Delayed Dynamics Analysis of SEI2RS Malware Propagation Models in Cyber - Physical Systems

D. Nithya[1], V Madhusudanan[2], B.S.N. Murthy[3], R. Geetha[4], Nguyen Xuan Mung[5], Nhu-Ngoc Dao[6], and Sungrae Cho[7]

[1]Department of Mathematics, S.A Engineering College, Chennai-600077, Tamilnadu, India

[2]Department of Mathematics, S.A Engineering College, Chennai-600077, Tamilnadu, India

[3]Department of Mathematics, Aditya College of Engineering and Technology, Surampalem, India

[4]Department of Computer Science and Engineering, S.A Engineering College, Tamil Nadu, India

[5]Faculty of Mechanical and Aerospace Engineering, Sejong University, Seoul 05006, South Korea

[6]Department of Computer Science and Engineering, Sejong University, Seoul 05006, South Korea

[7]School of Computer Science and Engineering, Chung-Ang University, Seoul 06974, South Korea

Emails: nithyadakshna@gmail.com (D. Nithya), mvms.maths@gmail.com (V. Madhusudanan), bsn3213@gmail.com (B.S.N. Murthy), geetha@saec.ac.in (R. Geetha), xuanmung@sejong.ac.kr (N.X. Mung), nndao@sejong.ac.kr (N.-N. Dao), srcho@cau.ac.kr (S. Cho)

Abstract:

Cyber-physical systems facilitate seamless interaction between the physical and digital elements for improved efficiency, automation, and real-time monitoring across domains. This study analyzes a novel virus-spreading model called the delayed SEI2RS model, which is specifically designed for cyber-physical systems. This model incorporates a saturated incidence rate and treatment. An emphasis of this research is to explore the impact of time delay on the transient immunity interval of restored nodes. By using the time delay associated with the transitory immunity interval of recovered nodes as the bifurcation parameter, we derive a comprehensive set of appropriate conditions to assess the local stability of the malware-existence equilibrium and determine Hopf bifurcation. The center manifold theorem and normal form theory are employed to investigate the path and stability of Hopf bifurcation. Numerical calculations were used to validate the results, providing empirical evidence for the proposed model and its implications.

Keywords: SEI2RS, virus spreading model, Cyber-physical system, delay analysis, Hopf bifurcation

1. Introduction

Malware propagation involves the dissemination of malicious software among interconnected nodes such as sensor networks, mobile phones, and cyber-physical systems (CPS), compromising their functionality and potentially causing disruptions or unauthorized data access [1,2]. Cybersecurity entails a proactive strategy aimed at protecting computers, mobile devices, servers, electronic systems, data and networks from potential malicious attacks. The frequency of data breaches has been on the rise, reflecting the rapid evolution of global

cyber threats. A survey conducted by Risk Based Security revealed a staggering exposure of 7.9 billion records in the first nine months of 2019 alone, marking a 112% increase compared to the same period in 2018. These systems represent a novel category of intelligent systems, seamlessly blending communication, computation, and control technologies to intricately integrate computing with physical resources [3-5]. The malware attacks on different cyber physical systems during the period 2019-2022 represented in the Fig.1.

