Smartphone Malware and Its Propagation Modeling: A Survey

Sancheng Peng, Shui Yu, and Aimin Yang

***Abstract*—Smartphones are pervasively used in society, and have been both the target and victim of malware writers. Motivated by the significant threat that presents to legitimate users, we survey the current smartphone malware status and their propagation models. The content of this paper is presented in two parts. In the first part, we review the short history of mobile malware evolution since 2004, and then list the classes of mobile malware and their infection vectors. At the end of the first part, we enumerate the possible damage caused by smartphone malware. In the second part, we focus on smartphone malware propagation modeling. In order to understand the propagation behavior of smartphone malware, we recall generic epidemic models as a foundation for further exploration. We then extensively survey the smartphone malware propagation models. At the end of this paper, we highlight issues of the current smartphone malware propagation models and discuss possible future trends based on our understanding of this topic.**

***Index Terms*—smartphone; mobile malware; propagation modeling; simulator.**

I. Introduction

SMARTPHONES combine the communication capability of cellphones with the functions of PDAs (personal digital assistant). Such a device enables users to access a large variety of ubiquitous services, such as surfing the web, sending or receiving emails, and online shopping. In addition, an application-based interface is employed in most smartphones, which enables users to download individual programs that can perform a variety of tasks. However, the availability of these ubiquitous and mobile services provided by smartphones increases their vulnerability to malware attacks. Meanwhile, few smartphones have been designed to guard against malware attacks, making them an enticing target for hackers and malware writers. If a smartphone has been compromised by malware, it may cause disruption to the service of users, e.g., damage to the system, financial loss, data loss, or privacy leakage [1].

In recent years, the expanding smartphone market has become an increasingly attractive target for malicious attacks [2]. According to recent security reports [3]–[5], executed attacks have increased in the past few years. In 2010, more than 1 million cell phone users in China were infected by the 'Zombie' virus that automatically sent text messages. The attack cost users around 300,000 US dollars per day. In 2011, nearly 7,000 Android threats had been collected and identified during the first quarter of the year. By the end of 2011, McAfee Labs had collected more than 75 million malware samples. In 2011, Juniper Networks Mobile Threat Center (MTC) released its 2011 Mobile Threats Report in February 2012, which showed that mobile malware increased 155% across all platforms compared to the previous year, and provided an evidence of a new maturity in security threats that targeted mobile devices.

This trend was caused by two key factors [6]. One factor was the increasing popularity of smartphones and the size of the mobile device market is increased as evidenced from the latest reports issued by the ITU [7]. These reports indicate the number of mobile phone users reached 5.9 billion by the end of 2011. Canalys [8] published its "Smart phones overtake client PCs in 2011" on the smartphone market in February 2012. This showed the bumper quarter took the total global shipments for the whole of 2011 to 487.7 million units, up 63% on the 299.7 million smart phones shipped throughout 2010.

On the other hand, there exists a high similarity between the PC operating systems and the mobile platforms of smartphones, such as AndroidOS, SymbianOS, iOS, BlackberryOS, and Windows Mobile. Thus, in order to enforce the security of smartphones, we have to deal with the challenges present in PC platforms. In addition, there are various channels that are used by smartphones malware to transmit an infection to other susceptible smartphones. Smartphones can be subjected to various attack vectors, such as SMS, MMS, Bluetooth, WiFi, Web browsing, applications and emails. Therefore, the standard malicious attacks for PCs (e.g., worms and Trojans) and other infection vectors (e.g. Web browsing, SMS, MMS) are all applicable to smartphones.

Due to the huge potential damages that may be caused by malware, researchers have proposed many models to describe the dynamic process of malware propagation. The goals of these propagation models can be classified into the following categories: (1) gain a deep understanding of the propagation mechanisms of malware; (2) predict the scale of malware outbreak before it actually occurs; (3) evaluate how network provisioning impacts propagation and how propagation impacts the network; (4) characterize the infection dynamics of malware; and (5) design countermeasures to restrain malware propagation.

This paper aims to present the serious security issues of smartphones, and to survey the literature over the period of

Manuscript received October 3, 2012; revised January 27, 2013 and May 7 2013.

S. Peng is with the School of Computer Science, Zhaoqing University, Zhaoqing, Guangdong Province, 526061, P. R. China (e-mail: psc346@gmail.com).

S. Yu is with the School of Information Technology, Deakin University, 221 Burwood HWY, Burwood, VIC 3125, Australia (e-mail: shui.yu@deakin.edu.au).

A. Yang is with the School of Informatics, Guangdong University of Foreign Studies, Guangzhou, 510420, P. R. China (e-mail: amyang@mail.gdufs.edu.cn).

Digital Object Identifier 10.1109/SURV.2013.070813.00214.

2004-2012 by analyzing the basic characteristics of typical malware in smartphones. We aim to assist interested readers in understanding these problems, estimate the possible damage caused by malware, and to improve the development of detection and containment processes. We also review the evolution process, type, infection vectors, and the major risks of mobile malware, and summarize the current modeling theories and technologies of malware propagation.

The remainder of this paper is organized as follows: In Section II, we provide an overview of mobile malware, and provide a survey of generic epidemic modeling in Section III. In Section IV, we discuss smartphone malware propagation modeling and present existing problems and future trends in Section V. Finally, we conclude this paper in Section VI.

II. Mobile Malware

There are many different types of malware that takes advantage of many ways to propagate and infect victims. Malware [9] can infect targets by being bundled with other programs or attached as the macros of files. Others are installed by exploiting a known vulnerability of a mobile platform, network device, or other software. For example, malware writers use the vulnerability of a browser, or a smartphone will be infected if the owner uses the smartphone to access a specific web site. However, the vast majority of malware is installed through some action from the user, such as clicking a MMS message or opening an email attachment or downloading an application from the Internet.

A. Evolution of Mobile Malware

Since 2004, malware has spread among smartphones and other mobile devices through wireless networks. In June 2004, the first known smartphone worm was discovered in the SymbianOS, named Cabir [10]. It was propagated through Bluetooth as an infection vector. One of the best known local epidemics caused by Cabir took place in Helsinki in August 2005, during the 10th World Athletics Championship [11].

The evolution of mobile malware has been discussed in several investigations. SECURELIST [12] and Shih [13] have described the evolution of mobile malware from 2004 to 2006. Hypponen [14] categorized 517 families of mobile viruses, worms and Trojans during the period from 2004 to 2010. Schmidt and Albayrak [15] provided a complete list of mobile malware from 2004 to 2008. Felt et al. [16] formulated mobile malware that spread from January 2009 to June 2011. Polla et al. [17] surveyed state of the art on threats, vulnerabilities and security solutions for mobile devices over the period from 2004 to 2011.

The number of attacks on smartphones is increasing. Researchers have identified 30 new families and 143 new modifications in 2008, however, found 39 new mobile malware families and 257 new mobile malware in 2009 [18]. By mid-August 2009, the Kaspersky Lab recorded 106 families and 514 variants of malicious programs that targeted mobile devices. By the end of 2010, the numbers had grown to 153 families and over 1,000 variants. In other words, the attacks increased 65.12% from 2009 to 2010, and nearly doubled in number over 17 months [19].

TABLE I
THE NUMBER OF FAMILIES AND MODIFICATIONS FOR MALWARE

$Platform$	$Modifications$	$Families$
Android	4139	126
J2ME	1682	63
Symbian	435	111
Windows Mobile	81	23
Others	19	8

In August 2010, the Kaspersky Lab identified the first Trojan for the Android platform, named Trojan-SMS.AndroidOS.FakePlayer.a, which masqueraded as a media player application. In less than a year, Android malware quickly exploded and became the dominant mobile malware [20]. In 2011, 65% of new malicious mobile applications targeted the Android platform, compared with J2ME (27%), as well as Symbian (7%), and Windows Mobile (1%) [21]. In Table I, we show the statistics for the number of modifications and families of mobile malwares based on Kaspersky Lab's records to January 1, 2012 [22].

A comparison of unique mobile malware samples detected by Juniper MTC [5] in 2010 and 2011 indicate the vast majority of mobile malware was related to SymbianOS-based and J2ME-based devices prior to 2011. However, in 2011, Juniper MTC detected a substantial shift towards Android-based malware. In the near future, it is highly likely that malware will become even more complex and continue to grow. In addition, online banking systems will become primary targets of financial fraud and information phishing. As these services are rapidly developing in Southeast Asia and China, it is likely there will be more examples of unauthorized access to online banking systems in Asian countries.

The primary reasons for the increase in threats is summarized as follows [23]:

- The price of smartphones continues to drop, and more vendors are involved in smartphone production.
- Android's open-source kernel policy allows malware writers to gain a deeper understanding of mobile platforms.
- Users tend to deposit large amounts of private data into their smartphones. This is appealing to malware writers who financially gain from identity theft or misappropriation of credit card information.
- With the significant development of smartphone hardware, the capability of smartphone operating systems increases dramatically, offering malware writers increasing space to implement their plans.
- Programming software for smartphone platforms is similar to what is done with a PC, therefore, it is convenient for malware writers to move from a PC environment to a smartphone system.

B. Malware Classes

Malware is designed for either damaging or disrupting a computer system. This terminology is used to cover all hostile software, including virus, worm, Trojan, Spyware, backdoor, Rootkit, and Botnet [6], [24]. The differences between various malware is listed in Table II.

Virus [25]: A type of malware that enters a computer system via the hardware or software without the user's knowledge, and then attaches itself to a program file. The virus then starts to duplicate itself and commits malicious tasks that it was programmed to do. The severity of viruses includes the effects of data or software damage and denial-of-service (DoS) attacks.

Worm [26]: A type of malware that slips into computer systems without the owner's permission and operates without the owner's knowledge. Unlike viruses, which need human intervention to spread, worms can spread automatically from computer to computer. Worms can replicate themselves and send out hundreds or even thousands of copies from each infected computer, tapping into the user's email addresses to spread the infection. Worms can have a devastating impact on Internet traffic, web sites, and the user's own computer, which may be co-opted by the creator of worm. The infamous Blaster worm in November 2003 was brought to worldwide attention after its devastating impact.

Spyware: A type of malware that collects information for advertising purposes, usually for a secret a third party. The presence of spyware is typically hidden from users, and is difficult to detect. Spyware can obtain credit card numbers, passwords, and email addresses, and can also monitor a user's web activity, scan files, create pop-up ads, log keystrokes, or change the default page of web browsers. Spyware finds its way into computers as programs covertly bundled with downloaded software, through Peer-to-Peer (P2P) file sharing, or as a result of web browsing. For example, spyware with access to a video camera [27] can record video and transmit it using either email or MMS, which enables malicious remote surveillance.

Trojan [28]: A type of malware named after the wooden horse the Greeks used to infiltrate Troy [9]. It is a harmful piece of software that appears legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can attack the host any number of times, from irritating users with pop up windows or changing their desktop, to damaging the host by deleting files, stealing data, or activating and spreading other malware, such as viruses. Trojan is also known to create backdoors to provide malicious users access to the host. It is usually user-initiated and does not replicate. For example, Soundminer [29] is a Trojan targeting Android device that capable of extracting private data from audio sensors.

Backdoor [30]: A backdoor program is a remote administration utility. Once installed on a computer, backdoor allows attackers to access and control the host over a network or the Internet. A backdoor is usually able to gain control of a system because it exploits undocumented processes in the system's code. These utilities may be legitimate, or being used for legitimate reasons by authorized administrators. At the same time, they are also frequently used by attackers to gain control of a user's machine without their knowledge or authorization.

