

Dynamic Behaviors of Wireless Sensor Networks Infected by Virus with Latency Delay

Xiaopan Zhang^a, Lingyun Yuan^{a,b,*}, Jianhou Gan^b, and Cong Li^a

^a*School of Information Science and Technology, Yunnan Normal University, Kunming, 650500, China*

^b*Key Laboratory of Educational Information for Nationalities, Ministry of Education, Yunnan Normal University, Kunming, 650500, China*

Abstract

Oscillatory behavior is a ubiquitous phenomenon in various physical and biological processes. Recently, it has been reported that oscillations of wireless sensor networks infected by virus (WSNIVs) can potentially be deleterious to the security strength of systems and may even cause network congestion and paralysis. Moreover, it has been discovered that latency delays are essential for the function of WSNIVs and can drive instability and periodic oscillations, enhance complexity, and even lead to multistability and chaotic motion. However, the precise roles of such delay during the regulation process are still not completely understood. Here, the primary objective of this paper is to study oscillatory behaviors of WSNIVs with latency delay. In particular, the sufficient conditions for local stability and existence with Hopf bifurcation are obtained. Moreover, we further discuss the properties of Hopf bifurcation by using the normal form and the center manifold theorem. The obtained results show that the latency delay can drive the WSNIVs to be oscillatory even when the network is at a stable state, suggesting that such delay might be a potential hazard to the security of wireless sensor systems. Our findings highlight the importance of considering delays when developing safer and more effective wireless sensor networks. Finally, we test and analyze the above research results through numerical calculation with Matlab and simulation experiments with OPNET, and the conclusions are verified to be correct and effective in experiments.

Keywords: wireless sensor networks; virus; time delay; Hopf bifurcation; LEACH

(Submitted on October 23, 2018; Revised on November 24, 2018; Accepted on December 21, 2018)

© 2019 Totem Publisher, Inc. All rights reserved.

1. Introduction

Wireless sensor networks (WSNs) are a new technology rising rapidly in recent years with the development of the intelligent home, smart city, and intelligent transportation. They are mainly used for data acquisition of the health and environmental monitoring; beyond that, they are widely applied in the fields of military and intrusion detection and other engineering fields [1-4]. In these applications, the stability of WSNs is a prerequisite. In normal operation, the dynamics of WSNs are tightly controlled at a stable state. In contrast, WSNs lose their stability and further exhibit various complex behaviors under network attacks including sinkhole [5-6] wormhole [7], Trojan horse, and spyware [8]. Intriguingly, it has been recently reported that the oscillatory behavior of WSNIVs can threaten the network security strength seriously and may even cause network congestion and paralysis [9]. Therefore, a more significant point is to identify the transmission mechanisms of malware to ensure WSNs health.

Oscillatory dynamics can be typically generated through a delayed negative feedback loop in WSNIVs. Latency delays are critical and especially worthy of attention [10]. It is well known that the virus latency process is not instantaneous. In principle, time delays are unavoidable, from the initial infection to the existence of a complete virus node in WSNIVs. In wireless sensor networks, the main factors affecting the time delay include the distribution of nodes, rate of data packets generated by a node, and selection of routing and node transmission path. Recently, it was reported that such delay can induce the change of stability and cause oscillation in WSNIVs [11-12], which badly influences the dynamical behaviors. Previously, some scholars have proposed to explore the dynamic behavior of WSNIVs by building mathematical models, and some scientific research results have been obtained [13-24]. For example, Wang et al. proposed a model of worm

* Corresponding author.

E-mail address: blues520@sina.com

propagation in WSNs, and its dynamic behavior was studied and analyzed. Kusakabe et al. proposed a SEIRS-V model of worm propagation for studying and analyzing the dynamic behavior of worm propagation relative to time in WSNs. However, these modeling efforts did not include any time delay. Moreover, although some delayed models have been studied to test the effects of latency delay [25-27], the roles of such time delays are not completely understood; therefore, researchers highly depend on numerical analysis and simulation. Therefore, as a subject study with important theory meaning and practical significance, it is necessary to thoroughly investigate the effect of latency delays to regulate the dynamic behavior of WSNIVs.

Considering the above, based on the model of reference [24], we developed a delayed dynamical model in order to understand how latency delay affects dynamic behavior of the WSNIVs. For this purpose, we first discussed the stability and the Hopf bifurcation of such a model. Specifically, the proposed model introduced a simple delay into the system, and we found that the latency delay can drive the WSNIVs to be oscillatory even when the network is at a stable state. Finally, three indices to predict the reliability and practical significance of the delay-driven oscillations were obtained through the normal form theory and the center manifold reduction.

The structure and main content of the article are as follows: in Section 2, we analyze the time delay feature of the virus propagation with wireless sensor networks and construct a WSNIVS model with time delay. The stability and existence of Hopf bifurcations are studied by applying the Hopf bifurcation theorem in Section 3. In Section 4, three indices are derived to determine the direction, stability, and period of bifurcation periodic solutions by applying the normal form method and the center manifold theorem. In Section 5, numerical calculations are made to validate our conclusions, which support and extend the theoretical results. In Section 6, some simulation experiments for the virus propagation in WSNs are implemented, and the experimental results are analyzed in detail. Finally, some research results and conclusions are summarized and further research directions are given in Section 7.

2. Model Formulation

2.1. Time Delay Analysis of Node Infected with a Virus

In WSNs, the communication between nodes usually takes the form of single hop or multi-hop. When there is a virus carrier in the network and it communicates with other health nodes, it is possible to transmit the virus to other nodes. Therefore, we can treat the virus infection as a point-to-point infection process and can achieve the purpose of transmitting the virus through single-hop communication. Factors that affect the time delay of virus infection include the choice of routing protocols, the rate of data packets generated by nodes, and the location of nodes. For a general case of virus infection, and the basic postulates and the boundary conditions are given:

- (1) When all nodes are deployed, the positions of nodes are fixed.
- (2) Sensor nodes only send data packets to nodes within the communication range.
- (3) All nodes in wireless sensor networks have the same initial energy, communication radius, and packet generation rate.
- (4) There is no time interval between multiple packet transmission processes.

This paper defines three kinds of time delays:

- (1) The time when a node carrying a virus generates malicious packets is recorded as T_1 .
- (2) The time of the health node to deal with the malicious packets is recorded as T_2 .
- (3) The time consumed in the transmission of data packets is recorded as T_3 .

