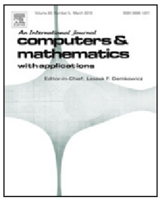
Contents lists available at ScienceDirect

Computers and Mathematics with Applications

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

ELSEVIER



Partial differential equation modeling of malware propagation in social networks with mixed delays

Bo Du [a,*], Haiyan Wang [b]

[a] Department of Mathematics, Huaiyin Normal University, Huaian Jiangsu, 223300, PR China
[b] School of Mathematical and Natural Sciences, Arizona State University, AZ, USA

ARTICLE INFO

Article history:
Received 6 December 2017
Received in revised form 30 January 2018
Accepted 11 February 2018
Available online xxxx

Keywords:
Information networks
Malware propagation
Hopf bifurcation
Local stability

ABSTRACT

With the wide applications of social networks, government and individuals increasingly emphasize information networks security. This paper is devoted to investigating a reaction–diffusion malware propagation model with mixed delays to describe the process of social networks. Applying matrix theory for characteristic values, we establish the local stability conditions of a positive equilibrium point. Based on the linear approximation method of nonlinear systems, the Hopf bifurcation at the positive equilibrium point is considered. Additionally, we identify some sensitive parameters in the process of malware propagation that are significant for control theory. Finally, numerical simulations are performed to illustrate the theoretical results.

1. Introduction

With the rapid development of the Internet, social networking has become the main platform for information spreading and diffusion. Establishing various social relations through social networking is the most important channel for information dissemination in our everyday life. More and more researches focus on social networking. Zhao, Wu and Xu [1] revealed complex dynamics of both the structure and the diffusion of large-scale online social networks and found that selecting proper weak ties can make the information diffuse quickly. Zheng, Lu and Zhao [2] considered an unknown–known–approved–exhausted four-status model. In view of effects of social reinforcement, they obtained that redundant signals can improve the probability of approval. In [3], according to frequent social activities of users, Liu and Zhang introduced a new link rewiring strategy based on the Fermi function, and obtained an interesting result: informed individuals tend to break old links and reconnect to their second-order friends who have more uninformed neighbors. With the widespread use of social networks, speed and scope of information transmission have been greatly promoted. Hence, social networks play a significant role in economic and social activities. However, the convenience of social networks, enhances the spread of various types of malware, which threatens the stability growth and rapid development of economies and simultaneously destroys social harmony and stability. Afer, Du, and Yin [4] carefully discussed relevant features to Android malware behavior captured at API level and gave different methods for controlling the spreading of Android malwares in social networks. Faghani and Nguyen [5] discussed recent advances on the topic of malware spreading through use of online social networking. Three malware propagation techniques, cross site scripting, Trojan and clickjacking types, and their characteristics were addressed by relevant models and numerical simulations in [5]. All in all, great deal of malware has

[*] Corresponding author.
E-mail address: dubo7307@163.com (B. Du).

https://doi.org/10.1016/j.camwa.2018.02.015

appeared widely in social networks, and some highly destructive malwares continue to emerge. Given this grim situation, we need to devote substantial attention to the spread of malware.

During the past decade, considerable attention has been paid to application and control problems of malware spreading models. Particularly, communication protocols, hardware design, resource efficiency, battlefield surveillance and home security have been extensively studied, see for example, [6–10]. Cheng et al. [6] studied the ripple-based spread of hybrid malware in generalized social networks including personal and spatial social relations. Nature, dynamics, and defense implications for malware propagation in online social networks were considered in [7]. Peng, Wang and Yu [8] studied a special social network (smart phone social network) and discussed the dynamic properties of malware programs in smart phone social networks. Chain exploitation of social networks malware was addressed by Sood and Enbody [9,10]. Where malware wireless sensor networks are concerned, the most important feature may be mobility, because of the wide applications in our everyday life [11]. For example, in an intelligent factory, nodes may be attached to equipment to collect information, such as running condition, efficiency of equipment and maintenance of equipment [12]. The purpose is to ensure, by monitoring equipment conditions, that the equipment is always running with high efficiency. For more applications to malware spreading models; see, for example, [13–15]. In fact, as Khan et al. [15] point out, the advantages of malware spreading models over static wireless sensor networks include enhanced target tracking, improved coverage, energy efficiency, and superior channel capacity. Owing to their wide application, malware wireless sensor networks are becoming malware targets [14]. Injecting malware often happens on the Internet, which causes damage to some nodes, especially mobile nodes, such as network paralysis, loss of data, and loss of online account.

