Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

Modeling the dynamics of a network-based model of virus attacks on targeted resources

Jianguo Ren[a,b,*], Jiming Liu[b], Yonghong Xu[c]

[a] College of Computer Science, Jiangsu Normal University, Xuzhou 221116, China
[b] Department of Computer Science, Hong Kong Baptist University, Kowloon, Hong Kong
[c] The Key Laboratory of Biotechnology for Medicinal Plants of Jiangsu Province, Jiangsu Normal University, Xuzhou 221116, China

ARTICLE INFO

Article history:
Received 5 December 2014
Revised 12 May 2015
Accepted 17 June 2015
Available online 26 June 2015

Keywords:
Computer viruses
Propagation modeling
Heterogeneous networks
Virus attacks
Dynamics

ABSTRACT

This paper extends a homogenous network model proposed by Haldar and Mishra (2014) into a heterogeneous one by taking into consideration the topology property of the Internet. The dynamics of this new model are investigated by studying the stability of its equilibria using mathematical methods. The qualitative analyses show that, because of the effect of the Internet topology, the results of the model exhibit several distinct features as compared to those of the original model. Some numerical experiments are also conducted to account for the potential scenarios of the model.

1. Introduction

Computer viruses that can cause serious damages to computer systems have drawn significant attention from researchers due to their subtle and sophisticated attack patterns. Some earlier efforts have been made to better understand such attacks [1–3] as well as corresponding countermeasures [4–9]. Recently, a mathematical model was proposed to capture the relationship between the distribution modes of attacks and the targeted attacks [10] by means of combining two frameworks: the classic *SIRS* (susceptible-infected-recovered-susceptible) model for a targeted population (labeled by superscript *T*) and the traditional *SIS* (susceptible-infected-susceptible) model for an attacking population (labeled by superscript *A*):

$$\begin{cases} \dfrac{\mathrm{d}S^T(t)}{\mathrm{d}t} = -\beta k S^T(t) I^A(t) + \alpha R^T(t), \\ \dfrac{\mathrm{d}I^T(t)}{\mathrm{d}t} = \beta k S^T(t) I^A(t) - \gamma I^T(t), \\ \dfrac{\mathrm{d}R^T(t)}{\mathrm{d}t} = \gamma I^T(t) - \alpha R^T(t), \\ \dfrac{\mathrm{d}S^A(t)}{\mathrm{d}t} = \mu - \beta k S^A(t) I^A(t) - \mu S^A(t) + \eta I^A(t), \\ \dfrac{\mathrm{d}I^A(t)}{\mathrm{d}t} = \beta k S^A(t) I^A(t) - (\mu + \eta) I^A(t). \end{cases} \tag{1.1}$$

[*] Corresponding author at: College of Computer Science, Jiangsu Normal University, Xuzhou 221116, China. Tel.: +86 13775848013.
E-mail address: rjgrjgrjgrjg@126.com (J. Ren).

http://dx.doi.org/10.1016/j.cnsns.2015.06.018
1007-5704/© 2015 Elsevier B.V. All rights reserved.

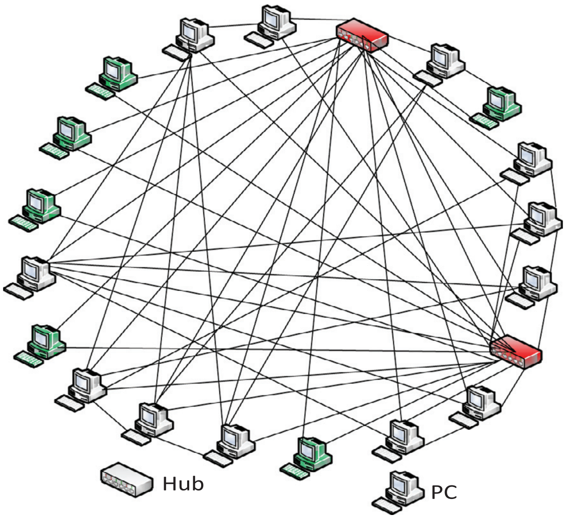

Fig. 1. A schematic diagram of the scale-free Internet.

In this model, the infected nodes strive to seek every possible chance to launch attacks on the targeted population and to find new hosts to transmit the attacks, whereas the recovered nodes with temporary immunity to the launch of attacks will stop spreading the attacks and remain unchanged. The model has an underlying assumption, that is, the effect of network topology is not incorporated and the mixing of nodes is homogenous.

It is well known that a computer virus usually launches its attacks through the Internet, which can be modeled as a representative BA scale-free network where node degree distributions follow a power-law distribution [11] indicating that the mixing of nodes is heterogeneous. Since the network topology over which a virus propagates plays a key role in determining the properties of virus epidemics [12,13], it is crucial that the model of virus attacks should consider the pivotal feature that appropriately characterizes the topology of the Internet.

In this paper, we develop the above mentioned model by putting an emphasis on the scale-free property of the Internet with the primary purpose of analyzing the way in which a computer virus spreads its attacks on the targeted resources on the Internet. It should be pointed out that since the influence of the mixing of the Internet nodes is heterogeneous, the developed model presents several distinct characteristics as compared to the original model [10]: (1) Our model admits a unique virus equilibrium under any conditions; (2) The Internet with a lower heterogeneity may be conducive to alleviate the attacks on targeted hosts, or with more nodes may conduce to foment such attacks; (3) The nodes with a higher degree are more sensitive to launching and suffering attacks than those with a lower degree; (4) Our simulation results show that towards a virus-free state, the larger the node degree is, the slower the virus propagation attacks will vanish.

In addition, we obtain the conditions for attacks to succeed or fail by mathematically investigating the threshold values and the stability of the virus-free equilibrium and the virus equilibrium. It is established that the virus-free equilibrium is globally asymptotically stable if the threshold value is less than a constant, while the virus equilibrium is globally attractive if the threshold value is greater than unity. Some numerical examples are also performed to account for the possible scenarios of the model.

The rest of this paper is organized as follows. In the next section, a mathematical model is proposed and its parameters are described. In Section 3, the existence and the stability of the virus-free equilibrium and the virus equilibrium are investigated. Some simulations are presented in Section 4. Section 5 concludes the paper.

2. Model formulation

The scale-free Internet can be characterized by the mechanism of growth and preferential attachment. There are initially m_0 fully-connected vertices; at each time step, a new m-edge ($m \le m_0$) vertex is connected to an old vertex i with probability $\prod(k_i) = k_i / \sum_j k_j$ where k_i is the degree of vertex i that is defined as the number of edges pointing to this vertex. As a result, the vertex degree distribution follows a power-law $P(k) \sim k^{-\gamma_1}$ [11], implying that there is a small fraction of highly-connected vertices called hubs, where $P(k)$ presents the probability that a randomly chosen vertex in the Internet has degree k. Fig. 1 presents a schematic diagram of the scale-free Internet with size 20.

Computers connected to the Internet are referred to as the nodes and the edges between them stand for the corresponding interactions that may allow the spread of virus attacks. In the course of such propagations over the Internet, at one time step, the total number of nodes connected to the Internet can be divided into two sets: targeted population and attacking population. The former can be further grouped into three compartments (or subsets), i.e., susceptible, infected and recovered, and their densities with degree k are denoted by $S_k^T(t)$, $I_k^T(t)$ and $R_k^T(t)$, respectively. The latter consists of two compartments (or subsets),