Hindawi
Complexity
Volume 2023, Article ID 8823080, 12 pages
https://doi.org/10.1155/2023/8823080

Research Article

A Malware Propagation Model with Dual Delay in the Industrial Control Network

Wei Yang,[1] Qiang Fu ,[2] and Yu Yao[3,4]

[1]*Software College, Northeastern University, Shenyang 110169, China*
[2]*College of Computer Science and Technology, Shenyang University of Chemical Technology, Shenyang 110142, China*
[3]*College of Computer Science and Engineering, Northeastern University, Shenyang 110169, China*
[4]*Engineering Research Center of Security Technology of Complex Network System, Ministry of Education, Shenyang, China*

Correspondence should be addressed to Qiang Fu; qiang.fu@outlook.com

Received 28 June 2023; Revised 23 September 2023; Accepted 17 October 2023; Published 30 October 2023

Academic Editor: Dan Selişteanu

The malware attacks targeting the industrial control network are gradually increasing, and the nonlinear phenomenon makes it difficult to predict the propagation behavior of malware. Once the dynamic system becomes unstable, the propagation of malware will be out of control, which will seriously threaten the security of the industrial control network. So, it is necessary to model and study the propagation of malware in the industrial control network. In this paper, a SIDQR model with dual delay is proposed by fully considering the characteristics of the industrial control network. By analyzing the nonlinear dynamics of the model, the Hopf bifurcation is discussed in detail when the value of dual delay is greater than zero, and the expression for the threshold is also provided. The results of the experiments indicate that the system may have multiple bifurcation points. By comparing different immune and quarantine rates, it is found that the immune rate can be appropriately increased and the isolation rate can be appropriately reduced in the industrial control network, which can suppress the spread of malware without interrupting the industrial production.

1. Introduction

The industrial control network is the key foundation for realizing digital transformation. It is an emerging business form and application model formed by the deep integration of new information technology and the industrial economy. ICS (industrial control system) has become an important component of many national infrastructures. With the continuous upgrading of the ICS, the connection between the industrial control network and the Internet is increasingly close, which leads to the further increase of security risks.

The number of the industrial control network security accidents is increasing year by year. In 2010, the Bushehr nuclear power plant in Iran was attacked by the Stuxnet worm [1]. Since then, many malwares targeting the industrial control network have been discovered, such as Night Dragon [2], Flame [3], Duqu/Duqu2.0 [4], Blaster [5], and BlackEnergy [6]. The typical PLC (programmable logic controller) worm Blaster spread through the control system of Siemens SIMATIC S7-1200 without any PCs. PLC Blaster can scan the ICS networks to find new targets and then attack the PLC and complete self-replication in the infected PLC. Some new types of malware can spread not only in PC networks but also in PLCs in the industrial control network. In 2012, Russian security experts discovered the flame virus spreading widely in the energy industry in the Middle East [7]. In December 2015, Ukraine was attacked by hackers which led to a large-scale power outage [8]. The malware Industroyer [9], which was found in 2017, is aimed at key ICS and can lead to power outages. In December 2017, due to the zero-day vulnerability of Schneider's Triconex SIS, a power plant in the Middle East was attacked and ultimately had to shut down [10]. The ransomware WannaCry can spread crazily globally in the same year and attack critical infrastructure [11]. In 2018, a chlorine gas station in Ukraine was attacked by VPNFilter virus [12]. In 2019, the power grid of Venezuela was attacked, and it led to large-scale power outages across the country [13]. The industrial control network has its own characteristics, for

example, industrial control protocols are lack of built-in security mechanisms. Also, the processing capacity of ICS is weak, and the system update is lagging behind. Based on the above situation, in order to address the security issues faced by the industrial control network, it is necessary to understand the propagation patterns of malware in the industrial control network and propose appropriate containment strategies. Therefore, it is particularly necessary to model and analyze the propagation behavior of malicious software in industrial control networks.

Researchers have proposed some important epidemic models to explore the dynamic behavior of malware propagation. For example, in the SIS model [14–17] and the SIR model [18–22], the early studies were focused on ordinary networks. On the basis of these traditional models, researchers have proposed new models to study the propagation of different types of malware. Chen et al. analyzed the propagation behavior of malware in Bluetooth and mobile applications and proposed a malicious software propagation model in mobile networks [23]. Inspired by the SEIR model [24], Xiao et al. introduced a new state (i.e., quarantined state) in the epidemic model, which is a malware propagation model in WiFi environments [25]. Wang et al. proposed a microscopic mathematical model to describe the propagation behavior of malware in a sensor network and designed a LDS (local defense strategy) using mobile "patches" (mobile components that can distribute patches) [26]. In the malware propagation model, if time delay (such as patch release and quarantine) is not considered, the model is an ordinary differential dynamical system, and the above models all belong to this category. If such delay factors are considered, the resulting model is a delay differential dynamic system. Yao et al. considered the delay caused by IDS (intrusion detection systems), analyzed nonlinear phenomena, and proposed a threshold for bifurcation [27]. Ren et al. considered the delay factor on the basis of the SIR model and analyzed the stability conditions of the dynamic system [28]. Subsequently, they proposed an epidemic model with time-varying latency and analyzed the bifurcation phenomenon [29]. On this basis, Wang et al. analyzed and discussed the chaos phenomenon of time-delay models [30]. Feng et al. considered the situation of dual delay and antimalware measures and studied the Hopf bifurcation phenomenon in malware propagation [31]. Wang et al. studied the threshold problem of stability in dynamic systems when the propagation rate varies linearly [32]. Khan et al. investigated a discretized two-dimensional model, and the results for the existence and uniqueness, and conditions for local stability with topological classifications of the equilibrium solutions are determined [33]. Wang et al. investigated the selection mechanism of the minimal wave speed for traveling waves to an epidemic model, and a threshold is defined by the eigenvalue problem of the linearized system [34].

Currently, there is limited research on the spread of malware in the industrial control network. The network of real industrial control systems is relatively complex, and the nonlinear phenomena (such as bifurcation and chaos) in the propagation process of malware also make it difficult to predict its propagation behavior, which can also lead to the failure of containment strategies, and then, it will lead to system instability and hinder the normal operation of industrial production. So we will propose a malware propagation model for the industrial control network. The industrial control network is different from the Internet, the industrial control equipment generally do not have powerful processors like computers, and the bandwidth requirements of the industrial control networks are much lower than those of the Internet. At the same time, the quarantine of industrial control equipment also needs to take into account production activities. Therefore, when dealing with infected industrial control equipment, it is difficult to repair them as quickly as computers. So we introduce immune delay and quarantine delay into the model, and it can describe the influence of malware containment strategies on the propagation in the industrial control network more accurately. Currently, some researchers have conducted some research on the problem of dual delay. Zhang et al. proposed the conditions for the asymptotic stability of Hopf bifurcation with dual delay [35]. Fan et al. introduced the stability and bifurcation of a coupled HR model with dual delay [36]. He et al. proposed a neural network model with unidirectional coupling delay and discovered double Hopf bifurcations in this model [37].