Rootkit [31]: A special type of malware that hides itself, specific files and processes, and network links in the compromised devices. It achieves the above goals by loading a special driver program or by modifying the kernel of the OS.

Bonet [32]: A type of malwre that allows an attacker to remotely control a set of compromised devices. Attackers often use it to launch large scale network attacks, such as a distributed denial of service attack (DDoS), massive spam mail, or to collect privacy information that can be used for illegal purposes.

Nowadays, the number of mobile malware threats for smartphones has increased dramatically, as shown in Figure 1 taken from F-Secure Lab's Q4 2011 Mobile Threat Report [33]. From Figure 1, we can see that the malware scene was dominated by Trojans during the years from 2004 to 2011.

C. Infection Vectors

There are multiple infection vectors for delivering malicious content to Smartphones. In this survey, we classify infection vectors into four categories: SMS/MMS, Bluetooth, Internet access, and file duplication with USB.

(1) SMS/MMS

Cellular services, such as short message service (SMS) and multimedia messaging service (MMS), can be used as attack vectors for smartphones. For example, SMS/MMS messages can be used to deliver malicious content and to maintain communication with an attacker. For example, ComWar is a worm which browses the host's phonebook and then spreads via SMS/MMS messages.

(2) Bluetooth

Bluetooth [34] is a short-range radio communication protocol that allows Bluetooth-enabled mobile devices (which could be mobile or stationary) within 10-100 meters to communicate with each other. Bluetooth-based attacks are a method used for device-to-device malware spreading. Once two Bluetooth-enabled devices are in range, the compromised device pairs with its target using default Bluetooth passwords. If the connection is established, the compromised device sends out malicious content. However, Bluetooth is a limited attack vector for injecting malicious content due to several security factors. First, mobile devices are not usually set in the discoverable state by default, and the period during which they can be discovered is limited. Second, the user has to confirm the file transfer and then the malware has to make itself part of the file exchanged via Bluetooth.

(3) Internet access

Smartphones can access the Web using Wi-Fi networks or 3G networks, which allows users to use the most common Internet application services, such as surfing the web, sending or receiving emails with attachments, or downloading application software. Although such high speed Internet connections can provide many convenient services, they also expose smartphones to the same threats as personal computers (PCs). In addition, smartphones are constantly switched on, which increases the chance of a successful malicious attack, if they maintain a continuous connection to the Internet.

(4) File duplication with USB

Apart from the aforementioned infection vectors, smartphones could be compromised using other methods, e.g., use of USB. If the files used to synchronize smartphones were compromised, malware can also infect smartphones. As a result, attackers can access the host's private information and install malicious applications on the smartphone.

TABLE II
DIFFERENCES BETWEEN MALWARE

Type	*Virus*	*Worm*	*Trojan*	*Backdoor*	*Spyware*	*Rootkit*	*Botnet*
Existing form	Parasitic	Independent entity	Disguised as other files	Disguised as other files	Disguised as other files	Disguised as other files	Disguised as other files
Propagation mode	Depends on the host file or media	Self replicates	Deceptive means	Deceptive means	Deceptive means	Deceptive means	Deceptive means
Attack target	Local file	Network host or network itself	System	System	System	System	System
Human intervention	Yes	System bugs: No; Others: Yes	Yes	Yes	Yes	Yes	Yes
Major risks	System damage, delete files, data loss	Network paralysis, data loss	Information leakage	Information leakage	Information leakage	Information leakage	Information leakage and System damage
Spreading speed	Fast	Very fast	Slow	No	Slow	Fast	Very fast
Detection method	Simple	Very complex	Complex	Complex	Complex	Complex	Complex

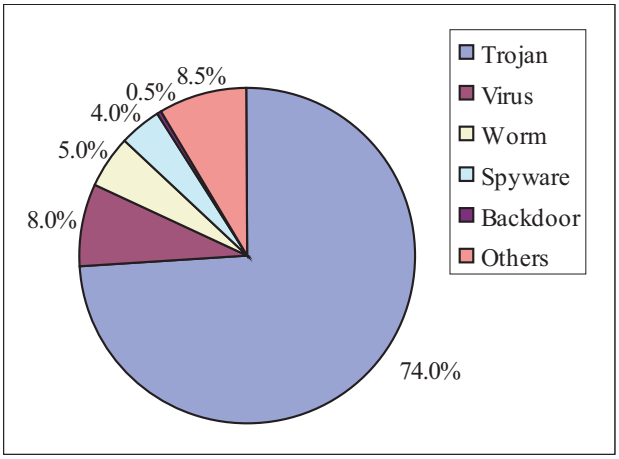


Fig. 1. Mobile threats by type from 2004 to 2011

D. Risk of Malware

Once smartphones have been compromised by malware, it may cause interruption to the service of users, such as system damage, economic loss, information leakage, or disruption to a mobile network. We list more details of each category as follows.

(1) System damage

- Battery draining: Some malware commits their attack goal by continuously searching and infecting other phones (i.e., Cabir, Lasco, and Mabir), or continuously sending SMS or MMS messages (i.e., RedBrowser). As a result, hosts quickly lose their battery power.
- Disabling system functions: Some malware can make the system unable to operate normally, such as Skulls. Some malware can even block calling functionality, for example, Locknut.
- Change system configurations: Some malware can change the background wallpaper on the device, such as Ikee.

(2) Economic loss

- Sending SMS or MMS messages to premium numbers: A successfully executed attack can force the compromised smartphone to send SMS or MMS messages to premium numbers, such as Mquito [35], which may cause financial loss to the smartphone owner.
- Dialing premium numbers: A successfully executed attack can force the compromised smartphone to dial premium numbers, such as BaseBridge, which may cause financial loss to the smartphone user.
- Deleting important data: Any data stored in the device's memory or on an SD card, e.g., documents, photos or videos, may be compromised and then be deleted by attackers.

(3) Information leakage

- Privacy breach: A successfully executed attack can also empower an attacker with the ability to browse SMS or MMS messages, emails, call logs, and contact details from compromised smartphones.
- Remote surveillance: An attacker can turn an infected smartphone into a listening device by utilizing the voice recording hardware, and can access the camera of the infected smartphones to take photos or record video clips of the surroundings of the smartphone user.
- Stealing bank account information: Online banking is constantly under attack by using Trojans to steal passwords, such as ZeuSMitMo [36].

(4) Disturbing mobile networks

- Denial-of-service (DoS): If compromised smartphones can secretly and continuously send SMS or MMS messages or dial premium rate numbers. It can also result in DoS attacks by occupying network bandwidth. This is a conventional DoS attack, which is flooding-based so an attacker can generate high-rate, high-volume network traffic in order to deplete network resources.
- Signaling channel attack: This is a novel DoS attack and seeks to overload the control plane of a 3G wireless network using low-rate, low-volume attack traffic based on some of the aforementioned 3G-specific vulnerabilities. Unlike traditional DoS attacks that focus on the data plane, a signaling attack creates havoc in the signaling

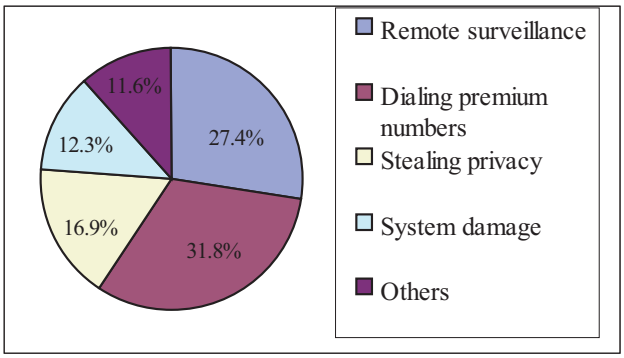


Fig. 2. Mobile risks by type from January to June in 2012

plane of a 3G network by repeatedly triggering radio channel allocations and revocations [37].

E. Malware on Mobile Platforms

Modern mobile devices run sophisticated OSs, such as Symbian, Android, iOS, J2ME, and Windows Mobile. All of these confront similar risks as desktop computers do.

(1) Symbian: Symbian is an open source OS designed for smartphones. With the launch of the Ericsson R380 in the year 2000, Symbian became the first modern mobile OS for smartphones. From 2004 to 2006, Symbian was the platform frequently targeted by malware writers. Cabir [10] was not only one of the first malware for Symbian, but also one of the first to use Bluetooth to propagate malware. This worm consists of a message that contains an application file, caribe.sis, which disguises a security manager utility. If installed, the worm uses the device's native Bluetooth functionality to search for other Bluetooth-discoverable devices. The worm then attempts to send infected SIS files to the discovered devices as well. Mquito [35] became the first Trojan for smartphones and was discovered in August 2004. This Trojan makes infected phones send SMS text messages to other phones resulting in charges to the smartphone owner.

(2) Android: Android is a mobile OS based on a Linux-derived OS backed by Google, along with dominant hardware and software developers (such as Intel, HTC, ARM, Samsung, and Motorola), which form the Open Handset Alliance. Android was released on November 5th, 2007 and received praise from a number of developers upon its introduction. A steady rise in the number of threats targeting Android was observed during the first half of 2011. For example, Fakeplayer.A [38] is a Trojan that affects smartphones run by Android. It sends certain SMS messages to specific numbers, which may lead to users being charged for transactions without the consent of the smartphone owner. BaseBridge.B [39] is another Trojan affecting Android-based mobile devices. This Trojan steals sensitive data, sends it to a remote server, and may terminate certain applications.

(3) iOS: iOS is Apple's mobile OS that was derived from Mac OS X. It was originally developed for iPhones, but now has been extended to support other devices, such as iPod Touch, iPad, and second-generation Apple TV. Since the release of iOS 2.0 on July 11th, 2008, it officially began to support third party applications [40], [41]. Ikee [42] is the first self-propagating worm targeting Apple iPhones. This worm attacks only jail-broken iPhones using the installed SSH server and the default root password. Its most notable action involves changing the iPhones background wallpaper. Ikee.B [43] is the second variant of the Ikee worm, and is the first Bonet with a clearly malicious attack. However, unlike iKee, Ikee.B includes command and control logic to render all infected iPhones under the control of a Botnet master.

(4) J2ME: J2ME (Java 2 Micro Edition) is a kind of highly optimized Java running environment. It provides a robust, flexible environment for applications running on mobiles and embedded devices, such as mobile phones, personal digital assistants (PDAs), and printers. Redbrowser [44] is a J2ME-based Trojan that sends SMS messages to specific phones. The Redbrowser pretends to be a WAP browser that offers free WAP browsing using free SMS messages to send WAP page contents. But what it actually does is send SMS messages to one specific phone number, which may cause financial loss to users.

(5) Windows Mobile: Windows Mobile is an OS developed by Microsoft for smartphones. Based upon Windows CE 5.2 kernel, Windows Mobile was designed to be similar to the desktop versions of Windows, and is now superseded by Windows Phone 7. Third-party software development is also available, and customers can purchase software applications via Windows Marketplace for Mobile. Brador [45] is a family of Backdoors that affects mobiles, and ARM-based devices running Windows CE operating system version 2.0 or later. This Backdoor sends an email containing the compromised system's host name and IP address to the attacker. It also opens up a TCP/IP connection and listens on the local port to enable remote access and control of the compromised device. PhoneCreeper [46] is a publicly available monitoring program designed to run on mobile phones using the Windows Mobile 5 to 6.5 operating systems. If installed, the targeted phone may be remotely directed via specific SMS text messages to perform a wide range of actions, all of which are hidden from the smartphone user. These actions may or may not result in owners incurring high phone charges.