Then, the time delay of virus propagation is

$$T = T_1 + T_2 + T_3$$

Where

$$T_1 = \frac{N_p}{C_1} k, \quad T_2 = \frac{N_p}{C_2} k, \quad T_3 = \frac{L}{C_3}$$

Where N_p is the packet size, k is the number of packets, C_1 is the rate of nodes producing packets, C_2 is the rate of node processing data packets, L is the distance between nodes, and C_3 is the rate of packet transmission. When the distance between two nodes is very short, T_3 is almost negligible. For convenient analysis, the time delay T is represented by the mathematical symbol τ in Section 2.2.

2.2. Model

The WSNs are made of many identical or different wireless sensors and sink nodes, and each of them can be regarded as a node. In the meantime, when a node is connected to the WSNs, we call it an internal node; otherwise, it an external node. A node is called infected if malware exists in a node. If a malware is not in the node but it can be infected by the intrusion of the malware, it is called susceptible. In this section, we abstract the problem using a susceptible-infected-external-susceptible (SIES) model and a graphical representation.

Based on the existing virus model [24], we consider the following two facts:

(1) At any time, an external node is connected to the WSNs, and it is susceptible or infected.

(2) When the nodes are disconnected from WSNs, more and more nodes become external nodes. When nodes become external nodes, the malware will not be able to infect these external nodes. This has proven that these external nodes will not impact the propagation of malware in WSNs.

Based on the above discussion, these nodes are divided into three different states in WSNs:

(1) Susceptible state (S): S represents all internal sensor nodes that are not infected by virus but remain very vulnerable to malware in WSNs.

(2) Infected state (I): I represents all internal sensor nodes infected with malware that have the ability to infect other healthy or susceptible nodes.

(3) External state (E): E represents all external sensor nodes.

From the first section, we can determine that the malware infection process is not instantaneous; there is a time delay before these nodes become infected nodes. Until now, no scholars have studied the dynamic behavior with time delay for the model [24]; therefore, it is meaningful to analyze the proposed model with latency delays. Inspired by this fact, the SIES model can be represented as the following Equation (1), and our assumptions about the state transitions of nodes are shown in Figure 1.

$$\begin{cases} \dot{S}(t) = \gamma_2 I(t) + \eta_2 E(t) - \mu S(t) - \gamma_1 S(t) - \beta S(t - \tau) I(t) \\ \dot{I}(t) = \beta S(t - \tau) I(t) - \mu I(t) - \gamma_1 I(t) - \gamma_2 I(t) + \eta_1 E(t) \\ \dot{E}(t) = \delta + \gamma_1 S(t) + \gamma_1 I(t) - \mu E(t) - \eta_1 E(t) - \eta_2 E(t) \end{cases} \quad (1)$$

Where τ is the latency delay. $S(t)$, $I(t)$, and $E(t)$ represent the numbers of S , I , and E at instant t , respectively.

Then, the conversion relationship between the three states is as follows:

(1) μ is the death probability of the nodes in WSNs.

(2) γ_1 is the rate at which internal infected sensor nodes are disconnected to the WSNs, and it is also the rate at which internal susceptible sensor nodes are disconnected from the WSNs.

(3) β is the rate of the nodes from S state to I state due to the infection of malware.

(4) γ_2 is the curing rate of infection sensor nodes due to the effect of cure.

(5) The rate at which a new node becomes an external node is δ .

(6) The external nodes of E are connected to the WSNs at a rate of η_1 .

(7) The external nodes of S are connected to the WSNs at a rate of η_2 .

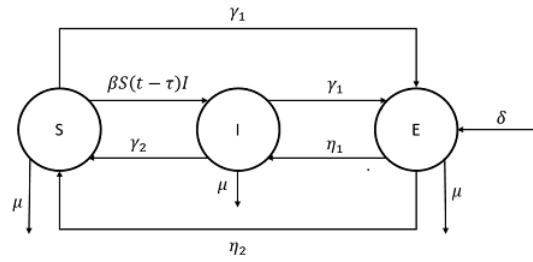


Figure 1. The relationship between S , I , and E

By using the technique in the study [28], we have shown that the solutions $S(t)$, $I(t)$, and $E(t)$ of Equation (1) are positive and bounded. Next, we give the positive invariant region Ω for Equation (1):

$$\Omega = \left\{ (S, I, E) : S \geq 0, I \geq 0, E \geq 0, S + I + E \leq \frac{\delta}{\mu} \right\}$$

Although Equation (1) is a virus propagation model built on Gan et al.'s work, there is a key difference. The model proposed by Gan et al. only considers the general characteristics of malware propagation and ignores the influence of time delay, which is a key issue in our study. In addition, Equation (1) is better able to reflect the main characteristics of the transmission of the wireless sensor network malware and can be given more effective theoretical basis for the prevention of network virus when the delay is introduced.

3. Stability of the Equilibrium and Local Hopf Bifurcations

Now, we analyze the stability and Hopf bifurcations of Equation (1) by using Hopf bifurcations theorem.

Let (S^*, I^*, E^*) be an equilibrium of Equation (1) and assume $\bar{S}(t) = S(t) - S^*$, $\bar{I}(t) = I(t) - I^*$, and $\bar{E}(t) = E(t) - E^*$.

Then, Equation (1) becomes

$$\begin{cases} \dot{\bar{S}}(t) = -(\gamma_1 + \mu)\bar{S}(t) - \beta I^* \bar{S}(t - \tau) + \eta_2 \bar{E}(t) + (\gamma_2 - S^* \beta) \bar{I}(t) - \beta \bar{I}(t) S(t - \tau) \\ \dot{\bar{I}}(t) = \beta I^* \bar{S}(t - \tau) + (S^* \beta - \mu - \gamma_1 - \gamma_2) \bar{I}(t) + \eta_1 \bar{E}(t) + \beta \bar{I}(t) S(t - \tau) \\ \dot{\bar{E}}(t) = \gamma_1 \bar{S}(t) + \gamma_1 \bar{I}(t) - (\eta_1 + \eta_2 + \mu) \bar{E}(t) \end{cases} \quad (2)$$

