Commun Nonlinear Sci Numer Simulat 37 (2016) 249–264

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

journal homepage: www.elsevier.com/locate/cnsns

Modeling the propagation of mobile malware on complex networks

Wanping Liu[a,*], Chao Liu[a], Zheng Yang[a], Xiaoyang Liu[a], Yihao Zhang[a], Zuxue Wei[b]

[a] College of Computer Science and Engineering, Chongqing University of Technology, Chongqing 400054, China
[b] College of Electronic and Information Engineering, Chongqing Three Gorges University, Chongqing 404100, China

ARTICLE INFO

Article history:
Received 2 November 2015
Revised 31 December 2015
Accepted 24 January 2016
Available online 3 February 2016

Keywords:
Malware propagation
Mobile network
Complex network
Network topology

ABSTRACT

In this paper, the spreading behavior of malware across mobile devices is addressed. By introducing complex networks to model mobile networks, which follows the power-law degree distribution, a novel epidemic model for mobile malware propagation is proposed. The spreading threshold that guarantees the dynamics of the model is calculated. Theoretically, the asymptotic stability of the malware-free equilibrium is confirmed when the threshold is below the unity, and the global stability is further proved under some sufficient conditions. The influences of different model parameters as well as the network topology on malware propagation are also analyzed. Our theoretical studies and numerical simulations show that networks with higher heterogeneity conduce to the diffusion of malware, and complex networks with lower power-law exponents benefit malware spreading.

1. Introduction

With the rapid worldwide adoption and innovation of mobile devices, the massive growth of mobile applications makes a significant influence on our economic and social life. Owing to the mobility of wireless devices, people are more convenient to handle business affairs, e.g., shopping online and immediately completing the payment via their smartphones. Unfortunately, the secure ecosystem of mobile devices is becoming a challenging problem. A large amount of vulnerabilities within mobile devices are usually exploited by cyber-criminals to compromise the integrity, confidentiality or availability of the system. In recent years attacks and threats occurred on mobile devices are frequently reported.

Mobile malware refers to a new kind of malicious software programmed specifically to target mobile devices, such as smartphones or tablets. Cyber attacks by this type of malware present one of the most dangerous threats to the security and integrity of mobile telecommunications networks. Most of mobile malware is designed for malicious attackers to remotely control the device or to unknowingly steal valuable information stored in the device [1]. The Cabir and Commwarrior, for example, infected hundreds of thousands of smartphones at alarming speeds and the resulting malware epidemics cost both the public and the private sector a great amount of money.

Attacks through Internet have become the subject of extensive empirical, theoretical and simulation studies. These investigations have greatly contributed to our understanding of the properties of malicious objects and have inspired the design

[*] Corresponding author. Tel.: +86 2362563072.
E-mail address: lwphe@163.com (W. Liu).

http://dx.doi.org/10.1016/j.cnsns.2016.01.019
1007-5704/© 2016 Elsevier B.V. All rights reserved.

of more effective immunization strategies to prevent and combat malware epidemics [2–4]. As mobile malware proliferates both in their volume and complexity, new models and strategies are necessary to prevent intrusions and to cope with their impact [5–7]. Motivated by the strong similarities between malicious codes and biological epidemics [8–11], some models and strategies implemented against infectious diseases are modified to study and fight malicious software [12–16]. However, all susceptible nodes in these models are considered to be homogeneous and are categorized into a single compartment called *susceptible* (S). This is not consistent with the real situation that the susceptible mobile devices are actually heterogeneous in terms of varying levels of security protection. Motivated by this fact, Liu et al. [17] made a more practical assumption that the immunization of different susceptible nodes against malware can be variable, and developed a new model, known as WSIS model, in which the whole susceptible nodes are further divided into two groups: *strongly-protected* and *weakly-protected*, depending on whether they have up-to-date real-time protection of security products or not. But, the effect of network topology on malware propagation is ignored in the above models.