Recently, the number of risks to smartphones has increased, as shown in Figure 2 which was taken from NetQin Labs 2012 Security Report on mobile phones [47]. It is well known that the first most common risk is calling paid services, such as sending SMS or MMS messages to premium numbers and dialing premium numbers.

From the examples of mobile malware listed in Table III, we can see that the current type of malware includes worm, Trojan, virus, Spyware, Botnet, and Backdoor for the system platform of smartphones, such as Symbian, WinCE, J2ME, iOS, and Android.

III. Generic Epidemic Modeling

Epidemic modeling has a long history in the study of biological infectious diseases. In 1927, 1932 and 1933, Kermack and McKendrick published a series of papers titled "Contributions to the mathematical theory of epidemics" [48]. These papers are often seen as the basis of further research using

TABLE III
EXAMPLES OF MOBILE MALWARE

Name	*Type*	*OS*	*Time*	*Infection vectors*	*Risk*
Cabir	Worm	Symbian	Jun. 2004	Bluetooth	System damage
Brador	Backdoor	WinCE	Aug. 2004	Network API	Privacy steal
Mquito	Trojan	Symbian	Aug. 2004	Embedded in a game	Fee consume
Skuller	Trojan	Symbian	Nov. 2004	Download from Internet	System damage
Lasco	Worm	Symbian	Jan. 2005	Bluetooth	System damage
Locknut	Trojan	Symbian	Feb. 2005	Download from Internet	System damage
ComWar	Worm	Symbian	Mar. 2005	MMS, Bluetooth	System damage
Drever	Trojan	Symbian	Mar. 2005	Download from Internet	System damage
Mabir	Worm	Symbian	Apr. 2005	MMS, Bluetooth	System damage
Redbrower	Trojan	J2ME	Feb. 2006	SMS	Fee consume
StealWar	Trojan	Symbian	Mar. 2006	Bluetooth, MMS	System damage, Privacy steal
Cxover	Virus	WinCE	Mar. 2006	Download from Internet	System damage
Rommwar	Trojan	Symbian	Apr. 2006	Download from Internet	System damage
FlexiSpy	Spyware	Cross-platform	Apr. 2006	Download from Internet	Privacy steal
Mobler	Worm	Cross-platform	Aug. 2006	Via memory card	System damage, DoS
Viver	Trojan	Symbian	May 2007	Download from Internet	Fee consume
Reboot	Trojan	Symbian	Aug. 2007	Download from Internet	System damage
HatiHati	Worm	Symbian	Dec. 2007	Via MMC memory cards	Fee consume
Beselo	Worm	Symbian	Jan. 2008	MMS, Bluetooth	System damage
Swapi	Trojan	J2ME	Feb. 2008	Download from Internet	Fee consume
Blocker	Trojan	Symbian	Jun. 2008	Download from Internet	System damage
Small	Trojan	J2ME	Dec. 2008	Download from Internet	Fee consume
Yxe	Worm	Symbian	Jan. 2009	SMS	System damage
PbevBow	Trojan	Symbian	Oct. 2009	Download from Internet	Fee consume
VScreener	Trojan	J2ME	Nov. 2009	Download from Internet	Fee consume
Ikee	Worm	iOS	Nov. 2009	Install application software	System damage
Ikee.B	Worm,Botnet	iOS	Nov. 2009	Install application software	System damage
ZeusMitmo	Trojan	Symbian	Feb. 2010	SMS	Privacy steal
FakePlayer	Trojan	Android	Aug. 2010	Download from Internet	Fee consume
Zbot	Trojan	Symbian	Sep. 2010	Download from Internet	Privacy steal
PhoneCreeper	Backdoor	WinCE	Oct. 2010	Download from Internet	Privacy steal, Remote control
iSAM	Hybrid malware	iOS	Jun. 2011	Install application software	Privacy steal, Remote control
Adrd	Trojan	Android	Feb. 2011	Download from Internet	Privacy steal, Remote control
Boxer	Trojan	Symbian	Feb. 2011	Download from Internet	Privacy steal
BaseBridge	Trojan	Android	Mar. 2011	Download from Internet	Fee consume, Privacy steal
DroidDream	Trojan	Android	Mar. 2011	Download from Internet	Privacy steal
Zsone	Trojan	Android	May 2011	Install application software	Fee consume
LightDD	Virus	Android	Jul. 2011	Download from Internet	Privacy steal, Fee consume, Remote control
OpFake	Trojan	Cross-platform	Oct. 2011	Download from Internet	Fee consume
Kituri	Trojan	Android	Oct. 2011	Download from Internet	Fee consume
UpdtKiller	Trojan	Android	Apr. 2012	Download from Internet	System damage, Remote control
FakeToken	Trojan	Android	May 2012	SMS	Privacy steal

mathematical (especially deterministic) modeling to explore the spread of infectious diseases. The most classical epidemic models [49] include the SI (susceptible-infectious) model [50], the SIS (susceptible-infectious-susceptible) model [51], and the SIR (susceptible-infectious-recovery) model [52].

In general, there are three different states for each individual in epidemic modeling:

- Susceptible (S): The susceptible individuals are those who have not been infected, but could be infected.
- Infected (I): The infected individuals are those capable of spreading a disease.
- Recovered (R): The recovered individuals that used to be infected by disease or they have died from a disease. They are clear of diseases and immune to the same type of diseases.

Epidemic models are usually classified into three categories: deterministic models [53], stochastic models [54], and spatial-temporal models [55], [56].

A. Deterministic Epidemic Models

In this subsection, we focus on discussing SI, SIS, SIR, and SIRS epidemic models [57], [58]. In these four models, individuals in the population are classified according to disease status: susceptible (S), infectious (I), or recovered (R). The basic deterministic epidemic models include the SI epidemic model (e.g., Fig. 3 (a)), the SIS epidemic model (e.g., Fig. 3 (b)), the SIR epidemic model (e.g., Fig. 3 (c)), and the SIRS epidemic model (e.g., Fig. 3 (d)).

Some of the terms for these models are explained as follows:

- μ denotes birth rate, which refers to the ratio of the number of newly-born individuals via the total population per unit time.
- λ denotes death rate, which refers to the ratio of the number of infections via the number of death due to infection in a certain period of time (usually 1 year).
- N denotes the total number of susceptible, infected, and recovered individuals. Let the birth rate not be equal to the death rate, the total population size is a variable.
- $S(t)$ is used to represent the number of individuals not yet

infected with the disease at time t, or they are susceptible to the disease.
- $I(t)$ denotes the number of individuals who have been infected by disease and are capable of spreading the disease to those in the susceptible category.
- $R(t)$ is the compartment used for those individuals who have been infected and then recovered from a disease. Those in this category can not be infected again or transmit the infection to others.
- β represents the average number of adequate contacts made by an infected individual per unit time. This is called contact rate or infection rate.
- α represents the mean recovery rate.
- δ represents the average loss of immunity rate of recovered individuals or denotes the rate when recovered individuals become susceptible again.
- βSI represents the number of new infections per unit time.
- αI represents the number of new recoveries or denotes the number of new susceptibles per unit time.
- δR represents the number of new susceptibles per unit time.

(1) SI epidemic model

In the SI epidemic model, we suppose a susceptible individual, after successful contact with an infectious individual, becomes infected, but does not develop immunity to the disease. Therefore, the differential equations describing the dynamics of an SI epidemic model based on the preceding assumptions are listed as follows:

$$\begin{cases} S(t) = \frac{\left(\frac{N-I_0}{I_0}\right)Ne^{-N\beta t}}{1+\left(\frac{N-I_0}{I_0}\right)e^{-N\beta t}} \\ I(t) = \frac{N}{1+\left(\frac{N-I_0}{I_0}\right)e^{-N\beta t}} \\ N = S(t) + I(t) \\ I_0 = I(0) \end{cases} \tag{1}$$

(2) SIS epidemic model

In the SIS epidemic model, we assume a susceptible individual, after successful contact with an infectious individual, becomes infected, but does not develop immunity to the disease. Hence, after recovery, infected individuals return to the susceptible. Therefore, the differential equations describing the dynamics of an SIS epidemic model based on the preceding assumptions are listed as follows:

$$\begin{cases} \frac{\mathrm{d}S(t)}{\mathrm{d}t} = -\frac{\beta S(t)I(t)}{N} + (\alpha+\lambda)I(t) \\ \frac{\mathrm{d}I(t)}{\mathrm{d}t} = \frac{\beta S(t)I(t)}{N} - (\alpha+\lambda)I(t) \\ N = S(t) + I(t) \end{cases} \tag{2}$$

(3) SIR epidemic model

In the SIR epidemic model, when individuals become infected, they develop immunity and enter the immune state R. The SIR epidemic model has been applied to childhood diseases such as chickenpox, measles, and mumps. Therefore, the differential equations describing the dynamics of an SIR epidemic model are described as follows:

$$\begin{cases} \frac{\mathrm{d}S(t)}{\mathrm{d}t} = -\frac{\beta S(t)I(t)}{N} + \lambda(I(t)+R(t)) \\ \frac{\mathrm{d}I(t)}{\mathrm{d}t} = \frac{\beta S(t)I(t)}{N} - (\alpha+\lambda)I(t) \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} = \alpha I(t) - \lambda R(t) \\ N = S(t) + I(t) + R(t) \end{cases} \tag{3}$$

(4) SIRS epidemic model

In the SIRS epidemic model, the assumption is that infected individuals can recover and will become susceptible again after recovering. Therefore, the differential equations describing the dynamics of an SIRS epidemic model are described as follows:

$$\begin{cases} \frac{\mathrm{d}S(t)}{\mathrm{d}t} = -\frac{\beta S(t)I(t)}{N} + \lambda(I(t)+R(t)) + \delta R(t) \\ \frac{\mathrm{d}I(t)}{\mathrm{d}t} = \frac{\beta S(t)I(t)}{N} - (\alpha+\lambda)I(t) \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} = \alpha I(t) - \lambda R(t) - \delta R(t) \\ N = S(t) + I(t) + R(t) \end{cases} \tag{4}$$

B. Stochastic Epidemic Models

Stochastic epidemic models [59]–[61] mainly include three types: (1) the discrete time Markov chain (DTMC) model, (2) the continuous time Markov chain (CTMC) model, and (3) the stochastic differential equation (SDE) model. These stochastic models differ in their underlying assumptions regarding time and state variables. In the DTMC model, time and state variables are discrete. In the CTMC model, time is continuous, but the state variable is discrete. Finally, the SDE model is based on a diffusion process, where both time and state variables are continuous. In the three stochastic population models, the random nature of the individual birth and death processes-demographic variability is taken into account. For stochastic epidemic models, we focus on analyzing the DTMC SIS and CTMC SIS model in this survey.

Let $Y(t)$ be the random variable for the size at time t. It is assumed that incidence rate, β_i, and the recovery rate, α_i are continuous and differentiable functions of the population size i. In addition, it is assumed there exists numbers K and N such that $0 < K < N$ and: (1) $\beta_0 = \alpha_0 = 0$ and $\beta_i = 0$ for $i \geq N$, (2) $\beta_i > 0$ and $\alpha_i > 0$ for $0 \leq i \leq N$, (3) $\beta_i > \alpha_i$ for $0 \leq i \leq K$, (4) $\beta_i < \alpha_i$ for $K < i \leq N$.