Based on Equation (2), we can obtain the Jacobin matrix A in the following form:

$$A = \begin{pmatrix} -\gamma_1 - \mu - \beta I^* e^{-\lambda\tau} & -\beta S^* + \gamma_2 & \eta_2 \\ I^* \beta e^{-\lambda\tau} & \beta S^* - \mu - \gamma_1 - \gamma_2 & \eta_1 \\ \gamma_1 & \gamma_1 & -\eta_1 - \eta_2 - \mu \end{pmatrix} \quad (3)$$

Based on Equation (3), we can calculate its characteristic equation as follows:

$$\lambda^3 + k_0 \lambda^2 + k_1 \lambda + k_2 + (k_3 \lambda^2 + k_4 \lambda + k_5) e^{-\lambda\tau} = 0 \quad (4)$$

Where

$$\begin{aligned} k_0 &= -\beta S^* + 2\gamma_1 + \gamma_2 + \eta_1 + \eta_2 + 3\mu \\ k_1 &= -\beta \gamma_1 S^* + \gamma_1^2 + \gamma_1 \gamma_2 - S^* \beta \eta_1 + \gamma_1 \eta_1 + \gamma_2 \eta_1 - S^* \beta \eta_2 + \gamma_1 \eta_2 + \gamma_2 \eta_2 \\ &\quad - 2S^* \beta \mu + 4\gamma_1 \mu + 2\gamma_2 \mu + 2\eta_1 \mu + 2\eta_2 \mu + 3\mu^2 \\ k_2 &= -\beta \mu^2 S^* + 2\gamma_1 \mu^2 + \gamma_2 \mu^2 + \eta_1 \mu^2 + \eta_2 \mu^2 + \mu^3 - \beta \gamma_1 \mu S^* + \gamma_1^2 \mu + \gamma_1 \gamma_2 \mu \\ &\quad - S^* \beta \eta_1 \mu + \gamma_1 \eta_1 \mu + \gamma_2 \eta_1 \mu - S^* \beta \eta_2 \mu + \gamma_1 \eta_2 \mu + \gamma_2 \eta_2 \mu \\ k_3 &= I^* \beta \\ k_4 &= \beta \gamma_1 I^* + \beta \eta_1 I^* + \beta \eta_2 I^* + 2\beta \mu I^* \\ k_5 &= I^* \beta \gamma_1 \mu + I^* \beta \eta_1 \mu + I^* \beta \eta_2 \mu + I^* \beta \mu^2 \end{aligned} \quad (5)$$

Obviously, we know that the root of Equation (4) is not $\lambda = 0$. Meanwhile, the root of Equation (4) determines the stability of $P_*(S^*, I^*, E^*)$.

For $\tau = 0$, Equation (4) becomes

$$\lambda^3 + (k_0 + k_3) \lambda^2 + (k_1 + k_4) \lambda + k_2 + k_5 = 0 \quad (6)$$

From Equations (5) and (6), we can obtain the following results by using the Routh-Hurwitz theorem.

Lemma 3.1 Suppose the constants $k_i (i = 0, 1, 2, 3, 4, 5)$ satisfy the following assumptions:

(H1):

$$k_0 + k_3 > 0, k_2 + k_5 > 0 \quad \text{and} \quad (k_0 + k_3)(k_1 + k_4) > k_2 + k_5$$

If (H1) holds, we can determine that the equilibrium $P_*(S^*, I^*, E^*)$ is asymptotically stable when $\tau = 0$.

In the following, the effect of time delay τ on Equation (1) will be discussed. First, we assume that $\pm i\omega (\omega > 0)$ is a pair of roots of Equation (4) for $\tau > 0$, and then

$$\begin{aligned} -i\omega^3 - k_0 \omega^2 - k_3 \omega^2 \cos(\omega\tau) + k_3 i \omega^2 \sin(\omega\tau) + k_1 i \omega + k_4 i \omega \cos(\omega\tau) + k_4 \omega \sin(\omega\tau) \\ + k_2 + k_5 \cos(\omega\tau) - i k_5 \sin(\omega\tau) = 0 \end{aligned} \quad (7)$$

Separating the real and imaginary parts of Equation (7), we have

$$(k_5 - k_3 \omega^2) \cos(\omega\tau) + k_4 \omega \sin(\omega\tau) = -k_2 + k_0 \omega^2 \quad (8)$$

$$k_4 \omega \cos(\omega\tau) - (k_5 - k_3 \omega^2) \sin(\omega\tau) = -k_1 \omega + \omega^3 \quad (9)$$

Adding the squares of (8) and (9) yields

$$\omega^6 + p\omega^4 + q\omega^2 + r = 0 \quad (10)$$

Let $z = \omega^2$, and denote

$$\begin{aligned} p &= k_0^2 - 2k_1 - k_3^2 \\ q &= k_1^2 - 2k_0k_2 - k_4^2 + 2k_3k_5 \\ r &= k_2^2 - k_5^2 \end{aligned}$$

Then, Equation (10) is equivalent to

$$z^3 + pz^2 + qz + r = 0 \quad (11)$$

Let $h(z) = z^3 + pz^2 + qz + r = 0$ and $\Delta = p^2 - 3q$.

Without loss of generality, we suppose that Equation (11) has three positive roots, denoted by z_1 , z_2 , and z_3 . Then, we can obtain the three positive roots of Equation (10), denoted by $\omega_1 = \sqrt{z_1}$, $\omega_2 = \sqrt{z_2}$, and $\omega_3 = \sqrt{z_3}$. We arrive at the following equation with (8) and (9):

$$\tau_l^{(j)} = \frac{1}{\omega_l} \arccos \left[\frac{(-k_2 + k_0\omega^2)(k_5 - k_3\omega^2) + (-k_1\omega + \omega^3)}{(k_5 - k_3\omega^2)^2 + (k_4\omega)^2} \right] + \frac{2j\pi}{\omega_l}, \quad (j = 0, 1, 2, 3, \dots; \quad l = 1, 2, 3) \quad (12)$$

Define

$$\tau_0 = \tau_{l0}^{j0} = \min_{1 \leq l \leq 3, j \geq 0} \{\tau_l^j\}, \quad \omega_0 = \omega_{l0} \quad (13)$$

Set

$$\lambda(\tau) = \eta(\tau) + i\omega(\tau) \quad (14)$$

This is a root of Equation (4) satisfying

$$\eta(\tau_0) = 0, \quad \omega(\tau_0) = \omega_0 \quad (15)$$

With the arguments above, the main theoretical results are presented as follows:

Theorem 3.1 For Equation (1), suppose the above equations and conditions hold, and then the following theoretical results are obtained.