Based on the above works, we consider the dual delay in the industrial control network and propose a new malware propagation model and the propagation behavior of malware, and the bifurcation phenomena is analyzed under different cases. The innovation of this model lies in the inclusion of two different delays, which makes it more suitable for the actual situation of the industrial control network. This model can provide a security defense strategy against the spread of malware for the industrial control networks without affecting industrial production as much as possible. In addition, in the industrial control networks, our research results demonstrate how to suppress the spread of malware while maintaining the stability of industrial control systems. The organization of the paper is as follows: Section 2 explains how the model is established in the industrial control network, Section 3 analyzes the stability of the equilibrium of the dynamic system, Section 4 presents the experimental results, and Section 5 is a conclusion.

2. Model Formulation

In actual industrial control networks, the propagation delay of malware objectively exists and can take various forms. For example, the delay caused by malware latency, and the delay caused by upgrading and patching the software and hardware of susceptible equipment. During the detection process, the time window mechanism is used for quarantine, and it will cause quarantine delay. Based on these characteristics, we propose a malware propagation model with dual delay. Namely, the delay is caused by upgrading and patching the software and hardware of susceptible equipment, and it is called immune delay. Another delay is caused by using the time window mechanism to quarantine infected equipment, which is referred to as quarantine delay. The time window mechanism can improve the accuracy of detection, so as not to affect the normal production of the factory due to false alarms. That is to say, when abnormal behavior is detected, an alarm will not be

triggered immediately. Only when this abnormal behavior reaches a preset threshold, it will be considered an intrusion behavior, and an alarm will be issued. Time window mechanism will cause a delay before quarantine, and it will bring complex dynamic changes to the spread of malware. We will use the stability switching principle [38] to study the stability of the dynamic system with dual delay in the next section, and the assumptions for model formulation are listed as follows:

(a) In our model, the industrial control network is assumed as a homogeneous network

(b) It is assumed that the total number of all equipment remains unchanged, and the number is N

(c) The equipment in the industrial control network has functions such as software upgrade and patching, and a time window mechanism is adopted

$$\begin{cases} \dfrac{dS(t)}{\mathrm{dt}} = \varphi R(t) - \theta_1 S(t) - \beta I(t) S(t), \\ \dfrac{dI(t)}{\mathrm{dt}} = \beta I(t) S(t) - \theta_2 I(t), \\ \dfrac{dD_1(t)}{\mathrm{dt}} = \theta_1 S(t) - \theta_1 S(t-\tau_1), \\ \dfrac{dD_2(t)}{\mathrm{dt}} = \theta_2 I(t) - \theta_2 I(t-\tau_2), \\ \dfrac{dQ(t)}{\mathrm{dt}} = \theta_2 I(t-\tau_2) - \gamma Q(t), \\ \dfrac{dR(t)}{\mathrm{dt}} = \gamma Q(t) + \theta_1 S(t-\tau_1) - \varphi R(t). \end{cases} \tag{1}$$

In our proposed SIDQR dual-delay model, each industrial control equipment may have six states: susceptible (S) state, infected (I) state, immune delay (D_1) state, quarantine delay (D_2) state, quarantine (Q) state, and recovery (R) state. The recovery rate of the susceptible equipment is θ_1, the quarantine rate of the infected equipment is θ_2, the infection rate of the susceptible equipment is β, and the recovered rate of the quarantined equipment is γ. When facing new malware, there is a probability φ that recovered equipment will return to susceptible equipment. The transition diagram among the different states is shown in Figure 1. In summary, assuming the total number of all equipment is N, the differential equation system (1) of the SIDQR model with dual delay can be obtained, and the immune delay is τ_1, and the quarantine delay is τ_2.

3. Stability of Equilibrium

The stability of the equilibrium of system (1) is studied in this section, we focus on discussing the situation of $\tau_1 > 0, \tau_2 > 0$, and we provide an expression for the threshold. For system (1), the following theorem can be obtained.

Theorem 1. *System (1) has an unique positive equilibrium point* $E^* = (S^*, I^*, D_1^*, D_2^*, Q^*, R^*)$ *when* $R_0 = \beta N/\theta_2 > 1$, *where* R_0 *is the basic reproduction number, and it means that the basic reproduction number is positive as an initial condition.*

Proof. When system (1) is stable, that is, the left side of the differential equation system is equal to zero, and thus, the equilibrium point can be obtained:

$$\begin{cases} S^* = \dfrac{\theta_1 + \gamma}{\beta}, I^*, \\ {D_1}^* = \theta_1 \tau_1 S^*, {D_2}^* = \theta_2 \tau_2 I^*, \\ Q^* = \dfrac{\theta_2}{\gamma} I^*, R^* = \dfrac{\theta_1 + \gamma}{\varphi} I^*. \end{cases} \tag{2}$$

Since the total number of all equipment is N, the equation with I^* as the root can be obtained as

$$\frac{\theta_1 + \gamma}{\beta} + I^* + \theta_1 \tau_1 \frac{\theta_1 + \gamma}{\beta} + \theta_2 \tau_2 I^* + \frac{\theta_2}{\gamma} I^* + \frac{\theta_1 + \gamma}{\varphi} I^* = N. \tag{3}$$

Obviously, equation (3) has a unique positive real root I^* and a unique positive equilibrium point $E^* = (S^*, I^*, D_1^*, D_2^*, Q^*, R^*)$. Then, $Q(t) = N - S(t) - I(t) - D_1(t) - D_2(t) - R(t)$, and system (1) can be simplified into the following form:

$$\begin{cases} \dfrac{dS(t)}{\mathrm{dt}} = \varphi R(t) - \theta_1 S(t) - \beta I(t) S(t), \\ \dfrac{dI(t)}{\mathrm{dt}} = \beta I(t) S(t) - \theta_2 I(t), \\ \dfrac{dD_1(t)}{\mathrm{dt}} = \theta_1 S(t) - \theta_1 S(t-\tau_1), \\ \dfrac{dD_2(t)}{\mathrm{dt}} = \theta_2 I(t) - \theta_2 I(t-\tau_2), \\ \dfrac{dR(t)}{\mathrm{dt}} = \gamma \left[N - S(t) - I(t) - D_1(t) - D_2(t) - R(t) \right] + \theta_1 S(t-\tau_1) - \varphi R(t). \end{cases} \tag{4}$$

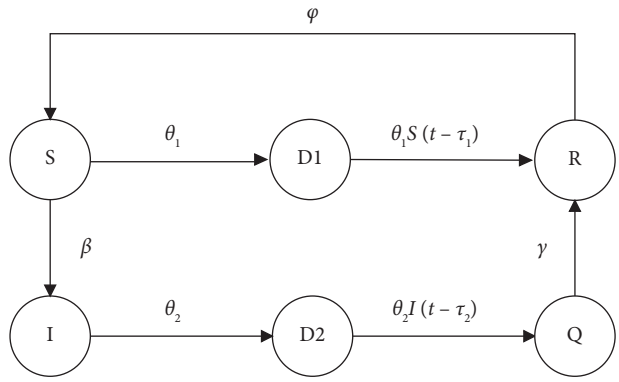

Figure 1: The transition diagram among different states in the industrial control network.