In the DTMC SIS epidemic model, both the time and population size are discrete-valued. Let Δt be a fixed time interval and $t \in \{0, \Delta t, 2\Delta t, \cdots\}$. It is assumed that Δt is sufficiently small, so that at most one event occurs during the time interval Δt. This event will either be an infection, recovery, birth, or death, which only depends on the values of state variables at the current time. Since the population size remains constant, a birth and death must occur simultaneously. Let the probabilities associated with $Y(t)$ be denoted as $p_i(t) = \mathrm{Prob}\{Y(t) = i\}$ and $p(t) = (p_0(t), ..., p_N(t))^T$. Thus, the transition probabilities are denoted as follows.

$$\begin{cases} P\{Y(t+\Delta t)=i-1|Y(t)=i\}=\alpha_i\Delta t \\ P\{Y(t+\Delta t)=i+1|Y(t)=i\}=\beta_i\Delta t) \\ P\{Y(t+\Delta t)=i|Y(t)=i\}=1-(\alpha_i-\beta_i)\Delta t \\ P\{Y(t+\Delta t)=k|Y(t)=i\}=0, |i-k|\geq 2 \end{cases} \quad (5)$$

Since Equation (5) satisfies the difference equations $p_i(t+\Delta t)$ and $p_i(t+\Delta t)=\beta_{i-1}\Delta t p_{i-1}(t)+\alpha_{i+1}\Delta t p_{i+1}(t)+(1-(\beta_i+\alpha_i)\Delta t)p_i(t)$, the difference equations for the discrete-time model can be expressed in matrix form with the definition of the $(N+1)\times(N+1)$ transition matrix P.

$$P=\begin{pmatrix} 1 & \alpha_1\Delta t & \cdots & 0 \\ 0 & 1-(\beta_1+\alpha_1)\Delta t & \cdots & 0 \\ 0 & \beta_1\Delta t & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \alpha_N\Delta t \\ 0 & 0 & \cdots & 1-\alpha_N\Delta t \end{pmatrix} \quad (6)$$

To ensure P is a stochastic matrix, it is assumed that $\max_{i\in\{1,2,\cdots,N\}}\{(\beta_i+\alpha_i)\Delta t\}\leq 1$.

In the CTMC SIS epidemic model, the corresponding continuous-time model is a Markov jump process with the jumps forming a Markov chain, and the stochastic process depending on the collection of discrete random variables $t\in[0,\infty)$, $Y(t)\in\{0,1,2,\cdots,N\}$ and their associated probability functions $p(t)=(p_0(t),...,p_N(t))^T$, where $p_i(t)=\text{Prob}\{Y(t)=i\}$. The transition probabilities for the CTMC model are as follows:

$$\begin{cases} P\{Y(t+\Delta t)=i-1|Y(t)=i\}=\alpha_i\Delta t+o(\Delta t) \\ P\{Y(t+\Delta t)=i+1|Y(t)=i\}=\beta_i\Delta t+o(\Delta t) \\ P\{Y(t+\Delta t)=i|Y(t)=i\}=1-(\alpha_i+\beta_i)\Delta t+o(\Delta t) \\ P\{Y(t+\Delta t)=k|Y(t)=i\}=o(\Delta t), |i-k|\geq 2 \end{cases} \quad (7)$$

Taking the limit as $\Delta t\to 0$, a system of differential equations for the probabilities $p_i(t)=\text{Prob}\{Y(t)=i\}$ can be shown to satisfy the forward Kolmogorov differential equations: $\frac{\mathrm{d}p_i(t)}{\mathrm{d}t}=\beta_{i-1}p_{i-1}(t)+\alpha_{i+1}p_{i+1}(t)-(\beta_i+\alpha_i)p_i(t)$ where $i\in\{1,\cdots,N\}$ and $\frac{\mathrm{d}p_0(t)}{\mathrm{d}t}=\alpha_1 p_1(t)$. Thus, the difference equations for the continuous-time model can be expressed in matrix form with the definition of the transition matrix Q.

$$Q=\begin{pmatrix} 0 & \alpha_1 & 0 & \cdots & 0 \\ 0 & -(\beta_1+\alpha_1) & \alpha_2 & \cdots & 0 \\ 0 & \beta_1 & -(\beta_2+\alpha_2) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha_N \\ 0 & 0 & 0 & \cdots & -\alpha_N \end{pmatrix} \quad (8)$$

In the SDE model, both time and state are continuous variables, $t\in[0,\infty)$ and $Y(t)\in\{0,1,2,\cdots,N\}$ [61].

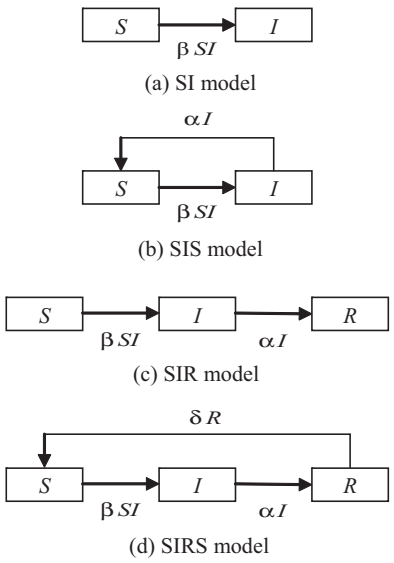


Fig. 3. Basic deterministic epidemic models

C. Spatial-Temporal Epidemic Models

The concept of cellular automata (CA) [62], [63] was first proposed by J. Von Neumann and Stan Ulam in the early 1950s. As the original theoretical concept is of universality, researchers have tried to develop simpler and more practical architectures of CA, which can be used to model widely divergent application areas. In this respect, two notable developments are credited to John Conway and Stephen Wolfram. In 1970, the mathematician John Conway proposed his now famous game of life, which received widespread interest among researchers. In the beginning of the 1980s, Stephen Wolfram studied a family of simple one-dimensional cellular automata rules (now referred to as Wolfram rules) and demonstrated that even the simplest of rules are capable of emulating complex behavior.

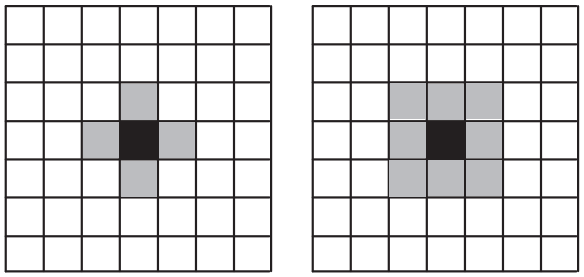
A CA is a discrete dynamic system, where space, time, and the state of the system are distinct. It is also a spatially and temporally discrete, deterministic mathematical model. In general, a CA can be defined as any dimensions. One-, two-, and three- dimensional cellular automata are often used by researchers. For example, a one-dimensional CA can be visualized as having a cell at each integral point on the real number line, and cell C_i has a left and a right neighbor (except edge conditions). A two-dimensional CA is represented as a regular spatial lattice or grid. At time t, each cell stays in one of a finite number of possible discrete states. By interacting with its neighbors, each cell updates its current state following a set of specific transition rules. According to the above description, a CA can be formally defined as a four-tuple, $\{C,S,V,f\}$. The elements are further explained as follows:

C denotes a cellular space, for a two-dimensional CA, $C=\{(i,j)|i,j\in Z, 1\leq i\leq L, 1\leq j\leq L\}$.

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

V denotes the neighborhood of each cell, for a two-dimensional CA, $V=\{(x_k,y_k), 1\leq k\leq N\}\subset Z\times Z$.

f denotes a set of local transition rules.



(a) Von Neumann (b) Moore

Fig. 4. Neighborhood of Von Neumann and Moore

As mentioned above, the most important types of neighborhoods are the Von Neumann neighborhood (see Fig. 4(a)) provided by the cell itself and four additional cells, and the Moore neighborhood (see Fig. 4(b)), formed by the cell itself and its eight nearest cells.

D. Comparison of Epidemic Models

(1) Deterministic models are the first and most popular. They are represented by differential equations of various forms. It is assumed that the size of the susceptible and infectious population is a definite function of time in these models.

- Advantages: These models can describe the dynamic inter-relations among the rates of change and population size. The mathematical theories for these types of models have been well developed, and are suitable for making predictions.
- Disadvantages: During an early stage of malware propagation, these models may not accurately characterize the spread of malware as the number of infected hosts is small.

(2) The modeling mechanism for stochastic models is the stochastic process. The populations in this type of model are represented by the stochastic process. These models can describe the dynamic interrelations of their probability distributions.

- Advantages: Stochastic models are suitable for studying a small community.
- Disadvantages: Due to lack of a general mathematical formulation, it is difficult to perform mathematical analysis in stochastic models.

(3) The modeling basis for spatial-temporal models is CAs. A CA contains a large number of simple identical components with local interactions, and is capable of simulating complex systems and their spatial-temporal evolution process.

- Advantages: It becomes an important tool for studying the space-time evolution of a self-organizing system due to its capability, and to characterize the characteristics of complex systems based on local evolution rules.
- Disadvantages: The transition rules are vulnerable to human interference during the defining process.

The basic models for propagation dynamics are listed in Table IV.

IV. Smartphone Malware Propagation Modeling

As Internet viruses are similar to biological viruses in their self-replicating and propagation behaviors, epidemiological models for analyzing the propagation of Internet worms is nothing new, as there has been tremendous interest in modeling the propagation of Internet viruses over a number of decades [64]–[69]. The study of computer viruses in general, and Internet viruses in particular, is a very popular topic of research. The security issue regarding malware propagation that exploits geographic proximity of wireless-enabled devices has received significant attention in recent years. Many efforts have been made to model the propagation behavior of malware in wireless networks, such as wireless sensor networks [70]–[73] and wireless ad-hoc networks [74]–[78].

Due to the strong similarity in the behaviors of self-replicating and propagation between mobile malware and biological viruses, most investigations of malware propagation in smartphones focus predominately on modeling the malware propagation by employing the classical epidemic theories in epidemiology. For example, the mathematical models developed for biological infectious diseases have been applied to the research of malware propagation in smartphones.

Mobile malware has been extensively studied in the literature and a large number of malware propagation models, such as mathematical-based and simulator-based approaches, have been proposed to study epidemiological problems in smartphones. Mathematical models and their analysis play a natural role in understanding and predicting the propagation dynamics of an infection. Simulators provide a very useful tool for the analysis of real epidemics, offer an effective verification method for mathematical models, and provide quantitative insight into the dynamics of how an infection spreads.

A. Mathematical-Based Propagation Models

In this subsection, we investigate the malware propagation models in smartphones including Bluetooth-based and hybrid-based models.

(1) Yan's model (analytical model on Bluetooth worms)

Yan and Eidenbenz [79], [80] built an analytical model to study the spread of Bluetooth worms. In this model, let $i(t)$ be the average density of infected devices in the network considered at time t, let $\rho(t)$ denote the device density at time t, and let $i(t_k)$ denote the infection density at time $t_k (k \geq 0)$. The next time point and the associated worm propagation status are denoted by t_k+1 and $i(t_k$+1), respectively. Thus, the worm propagation curve is expressed as follows:

$$i(t_{k+1}) = \frac{i(t_k)\rho(t_k)}{i'(t_k) + (\rho(t_k) - i'(t_k))e^{-\psi}} \tag{9}$$

$$\alpha(t) = \Omega(t, 1, T_{inq}(t), < 0, 0, 0, 1, 0 >), \tag{10}$$

where $\psi = -\alpha(t_k) \cdot \rho(t_k)/(\rho(t_k) - i'(t_k))$, $\rho(t_k)$ denotes the average density at time t_k.