(i) If $r \geq 0$ and $\Delta < 0$ hold, for all $\tau \geq 0$, the equilibrium point P_* of Equation (1) is absolutely stable.

(ii) If $r < 0$ or $r \geq 0$, $z_1' = \frac{1}{3}(-p + \sqrt{\Delta}) > 0$ and $h(z_1') < 0$ hold, and for $\tau \in [0, \tau_0)$, the equilibrium point P_* of Equation (1) is asymptotically stable.

(iii) If the conditions in (ii) hold, $\tau = \tau_0$, $h'(z_0) \neq 0$, and $z_0 = \omega_0^2$, and then $\pm i\omega_0$ is a pair of purely imaginary roots of Equation (4) and all other roots have negative real parts. In addition, $\frac{d\operatorname{Re}(\lambda(\tau_0))}{d\tau} > 0$. Therefore, Equation (1) exhibits the Hopf bifurcation near $P_*(S^*, I^*, E^*)$.

4. Direction and Stability of the Hopf Bifurcation

In this section, we shall further discuss the properties of the Hopf bifurcation by employing the center manifold theorem and the normal form theory, which mainly includes direction and stability.

To this end, we always assume that Equation (1) undergoes Hopf bifurcations at the equilibrium $P_*(S^*, I^*, E^*)$ for $\tau = \tau_0$. By Hassard et al. [29], the properties of Hopf bifurcation are determined by the signs μ_2 , β_2 , and T_2 , where

$$\begin{aligned} c_1(0) &= \frac{i}{2\omega_0\tau_0} (g_{11}g_{20} - 2|g_{11}|^2 - \frac{|g_{02}|^2}{3}) + \frac{g_{21}}{2} \\ \mu_2 &= -\frac{\Re(c_1(0))}{\Re(\lambda'_0(\tau_0))} \\ \beta_2 &= 2\Re(c_1(0)) \\ T_2 &= -\frac{\Im(c_1(0)) + \mu_2\Im(\lambda'_0(\tau_0))}{\omega_0\tau_0} \end{aligned} \quad (16)$$

Here,

$$\begin{aligned} g_{20} &= 2\bar{G}\tau_0(e^{-i\tau_0\omega_0}v_1\bar{v}_1^*\beta - e^{-i\tau_0\omega_0}v_1\beta) \\ g_{11} &= \bar{G}\tau_0(e^{i\tau_0\omega_0}v_1\bar{v}_1^*\beta + e^{-i\tau_0\omega_0}\bar{v}_1v_1\beta - e^{i\tau_0\omega_0}v_1\beta) - \bar{G}\tau_0(e^{-i\tau_0\omega_0}\bar{v}_1\beta) \\ g_{02} &= 2\bar{G}\tau_0(e^{i\tau_0\omega_0}\bar{v}_1\bar{v}_1^*\beta - e^{i\tau_0\omega_0}\bar{v}_1\beta) \\ g_{21} &= 2\bar{G}\tau_0(v_1\bar{v}_1^*W_{11}^1(0)\beta - v_1W_{11}^1(0)\beta) + 2\bar{G}\tau_0(-e^{-i\tau_0\omega_0}W_{11}^2(0)\beta + e^{-i\tau_0\omega_0}\bar{v}_1W_{11}^2(0)\beta) \\ &\quad + 2\bar{G}\tau_0(-\frac{1}{2}\bar{v}_1W_{20}^1(0)\beta + \frac{1}{2}v_1\bar{v}_1^*W_{20}^1(0)\beta) + 2\bar{G}\tau_0(-\frac{1}{2}e^{i\tau_0\omega_0}W_{20}^2(0)\beta + \frac{1}{2}e^{i\tau_0\omega_0}\bar{v}_1W_{20}^2(0)\beta) \end{aligned}$$

and

$$\begin{aligned} v_1 &= \frac{\eta_2(N_2\gamma_1 - \gamma_1(N_1 - e^{-i\omega_0\tau_0}I^*\beta - i\omega_0))}{N_2(N_2(N_4 - i\omega_0) - \gamma_1\eta_2)} - \frac{N_1 - e^{-i\omega_0\tau_0}I^*\beta - i\omega_0}{N_2} \\ v_2 &= -\frac{N_2\gamma_1 - \gamma_1(N_1 - e^{-i\omega_0\tau_0}I^*\beta - i\omega_0)}{-\gamma_1\eta_2 + N_2(N_4 - i\omega_0)} \\ v_1^* &= -\frac{-iN_1 + iN_2 + ie^{i\omega_0\tau_0}I^*\beta + \omega_0}{-iN_3 + ie^{i\omega_0\tau_0}I^*\beta + \omega_0} \\ v_2^* &= -\left[\frac{e^{i\omega_0\tau_0}I^*\beta N_2 - (N_3 + i\omega_0)(N_1 - e^{i\omega_0\tau_0}I^*\beta + i\omega_0)}{e^{i\omega_0\tau_0}I^*\beta\gamma_1 - \gamma_1(N_3 + i\omega_0)} \right] \end{aligned}$$

In order to determine g_{21} , we must further compute $W_{20}(\theta)$ and $W_{11}(\theta)$. Using the same procedures as those in [29], we have

$$\begin{aligned} W_{20}(\theta) &= \frac{ig_{20}}{\omega_0\tau_0}q(0)e^{i\omega_0\tau_0\theta} + \frac{i\bar{g}_{02}}{3\omega_0\tau_0}\bar{q}(0)e^{-i\omega_0\tau_0\theta} + E_1e^{2i\omega_0\tau_0\theta} \\ W_{11}(\theta) &= -\frac{ig_{11}}{\omega_0\tau_0}q(0)e^{i\omega_0\tau_0\theta} + \frac{i\bar{g}_{11}}{\omega_0\tau_0}\bar{q}(0)e^{-i\omega_0\tau_0\theta} + E_2 \end{aligned}$$

