Neurocomputing 149 (2015) 1370–1386

Contents lists available at ScienceDirect

Neurocomputing

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

Dynamical analysis and optimal control for a malware propagation model in an information network

Linhe Zhu, Hongyong Zhao *

Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China

ARTICLE INFO

Article history:
Received 30 June 2014
Accepted 29 August 2014
Communicated by H. Jiang
Available online 16 September 2014

Keywords:
Information networks
Stability
Hopf bifurcation
Malware propagation
Optimal control strategy

ABSTRACT

With the rapid development of network information technology, information networks security has become a very critical issue in our work and daily life. This paper investigates a nonlinear malware propagation model in wireless sensor networks (WSNs) based on SIR epidemic model. Sufficient conditions for the local stability of the positive equilibrium point and the existence of Hopf bifurcation are obtained by analyzing the associated characteristic equation. Moreover, formulas for determining the properties of the bifurcating periodic oscillations are derived by applying the normal form method and center manifold theorem. Furthermore, with the help of the Maximum Principle of Pontryagin, we design an optimal control strategy for the previous model to extend the region of stability and reduce the density of infected nodes in WSNs. Finally, we conduct extensive simulations to evaluate the proposed model. Numerical evidence shows that the dynamic characteristics of malware propagation in WSNs are closely related to the immune period of a recovered node and the rate constant for nodes becoming susceptible again after recovered. Besides, we obtain that the optimal control strategy effectively improves the performance of the networks.

1. Introduction

With the rapid development of the information and communication technology, information networks have become more prevalent in our work and daily life. Over the years, these information networks have been successfully used in hardware design, communication protocols, resource efficiency, home security, battlefield surveillance and other aspects [1–3]. Wireless sensor network, as a novel information and communication network, has gained worldwide attention in recent years [4–6]. In general, a WSN is composed of hundreds or even thousands of small, low cost, low power sensor nodes, which has facilitated the development of smart sensors. However, as WSNs are unfolding their vast potential in a plethora of application environment, information security has become one of the most critical challenges yet to be fully addressed. Because sensor nodes are resource constrained, they generally have weak defense capabilities and are attractive targets for software attacks (like malware attacks on the information networks). As malware being injected into some nodes in WSNs, the networks will fall out of stability and at the same time the oscillation by large amplitude occurring through Hopf bifurcation may appear, which possibly leads to that the utilization of the network decreases and the network performance declines. The oscillatory phenomena have been observed in many other similar networks, with rhythms originating from isolated components or emerging as a property of a network as a whole [7–9].

To defend against the malware propagation, we need to accurately understand the dynamic characteristics of malware propagation. In recent years, some analytical models have been brought into malware propagation system so that large strides have been taken in the research in WSNs [10–16]. The simulations and matching with practical data show that most of these models can not only describe the process of information and disease diffusion in human society, but also capture the process of malware propagation in computer networks such as the Internet and WSNs. In [13], the author proposed a percolation theory based evaluation of the spread of an epidemic on graphs with given degree distributions. However, [13] had payed little attention to the temporal dynamics of epidemic spread and only studied the final outcome of an infection spread. The authors in [14] proposed a spatial-temporal model for characterizing malware propagation in networks based on probabilistic graphs and spatial-temporal random processes. The basic idea was to abstract malware propagation into a probabilistic graph, and described the statistical dependence of malware propagation in arbitrary topologies using a spatial-temporal random process. Based on the ordinary differential equation and the SIR model, Wang in [15,16] derived the threshold for a piece of malware

* Corresponding author.
E-mail address: hongyongz@126.com (H. Zhao).

http://dx.doi.org/10.1016/j.neucom.2014.08.060
0925-2312/© 2014 Elsevier B.V. All rights reserved.

to propagate in WSNs, where all the nodes were supposed to be stationary. Furthermore, the author gave the sufficient conditions of stability and Hopf bifurcation of the malware propagation model.

As is well known, the periodic oscillation occurring through Hopf bifurcation in WSNs may destroy, block regular communications, or even damage the integrity of regular data packets. Thus, it is necessary to propose a control strategy to ensure that the system is stable and reliable operation. On the other hand, in order to reduce infected nodes in WSNs at minimal cost, in this paper we consider optimal control strategies associated with elimination policy and defense policy including execution costs based on the previous model. In fact, the optimal control theory [17], which was developed by Pontryagin and his co-workers in the late 1950s, has been applied to many areas including economics, management, engineering and biology [18–21]. In [22], Gumel and Moghadas proposed a model for the dynamics of an infectious disease in the presence of a preventive vaccine considering non-linear incidence rate and found the optimal vaccine coverage threshold needed for disease control and eradication. Swan [23] applied control theory to obtain maximal benefits interims of social benefits from the parsimonious use of insufficient public funds in the control of epidemics. With the help of the Maximum Principle of Pontryagin [24,25] and an iterative method we shall develop some new model with optimal control strategy. The goal of this work is not to consider a process of malware propagation but to present a method of how to treat this class of optimization problems. Our main contributions are summarized as follows.