In the proposed model, the impact of mobility patterns on Bluetooth worm propagation can be investigated by introducing the input parameters, such as average node degree, average node meeting rate, and the link duration distribution.

TABLE IV
BASIC MODELS FOR PROPAGATION DYNAMICS

Type	*Deterministic model*	*Stochastic model*	*Spatial − temporal model*
Theory	Differential equation	Markov process	Cellular automata
Spatially	Continuous	Continuous	Discrete
Temporal	Continuous	Continuous or discrete	Discrete
Dividual state	Continuous	Discrete	Discrete
Dividual interaction	No	No	Yes
Adaptive scope	Randomly moving individuals	A small number of individuals	Large number of individuals
Model description	Differential equation	Continous or discrete time Markov chain	Stochastic evolution rules

(2) SIP model

Rhodes and Nekovee [81] investigated the effect of population characteristics and device behavior on the outbreak dynamics of Bluetooth worms using the SIP model. In the SIP model, let a population of N individual devices exist at a density ρ and move with a mean speed $\overline{v}$. It is assumed there is a single infected device capable of spreading a worm with a probability p to any other device that finds itself within a wireless communications radius R. If a worm is introduced into the system, each device can be either susceptible (S), infected (I) or recovered (P). Thus, in a finite population of fixed size, worm propagation is described as follows:

$$\begin{cases} \frac{\mathrm{d}S}{\mathrm{d}t} = -2R\rho\bar{v}p\frac{SI}{N} \\ \frac{\mathrm{d}I}{\mathrm{d}t} = -2R\rho\bar{v}p\frac{SI}{N} - \delta I \\ \frac{\mathrm{d}P}{\mathrm{d}t} = \delta I \end{cases} \tag{11}$$

However, Rhodes and Nekovee did not characterize the spatial-temporal characteristics of the propagation dynamics of Bluetooth worms, and also did not consider the impact of individual difference on the propagation dynamics of different worms.

(3) SIS model

Martin et al. [82] predicted the spread of cell phone viruses using the SIS model from mathematical epidemiology. In the SIS model, let I denote the ratio of the number of infected cell phones to the total number of cell phones, S represent the ratio of the number of susceptible cell phones to the total number of cell phones, α denote the rate at which infected cell phones recover and return to the susceptible state, and β represent the transmission rate between susceptible and infected cell phones based on binary contacts. Thus, the SIS model is given by Equation (2).

However, the authors did not take into account the impact of individual difference on the propagation dynamics of proximity-based viruses, and did not characterize the spatial-temporal characteristics on the propagation dynamics of proximity-based viruses.

(4) Mickens's model (probabilistic queuing framework)

Mickens and Noble [83] proposed a probabilistic queuing framework to model the propagation of mobile viruses over short-range wireless interfaces. In this model, let $P(k)$ denote the connectivity distribution for the network. The queuing model is initialized by inserting $N_k = P(k)N$ nodes into each Q_k. Thus, the standard homogeneous infection dynamics in each queue is simulated by:

$$\frac{\mathrm{d}I_k}{\mathrm{d}t} = \beta k_i I_k(1 - I_k) - \delta I_k \tag{12}$$

The global number of infected nodes is given by $\sum_{k=0}^{N-1}[I_k N_k]$. The authors demonstrated the impact of node speed upon the steady state infection level of the network, and provided a preliminary stochastic counterpart for the deterministic model. However, they did not characterize the impact of individual difference on the propagation dynamics of viruses, and did not characterize the spatial-temporal characteristics on the propagation dynamics of viruses.

(5) Two-layer propagation model

Gao and Liu [84], [85] proposed a two-layer model to simulate the propagation process of Bluetooth-based and SMS-based viruses in the geographic network composed of cell towers and the logical contact network composed of mobile phones, respectively. The lower layer is a cell tower network based on geographical information. Bluetooth-based viruses can spread in this layer based on local positions of mobile phones. The upper layer is a logical network based on the address book of each phone. SMS-based viruses propagate in this layer based on the contact relationships among mobile users. In this model, a geographical network is represented as a 2-dimensional grid, $G[N][N]$, and N is the total size of the grid. A cell tower is denoted as T_i, which is a tuple $< r, p(x,y), n_{tp}, T_{link} >$, where r is the service radius of a cell tower; $p(x,y)$ records the coordinates of T_i; n_{tp} is the total number of phones in the service area of T_i; T_{link} is an information list about the adjacent neighbors of T_i. In addition, the typical SIR model is used to characterize the propagation process of Bluetooth-based viruses in each tower. In a logical contact network, each phone v_i is represented as a tuple $< T_{id}, l(x,y), on-off, t_{on}, p_{click}, P_{link} >$, where T_{id} is the ID of a cell tower that provides wireless service for v_i. $l(x,y)$ records the coordinates of v_i in the geographic network; $on-off$ is a boolean variable that is used to verify whether or not v_i is open. t_{on} records the time v_i is open; p_{click} is the probability of a user clicking a suspicious message, which is determined by the security awareness of the user; P_{link} records the address book of v_i.

With this model, the effects of human operations are evaluated on SMS-based virus propagation in contact networks, and the effects of human mobility are evaluated on Bluetooth-based virus propagation in geographic networks.

(6) Cheng's model (analytical model on hybrid malware)

Cheng et al. [86] proposed an analytical model to analyze the speed and severity of spreading hybrid malware, such as Commwarrior that targets MMS and Bluetooth. In this paper, the dynamics of an infected subpopulation by MMS with time t is described using a basic differential equation as follows:

$$\frac{\mathrm{d}I_{MMS}(t)}{\mathrm{d}t} = \beta_{MMS}\frac{S(t)(\eta_{MMS}-1)}{N}I(t) \tag{13}$$

The incremental spatial infection at time t of all infection circles is given by:

$$\frac{\mathrm{d}I_{BT}(t)}{\mathrm{d}t} = \int_0^t I'_{MMS}(\tau)G'(\tau, t-\tau)\mathrm{d}\tau \tag{14}$$

However, the authors did not characterize the impact of individual difference on the propagation dynamics of malware, and also did not characterize the spatial-temporal characteristics on the propagation dynamics of malware.

(7) SEIR model (Ramachandran)

Ramachandran and Sikdar [87] presented an analytical model to explore the impact of various spreading mechanisms such as downloads from the Internet or P2P networks, transfers through Bluetooth, WLAN and infra red interfaces and through MMS or SMS messages on the dynamics of malware propagation in smartphone networks. In their model, four equations are used to characterize each location a cell phone may visit. The locations are classified into P patches and the total number of equations is reduced to $4P$. Let m_{pq} denote the rate of travel from patch q to patch p. S_p, E_p, I_p, and R_p denote the rate of change for the susceptible, exposed, infectious and recovered populations in patch $p(1 \le p \le P)$, respectively. The malware propagation in cell phones is described by the following equations:

$$\begin{cases} \frac{dS_p}{dt} = d_p(N_p - S_p) - p^p_{on}\gamma_p(t)S_p - p^p_{on}\beta_p S_p\frac{I_p}{N_p} \\ \qquad - \sum_{i=1}^{\mathrm{P}}\alpha(1-\rho)S_p\frac{I_i}{N_i} + \sum_{q=1}^{\mathrm{P}} m_{pq}S_q - \sum_{q=1}^{\mathrm{P}} m_{pq}S_p \\ \frac{dE_p}{dt} = \sum_{i=1}^{\mathrm{P}}\alpha(1-\rho)S_p\frac{I_i}{N_i} - (d_p+\varepsilon_p) - \sum_{q=1}^{\mathrm{P}} m_{pq}E_q \\ \frac{dI_p}{dt} = p^p_{on}\gamma_p(t)S_p + p^p_{on}\beta_p S_p\frac{I_p}{N_p} - (d_p+\delta_p)I_p \\ \qquad + \varepsilon_p E_p + \sum_{q=1}^{\mathrm{P}} m_{pq}I_q - \sum_{q=1}^{\mathrm{P}} m_{pq}I_p \\ \frac{dR_p}{dt} = \delta_p I_p - d_p R_p + \sum_{q=1}^{\mathrm{P}} m_{pq}R_q - \sum_{q=1}^{\mathrm{P}} m_{pq}R_p \end{cases} \tag{15}$$

where $N_p = S_p + E_p + I_p + R_p; S_p, E_p, I_p, R_p \ge 0 \quad at \quad t = 0$.

However, Ramachandran and Sikdar did not characterize the effect of human behavior on the malware propagation.

(8) SEIRD model

Xia et al. [88] built a susceptible-exposed-infected-recovered-dormancy (SEIRD) model for the Bluetooth and MMS hybrid spread mode according to the ComWar worm. They divided phone nodes into five states, such as S, E, I, R, and D, and 11 kinds of state conversions, such as (i) $S \to I$, $I \to D$, $D \to I$, with $E \to I(\beta)$ related to the Bluetooth spread mode; (ii) $S \to E$, $E \to S$, $E \to R$, and $E \to I(\mu)$ are related to the SMS/MMS spread mode; (iii) $S \to R$, $I \to S$, and $I \to R$ are related to the combination of both Bluetooth and SMS/MMS modes. The SEIRD model can be described with the following differential equations:

$$\begin{cases} \frac{\mathrm{d}S(t)}{\mathrm{d}t} = P_{ES}E(t) + P_{IS}I(t) - \beta\bar{k}S(t)I(t) - \lambda(t)S(t) \\ \qquad - P_{SR}S(t) \\ \frac{\mathrm{d}E(t)}{\mathrm{d}t} = \lambda(t)S(t) - \beta\bar{k}E(t)I(t) - (\mu + P_{ES} + P_{ER})E(t) \\ \frac{\mathrm{d}I(t)}{\mathrm{d}t} = \beta\bar{k}(S(t)+E(t))I(t) + \mu E(t) + \theta D(t) \\ \qquad - (\gamma + P_{IS} + \varepsilon)I(t) \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} = \gamma I(t) + P_{ER}E(t) + P_{SR}S(t) \\ \frac{\mathrm{d}D(t)}{\mathrm{d}t} = \varepsilon I(t) - \theta D(t) \\ N = S(t) + E(t) + I(t) + R(t) + D(t) \\ \bar{k} = \sigma(v\sqrt{4r^2 - (\Delta t)^2 v^2} + \pi r^2 - \frac{\pi}{4}(\Delta t)^2 v^2) - 1 \\ \lambda(t) = w\eta\frac{I(t)}{N}\frac{S(t)}{S(t)+I(t)} \end{cases} \tag{16}$$

where β is the infection rate, $\overline{k}$ denotes the average degree of nodes, η is the probability an infected smartphone will spread the virus to its contacts, γ is the probability that an infectious smartphone gains overall technical support and is removed, μ is the probability that the exposed smartphone becomes infectious, ε is the probability the infectious smartphone whose battery is exhausted through Bluetooth technology, enters the dormancy state, θ is the probability that a dormant smartphone becomes infectious after recharging.

However, Xia et al. did not take the variability of the malware on propagation consideration nor characterized the effect of human behavior on malware propagation.