Where $E_1 = (E_1^{(1)}, E_1^{(2)}, E_1^{(3)})^T$ and $E_2 = (E_2^{(1)}, E_2^{(2)}, E_2^{(3)})^T$, which are satisfied by the following equations, respectively:

$$\begin{pmatrix} 2i\omega_0 + I^* \beta e^{-2i\omega_0 \tau_0} - N_3 & -N_2 & -\eta_2 \\ -I^* \beta e^{-2i\omega_0 \tau_0} & 2i\omega_0 - N_3 & -\eta_1 \\ -\gamma_1 & -\gamma_2 & 2i\omega_0 - N_4 \end{pmatrix} E_1 = 2 \begin{pmatrix} -e^{-i\omega_0 \tau_0} v_1 \beta \\ e^{-i\omega_0 \tau_0} v_1 \beta \\ 0 \end{pmatrix} \quad (17)$$

and

$$\begin{pmatrix} I^* \beta - N_3 & -N_2 & -\eta_2 \\ -I^* \beta & -N_3 & -\eta_1 \\ -\gamma_1 & -\gamma_2 & -N_4 \end{pmatrix} E_2 = 2 \begin{pmatrix} -e^{i\omega_0 \tau_0} v_1 \beta - e^{-i\omega_0 \tau_0} \bar{v}_1 \beta \\ e^{-i\omega_0 \tau_0} v_1 \beta - e^{i\omega_0 \tau_0} \bar{v}_1 \beta \\ 0 \end{pmatrix} \quad (18)$$

According to the above discussion, we have the following theoretical results:

Theorem 4.1 For Equation (2), we can obtain the following results from (16):

- (i) The direction of the Hopf bifurcation is determined by μ_2 : if $\mu_2 > 0$ ($\mu_2 < 0$), then the Hopf bifurcation is supercritical (subcritical).
- (ii) The stability of the bifurcating periodic solutions is determined by β_2 : if $\beta_2 < 0$ ($\beta_2 > 0$), then the bifurcating periodic solutions are stable (unstable).
- (iii) The period of the bifurcating periodic solution is determined by T_2 : if $T_2 > 0$ ($T_2 < 0$), then the bifurcating periodic solutions increase (decrease).

5. Numerical Simulations and Analysis

In this section, some numerical simulations are presented to support the results in Sections 3 and 4. Here, the experimental parameters are set as follows: $\beta = 0.03$, $\delta = 0.8$, $\mu = 0.01$, $\eta_1 = 0.2$, $\eta_2 = 0.4$, $\gamma_1 = 0.8$, and $\gamma_2 = 0.2$, which are consistent with the parameters in a previous work [Gan C. et al., 2013]. Moreover, τ is chosen as the bifurcation parameter. Under these parameter values, we obtain a specific Equation (1):

$$\begin{cases} \dot{S}(t) = 0.2I(t) + 0.4E(t) - 0.01S(t) - 0.8S(t) - 0.03S(t-\tau)I(t) \\ \dot{I}(t) = 0.03S(t-\tau)I(t) - 0.01I(t) - 0.8I(t) - 0.1I(t) - 0.2E(t) \\ \dot{E}(t) = 0.8 + 0.8S(t) + 0.8I(t) - 0.01E(t) - 0.2E(t) - 0.4E(t) \end{cases} \quad (19)$$

By simple calculation, the unique positive equilibrium $P_*(16.34, 17.69, 45.96)$ of Equation (19) can be easily obtained. Moreover, we can obtain $\tau_0 = 26.9699$ and $k_0 = 1.93951$, $k_1 = 0.751798$, $k_2 = 0.00732503$, $k_3 = 0.530783$, $k_4 = 0.753711$, and $k_5 = 0.00748403$. Therefore, according to (H1) and Lemma 3.1, we choose $\tau = 0$ for numerical simulation analysis. From Figure 2, we can see that the positive equilibrium point $P_*(16.34, 17.69, 45.96)$ is asymptotically stable. Furthermore, from Theorem 3.1, we show that $P_*(16.34, 17.69, 45.96)$ is asymptotically stable for $0 \leq \tau < \tau_0$ and unstable when $\tau > \tau_0$, and that Equation (19) can undergo a Hopf bifurcation at the positive equilibrium P_* when τ is larger than the critical value τ_0 . This result demonstrates that under the effect of such delay, a family of periodic solutions bifurcate from P_* , as illustrated by Figures 3 and 4.

Next, the different parameter τ is adopted to study the effect of the time delay on the oscillation and analyze the relationship between amplitudes and periods of oscillation and parameter τ . Then, we give three different parameters $\tau = 32, 34, 36$ to describe the different time courses, which are all larger than parameter $\tau_0 = 26.9699$. From Figure 5, we can see that the amplitudes and the periods increase with the parameter τ . Therefore, we can conclude that the amplitudes

and the periods of the oscillation all rely heavily on the time delay τ . This phenomenon indicates that parameter τ can serve as an important regulation factor of the amplitudes and periods of the oscillation to provide a new solution for WSNIV security.

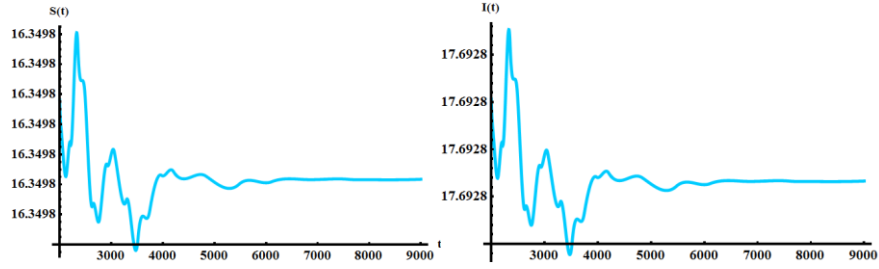


Figure 2. When $\tau = 0$, the positive equilibrium $P_*(16.34, 17.69, 45.96)$ is asymptotically stable

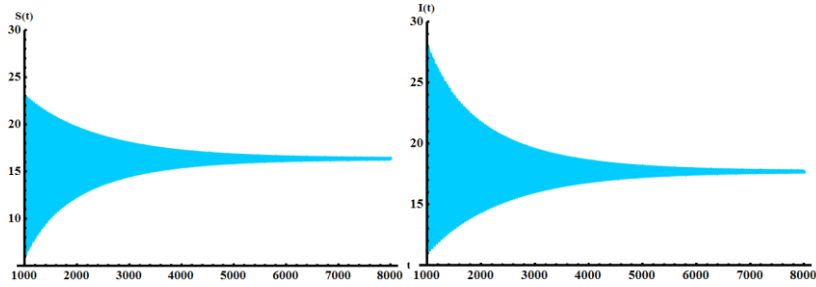


Figure 3. When $\tau = 20 < \tau_0 = 26.9699$, the positive equilibrium $P_*(16.34, 17.69, 45.96)$ is asymptotically stable