The Jacobi matrix of the equilibrium point is

$$J(E^*) = \begin{pmatrix} -\theta_1 - \beta I^* & -\beta S^* & 0 & 0 & \varphi \\ \beta I^* & \beta S^* - \theta_2 & 0 & 0 & 0 \\ \theta_1 - \theta_1 e^{-\lambda\tau_1} & 0 & 0 & 0 & 0 \\ 0 & \theta_2 - \theta_2 e^{-\lambda\tau_2} & 0 & 0 & 0 \\ \theta_1 e^{-\lambda\tau_1} - \gamma & -\gamma & -\gamma & -\gamma & -\gamma - \varphi \end{pmatrix}. \tag{5}$$

Then, the following equation can be obtained:

$$\lambda \mathbf{E} - J(E^*) = \begin{pmatrix} \lambda + \theta_1 + \beta a_1 & -\beta a_2 & 0 & 0 & \varphi \\ \beta a_1 & \lambda - \beta a_2 + \theta_2 & 0 & 0 & 0 \\ \theta_1 - \theta_1 e^{-\lambda\tau_1} & 0 & \lambda & 0 & 0 \\ 0 & \theta_2 - \theta_2 e^{-\lambda\tau_2} & 0 & \lambda & 0 \\ \theta_1 e^{-\lambda\tau_1} - \gamma & -\gamma & -\gamma & -\gamma & \lambda + \gamma + \varphi \end{pmatrix}, \tag{6}$$

where $a_1 = I^*, a_2 = S^*$.

Due to the existence of two delays in this model, in the process of solving characteristic equations, it is necessary to reduce the order and obtain the algebraic cofactors. The first algebraic cofactor is

$$(\lambda + \theta_1 + \beta a_1) \begin{pmatrix} \lambda - \beta a_2 + \theta_2 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ \theta_2 - \theta_2 e^{-\lambda\tau_2} & 0 & \lambda & 0 \\ -\gamma & -\gamma & -\gamma & \lambda + \gamma + \varphi \end{pmatrix}, \tag{7}$$

the second algebraic cofactor is

$$\beta a_2 \begin{pmatrix} \beta a_1 & 0 & 0 & 0 \\ \theta_1 - \theta_1 e^{-\lambda\tau_1} & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ \theta_1 e^{-\lambda\tau_1} - \gamma & -\gamma & -\gamma & \lambda + \gamma + \varphi \end{pmatrix}, \tag{8}$$

and the third algebraic cofactor is

$$\varphi \begin{pmatrix} \beta a_1 & \lambda - \beta a_2 + \theta_2 & 0 & 0 \\ \theta_1 - \theta_1 e^{-\lambda\tau_1} & 0 & \lambda & 0 \\ 0 & \theta_2 - \theta_2 e^{-\lambda\tau_2} & 0 & \lambda \\ \theta_1 e^{-\lambda\tau_1} - \gamma & -\gamma & -\gamma & -\gamma \end{pmatrix}. \tag{9}$$

Then, we calculate the three cofactors separately and add them together to obtain the characteristic equation of the system:

$$P(\lambda) + Q_1(\lambda) e^{-\lambda\tau_1} + Q_2(\lambda) e^{-\lambda\tau_2} = 0, \tag{10}$$

where

$$\begin{aligned} P(\lambda) &= \lambda^5 + p_4\lambda^4 + p_3\lambda^3 + p_2\lambda^2 + p_1\lambda, \\ Q_1(\lambda) &= q_1 e^{-\lambda\tau_1}, Q_2(\lambda) = q_2 e^{-\lambda\tau_2}, \\ p_4 &= \theta_1 + \beta a_1 + \gamma + \varphi + \theta_2 - \beta a_2, \\ p_3 &= \begin{pmatrix} \theta_1\gamma + \beta a_1\gamma + \theta_1\varphi + \beta a_1\varphi + \theta_1\theta_2 + \beta a_1\theta_2 + \theta_2\gamma + \theta_2\varphi \\ + \beta a_2\beta a_1 - \beta a_2\theta_1 - \beta a_1\beta a_2 - \beta a_2\varphi - \beta a_2\gamma - \gamma\varphi \end{pmatrix}, \\ p_2 &= \begin{pmatrix} \theta_1\theta_2\gamma + \beta a_1\theta_2\gamma + \theta_1\theta_2\varphi + \beta a_1\theta_2\varphi + \gamma\beta a_2\beta a_1 \\ - \theta_1\beta a_2\gamma - \beta a_2\beta a_1\gamma - \beta a_2\varphi\theta_1 - \beta a_2\varphi\beta a_1 \\ + \varphi\beta a_2\beta a_1 + \gamma\varphi\beta a_2 + \varphi\theta_1\gamma - \gamma\varphi\theta_2 - \varphi\beta a_1\gamma \end{pmatrix}, \\ p_1 &= (\varphi\theta_2\theta_1\gamma - \varphi\beta a_2\theta_1\gamma + \gamma\varphi\beta a_1\theta_2), \\ q_1 &= \left[\varphi\lambda^3 + (\varphi\theta_2 - \gamma\varphi - \varphi\beta a_2)\lambda^2 + (\varphi\beta a_2\gamma - \varphi\theta_2\gamma)\lambda\right]\theta_1, \\ q_2 &= -\gamma\varphi\beta a_1\theta_2\lambda. \end{aligned} \tag{11}$$

For system (1), the stability of the equilibrium point needs to be discussed in different cases. The cases $\tau_1 = \tau_2 = \tau$, $\tau_1 = 0$, $\tau_2 > 0$, and $\tau_1 > 0, \tau_2 = 0$ are essentially the same as the single delay model discussed in paper [27–29, 32], and we will not repeat the proof here. Our main analysis here is the stability of the equilibrium in the case of $\tau_1 > 0, \tau_2 > 0$. In this case, the stability analysis of the system requires fixing the value range of one delay within the threshold, that is, $\tau_1 > 0, \tau_2 < \tau_k$ or $\tau_1 < \tau_k$, $\tau_2 > 0$; at this point, the variable can be considered as one of the delays (τ_1 or τ_2). Let us take the case of $\tau_1 > 0, \tau_2 < \tau_k$ as an example to discuss here. The root of the system characteristic equation is $\lambda = i\omega_1$. By substituting it into equation (10) and separating the real and imaginary parts, we can obtain

$$p_4{\omega_1}^4 - p_2{\omega_1}^2 + q_2\cos(\omega_1\tau_2) + q_1\omega_1\sin(\omega_1\tau_1) = 0, \tag{12}$$

$${\omega_1}^5 - p_3{\omega_1}^3 + p_1\omega_1 - q_2\sin(\omega_1\tau_2) + q_1\omega_1\cos(\omega_1\tau_1) = 0. \tag{13}$$

By combining equation (12) and (13), it can be obtained that

$$\begin{aligned}{\omega_1}^{10} + D_6{\omega_1}^8 + D_5{\omega_1}^6 + D_4{\omega_1}^4 + D_3{\omega_1}^3 \\ + D_2{\omega_1}^2 + D_1\omega_1 + D_0 = 0,\end{aligned} \tag{14}$$

where

$$\begin{aligned}D_6 &= {p_4}^2,\\ D_5 &= {p_3}^2 - 2p_2,\\ D_4 &= {p_2}^2 - 2p_1p_3 + 2q_2\cos(\omega_1\tau_2),\\ D_3 &= 2q_2p_3\sin(\omega_1\tau_2),\\ D_2 &= {p_1}^2 - {q_1}^2 - 2p_2q_2\cos(\omega_1\tau_2),\\ D_1 &= -2p_2q_2\sin(\omega_1\tau_2),\\ D_0 &= {q_1}^2.\end{aligned} \tag{15}$$