(9) SEIR model (Fan)

Fan et al. [89] built a Susceptible-Exposed-Infected-Recovered (SEIR) model for the Bluetooth and SMS/MMS hybrid spread mode, based on the preventive immunity and mutation of the mobile phone virus. They further discussed at length the influence of the propagation parameters, such as preventive immunity of mobile phone users, mutation of virus, immunity structure in the SMS/MMS network, and node average degree in the Bluetooth network on the propagation of the virus. The phone nodes are divided into 4 states and 8 kinds of state conversions, among them: $S \to I$ and $E \to I(\beta_1)$ are Bluetooth spread mode; $S \to E$, $E \to I(\beta_2)$, and $E \to R$ are SMS/MMS spread mode; $S \to R$, $R \to S$, and $I \to R$ are the combination of both Bluetooth and SMS/MMS modes. Thus, the SEIR model can be described by the following differential equations:

$$\begin{cases} \frac{\mathrm{d}S(t)}{\mathrm{d}t} = -\beta_1\bar{k}S(t)I(t) - P_{SE}S(t) - \mu_1 S(t) + P_{RS}R(t) \\ \frac{\mathrm{d}E(t)}{\mathrm{d}t} = P_{SE}S(t) - \beta_1\bar{k}E(t)I(t) - (\mu_2+\beta_2)E(t) \\ \frac{\mathrm{d}I(t)}{\mathrm{d}t} = \beta_1\bar{k}(S(t)+E(t))I(t) + \beta_2 E(t) - \delta I(t) \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} = \mu_1 S(t) + \mu_2 E(t) + \delta I(t) - P_{RS}R(t) \\ N = S(t) + E(t) + I(t) + R(t) \\ \bar{k} = \rho\pi\gamma^2(1-\alpha) + \rho[3\Delta t v\sqrt{r^2 - \frac{1}{4}(\Delta t)^2 v^2} \\ \qquad + 2r^2\arccos(\frac{\frac{1}{2}\Delta t v}{r})]\alpha - 1 \\ P_{SE} = \lambda(t) = \omega\eta\frac{I(t)}{N}\frac{S(t)}{S(t)+I(t)} \\ P_{RS} = f(t-t_0)\varepsilon \end{cases} \tag{17}$$

where $\overline{k}$ denotes the average degree of nodes, η is the probability that infected smartphones will spread the virus to its contacts, β_1 is the rate the susceptible or exposed smartphones become infected via Bluetooth, β_2 is the rate the exposed smartphones become infected via SMS/MMS, δ is the probability the infected smartphones remove the infected viruses using anti-virus software, patches etc. and recover, μ_1 is the probability susceptible smartphones gain pre-immunity using defense technologies such as updating its virus database, or using patches, μ_2 is the probability exposed smartphones will gain pre-immunity by defense technologies such as updating its virus database, and using patches.

However, Fan et al. did not characterise the effect of human behaviors on the malware propagation.

(10) WPM model

Peng and Wang [90], [91] proposed a worm propagation modeling scheme (WPM). WPM utilizes the two-dimensional (2D) cellular automata to simulate the dynamics of the worm propagation process from a single node to an entire network. The WPM scheme integrates an infection factor, which evaluates the degree of spread for infected nodes, and the resistance factor, which offers a resistance evaluation towards susceptible nodes. Let N_u denote the number of each node's neighbor nodes. Let $\Phi_{C_{ij},C_{kl}}$ denote the interaction coefficient between cell C_{ij} and its neighbors, which is defined as the strength or likelihood of infection from one cell to another. Let δ denote the infection index, which is calculated as a ratio of the interaction coefficient between cell C_{ij} and its neighbors to its resisted factor. Thus, $\Phi_{C_{ij},C_{kl}}$ and δ are described as follows:

$$\Phi_{C_{ij},C_{kl}} = \sum_{v=1}^{v=N_u} \frac{IF_{vu}}{\sqrt{(i-k)^2+(j-l)^2}} \tag{18}$$

$$\delta = \frac{\Phi_{C_{ij},C_{kl}}}{RF} \tag{19}$$

where IF_{vu} is the infected factor, which denotes infection degree from node v to node u ($0 \leq IF \leq 1$). RF is the resisted factor, which denotes the resistance degree of the node on infection from other nodes ($0 \leq RF \leq 1$). However, the authors do not take the dynamics characteristics of the hybrid spread mode into consideration.

(11) Wang's model

Wang et al. [92] presented a model on mobile malware using the SI model and studied spreading patterns of both Bluetooth and MMS worms. In this model, mobile phone data was processed to obtain the mobility of devices at a cell-tower resolution. Let an infected user (I) infect a susceptible user (S), thus, the number of infected users evolves in time (t) and can be represented as follows:

$$\frac{\mathrm{d}I}{\mathrm{d}t} = \frac{bSI}{N} \tag{20}$$

where $b = m < k >$ is the effective infection rate with m = 1, N is the number of users in the tower area, and the average number of contacts is $< k >= rA = NA/A_{tower}$, where $A = pr^2$ represents the Bluetooth communication area and $r = N/A_{tower}$ is the population density inside a tower's service area.

Once an infected user moves into the vicinity of a new tower, it serves as a source for a Bluetooth infection in its new location. However, the authors proposed a more realistic propagation model to study Bluetooth-based and MMS-based worms by analyzing and predicting the mobility patterns in real world situations. Moreover, they extracted the characteristics of human mobility from real data traces, and then proposed a model to predict mobility patterns. However, human behavior (i.e., whether or not a user opens an infected message) was ignored in this model.

(12) Szongott's model

Szongott et al. [93] presented a schema to show how mobile malware can spread epidemically on a device-to-device infection vector, and almost infect an entire metropolitan area within a couple of hours, such as downtown Chicago. This schema has a difference between two distinct infection environments: roads and locations. The infection probability for devices located in these locations is defined as follows:

$$A_i = \beta \times \frac{l \times a}{i} \tag{20}$$

where A_i denotes the area per infected visitor, which is determined by dividing the total area of the location as determined by its story count l and its base area a by the number of infected devices i. β is used to dampen the infection rate to account for the fact that people in the building will seldom be distributed equally, and to account for the fact that in buildings with different infrastructure and ad-hoc networks, they will disturb each other and thereby make an infection less likely. Let t_{loc} denote the device activation interval, and t_{visit} denote the duration of its visit. The final infection probability P_i is obtained by the combination of these two factors.

$$P_i = \frac{t_{visit}}{t_{loc}} \times \frac{\pi r^2}{A_i} \tag{21}$$

where r denotes the Wi-Fi range.

This schema considers the spatial-temporal evolution process of mobile malware propagation and characterized the effect of human behaviors on malware propagation. However, the authors failed to characterize the impact of individual difference on the propagation dynamics of malware.

A comparison of malware propagation models is listed in Table V. From Table V, it is known that differential equations are widely used to model malware propagation in existing work. That is, most malware propagation models are based on deterministic models, and only a small number are based on stochastic and spatial-temporal models.

B. Simulators for Mobile Malware Propagation

In this subsection, we investigate the simulator for malware propagation models in smartphones, such as event-based simulator [94], EpiNet [95], EpiCure [96], ns-2 simulator [97], trace-driven simulator [98], [99], and agent-based simulator [100].

Fleizach et al. [94] developed an event-based simulator to evaluate the effects of malware propagation using communication services like VOIP and MMS in mobile phone networks.

Channakeshava et al. [95] presented an end-to-end framework for simulating the spread of worms over wireless

TABLE V
COMPARISON OF MALWARE PROPAGATION MODELS

Model	*Modeling theory*	*Malware type*	*Individual difference*	*Hunman behaviors*	*Mobility*
Yan [79], [80]	Differential equations	Bluetooth worm	No	No	Yes
SIP [81]	Differential equations	Bluetooth worm	No	No	Yes
SIS [82]	Differential equations	Bluetooth worm	No	No	No
Micken [83]	Differential equations	Bluetooth worm	No	No	No
Two-layer [84], [85]	Differential equations	Bluetooth and SMS worm	No	Yes	Yes
Cheng [86]	Differential equations	Bluetooth and MMS worm	No	No	No
SEIR [87]	Differential equations	Bluetooth and SMS/MMS worm	No	No	No
SEIRD [88]	Differential equations	Bluetooth and MMS worm	No	No	Yes
SEIR(Fan) [89]	Differential equations	Bluetooth and SMS/MMS worm	No	No	Yes
WPM [90]	Cellular automata	Bluetooth worm	Yes	No	No
Wang [92]	Differential equations	Bluetooth and MMS worm	No	No	Yes
Szongott [93]	Spatial-temporal model	Hybrid malware	No	Yes	Yes

networks, named EpiNet. Based on [95], Channakeshava et al. [96] also proposed an individual-based, named EpiCure, which can be used to study malware propagation over realistic mobile networks. In comparison to EpiNet, EpiCure has two advantages: scalability for very large networks and support for complex interventions.

Yan and Eidenbenz [101] used the ns-2 simulator to study the nature, characteristics and spreading dynamics of mobile worms and the effectiveness of several parameters on worm spreading. However, it failed to provide a flexible and scalable computational framework to evaluate and analyze a large scale wireless epidemic in the ns-2 simulator.

Su et al. [98] investigated whether or not a large-scale Bluetooth worm outbreak is viable in practice. The authors used trace-driven simulations to examine the propagation dynamics of Bluetooth worms and found that Bluetooth worms can infect a large population relatively quickly, in just a few days.

Miklas et al. [99] built a trace-driven simulator to study the interactions between Bluetooth devices. They concluded that Bluetooth-based worms spread more widely by exploiting contacts between 'strangers' instead of 'friends'.

Bose and Shin [100] modeled malware propagation through both MMS/SMS and Bluetooth vectors using a fine-grained agent-based simulator, and emulated the propagation of this virus in a small mobile network representative of a public meeting place, such as a stadium or airport, using data from a real-world SMS network.

The comparison of simulator for malware propagation is shown in Table VI.

V. PROBLEMS OF CURRENT MODELS AND FUTURE TRENDS

Based on our study of this topic, we summarize the shortcomings of smartphone malware propagation models that we have surveyed in this paper, and point out possible future trends in this field.

A. Existing Problems

Due to the short history of smartphone malware, related research on this topic is still in its infancy. We list the disadvantages of the surveyed modeling techniques based on our knowledge of the field as follows:

(1) Diversity of propagation models.

In general, each of the existing smartphone malware propagation models were proposed based on specific malware. For example, the WPM model is based on a Bluetooth worm, while the SEIRD model is based on Bluetooth and MMS worms. A representative unified and integrated propagation model remains unknown to the cyber security community. Of course, this is extremely challenging and a solution may not exist.

(2) Difficulty comparing performance among different propagation models.

It is very difficult to compare the performance between any two models we have studied in this paper. In the aforementioned mathematical-based models, the evaluation of their performance is completed by simulations. As to most of the existing models, they fail to make a comparative analysis with other models, and fail to evaluate the performance in a practical environment as well.

(3) Modeling based on partial information

From Table V, we can see that most existing models fail to consider all possible input parameters. For example, most models have neither considered the impact of individual differences on malware propagation, nor considered the impact of human behavior on malware propagation. Nor did any describe the impact of random mobility on smartphone users.

B. Future Trends

Combining the issues raised in the previous sections, and based on our understanding, we believe the following directions [102], [103] are promising for further research into smartphone malware propagation modeling.

(1) Integration of knowledge from cross disciplines.