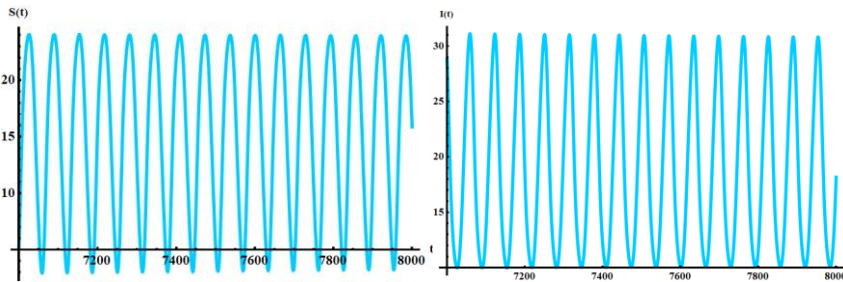


Figure 4. When $\tau = 30 > \tau_0 = 26.9699$, the positive equilibrium $P_*(16.34, 17.69, 45.96)$ is unstable and the stable periodic solution bifurcates from $P_*(16.34, 17.69, 45.96)$

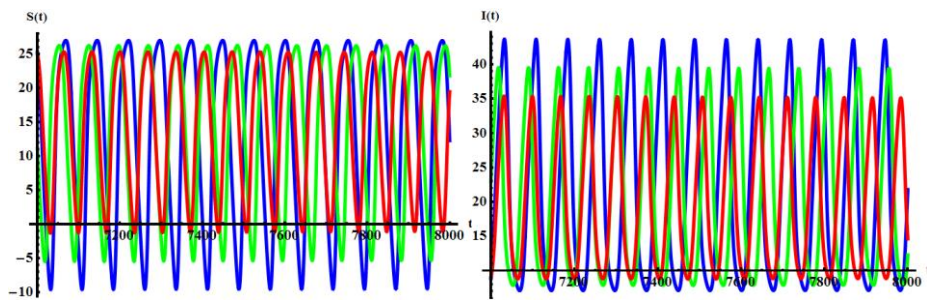


Figure 5. Impact of the delay on the WSNs: the red, green, and blue lines respectively represent the time courses with $\tau = 32$, $\tau = 34$, and $\tau = 36$

Finally, to investigate the stability of oscillation, using Formulas (16)-(18), we find that $\mu_2 > 0$, $T_2 > 0$, and $\beta_2 < 0$ for $\tau = 26.9699$. Therefore, this fully testifies three facts the Hopf bifurcation in Equation (1):

- (1) It is supercritical bifurcation.
- (2) The bifurcating periodic solutions presents a stable tendency.

(3) The period of bifurcating periodic solutions is increasing.

6. Experimental Verifications

A simulation experiment of virus propagation in wireless sensor networks with the LEACH routing protocol is designed and built based on OPNET. The results can be compared with those from the theoretical model in the previous section.

6.1. Experimental Setup

The experimental simulation scene is shown in Figure 6. The experimental system consists of three parts: RxGroup Config, sink node, and normal sensor nodes. 100 normal sensor nodes are deployed randomly in the experimental environment of 100m×100m . Moreover, the initial energy and communication radius of all nodes are identical. The sink node is located at the center of the area, and it is assumed that it has enough energy. RxGroup is used to configure the nodes of the single-hop communication distance.

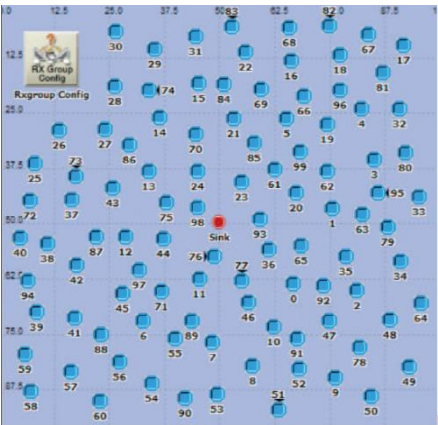


Figure 6. Experimental simulation scene

Relevant parameters chosen for the experiment are shown in Table 1. The basic principle of the experiment is that a node is randomly selected as an infected node in the network, and when communicating with the neighbor node, it will propagate malware to the neighbor node. At the same time, the node infected by malicious software is infective. Likewise, after a period of time, all nodes will be infected by malware.

Table 1. Experimental parameters

Parameter	Value
Scene size	100M×100M
Number of nodes	100
Cluster head ratio	0.1
Initial virus node ID	15
Infection probability	0.1
Communication radius	10M
Initial energy of node	20J
Simulation time	24 hours

6.2. Results and Analysis

According to the parameter settings given in Table 1, we randomly select a node as a malicious node for experimental simulation. In the experiment, we analyze two cases: one is the existence of a virus in the WSNs, and the other is no virus.

6.2.1. Impacts of Malware Propagation on Network Energy Consumption

As can be seen from Figures 7 and 8, when there are malicious nodes in the WSNs, the other nodes will be infected by the malicious nodes. The nodes will also consume more energy, which makes the number and survival time of nodes decrease sharply, thus shortening the whole network lifecycle. In particular, we can see from Figure 8 that nodes begin to die 5 hours later and the number of active nodes drops dramatically. The number of active nodes is less than 10% when the time exceeds 24 hours. It also shows that it is necessary to study the transmission of malicious viruses in WSNs. In addition,

malware must be interfered with in the early stages of malware infection to minimize the consumption of malware for network energy.

