Journal of Computer and System Sciences 79 (2013) 586–595

Contents lists available at SciVerse ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Modeling the dynamics of worm propagation using two-dimensional cellular automata in smartphones

Sancheng Peng [a], Guojun Wang [b,*], Shui Yu [c]

[a] School of Computer Science, Zhaoqing University, Zhaoqing, 526061, China
[b] School of Information Science and Engineering, Central South University, Changsha, 410083, China
[c] School of Information Technology, Deakin University, 221 Burwood HWY, Burwood, VIC 3125, Australia

ARTICLE INFO

Article history:
Received 1 March 2012
Received in revised form 29 September 2012
Accepted 8 November 2012
Available online 14 December 2012

Keywords:
Smartphones
Worm propagation
Bluetooth
Cellular automata

ABSTRACT

Smartphones combine the communication capabilities of cellphones and the functions of PDA (personal digital assistant), which enable us to access a large variety of ubiquitous services, such as surfing the web, sending/receiving emails, MMS, and online shopping. However, the availability of these services provided by smartphones increases the vulnerability to worm attacks. In addition, modeling on worm propagation in smartphones is particularly challenging because it is difficult to piece together dynamics from pair-wise device interactions. To characterize the propagation dynamics of worms in smartphones, we propose an efficient worm propagation modeling scheme using a two-dimensional cellular automata based on the epidemic theory. A set of suitable local transition rules is designed for the two-dimensional cellular automata in this scheme. Moreover, this scheme integrates an infection factor to evaluate the spread degree of infected nodes, and a resistance factor to evaluate the degree that susceptible nodes resist. Five classes of epidemic states are considered: susceptible, exposed, infected, diagnosed, and recovered. We explore a strategy for simulating the dynamics of worm propagation process from a single node to the entire network. The effectiveness and rationality of the proposed model have been validated through extensive simulations.

1. Introduction

Smartphones combine the wireless communication capabilities of cellphones and the functionalities of personal digital assistants (PDAs). They can be used to surf the web, send/receive emails, store and play music, and take photographs and videos. In addition, most smartphones use an application-based interface, which allows users to download individual programs that can perform a variety of tasks. Canalys [1] published its final worldwide country-level Q2 2011 smart phone market estimates in August 1, 2011, showing a substantial market growth in all regions of the world. Globally, the market grows 73% year-on-year, with around 107.7 million units shipped in the second quarter of 2011.

As the popularity of smartphones increases, the number of smartphones on the market is steadily increasing. To more and more users, smartphones are becoming an integral part of their everyday lives. Moreover, most smartphones are now being equipped with advanced features, such as e-mail access and multimedia messaging, which increases their vulnerability to infection. Yet, fewer smartphones are being designed to guard against worm attacks, which makes them a more appealing target to hackers and worm writers.

* Corresponding author.
E-mail address: csgjwang@mail.csu.edu.cn (G. Wang).

0022-0000/$ – see front matter
http://dx.doi.org/10.1016/j.jcss.2012.11.007

Worms are self-replicating computer viruses, which can propagate through computer networks without any human intervention. They have been rampant in the Internet for more than two decades. Since 2004, worms have been known to spread among smartphones and other mobile devices through wireless networks. The first known worm in smartphones emerged in June 2004. It was called Cabir [2] and was propagated through Bluetooth [3,4] as an infection vector.

There are various channels used by malware in smartphones to transmit an infection to other susceptible smartphones. Smartphones can be subjected to various attack vectors, such as SMS, Bluetooth, WiFi, Web browsers, and emails. These become a step stone that allows a hacker to have access to personal information on personal smartphones. In this paper, we focus on proximity based communication channels, namely, we concentrate our study on modeling and analysis of Bluetooth-based worm propagation, which provides a means of message transfer similar to the method of spreading infectious diseases. A preliminary version of this paper appeared in [5].

Mathematical epidemiology has existed for over a hundred years. Epidemic modeling is used to imitate the spreading of infectious diseases for a given population, such as H1N1, SARS, and influenza. Infected individuals spread the virus to healthy individuals that they contact with. We can use this model to predict the transmission rate of mobile malware in smartphones based on contact via proximity.

Since Internet worms are similar to biological viruses in their self-replicating and propagative behaviors, epidemiological models for analyzing the propagation of Internet worms is nothing new to us, as there has been tremendous interest in modeling the propagation of Internet worms over the past decades [6–8]. The study of computer worms in general, and Internet worms in particular, is a very popular topic of research.

The security issue regarding worm 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 behaviors of worms in wireless networks, such as wireless sensor networks [9] and wireless ad-hoc networks [10]. Most epidemic models have focused almost entirely on the technology of the differential equations [9] and the Markov chain [10].

Although most previous work can provide some valuable insight into the characteristics and dynamics of worm propagation, the models based on differential equations fail to capture the local characteristics of spreading processes, nor do they include interaction behaviors among individuals. Furthermore, the models based on the Markov chain are difficult to describe the spatial–temporal process of worm propagation.

Cellular automata (CA) [11] can overcome these drawbacks and has been used as an efficient alternative method to characterize epidemic spreading [12–15] and malware propagation [16]. Generally speaking, cellular automata can model the computation capability characterizing physical, biological, or environmental complex phenomena, such as growth processes, reaction–diffusion systems, epidemic models, and the spread of forest fire.

Even though CAs have been used for several decades in the domain of computational models, modeling worm propagation has rarely been utilized to its full potential. The main goal of our work is to verify the applicability using the cellular automata to characterize the propagation dynamics of Bluetooth worms. We believe that CAs can be useful in simulating this kind of network because the behavior and/or the state of a wireless node are/is capable of modifying all network behaviors. This characteristic is similar to that found in many dynamic systems, which are commonly simulated through CAs.

In this paper, based on cellular automata, we present a detailed analytical model that characterizes the propagation dynamics of Bluetooth worms by considering the following realistic modeling assumptions: 1) the infection factor of an infectious device for susceptibility is different, and 2) the resistance factor of each device for spreading a worm is different. These assumptions are not usually addressed in previous analytical work due to their simplicity. The goal of our work is summarized as follows:

- To characterize the propagation dynamics of Bluetooth worms by exploiting cellular automata and by introducing an infection index to measure the state of transition to susceptible individuals.
- To formulate the impact of individual difference on the propagation dynamics of Bluetooth worm by introducing an infection factor and/or resistance factor of individuals.
- To show the effectiveness and rationality of the proposed approach through extensive simulations and numerical analysis.

The remainder of this paper is structured as follows: In Section 2, we provide an overview of related work and discuss the system model in Section 3. In Section 4, we present a model to characterize the spreading of the epidemic. We show the results of model validation in Section 5, and conclude the paper in Section 6.

2. Related work

In this section, we investigate related work in three dimensions. The first dimension is the Bluetooth-based worm propagation model; the second is related to the SMS/MMS-based worm propagation model; and the last is related to the hybrid worm propagation model.