To reduce or eliminate the damage caused by malware, we must first understand the dynamic characteristics of malware propagation. Malware propagation systems have been studied by some authors, and some interesting results have been obtained. Since the malware propagation model is based on the epidemic model, we shall review the related works for the epidemic model. Newman [16] studied a large class of standard epidemiological models that can be solved exactly on a wide variety of networks, and proposed a percolation theory based upon evaluation of the spread of an epidemic on graphs with given degree distributions. However, the temporal dynamics of epidemic spread were not considered by Newman. Liu et al. [17] considered the spreading behavior of malware across mobile. Based on the theory of complex networks, the spreading threshold that monitors the dynamics of the model was calculated, and the properties of malware epidemics were investigated in [17]. Wang [18,19] also obtained the threshold for a kind of malware to propagate in social networks, where all the nodes were supposed to be stationary.

We note that the above malware spreading models have been constructed by ordinary differential equations. As is well known, partial differential equations (PDEs) can depict the real world more accurately. Many complex models can be established only by PDEs. However, the malware spreading models by PDEs are rarely small. We find Wang et al. [20–22] constructed an intuitive cyber-distance among online users to study both temporal and spatial patterns of information diffusion process on social networks by using PDEs. Using real data coming from Digg (an online social network), Wang verified the reliability of the PDE model. Zhu, Zhao and Wang [23–25] studied several reaction–diffusion malware propagation models and obtained some results for stability and bifurcation of positive equilibrium points. Dai et al. [26] studied a partial differential equation with a Robin boundary condition in online social networks and discussed temporal and spatial properties of social networks. In general, matrix theory cannot be used easily in PDE models, because PDEs have complex natures and no standard characteristic equations. Hence, the research for malware propagation models with PDEs is just getting started, there are still many problems to be solved. In the present paper, we will try to construct a reaction–diffusion malware propagation model (PDE model) for developing the above research.

On the other hand, delays exist extensively in certain dynamic systems, such as various engineering, biological, and economic systems (see, for example, [27–31]). It is well known that delay falls into many categories, such as constant delay (discrete delay), time-varying delay and distribution delay. For the dynamical behavior analysis of delayed networks system, different types of time delays, have been taken into account, using a variety of techniques that include Lyapunov functional method, M-matrix theory, topological degree theory, and techniques of inequality analysis; see, for example, [32–39]. Recently, Zhu, Zhao and Wang [23,24] studied two kinds of reaction–diffusion malware propagation model with discrete delay, as follows:

$$\begin{cases} \dfrac{\partial S}{\partial t} = d\nabla^2 S + rS(1 - S/k) - \beta SI(t-\tau) - \varepsilon_1 S - \eta S \\ \dfrac{\partial I}{\partial t} = d\nabla^2 I + \beta SI(t-\tau) - \varepsilon_2 I - \eta I \\ \dfrac{\partial R}{\partial t} = d\nabla^2 S + \varepsilon_1 S + \varepsilon_2 I - \eta R \\ 0 < x\,, y < L, \quad t > 0, \\ \dfrac{\partial S}{\partial \phi} = \dfrac{\partial I}{\partial \phi} = \dfrac{\partial R}{\partial \phi} = 0, \quad x, y = 0, L, \ t \geq 0 \end{cases} \tag{1.1}$$

Please cite this article in press as: B. Du, H. Wang, Partial differential equation modeling of malware propagation in social networks with mixed delays, Computers and Mathematics with Applications (2018), https://doi.org/10.1016/j.camwa.2018.02.015.