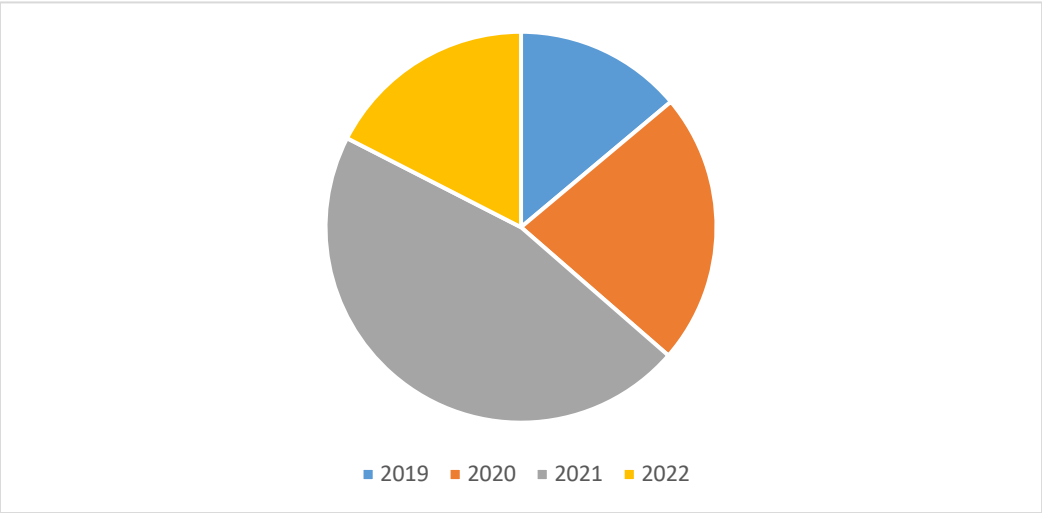


Fig 1 World-wide malware attacks (in millions) between 2019-2022

Various safety-critical sectors, such as energy, transportation, healthcare, and the military, have extensively adopted Cyber-Physical Systems, characterized by their openness and dynamic nature. These systems adhere to stringent standards concerning security, safety, and reliability. As CPSs evolve continuously, their multi functionality and complexity also grow, inevitably leading to the emergence of numerous security vulnerabilities that can be exploited in cyber-attacks. The sectors most susceptible to breaches include healthcare, retail, and the public sector, with malicious actors frequently responsible for these incidents. Certain industries, such as healthcare and finance, are particularly appealing to cybercriminals due to the sensitive financial and medical data they handle. However, any organization utilizing networks is potentially at risk of customer data theft, corporate espionage, or other cyber threats. Despite their prevalence in security-critical domains, CPSs are not immune to malicious code attacks and virus infections which can compromise their functionality and give rise to security concerns. The malware attacks on critical infrastructure in the year 2022 represented in the Fig.2.

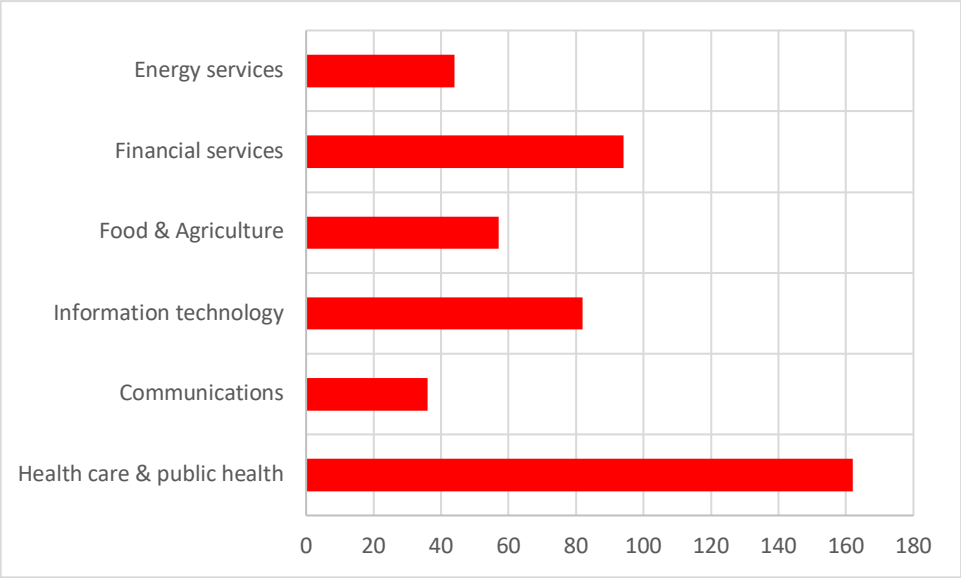


Fig 2. Malware attacks on critical infrastructure in the year 2022.

1.1. Motivations

This unauthorized malware dissemination severely impacts network efficiency, security, and overall performance. Cyber security safeguards electronic systems, networks, and data from harmful attacks to ensure their protection [3]. The number of data breaches is showing an annual escalation, marked by a significant yearly increase compared with the preceding periods. This exposes billions of records, as evidenced by a study conducted by risk-based security. A CPS integrates physical processes, computation, and networking, enabling computational algorithms and networks to observe and govern the physical components. The demand for CPSs has rapidly grown because of evolving physical world requirements and information technology (IT) advancements. The increasing physical environment demands, driven by rapid IT growth, have led to a substantial rise in the demand for CPSs. This rise in demand for CPSs is primarily attributed to the expansion of IT and diverse needs in various industries. CPSs represent a different category of intelligent systems that incorporate computation, communication, and control technologies, effectively combining physical and computing resources [4,5].