Assuming that equation (15) has finite positive roots $\omega_{11}, \omega_{12}, \omega_{13}...\omega_{1k}$, using the Routh–Hurwitz criterion, for each value of k, the corresponding threshold of delay is

$$\tau_{1k}^j = \frac{1}{\omega_{1k}}\arccos\left(\frac{-\omega_1^5 + p_3\omega_1^3 - p_1\omega_1 - q_2\sin(\omega_1\tau_2)}{q_1\omega_1}\right) + \frac{2k\pi}{\omega_0}, \tag{16}$$

where k and j are both positive real numbers, let $\tau_1^* = \min\{\tau_{1k}^0\}$, $\omega_1^* = \omega_{1k}$ and the transversality condition holds, and the following conclusion can be obtained based on Rouche's theorem:

$$\left.\frac{d(\mathrm{Re}\lambda)}{d\tau}\right|_{\tau_1=\tau_1^*} > 0. \tag{17}$$

□

Theorem 2. *Assuming that $R_0 = \beta N/\theta_2 > 1$, then the following can be obtained, and it is quoted in reference [27, 39].*

(1) When $\tau_1 \in [0, \tau_1^*)$, for system (1), the positive equilibrium point $E^* = (S^*, I^*, D_1^*, D_2^*, Q^*, R^*)$ is locally asymptotically stable. When $\tau_1 > \tau_1^*$, the positive equilibrium point is unstable.

(2) When system (1) satisfies $d(Re\lambda)/d\tau|_{\tau_1=\tau_1^*} > 0$, the positive equilibrium point $E^* = (S^*, I^*, D_1^*, D_2^*, Q^*, R^*)$ of the system will undergo a Hopf bifurcation at $\tau_1 = \tau_1^*$, and the system will lose stability.

(3) In equation (16), k and j are both positive real numbers, and the value of τ_{1k} is also affected by τ_2. Therefore, when $\tau_1 > 0, \tau_2 > 0$, the system may have multiple bifurcation points.

4. Experiments

In order to demonstrate the impact of dual delay on the propagation of malware, numerical experiments analysis is conducted in this section. The infection rate is assumed that $\beta = 0.5$, the recovered rate of the susceptible equipment is assumed that $\theta_1 = 0.01$, the quarantine rate of the infected equipment is assumed that $\theta_2 = 0.04$, the recovered rate of the quarantined equipment is assumed that $\gamma = 0.02$, and the probability of the recovered equipment becoming susceptible to infection is $\varphi = 0.05$. At the initial stage, the total number of equipment is 10000, assuming that the number of infected equipment (I) is 50 and the other equipment were susceptible (S). Due to the existence of a double delay, this section first presents the overall nonlinear phenomenon of the model through the bifurcation diagram.

4.1. Case 1 with $\tau_1 = 0$. The first to discuss is the bifurcation phenomenon of the system when $\tau_1 = 0$, as shown in Figure 2. The dynamic system in this case is equivalent to a single delay situation, where Hopf bifurcation occurs when the delay value exceeds the threshold. That is to say, in this situation, it is necessary to control the quarantine delay in the ICS to ensure that the malware will not get out of control. The quarantine delay needs to be less than the threshold, so that the dynamic system will eventually reach equilibrium after oscillation. Also, the curves of the equipment in different states are shown in Figure 3 ($\tau_1 = 0, \tau_2 = 300$) and Figure 4 ($\tau_1 = 0, \tau_2 = 550$), which also validate Theorem 5 of the single delay model in paper [27].

4.2. Case 2 with $\tau_2 = 0$. What needs to be discussed next is the bifurcation phenomenon of the system when $\tau_2 = 0$. As shown in Figure 5, the Hopf bifurcation diagram in this case is different from the ordinary single delay bifurcation. When the value of delay exceeds the threshold, a curve is in a fluctuating state, but it has no effect on the system bifurcation, and the entire dynamic system is still in a bifurcation state. This can indicate that in this dual-delay model, τ_1 has a greater impact on the dynamic system, which means that immune delay will make the nonlinear phenomena of the system more complex. Figures 6 and 7 show the curves of the number of equipment at $\tau_2 = 0, \tau_1 = 900$ and $\tau_2 = 0, \tau_1 = 1200$, respectively. The propagation process shown in Figures 6 and 7 can verify the results of Figure 5.

When $\tau_2 = 0$, that is, the quarantine delay is zero, the dynamic system may be in a bifurcation state. When the immune delay is less than the threshold value ($\tau_1 < 1100$), the system will be stable, and the curves finally reach equilibrium and no longer fluctuate, as it is shown in Figure 6. In Figure 7, the number of equipments in different states fluctuates continuously over time, indicating that the system cannot be controlled. In this situation, the number of infected equipment and the spread trend of malware become difficult to predict. This will pose a serious threat to the equipment in the ICS.

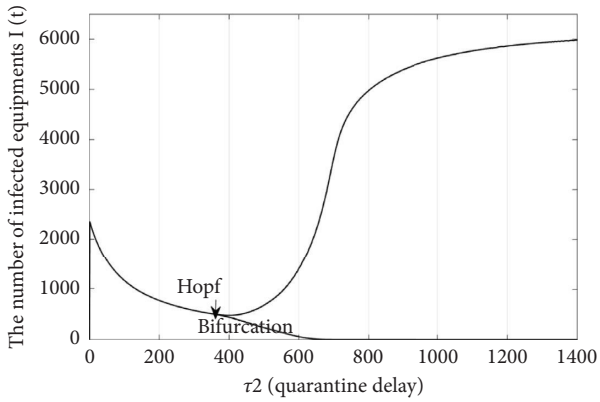

Figure 2: Hopf bifurcation diagram of the system with $\tau_1 = 0$.

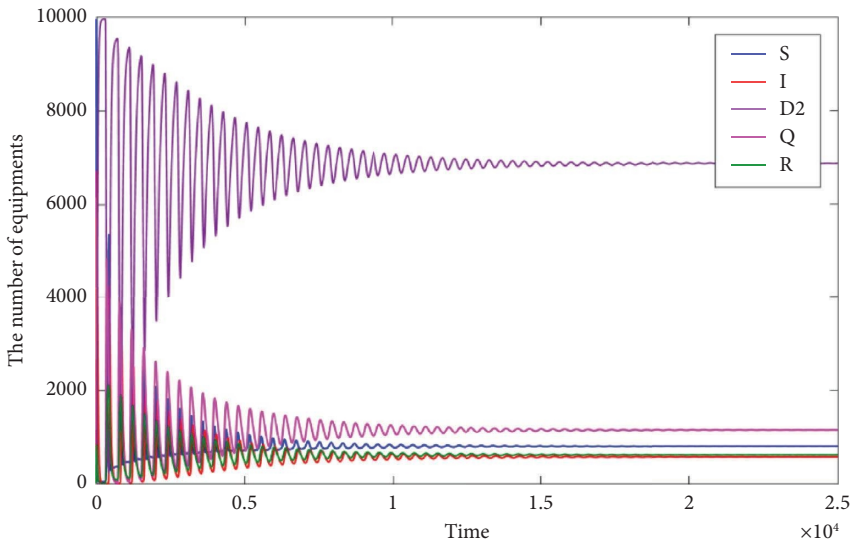

Figure 3: The malware propagation with $\tau_1 = 0, \tau_2 < \tau_{2k}$.