Complex networks, or *scale-free networks*, are confirmed to be ubiquitous in nature and society, such as biological networks, technological networks, social networks, and computer networks [18]. Specifically, they are a kind of networks that feature patterns of connection between their vertices that are neither purely regular nor purely random. That is, the node-connectivity of these networks follows a power law distribution [19]. Despite their relevance to many real-life phenomena the properties of these networks are much less studied than abstract graphs. By now, investigation of malware spreading in general mobile networks is in its infancy, and there have been very limited studies which address this problem. Like traditional malicious software, mobile malware can proliferate through dozens of different ways, such as Email networks, social networks, and communication networks. However, the difference is that mobile malicious objects can also spread using short-range radio transmissions (Bluetooth network and WiFi-based wireless ad hoc networks), because of the novel feature that Internet connectivity is not necessarily required for their spread. The transmission of malware comes through a contact or interaction between a susceptible and an infected node. It is confirmed that the topological characteristics of networks significantly affect malware propagation. The study of malware spread on complex networks is important as their topology provides a clear-cut example of the above mobile propagation networks [20].

In this work we introduce static complex networks to model the propagation networks and develop a novel mathematical model for the spread of mobile malware over mobile networks. The properties of malware epidemics in these networks are investigated via the theory of complex networks. Theoretical results and numerical simulations show that epidemic spreading in complex networks is significantly different from the previously studied epidemics in regular networks. The initial growth of the epidemic is significantly slower than the exponential growth observed for malware spreading in the fully-connected networks, and the epidemic prevalence exhibits a density-dependent critical threshold which is higher than the value predicted by the mean-field theory. We show that these differences are due to the network topology which characterizes these networks.

2. Model description

We are devoted in this section to developing a new compartmental model for the spread of mobile malware. Before proceeding with the mathematical formulation, we briefly discuss the basic assumptions that guide the structural side of the proposed model. The practical networks over which mobile malware propagates are abstracted and described by graphs, where the nodes and links represent terminal devices connected to mobile/communication networks and communication links between them, respectively. In the sequel, the propagation networks are considered to be characterized by *static complex networks* whose node degrees are supposed to asymptotically follow a power law distribution, i.e., $P(k) \sim k^{-r}$ (r is a constant index) which means the probability of nodes with exact k neighbors.

In our model, we neglect the details of malware infection. The total size of the network is considered to be fixed, and all the hosts are generally categorized as three groups: weakly-protected susceptible nodes (W-nodes), strongly-protected susceptible nodes (S-nodes), and infected nodes (I-nodes). From the perspective of complex network theory, our new model is intended to focus on the impact of network topology on the spread of malware. Thus, in order to deeply describe the evolutions of malware spread, each compartment is further divided into several sub-compartments corresponding to the node degree.

For convenience, some notations and quantities are introduced as follows:

(1) Δ: the maximum node degree of a static complex network, indicating that $P(k) = 0$ for all $k > \Delta$.
(2) $W_k(t)$: the number of W-nodes with degree k at time t.
(3) $S_k(t)$: the number of S-nodes with degree k at time t.
(4) $I_k(t)$: the number of I-nodes with degree k at time t.
(5) $N_k(t)$: the number of nodes over the network with degree k at time t. That is, $N_k(t) := W_k(t) + S_k(t) + I_k(t)$.
(6) $W(t)$: the number of W-nodes at time t, i.e., $W(t) = \sum_k W_k(t)$.
(7) $S(t)$: the number of S-nodes at time t, i.e., $S(t) = \sum_k S_k(t)$.
(8) $I(t)$: the number of I-nodes at time t, i.e., $I(t) = \sum_k I_k(t)$.
(9) $N(t)$: the total number of nodes at time t. That is, $N(t) := W(t) + S(t) + I(t)$.
(10) $w_k(t)$: the relative density of W-nodes with degree k at time t, i.e., $w_k(t) = W_k(t)/N_k(t)$.
(11) $s_k(t)$: the relative density of S-nodes with degree k at time t, i.e., $s_k(t) = S_k(t)/N_k(t)$.