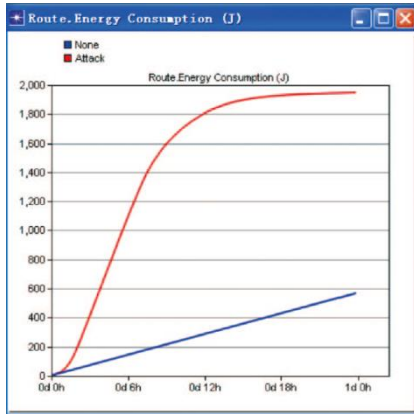


Figure 7. Network energy consumption

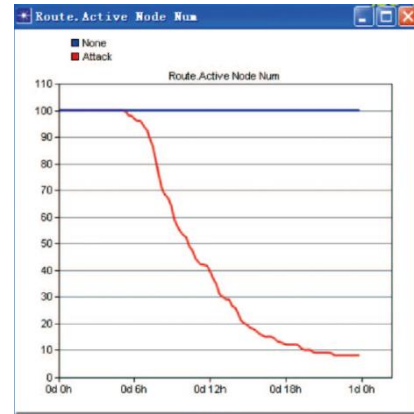


Figure 8. Active node number

6.2.2. Impacts of Malware Propagation on Network Performance

Figure 9 shows the experimental results of network performance over time. As can be seen from Figure 9, network throughput is less volatile when there are no malicious nodes in the WSNs. However, when the network is attacked by a malicious node, it accelerates the energy consumption of the node and causes the node to die prematurely. Equally, when malware invades the network for more than 5 hours, the death of the node results in a decrease in network throughput. After 18 hours, the network throughput drops from 18000bps to 0bps. This case once again illustrates the impact of malware on the network. Therefore, it is necessary to clear the malicious software in the node to ensure the network performance.

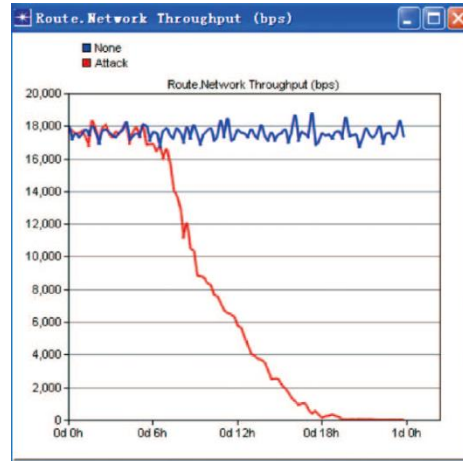


Figure 9. Network throughput

6.2.3. Malware Infection Delay

Through the discussion in the previous chapters, we can see that the normal node transform from state S to state I is not instantaneous. With the passage of time, however, increasing the number of nodes damaged by malicious attacks will reduce the network performance and sometimes even lead to network paralysis. Once a malicious attack occurs, if there is no timely processing of malicious nodes, there will be needless losses; therefore, the time threshold for the spread of the virus in the WSNs is extremely important for preventing virus attacks. In the emulation, this paper counted and analyzed the average time of virus infection by the virus in the WSNs based on the LEACH routing protocol. The results of the experiment are shown in Figure 10.

The calculated results show that the average time of the sensor node being infected by the virus is 86.875 seconds. From Figure 10, we can see that the first sensor node is infected by the virus at 800 seconds, which is far more than the average infection time. Therefore, if effective measures are taken before the virus spreads widely across the network, the impact of malicious nodes on the network will be minimized and may not even affect the performance of the network.

Therefore, we should pay more attention to the influence of time lag on the transmission of viruses in the study of the virus propagation model.

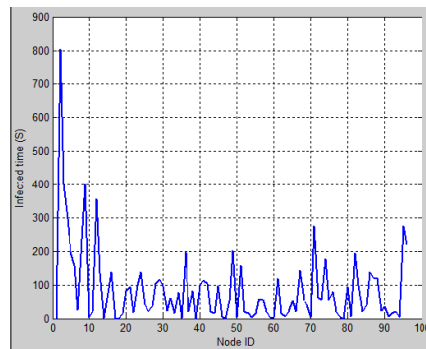


Figure 10. Node infection time

7. Conclusions

Time delay is an important factor in the virus propagation of wireless sensor networks. In order to study its influence, we mainly improve a SEIS model of the existing virus propagation. On this basis, by applying the Hopf bifurcation theorem, some sufficient conditions are given for local stability and existence with Hopf bifurcation. Moreover, we obtain a critical value τ_0 of the time delay by numerical calculation. The results indicate that Equation (1) is stable when the time delay is less than τ_0 . Conversely, when it is unstable, the WSNs are destroyed. The normal form method and the center manifold theorem are applied to study the properties of Hopf bifurcation, and then a numerical simulation is given to validate the effectiveness of the results. This paper builds a simulation model using simulation software and finally, though this simulation, we verify the theory correctness.

In summary, the results show that time delays play a role in malware propagation over WSNs, and we know that the time delay should be kept below the corresponding threshold to control the propagation of the malware by reducing the time to clean the malware. To this end, we can adjust the parameters of our proposed model in real-world wireless sensor networks, such as by improving and updating the defensive measures on wireless sensor nodes, correctly controlling the number of sensor nodes connected to the WSNs, and timely disconnecting wireless sensor nodes from the wireless sensor network. Of course, it should be pointed out that the delayed model in this paper only considers the latency delay of the virus. There are also other types of delays in wireless sensor networks, such as communication delays and multi-hop forwarding delays. In our next study, we also want to explore the effects of these delays on the spread of viruses in WSNs.

Acknowledgements

This work is supported by the National Natural Science Fund Project (No. 61561055), the Ministry of Education of Humanities and Social Science Youth Fund Project (No. 13YJCZH233), and the Applied Basic Research Plan on the Project in Yunnan Province (No. 2013).

The authors wish to thank all authors included in the citations for providing ideas for this work. They are also thankful for all the anonymous reviewers for reviewing this article and providing invaluable comments and suggestions.