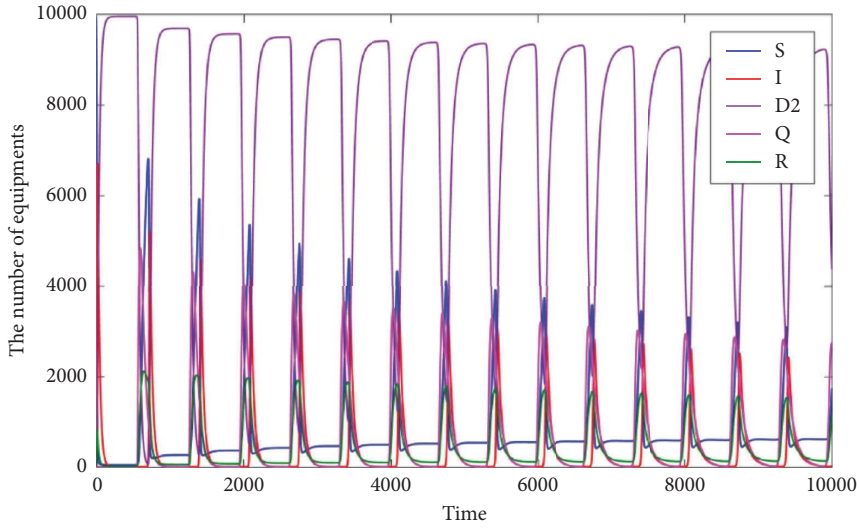

Figure 4: The malware propagation with $\tau_1 = 0, \tau_2 > \tau_{2k}$.

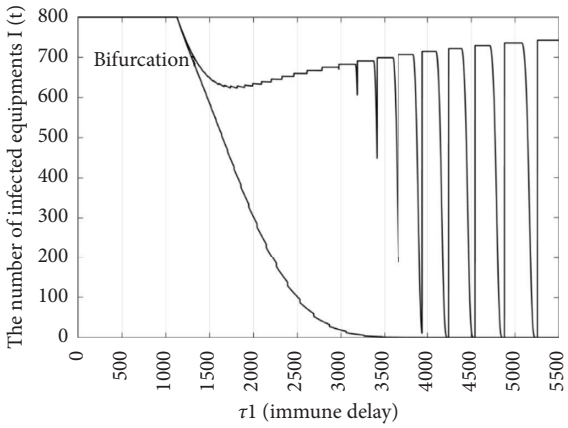

Figure 5: Hopf bifurcation diagram of the system with $\tau_2 = 0$.

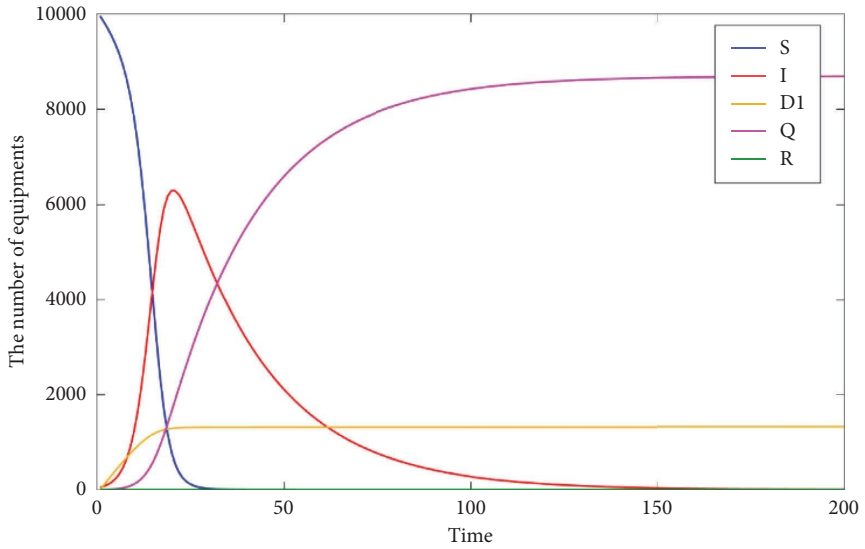

Figure 6: The malware propagation with $\tau_2 = 0, \tau_1 < \tau_{1k}$.

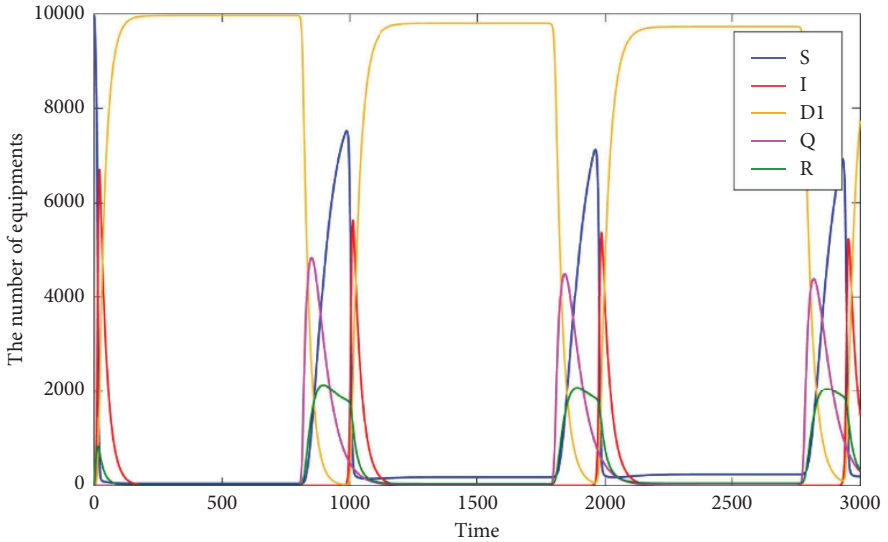

Figure 7: The malware propagation with $\tau_2 = 0, \tau_1 > \tau_{1k}$.

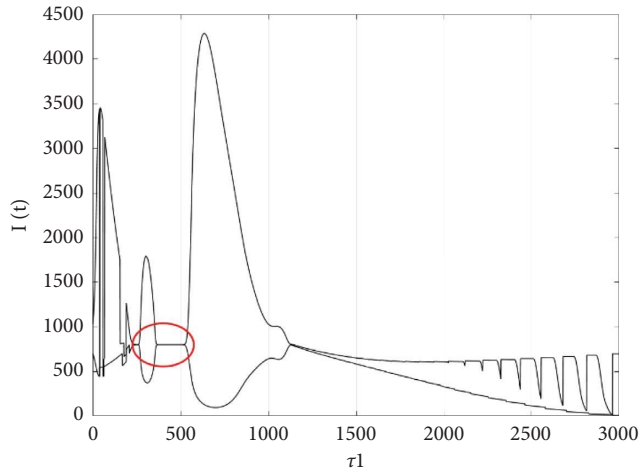

Figure 8: Hopf bifurcation diagram of the system with $\tau_1 > 0, \tau_2 < \tau_{2k}$.