Due to the complexity of the topic, and in order to address the problem, it is necessary to integrate the knowledge of cross disciplines, such as complex network theory, social network theory, machine learning, artificial intelligence, the stochastic process, and graph theory. The integration of this knowledge can offer us a model that is close to real malware propagation scenarios, e.g., transmission capacity, speed and possible damage, and can also offer us to the opportunity

TABLE VI
COMPARISON OF SIMULATOR FOR MALWARE PROPAGATION MODELS

	$ns-2$ [97]	$Trace-driven$ [98], [99]	$Agent-based$ [100]	$Event-based$ [94]	$EpiNet$ [95]	$EpiCure$ [96]
Time	1986	2006	2006	2007	2009	2011
Platform framework	Complex	Simple	Simple	Simple	Simple	Simple
Purpose	Examine the performance of wired networks or wireless networks	Examine the propagation dynamics of Bluetooth worms	Study mobile viruses that spread through Bluetooth and SMS/MMS	Study malware that spread through VoIP and MMS	Wireless epidemiology	Wireless epidemiology
Network type	Wired networks or wireless networks	Mobile phone networks	Mobile phone networks	Mobile phone networks	Wireless networks	Wireless networks
Network scale	Medium	Medium	Medium	Medium	Medium	Large
Simulation speed	Slow	Quick	Slow	Quick	Quick	Quick
Simulation implementation	Difficult	Easy	Easy	Easy	Easy	Easy

design a node misbehavior model [104], that can be used to describe the complexity and uncertainty of virus propagation.

(2) A social network is a critical component to solving the problem.

A social contact network is the basis of malware propagation, and complex human relationships combine with ever-changing personal behavior leads to a complex morphology of the actual social network. Therefore, the formation mechanism of a social network and its evolution are core issues for the dynamics of malware propagation. The recently appeared on network science is a good direction for us to explore.

(3) Mobile social networks are an essential element of the problem.

In mobile social networks [105], there is potential for collaborative data gathering via already deployed and human maintained devices. Mobile social networks provide an in-depth understanding about the impact of human behavior on malware propagation in smartphones, such as social relationships, human operations, and mobility patterns. Under realistic scenarios, we need to model malware propagation to characterize its speed and severity in smartphone-based mobile networks, to understand how network topology affects propagation, how propagation affects the network, and to highlight the implications for network-based defenses against such malware.

VI. CONCLUSIONS

Recent advancements in mobile technology have brought smartphones and malware attacks into focus. The trend shows a severe increase in mobile malware as many other threats designed for PC operating systems, migrate to smartphone platforms. To characterize the risks and features of malware in smartphones, this paper has summarized advancements in this area of research. In this paper, we have outlined the current scenario of mobile malware in smartphones by reviewing the process of its evolution, infection vectors, and categories, along with the risks. We also provided several typical examples. We also surveyed the literature from 2004-2012 by analyzing the basic characteristics of typical malware in smartphones. The current modeling theory and technology of epidemics has been generalized by discussing the features of deterministic models, stochastic models, and spatial-temporal models. Moreover, we have summarized current malware propagation models in smartphones by focusing on existing mechanisms related to characterizing the dynamics of malware propagation based on the ordinary differential equations, the Markov process, or cellular automata. In the final section of this paper, we also presented the disadvantages of existing models and discussed future trends.

ACKNOWLEDGMENT

This work was partially supported by the National Natural Science Foundation of China under Grant No. 61073037, the Postdoctoral Science Foundation of China under Grant No. 2012M511757, and the Natural Science Foundation of Guangdong Province under Grant No. S2011040002356.

REFERENCES

[1] S. Peng, "A Survey on Malware Containment Models in Smartphones," *Applied Mechanics and Materials*, vol. 263-266, pp. 3005–3011, 2013.
[2] J. Jamaluddin, N. Zotou, and P. Coulton, "Mobile phone vulnerabilities: a new generation of malware," in *Proc. IEEE International Symposium on Consumer Electronics*, 2004, pp. 199–202.
[3] (2010, November) Hackers hijack 1 million china cell phones. [Online]. Available: http://www.informationweek.com/news/security/attacks/228200648
[4] (2012, May) Mobile malware attacks on the rise. [Online]. Available: http://www.cellular-news.com/story/54544.php
[5] (2012, February) 2011 mobile threats report. [Online]. Available: http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf
[6] G. Delac, M. Silic, and J. Krolo, "Emerging security threats for mobile platforms," in *Proc. 34th International Convention MIPRO*, Opatija, Croatia, May 2011, pp. 1468–1473.
[7] (2011, October) Ict facts and figures, 2011. [Online]. Available: http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf
[8] (2012, February) Smart phones overtake client pcs in 2011. [Online]. Available: http://www.canalys.com/newsroom/smart-phones-overtake-client-pcs-2011
[9] What is the difference: Viruses, worms, trojans, and bots? [Online]. Available: http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html#5
[10] 2004 threat summary. [Online]. Available: http://www.f-secure.com/en/web/labs_global/2004-threat-summary
[11] (2006, October) Mobile malware evolution: An overview, part 2. [Online]. Available: http://www.securelist.com/en/analysis?pubid=201225789
[12] (2006, September) Mobile malware evolution: An overview, part 1. [Online]. Available: http://www.securelist.com/en/analysis?pubid=200119916

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

[14] M. Hypponen, "Mobile security review september 2010," F-Secure Labs, HelsinkiFinland, Tech. Rep., September 2010.

[15] A. D. Schmidt and S. Albayrak, "Malicious software for smartphones," Technische Universitat Berlin - DAI-Labor, Tech. Rep. TUBDAI 02/08-01, February 2008.

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

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

[18] (2010, February) Kaspersky security bulletin 2009-malware evolution 2009. [Online]. Available: http://www.securelist.com/en/analysis/204792100/Kaspersky_Security_Bulletin_2009_Malware_Evolution_2009

[19] (2011, March) Mobile malware evolution: An overview, part 4. [Online]. Available: http://www.securelist.com/en/analysis/204792168/Mobile_Malware_Evolution_An_Overview_Part_4

[20] (2012, March) Kaspersky security bulletin malware evolution 2011. [Online]. Available: http://www.securelist.com/en/analysis/204792217/Kaspersky_Security_Bulletin_Malware_Evolution_2011

[21] (2012, March) Android malware continues to surge. [Online]. Available: http://www.informationweek.com/news/mobility/security/232601868

[22] (2012, February) Mobile malware evolution, part 5. [Online]. Available: http://www.securelist.com/en/analysis/204792222/Mobile_Malware_Evolution_Part_5

[23] Mobile malware: Threats and prevention. [Online]. Available: http://hackerzvoice.net/ceh/CEHv6%20Module%2036%20Hacking%20Mobile%20Phones,%20PDA%20and%20Handheld%20Devices/wp_malware7a_en.pdf

[24] (2004, November) Malware what is it and how to prevent it? [Online]. Available: http://arstechnica.com/security/2004/11/malware/

[25] (2011, May) What are viruses, trojans, worms & spyware. [Online]. Available: http://www.antivirusware.com/articles/viruses-trojans-worms-spyware.htm

[26] Computer worm. [Online]. Available: http://en.wikipedia.org/wiki/Computer_worm

[27] N. Xu, F. Zhang, Y. Luo, W. Jia, D. Xuan, and J. Teng, "Stealthy video capturer: a new video-based spyware in 3g smartphones," in *Proc. second ACM conference on Wireless network security (WiSec 2009)*, New York, NY, USA, March 2009, pp. 69–78.

[28] Trojan. [Online]. Available: http://www.f-secure.com/v-descs/trojan.shtml

[29] R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang, "Soundcomber: A stealthy and context-aware sound trojan for smartphones," in *Proc. Network and Distributed System Security Symposium (NDSS 2011)*, San Diego, California, USA, February 2011.

[30] Backdoor. [Online]. Available: http://www.f-secure.com/v-descs/backdoor.shtml

[31] Rootkit. [Online]. Available: http://en.wikipedia.org/wiki/Rootkit

[32] P. Porras, H. Saïdi, and V. Yegneswaran, "An Analysis of the iKee.B iPhone Botnet," *Security and Privacy in Mobile Information and Communication Systems, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 47, pp. 141–152, 2010.

[33] Mobile threat report q4 2011. [Online]. Available: http://www.f-secure.com/weblog/archives/Mobile_Threat_Report_Q4_2011.pdf

[34] (2011, December) Bluetooth overview. [Online]. Available: http://www.developer.nokia.com/Community/Wiki/Bluetooth_Overview

[35] Mquito. [Online]. Available: http://www.f-secure.com/v-descs/mquito.shtml

[36] Trojan:symbos/zeusmitmo.a. [Online]. Available: http://www.f-secure.com/v-descs/trojan_symbos_zeusmitmo_a.shtml

[37] P. P. C. Lee, T. Bu, and T. Woo, "On the detection of signaling DoS attacks on 3G/WiMax wireless networks," *J. Computer Networks*, vol. 53, no. 15, pp. 2601–2616, 2009.

[38] (2010, August) Research trojan:androidos/fakeplayer.a. [Online]. Available: http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Trojan:AndroidOS/Fakeplayer.A

[39] (2011, June) Research trojan:androidos/basebridge.b. [Online]. Available: http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Trojan%3AAndroidOS%2FBaseBridge.B

[40] D. Damopoulos, G. Kambourakis, and S. Gritzalis, "iSAM: An iPhone Stealth Airborne Malware," *Future Challenges in Security and Privacy for Academia and Industry, IFIP Advances in Information and Communication Technology, Springer, Berlin*, vol. 354, pp. 17–28, 2011.

[41] D. Damopoulos, G. Kambourakis, M. Anagnostopoulos, S. Gritzalis, and J. H. Park, "User privacy and modern mobile services: are they on the same path?" *Personal and Ubiquitous Computing, Springer-Verlag London*, no. DOI 10.1007/s00779-012-0579-1., June 2012.

[42] Worm:iphoneos/ikee. [Online]. Available: http://www.f-secure.com/v-descs/worm_iphoneos_ikee.shtml

[43] Worm:iphoneos/ikee.b. [Online]. Available: http://www.f-secure.com/v-descs/worm_iphoneos_ikee_b.shtml

[44] Trojan:java/redbrowser.a. [Online]. Available: http://www.f-secure.com/v-descs/redbrowser_a.shtml

[45] Brador. [Online]. Available: http://www.f-secure.com/v-descs/brador.shtml

[46] Backdoor:wince/phonecreeper.a. [Online]. Available: http://www.f-secure.com/v-descs/backdoor_wince_phonecreeper_a.shtml

[47] 2012 security report in mobile phone. [Online]. Available: http://cn.nq.com/neirong/2012shang.pdf

[48] J. P. Trapman, "On stochastic models for the spread of infections," Ph.D. dissertation, Vrije Universiteit Amsterdam, The Netherlands, September 2006. [Online]. Available: http://www2.math.su.se/~ptrapman/proefschrifttrapmanrevisie.pdf

[49] L. J. S. Allen, "Some discrete-time si, sir, and sis epidemic models," *Mathematical Biosciences*, vol. 124, no. 1, pp. 83–105, November 1994.

[50] R. M. Andersen and R. M. May, *Infectious Diseases of Humans: Dynamics and Control*. New York: Oxford University Press, 1992.

[51] W. O. Kermack and A. G. McKendrick, "Contributions to the mathematical theory of epidemics," in *Proc. Royal Society of London: Series A*, 1932, pp. 55–83.

[52] ——, "Contributions of mathematical theory to epidemics," in *Proc. Royal Society of London: Series A*, 1927, pp. 700–721.

[53] (2012, February) Epidemic model. [Online]. Available: http://en.wikipedia.org/wiki/Epidemic_model#Deterministic IEEE Trans.