References

1. M. E. Keskin, "A Column Generation Heuristic for Optimal Wireless Sensor Network Design with Mobile Sinks," *European Journal of Operational Research*, Vol. 260, No. 1, pp. 291-304, 2016
2. S. Yu, L. Shuai, and J. Peng, "A High-Efficiency Uneven Cluster Deployment Algorithm based on Network Layered for Event Coverage in UWSNs," *Sensors*, Vol. 16, No. 12, pp. 2103, 2016
3. T. Gao, D. Greenspan, M. Welsh, R. R. Juang, and A. Alm, "Vital Signs Monitoring and Patient Tracking over a Wireless Network," in *Proceedings of International Conference of the Engineering in Medicine & Biology Society*, pp. 102, 2005
4. A. Rasheed and R. N. Mahapatra, "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks," *IEEE Press*, pp. 958-965, 2012
5. M. H. R. Khouzani and S. Sarkar, "Maximum Damage Battery Depletion Attack in Mobile Sensor Networks," *IEEE Transactions on Automatic Control*, Vol. 56, No. 10, pp. 2358-2368, 2011
6. C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," in *Proceedings of IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113-127, 2003

7. Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks," in *Proceedings of Joint Conference of the IEEE Computer and Communications*, IEEE Societies, Vol. 3, pp. 1976-1986, 2003
8. M. H. R. Khouzani, S. Sarkar, and E. Altman, "Optimal Control of Epidemic Evolution," *IEEE INFOCOM*, Vol. 8, No. 1, pp. 1683-1691, 2011
9. L. Zhu, H. Zhao, and X. Wang, "Bifurcation Analysis of A Delay Reaction-Diffusion Malware Propagation Model with Feedback Control," *Communications in Nonlinear Science & Numerical Simulation*, Vol. 22, pp. 747-768, 2015
10. J. G. Ren, X. F. Yang, L. X. Yang, et al., "A Delayed Computer Virus Propagation Model and its Dynamics," *Chaos Solitons & Fractals*, Vol. 45, pp. 74-79, 2011
11. L. Zhu, H. Zhao, and X. Wang, "Stability and Bifurcation Analysis in a Delayed Reaction-Diffusion Malware Propagation Model," Pergamon Press, Inc., pp. 852-875, 2015
12. Z. Zhang and F. Si, "Dynamics of a Delayed SEIRS-V Model on the Transmission of Worms in a Wireless Sensor Network," *Advances in Difference Equations*, Vol. 2014, No. 1, pp. 1-15, 2014
13. M. E. J. Newman, "The Structure and Function of Complex Networks," *SIAM Review*, Vol. 45, No. 2, pp. 167-256, 2003
14. B. K. Mishra and N. Jha, "Fixed Period of Temporary Immunity after Run of Anti-Malicious Software on Computer Nodes," *Applied Mathematics & Computation*, Vol. 190, No. 2, pp. 1207-1212, 2007
15. B. K. Mishra and S. K. Pandey, "Fuzzy Epidemic Model for the Transmission of Worms in Computer Network," *Nonlinear Analysis Real World Applications*, Vol. 11, No. 5, pp. 4335-4341, 2010
16. X. Han and Q. Tan, "Dynamical Behavior of Computer Virus on Internet," *Applied Mathematics & Computation*, Vol. 217, No. 6, pp. 2520-2526, 2010
17. H. Yuan, G. Q. Chen, J. J. Wu, and H. Xiong, "Towards Controlling Virus Propagation in Information Systems with Point-to-Group Information Sharing," *Decision Support Systems*, Vol. 48, No. 1, pp. 57-68, 2009
18. B. K. Mishra and S. K. Pandey, "Dynamic Model of Worms with Vertical Transmission in Computer Network," *Applied Mathematics & Computation*, Vol. 217, No. 21, pp. 8438-8446, 2011
19. B. K. Mishra and D. K. Saini, "SEIRS Epidemic Model with Delay for Transmission of Malicious Objects in Computer Network," *Applied Mathematics & Computation*, Vol. 188, No. 2, pp. 1476-1482, 2007
20. B. K. Mishra and N. Jha, "SEIQRS Model for the Transmission of Malicious Objects in Computer Network," *Applied Mathematical Modelling*, Vol. 34, No. 3, pp. 710-715, 2010
21. B. K. Mishra and N. Keshri, "Mathematical Model on the Transmission of Worms in Wireless Sensor Network," *Applied Mathematical Modelling*, Vol. 37, No. 6, pp. 4103-4111, 2013
22. X. Wang, Q. Li, and Y. Li, "EiSIRS: a Formal Model to Analyze the Dynamics of Worm Propagation in Wireless Sensor Networks," *Journal of Combinatorial Optimization*, Vol. 20, No. 1, pp. 47-62, 2010
23. L. P. Song and R. P. Zhang, "Dynamical Analysis for a Malware Propagation Model in Wireless Sensor Network," *Journal of Measurement Science and Instrumentation*, 2016
24. C. Q. Gan, X. F. Yang, Q. Y. Zhu, J. Jin, and L. He, "The Spread of Computer Virus under the Effect of External Computers," *Nonlinear Dynamics*, Vol. 73, No. 3, pp. 1615-1620, 2013
25. L. P. Feng, X. F. Liao, H. Q. Li, and Q. Han, "Hopf Bifurcation Analysis of a Delayed Viral Infection Model in Computer Networks," *Mathematical & Computer Modelling*, Vol. 56, No. 7-8, pp. 167-179, 2012
26. J. G. Ren, Y. H. Xu, Y. C. Zhang, Y. Q. Dong, and G. S. Hao, "Dynamics of a Delay-Varying Computer Virus Propagation Model," *Discrete Dynamics in Nature and Society*, Vol. 2012, No. 6, pp. 857-868, 2012
27. T. Dong, X. Liao, and H. Li, "Stability and Hopf Bifurcation in a Computer Virus Model with Multistate Antivirus," *Abstract & Applied Analysis*, Vol. 2012, No. 2, pp. 374-388, 2012
28. H. R. Thieme and P. Van den Driessche, "Global Stability in Cyclic Epidemic Models with Disease Fatalities," *Differential Equations with Applications to Biology*, pp. 459-472, 1998
29. B. D. Hassard, N. D. Kazarinoff, and Y. H. Wan, "Theory and Applications of Hopf Bifurcation," Cambridge University Press, pp. 961-969, 1981

Xiaopan Zhang is currently pursuing a Master's degree in the School of Information Science and Technology at Yunnan Normal University. His current research interests include Internet of things and wireless sensor networks.

Lingyun Yuan received her Ph.D. from the Shenyang Institute of Automation at the Chinese Academy of Sciences. She is currently a professor in the School of Information Science and Technology at Yunnan Normal University. Her research interests include Internet of things and wireless sensor networks.

Jianhou Gan received his Ph.D. from Kunming University of Science and Technology. He is currently a professor in the Key Laboratory of Educational Information for Nationalities in the Ministry of Education at Yunnan Normal University. His research interests include artificial intelligence and knowledge engineering.

Cong Li is currently pursuing a Master's degree in the School of Information Science and Technology at Yunnan Normal University. His research interests include Internet of things and wireless sensor networks.