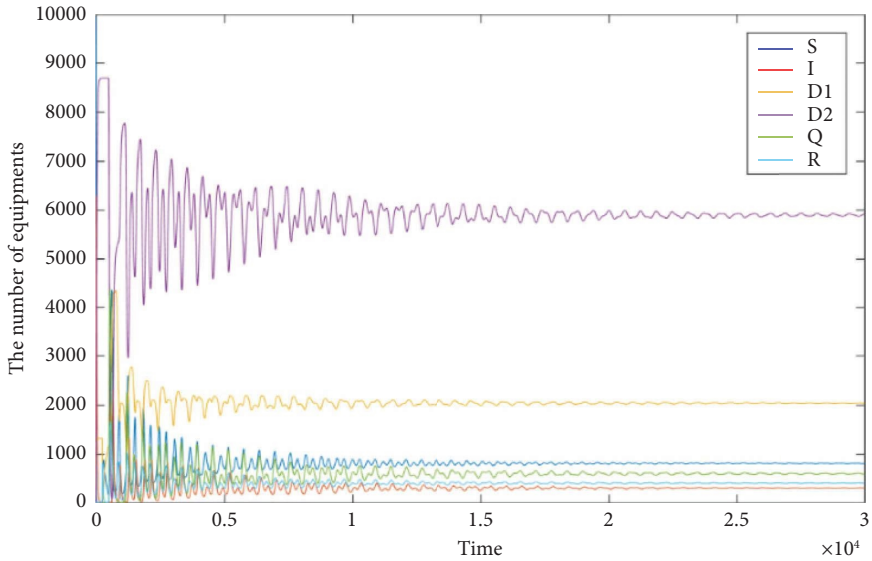

Figure 9: The malware propagation with $\tau_2 = 500, \tau_1 = 255$.

4.3. Case 3 with $\tau_1 > 0, \tau_2 > 0$. When $\tau_1 > 0, \tau_2 > 0$, it can be seen from the two situations mentioned above that immune delay has a significant impact on the stability of the system. Therefore, let us take $\tau_1 > 0, \tau_2 < \tau_{2k}$ to further discuss the impact on the system. Figure 8 shows the Hopf bifurcation diagram of the system in this case. It can be seen that when neither delay is zero and the value of τ_2 is fixed, then the system will have multiple bifurcation points. This indicates that the system will experience bifurcation and then return to a stable state, and then, as the value of τ_1 increases, the system will experience bifurcation again, which is consistent with the content of Theorem 2 in Section 3. To verify the result, the value of τ_1 will be taken within the red circle range in Figure 8, and the curves of different state equipment are also shown in Figures 9–11.

In Figures 9–11, the quarantine delay of the system is fixed at $\tau_2 = 500$, and the value of τ_1 is 255, 300, and 400, respectively. It can be seen that as the value of τ_1 increases, the system undergoes a process of stability, bifurcation, and then stability. This is completely consistent with the results in the red circle in Figure 8. It indicates that in a dual-delay system, it is necessary to clarify the impact of different delays on system stability. For example, in Case 3, we cannot simply demand that the immune delay be as small as possible, because it may also lead to the bifurcation. It requires us to specifically analyze the impact of immune delay on the dynamic system, accurately control it to ensure system stability, and suppress the spread of malware.

The experiments above demonstrate how to maintain the stability of the dynamic system by controlling the value of immune delay and quarantine delay. In addition, from equation (16), it can be seen that the stability of the dynamic system can also be maintained by adjusting the immune rate θ_1 and quarantine rate θ_2, that is, by changing the parameters so that the delay is less than the threshold. Figure 12 shows the curve of infected equipment under different immune

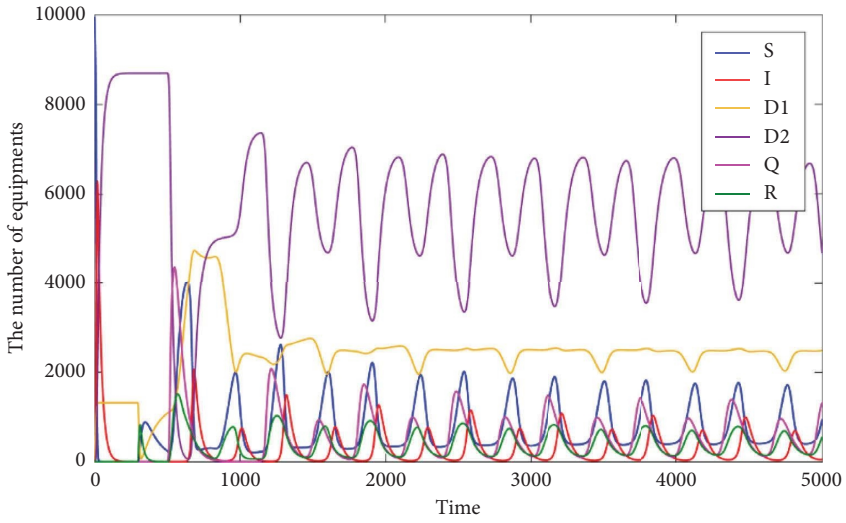

Figure 10: The malware propagation with $\tau_2 = 500, \tau_1 = 300$.

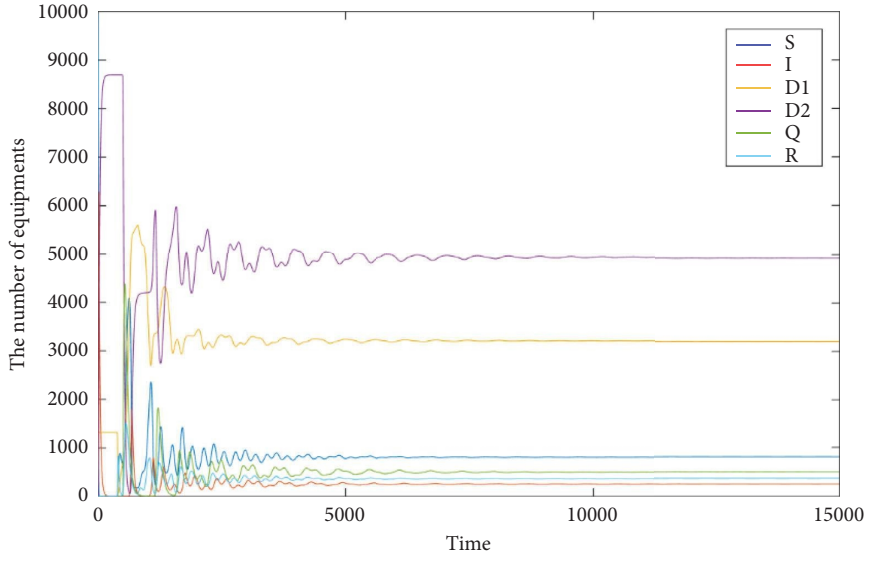

Figure 11: The malware propagation with $\tau_2 = 500, \tau_1 = 400$.

rates with $\tau_1 = 300, \tau_2 = 500$. It can be seen that as the immune rate θ_1 increases, the system changes from a bifurcation state to a stable state, and the number and peak value of infected equipment also decrease. It indicates that increasing the immune rate can maintain system stability and control the spread of malware.