(1) Through the analysis of the mechanism of malware propagation in WSNs, we generally quantify the process of malware propagation in WSNs based on the SIR model in the epidemic theory, and then we develop a delayed malware propagation model with logistic growth process. At the same time, we conduct extensive simulations on large-scale WSNs to evaluate the proposed model. Numerical evidence shows that the dynamic characteristics of malware propagation in WSNs are closely related to the immune period of a recovered node and the rate constant for nodes becoming susceptible again after recovered.
(2) Through the stability and Hopf bifurcation analysis of the positive equilibrium point for the proposed model, we obtain the sufficient conditions whether a series of oscillation phenomenon occurs through a Hopf bifurcation in WSNs. When the system occurs periodic oscillation, based on the normal form method and center manifold theorem we analysis the property of periodic oscillation.
(3) Based on our proposed model, with time increasing the distribution of infected nodes can be effectively predicted in advance. On this basis, the optimal control strategy we proposed can delay Hopf bifurcation and extend the stability region. Furthermore, we derive optimal state solutions associated with the optimal control variable $u^*(t)$ for the optimal control problem by means of the Pontryagin's Maximum Principle. Numerical results exhibit that the optimal control strategy ensures the security of WSNs and the regular communications between nodes. This will provide new insights on when and where countermeasures should be employed for preventing, controlling and removing malware propagation in WSNs.

The structure of this paper is arranged as follows. In Section 2, we consider the mechanism of malware propagation and the model formulation problem. In Section 3, we study the local stability and the existence of Hopf bifurcation. In Section 4, we give formula determining the direction of Hopf bifurcation and the stability of the bifurcating periodic solutions. In Section 5, we propose an optimal control strategy for malware propagation in WSNs. Finally, to support our theoretical predictions, some numerical simulations are given which support the analysis in Sections 3–5.

2. Model formulation

A WSN consists of many static and identical wireless sensors. Each wireless sensor is called a node. At any time, a node is classified as either *internal* or *external* accordingly as it is connected to the networks or not at that time. Generally, the nodes can be divided into three classes depending on their states: susceptible (healthy), infected and recovered (immunized). In this paper, we use $S(t)$, $I(t)$, $R(t)$ to denote the densities of susceptible nodes, infected nodes and recovered nodes at time t, respectively.

Based on the classical SIR epidemic model [26–28], we consider the following four facts:

(i) The susceptible nodes are assumed to have the logistic growth with carrying capacity K $(K>0)$ as well as intrinsic increase rate constant r $(r>0)$, and the incidence term is of bilinear mass action.
(ii) Users may immunize their nodes with countermeasures in state I.
(iii) Some recovered nodes go through a temporary immunity with probability δ.
(iv) As the energy of nodes is exhausted, more and more nodes become dead nodes. Any malware residing in other nodes cannot infect these dead nodes. Moreover, when a node dies, it becomes a dead node. All of the malware which ever resided in the dead nodes immediately disappear from the dead nodes. This means that the dead nodes no longer participate in the process of malware propagation in WSNs.

Our assumption on the dynamical transfer of the nodes is depicted in Fig. 1. As a result, the SIRS model can be formulated by the following delayed differential equations:

$$\begin{cases} \dfrac{dS}{dt} = rS\left(1-\frac{S}{K}\right) - \beta SI - \eta S + \delta R(t-\tau), \\ \dfrac{dI}{dt} = \beta SI - \varepsilon I - \eta I, \\ \dfrac{dR}{dt} = \varepsilon I - \eta R - \delta R(t-\tau), \end{cases} \tag{2.1}$$

with initial conditions

$$\begin{cases} S(t) = S_0 \ge 0, & t \in [-\tau, 0], \\ I(t) = I_0 \ge 0, & t \in [-\tau, 0], \\ R(t) = R_0 \ge 0, & t \in [-\tau, 0], \end{cases} \tag{2.2}$$

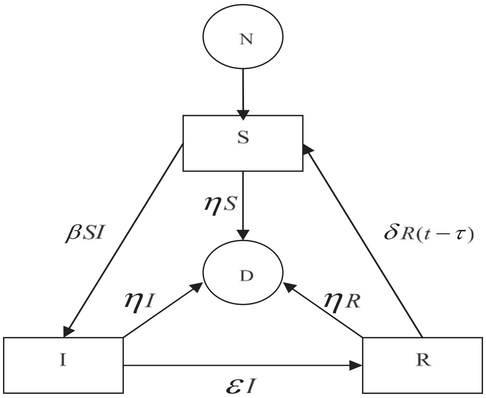

Fig. 1. Node state transition relationship, where N and D represent new nodes and death nodes, respectively.