[54] Z. S. Chen and C. Y. Ji, "Spatial-temporal modeling of malware propagation in networks," *IEEE Trans. Neural Netw.*, vol. 16, no. 5, pp. 1291–1303, 2005.

[55] Y. Song and G. Jiang, "Modeling malware propagation in wireless sensor networks using cellular automata," in *Proc. IEEE International Conference Neural Networks & Signal Processing (ICNNSP 2008)*, Zhenjiang, China, June 2008, pp. 623–627.

[56] A. R. Mikler, S. Venkatachalam, and K. Abbas, "Modeling infectious diseases using global stochastic cellular automata," *J. Biological Systems*, vol. 13, no. 4, pp. 421–439, 2005.

[57] M. Martin. An explicit si epidemic model. [Online]. Available: http://math.jccc.net:8180/webMathematica/JSP/mmartin/SImodelExplicit.jsp

[58] Epidemic model. [Online]. Available: http://en.wikipedia.org/wiki/Epidemic_model#The_SIR_Model

[59] L. J. S. Allen, *An Introduction to Stochastic Epidemic Models*, F. Brauer, P. van den Driessche, and J. Wu, Eds. Springer-Verlag, 2008.

[60] L. J. S. Allen and A. M. Burgin, "Comparison of deterministic and stochastic sis and s ir models in discrete time," *Mathematical Biosciences*, vol. 163, pp. 1–33, 2000.

[61] L. J. S. Allen and E. J. Allen, "A comparison of three different stochastic population models with regard to persistence time," *Theoretical Population Biology*, vol. 64, pp. 439–449, 2003.

[62] N. Ganguly, B. K. Sikdar, A. Deutsch, G. Canright, and P. P. Chaudhuri, "A survey on cellular automata," Centre for High Performance Computing, Dresden University of Technology, Tech. Rep., December 2003.

[63] S. H. White, A. M. del Rey, and G. R. Sanchez, "Modeling epidemics using cellular automata," *Applied Mathematics and Computation*, vol. 186, no. 1, pp. 193–202, March 2007.

[64] S. Qing and W. Wen, "A survey and trends on internet worms," *Computers & Security*, no. 24, pp. 334–346, 2005.

[65] J. Kephart and S. White, "Directed-graph epidemiological models of computer viruses," in *Proc. IEEE Computer Symposium on Research in Security and Privacy*, 1991, pp. 343–359.

[66] C. C. Zou, W. Gong, and D. Towsley, "Code red worm propagation modeling and analysis," in *Proc. ACM Conference on Computer and Communication Security (CCS 2002)*, Washington DC, USA: ACM press, 2002, pp. 138–147.

[67] S. Staniford, V. Paxson, and N. Weaver, "How to own the internet in your spare time," in *Proc. 11th USENIX Security Symposium*, San Francisco, USA: ACM Press, 2002, pp. 149–167.

[68] C. C. Zou, D. Towsley, and W. B. Gong, "Modeling and simulation study of the propagation and defense of internet e-mail worms," *IEEE Trans. Dependable Secure Comput.*, vol. 4, no. 2, pp. 105–118, 2007.

[69] Y. Gu and S. Wang, "A discrete probabilistic model of malware propagation," *Acta Electronica Sinica*, vol. 38, no. 4, pp. 894–898, 2010.

[70] Y. Yang, S. Zhu, and G. Cao, "Improving sensor network immunity under worm attacks: A software diversity approach," in *Proc. 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2008)*, Hong Kong, China, May 27-30 2008, pp. 149–158.

[71] S. Tang and B. L. Mark, "Analysis of virus spread in wireless sensor networks: An epidemic model," in *Proc. 7th International Workshop on Design of Reliable Communication Networks (DRCN 2009)*, Washington, D. C., USA, October 2009, pp. 86–91.

[72] Y. Song and G. Jiang, "Model and dynamic behavior of malware propagation over wireless sensor networks," in *The First International Conference on Complex Sciences: Theory and Application (COMPLEX 2009)*, Shanghai China, February 2009, pp. 487–502.

[73] S. A. Khayam and H. Radha, "Using signal processing techniques to model worm propagation over wireless sensor networks," *IEEE Signal Processing Mag.*, pp. 164–169, March 2006.

[74] M. Nekovee, "Worm epidemics in wireless ad hoc networks," *IEEE Signal Processing Mag.*, vol. 9, no. 189, pp. 1–13, June 2007.

[75] H. N. Nguyen and Y. Shinoda, "Modeling malware diffusion in wireless networks with nodes heterogeneity and mobility," in *Proc. 19th IEEE International Conference on Computer Communications and Networks (ICCCN 2010)*, Zurich, Switzerland, August 2010, pp. 1–8.

[76] J. Chen, S. Wei, and W. Peng, "General worm propagation model for wireless ad hoc networks," in *Proc. IEEE 2nd International Conference on Computer Science and Information Technology (ICCSIT 2009)*, Beijin, China, August 2009, pp. 468–473.

[77] C. Wang and J. Ma, "A malware propagation model in wireless ad hoc networks," *Acta Electronica Sinica*, vol. 35, no. 12, pp. 79–82, December 2007.

[78] V. Karyotis, A. Kakalis, and S. Papavassiliou, "Malware-propagative mobile ad hoc networks: asymptotic behavior analysis," *J. Computer Science and Technology*, vol. 23, no. 3, pp. 389–399, May 2008.

[79] G. Yan and S. Eidenbenz, "Modeling propagation dynamics of bluetooth worms," in *Proc. 27th International Conference on Distributed Computing Systems (ICDCS 2007)*, Toronto, Ontario, Canada, June 2007, pp. 42–51.

[80] ——, "Modeling propagation dynamics of bluetooth worms (extended version)," *IEEE Trans. Mobile Comput.*, vol. 8, no. 3, pp. 353–367, March 2009.

[81] C. J. Rhodes and M. Nekovee, "The opportunistic transmission of wireless worms between mobile devices," *Physica A: Statistical Mechanics and its Applications*, vol. 387, no. 27, pp. 6837–6844, December 2008.

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

[83] J. W. Mickens and B. D. Noble, "Modeling epidemic spreading in mobile environments," in *Proc. 4th ACM workshop on Wireless security (WiSe 2005)*, Cologne, Germany, September 2005, pp. 77–86.

[84] C. Gao and J. Liu, "Modeling and predicting the dynamics of mobile virus spread affected by human behavior," in *Proc. 12th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2011)*, Lucca, Italy, June 2011, pp. 1–9.

[85] ——, "Modeling and restraining mobile virus propagation," *accepted by IEEE Trans. Mobile Comput.*, no. Digital Object Identifier: 10.1109/TMC.2012.29, 2012.

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

[87] K. Ramachandran and B. Sikdar, "Modeling malware propagation in networks of smart cell phones with spatial dynamics," in *Proc. 26th IEEE International Conference on Computer Communications (INFOCOM 2007)*, Anchorage , Alaska , USA, May 2007, pp. 2516–2520.

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

[89] Y. Fan, K. Zheng, and Y. Yang, "Epidemic model of mobile phone virus for hybrid spread mode with preventive immunity and mutation," in *Proc. 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM 2010)*, Chengdu, China, September 2010, pp. 1–5.

[90] S. Peng and G. Wang, "Worm propagation modeling using 2d cellular automata in bluetooth networks," in *Proc. 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2011)*, Changsha, China, November 2011, pp. 282–287.

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

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

[93] C. Szongott, B. Henne, and M. Smith, "Evaluating the threat of epidemic mobile malware," in *Proc. IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2012)*, October 2012, pp. 443–450.

[94] C. Fleizach, M. Liljenstam, P. Johansson, G. M. Voelkery, and A. Mhes, "Can you infect me nnow? malware propagation in mobile phone networks," in *Proc. 5th ACM Workshop on Recurring Malcode (WORM 2007)*, Alexandria, VA, USA, November 2007, pp. 61–68.

[95] K. Channakeshava, D. Chafekar, K. Bisset, V. Kumar, and M. Marathe, "Epinet: A simulation framework to study the spread of malware in wireless networks," in *Proc. 2nd International Conference on Simulation Tools and Techniques (SIMUtools 2009)*, Rome, Italy, March 2009, pp. 1–10.

[96] K. Channakeshava, K. Bisset, V. Kumar, M. Marathe, and S. Yardi, "High performance scalable and expressive modeling environment to study mobile malware in large dynamic networks," in *Proc. IEEE International Parallel & Distributed Processing Symposium (IPDPS2011)*, Anchorage, Alaska USA, May 2011, pp. 770–781.

[97] The network simulator - ns-2. [Online]. Available: http://nsnam.isi.edu/nsnam/index.php/Main_Page

[98] J. Su, K. Chan, A. Miklas, A. A. K. Po, S. Saroiu, E. Lara, and A. Goel, "A preliminary investigation of worm infections in a bluetooth environment," in *Proc. 4th ACM Workshop on Recurring Malcode (WORM 2006)*, Fairfax, VA, USA, November 2006, pp. 9–16.

[99] A. Miklas, K. Gollu, K. Chan, S. Saroiu, K. Gummadi, and E. Lara, "Commwarrior worm propagation model for smart phone networks," *UbiComp 2007*, pp. 409–428, 2007.

[100] A. Bose and K. G. Shin, "On mobile viruses exploiting messaging and bluetooth services," in *Proc. Second International Conference on Security and Privacy in Communication Networks*, Baltimore, MD, August 2006, pp. 1–10.

[101] G. Yan and S. Eidenbenz, "Bluetooth worms: Models, dynamics, and defense implications," in *Proc. IEEE Twenty-Second Annual Computer Security Applications Conference (ACSAC 2006)*, Miami Beach, FL, USA, December 2006, pp. 245–256.

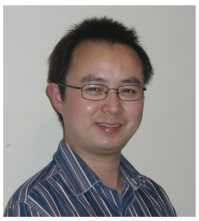
[102] N. Husted and S. Myers, "Why mobile-to-mobile wireless malware won't cause a storm," in *Proc. 4th USENIX conference on Large-scale exploits and emergent threats (LEET 2011)*, March 2011, pp. 7–14.

[103] M. Wilson, "Using the friendship paradox to sample a social network," *Physics Today*, vol. 63, no. 10, pp. 15–16, November 2010.

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

[105] S. Peng, G. Wang, and S. Yu, "Modeling malware propagation in smartphone social networks," in *Accepted by the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2013)*, Australia, July 2013.

Sancheng Peng received his Ph.D. degree in computer science from Central South University, Changsha, China, in 2010. He is now an Associate Professor with the School of Computer Science, Zhaoqing University, Zhaoqing, China. He was a Research Associate of City University of Hong Kong from 2008 to 2009. His research interests include network and information security, trusted computing, and mobile computing.



Shui Yu (M'05) received his B.Eng. and M.Eng. degrees from University of Electronic Science and Technology of China, Chengdu, China, in 1993 and 1999, respectively. He received his Ph.D. degree from Deakin University, Victoria, Australia, in 2004. He is currently a Lecturer with the School of Information Technology, Deakin University, Victoria, Australia. His research interests include networking theory, network security, and mathematical modeling. He is a member of IEEE.

Aimin Yang received his B.Eng. from Hunan University of Science and Technology, Xiangtan, China, in 1993. He received his M.Eng. degrees from National University of Defense Technology, Changsha, China, in 2001, and his Ph.D. degree from Fudan University, Shanghai, China, in 2005. He is currently a Professor with the School of Informatics, Guangdong University of Foreign Studies, Guangzhou, China. His research interests include intelligent computing, network traffic classification, and machine learning.