Figure 13 shows the curve of infected equipment under different quarantine rates with $\tau_1 = 300, \tau_2 = 500$. From Figure 13, it can be observed that when the quarantine rate $\theta_2 = 0.04$, the curve of infected equipment continues to fluctuate, and the system is in a bifurcation state. As the value of the quarantine rate θ_2 decreases, the number of infected equipment will gradually reach a stable state. From the results, it can be seen that the spread of malware cannot be controlled solely through a large number of quarantine equipment, which may lead to instability and also have a significant impact on industrial production. In summary, in the protection of the ICS, the value of the immune rate can be appropriately increased and the value of the isolation rate can be appropriately reduced, which can ensure the stability of the system and suppress the spread of malware.

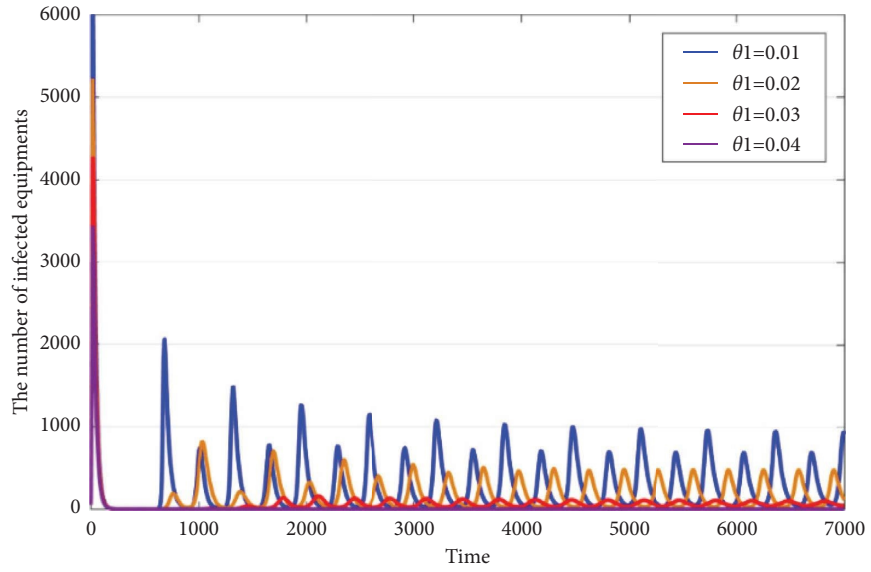

Figure 12: The number of $I(t)$ with different values of θ_1.

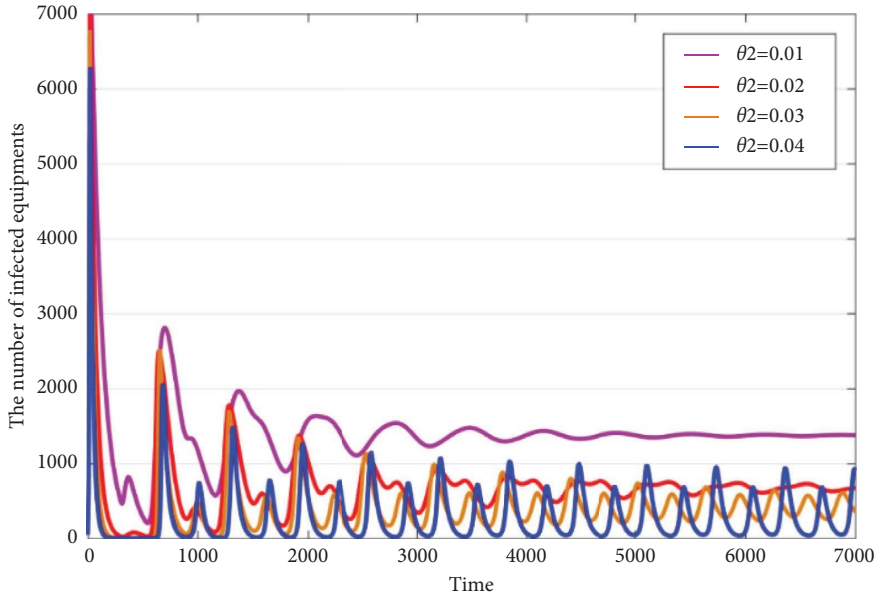

Figure 13: The number of $I(t)$ with different values of θ_2.

5. Conclusion

We fully consider the characteristics of the ICS and equipment in the industrial control network and propose a malware propagation model with dual delay. On this basis, we study the propagation of malware in the industrial control network and the stability and Hopf bifurcation of the dynamic system. Moreover, the containment strategy for malware in the industrial control network is proposed. In particular, the following conclusions can be obtained:

(1) In the industrial control network, the characteristics of immunity and quarantine in actual industrial production are considered, and the SIDQR model with dual delay is established. The model includes six states of industrial equipment: susceptible (S) state, infected (I) state, immune delay (D_1) state, quarantine delay (D_2) state, quarantine (Q) state, and recovery (R) state.

(2) The positive equilibrium point of the system is proven with Jacobian matrix and reduced order, the stability of the dynamic system at $\tau_1 > 0, \tau_2 > 0$ is discussed in detail, and an expression for the threshold is provided. When the delay exceeds the threshold, the system becomes unstable and Hopf bifurcation occurs. Also, the system may have multiple bifurcation points at $\tau_1 > 0, \tau_2 > 0$.

(3) Under different cases, the experiments demonstrate the propagation of malware in the industrial control

networks, and the possible bifurcation points of the system in different cases are shown. In addition, after comparing different immune and quarantine rates, the experimental results show that the immune rate can be appropriately increased and the quarantine rate can be appropriately reduced, which can ensure the stability of the ICS and suppress the spread of malware.

However, when the industrial control network encounters cross-network attacks, the model is not applicable. In addition, the importance of different equipment in the industrial control system also varies, and the key equipment such as SCADA servers is likely to play the role of key nodes. If malware prioritizes attacking these critical nodes, the propagation trend will undergo significant changes. How will the effectiveness of the containment strategy change when prioritizing the control of these key nodes during the defense process? These works need to be improved in subsequent research.

Data Availability

No underlying data were collected or produced in this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This paper was supported by National Key R&D Program of China under Grant no. 2021YFB3101700, Applied Basic Research Program of Liaoning Province under Grant no. 2022JH2/101300240, Fundamental Research Funds for the Central Universities under Grant no. N2324004-12, and Scientific Research Project of Liaoning Province Education Department under Grant no. LJKQZ20222457.

References

[1] L. J. Trautman and P. C. Ormerod, "Industrial cyber vulnerabilities: lessons from stuxnet and the internet of things," *Social Science Electronic Publishing*, vol. 72, pp. 767–770, 2017.

[2] D. Gewirtz, "Night dragon: cyberwar meets corpoiate espionage," *Journal of counterterrorism and homeland security International*, vol. 17, no. 2, p. 6, 2011.

[3] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi, "The cousins of stuxnet: duqu, flame, and gauss," *Future Internet*, vol. 4, no. 4, pp. 971–1003, 2012.

[4] P. Maynard, K. Mclaughlin, and S. Sezer, "Modelling duqu 2.0 malware using attack trees with sequential conjunction," *Proceedings of the International Conference on Information Systems Security and Privacy*, pp. 465–472, 2016.

[5] R. Spenneberg, M. Brüggemann, and H. Schwartke, "Plc-blaster: a worm living solely in the plc," *Black Hat Asia*, vol. 16, 2016.

