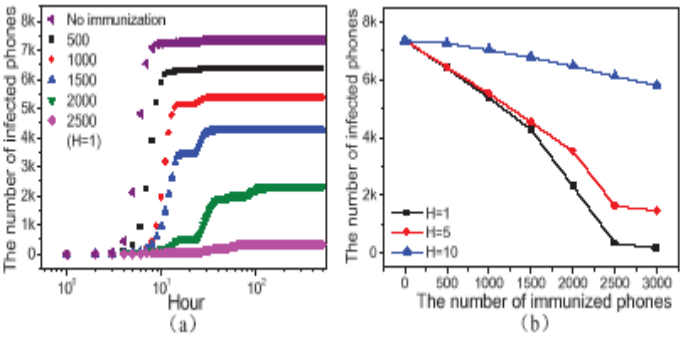


Fig 5: (a) the number of immunized phones with respect to virus propagation when the aoc-based preimmunization is deployed into the network at h = 1. (b) the relationship between the numbers of immunized phones and the number of infected phones.

2.2 Adaptive Patch Dissemination Strategy

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.

VI. Conclusion

In this paper, a two-layer network model for analyzing the spreading of SMS-based and BT-based viruses [3] is shown. The result shows that the Smartphone in spreading of viruses via different apps is being protected. This is support in android Smartphone and accurately detects and deletes the virus of the content before enter into the mobile operating system. Future work can be enhanced the virus content of data's enter into the Smartphone through Bluetooth and SMS channels it automatically filter the virus and data separately and delete the virus but not the data. The presented detection techniques are viable with the large scale testing requirement to find real world performance. As Android malware evolves hence the effectiveness of these types of measures will decrease. The understanding of interactions between human behaviors and the propagation dynamics of mobile viruses would be helpful to send security notifications to multiple users in order to improve

their security awareness, which can in turn to play a key role in restraining virus propagation.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] Chao Gao and Jiming Liu, "Modeling and Restraining Mobile Virus Propagation," *IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL.12, NO.3,* MARCH 2013.

[8] 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.

[9] 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.

[10] 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.

[11] Jiming Liu, Xiaolong Jin, Kwok ching Tsui, " Autonomous Oriented Computing(AOC): Formulating Computational Systems with Autonomous Components." *IEEE Trans on system, man and cybernetics,* pp.879-902,nov 2005.

[12] 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.

[13] 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.

[14] R. Pastor-Satorras and A. Vespignani, "Epidemic Spreading in Scale-Free Networks," *Physical Rev. Letters, vol. 86, no. 14,* pp. 3200-3203, 2001.

[15] http://en.wikipedia.org/wiki/Mobile_virus