[6] S. Raval, "Blackenergy a threat to industrial control systems network security," *International Journal of Advanced Research in Engineering and Technology*, vol. 2, no. 12, pp. 120–125, 2015.

[7] K. Lab, "The flame: questions and answers," 2012, https://securelist.com/the-flame-questions-and-answers/34344/.

[8] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: analysis and practical mitigation strategies," in *Proceedings of the 2017 70th Annual Conference For Protective Relay Engineers*, pp. 1–8, College Station, TX, USA, April 2017.

[9] A. Bindra, "Securing the power grid: protecting smart grids and connected power systems from cyberattacks," *IEEE Power Electronics Magazine*, vol. 4, no. 3, pp. 20–27, 2017.

[10] N. Kshetri and J. Voas, "Hacking power grids: a current problem," *Computer*, vol. 50, no. 12, pp. 91–95, 2017.

[11] J. M. Ehrenfeld and C. WannaCry, "WannaCry, cybersecurity and health information technology: a time to act," *Journal of Medical Systems*, vol. 41, no. 7, p. 104, 2017.

[12] J. C. Sapalo Sicato, P. K. Sharma, V. Loia, and J. H. Park, "VPNFilter malware analysis on cyber threat in smart home network," *Applied Sciences*, vol. 9, no. 13, p. 2763, 2019.

[13] S. Smith, "Massive blackout sparks boom in generator sales," *Greenwire*, vol. 1, p. 16, 2019.

[14] B. Jhun, M. Jo, and B. Kahng, "Simplicial SIS model in scale-free uniform hypergraph," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2019, Article ID 123207, 2019.

[15] A. Coronel, F. Huancas, and M. Sepúlveda, "A note on the existence and stability of an inverse problem for a SIS model," *Computers & Mathematics with Applications*, vol. 77, no. 12, pp. 3186–3194, 2019.

[16] X. Wang, Z. Wang, and H. Shen, "Dynamical analysis of a discrete-time SIS epidemic model on complex networks," *Applied Mathematics Letters*, vol. 94, pp. 292–299, 2019.

[17] M. Y. Zhou, W. M. Xiong, H. Liao, T. Wang, Z. W. Wei, and Z. Q. Fu, "Analytical connection between thresholds and immunization strategies of SIS model in random networks," *Chaos*, vol. 28, no. 5, Article ID 051101, 2018.

[18] M. Asif, S. U. Jan, N. Haider, Q. Al-Mdallal, and T. Abdeljawad, "Numerical modeling of npz and sir models with and without diffusion," *Results in Physics*, vol. 19, Article ID 103512, 2020.

[19] N. H. Du and N. N. Nhu, "Permanence and extinction of certain stochastic SIR models perturbed by a complex type of noises," *Applied Mathematics Letters*, vol. 64, pp. 223–230, 2017.

[20] R. Xu, Z. Ma, and Z. Wang, "Global stability of a delayed SIRS epidemic model with saturation incidence and temporary immunity," *Computers & Mathematics with Applications*, vol. 59, no. 9, pp. 3211–3221, 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] A. Taghvaei, T. T. Georgiou, L. Norton, and A. Tannenbaum, "Fractional SIR epidemiological models," *Scientific Reports*, vol. 10, no. 1, pp. 20882–20915, 2020.

[23] Z. Chen, M. Wang, L. Xu, and W. Wu, "Worm propagation model in mobile network," *Concurrency and Computation: Practice and Experience*, vol. 28, no. 4, pp. 1134–1144, 2016.

[24] H. Yuan and G. Chen, "Network virus-epidemic model with the point-to-group information propagation," *Applied Mathematics and Computation*, vol. 206, no. 1, pp. 357–367, 2008.

[25] X. Xiao, P. Fu, C. Dou, Q. Li, G. Hu, and S. Xia, "Design and analysis of SEIQR worm propagation model in mobile internet," *Communications in Nonlinear Science and Numerical Simulation*, vol. 43, pp. 341–350, 2017.

[26] T. Wang, Q. Wu, S. Wen et al., "Propagation modeling and defending of a mobile sensor worm in wireless sensor and actuator networks," *Sensors*, vol. 17, no. 12, p. 139, 2017.
[27] Y. Yao, Q. Fu, W. Yang, Y. Wang, and C. Sheng, "An epidemic model of computer worms with time delay and variable infection rate," *Security and Communication Networks*, vol. 2018, no. 5, Article ID 9756982, 11 pages, 2018.
[28] J. G. Ren, X. F. Yang, L. X. Yang, Y. Xu, and F. Yang, "A delayed computer virus propagation model and its dynamics," *Chaos, Solitons & Fractals*, vol. 45, no. 1, pp. 74–79, 2012.
[29] J. Ren, X. Yang, Q. Zhu, L. X. Yang, and C. Zhang, "A novel computer virus model and its dynamics," *Nonlinear Analysis: Real World Applications*, vol. 13, no. 1, pp. 376–384, 2012.
[30] S. J. Wang, Q. M. Liu, X. F. Yu, and Y. Ma, "Bifurcation analysis of a model for network worm propagation with time delay," *Mathematical and Computer Modelling*, vol. 52, no. 3-4, pp. 435–447, 2010.
[31] 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 and Computer Modelling*, vol. 56, no. 7-8, pp. 167–179, 2012.
[32] F. Wang, Y. Zhang, C. Wang, J. Ma, and S. Moon, "Stability analysis of a SEIQV epidemic model for rapid spreading worms," *Computers & Security*, vol. 29, no. 4, pp. 410–418, 2010.
[33] A. Q. Khan and F. Nazir, "Almatrafi Bifurcation analysis of a discrete Phytoplankton–Zooplankton model with linear predational response function and toxic substance distribution," *International Journal of Biomathematics*, vol. 16, no. 4, 2023.
[34] Y. Wang, X. Wang, and G. Lin, "Speed selection of traveling waves to an epidemic model," *International Journal of Biomathematics*, vol. 16, no. 04, Article ID 2250098, 2023.
[35] Z. Zhang, Y. Wang, D. Bi, and L. Guerrini, "Stability and Hopf bifurcation analysis for a computer virus propagation model with two delays and vaccination," *Discrete Dynamics in Nature and Society*, vol. 2017, Article ID 3536125, 17 pages, 2017.
[36] D. Fan, L. Hong, and J. Wei, "Hopf bifurcation analysis in synaptically coupled HR neurons with two time delays," *Nonlinear Dynamics*, vol. 62, no. 1-2, pp. 305–319, 2010.
[37] X. He, C. Li, T. Huang, and C. Li, "Codimension two bifurcation in a delayed neural network with unidirectional coupling," *Nonlinear Analysis: Real World Applications*, vol. 14, no. 2, pp. 1191–1202, 2013.
[38] J. Forde and P. Nelson, "Applications of Sturm sequences to bifurcation analysis of delay differential equation models," *Journal of Mathematical Analysis and Applications*, vol. 300, no. 2, pp. 273–284, 2004.
[39] J. Yang, X. Shi, X. Song, and Z. Zhao, "Threshold dynamics of a stochastic SIQR epidemic model with imperfect quarantine," *Applied Mathematics Letters*, vol. 136, Article ID 108459, 2023.