Cyber-attacks pose significant threats to Cyber-Physical Systems (CPSs), integral to overall system security. Such attacks can lead to catastrophic consequences for society, the economy, and critical infrastructure. Malware, a term denoting malicious software, stands out as a prevalent cyber threat. Crafted by hackers or cyber criminals, malware is designed to disrupt or harm the computers of legitimate users, often with financial or political motives [6-7]. It is commonly distributed through unsolicited email attachments or seemingly legitimate downloads.

1.2. Related work

The security of CPSs faces a substantial risk from malware, as highlighted in various research studies. Xu et al. [8] delve into malware attacks on the cyber-physical power system, proposing an analysis approach considering factors like malware incubation time and detection likelihood. Muthu Krishnan et al. [9] present an epidemic model for Susceptible-Infected-Traced-Susceptible in wireless sensor networks, exploring control strategies to impede malware spread. Shen et al. [10] focus on determining malware propagation thresholds in heterogeneous sensor networks. Mahboubi et al. [11] enhance the existing epidemic model for the Internet of Things, incorporating epidemic-specific states to construct a malware propagation model. These studies collectively underscore the urgency of addressing malware threats in CPSs through comprehensive analysis and strategic control measures.

Malware can interfere with a CPS's natural operation when it attacks it, infecting one or more nodes throughout its spread [12-15]. With the introduction of malware, CPS behaviour will change and exhibit nonlinear traits, allowing it to be categorized as a nonlinear dynamic system [16]. The exploration of malware propagation in cyber-physical systems has embraced the utilization of Lyapunov's approach to comprehend system behavior. Representing the stability of a system based on the Lyapunov model involves the identification of a positive definite function, referred to as a Lyapunov function, which decreases along the system's trajectory. In the examination of nonlinear systems, foundational theoretical knowledge and stability-related techniques are incorporated [17]. This analysis encompasses processes such as the linearization of differential equations and the examination of phase portraits [18]. Lyapunov stability systems are applied to evaluate the stability of these nonlinear systems. The current study integrates optimal stability assessment methods for nonlinear systems [19, 20] within the framework of malware propagation in cyber-physical systems. Ajayi et al. [21] discussed stability criteria for nonlinear systems and their associated properties. The research presented information on the Lyapunov stability analysis of nonlinear systems, offering an overview of ongoing research on the stability of nonlinear systems across various fields. Regarding the stability analysis of time-delay systems, Lyapunov functionals play a crucial role. Time delay systems have been investigated in extensive studies in the past decade, given the rapid growth in communications and network switching. It has been established that time delays are pervasive in technology-based control systems and can significantly impact the performance of closed-loop systems.

Extensive investigations have been conducted on the spread of malware in CPSs, its impact on cyber-physical power systems [8,12,13], wireless sensor networks [9,15,16,23,24 33], and heterogeneous sensor networks [10], aiming to analyze malware propagation, develop control techniques, and determine propagation thresholds to mitigate risks. Malware attacks disrupt CPSs, introducing nonlinear dynamic behavior, potentially leading to destructive phenomena such as chaos and bifurcation [25]. Bifurcation, for example,

can lead to voltage oscillation and other undesired effects in power networks, thereby affecting CPS stability [30,31]. Understanding malware transmission and dynamic behavior in CPSs is therefore crucial. On the other hand, temporal delays are a concern when examining the stability of mathematical models [15,18,26-29,32,33-37]. Fractional-order models [28] and stochastic models [11] have been employed to describe natural processes because the fractional derivative captures the entire period of biological activity. Neural networks based on delayed quaternion-valued fractional order have also been studied [30].

However, the multifunctionality and complexity of CPSs pose ongoing challenges, leading to potential security flaws and cyberattacks [22]. Industries such as healthcare, retail, and the public sector are prime targets for data breaches orchestrated by malicious criminals seeking financial or medical data. Any organization using networks can be a target for customer data theft, corporate espionage, or cyberattacks. CPSs, while widely used in security-critical domains, are vulnerable to malware attacks that compromise functionality and security.

1.3. Our contributions and paper organization

In this article, we studied the impact of time delay on malware propagation in CPSs. The main contributions of this article are as follows.

- A novel virus-spreading model for CPS, called the delayed Susceptible-Exposed-Low Infected-High Infected-Recovered-Susceptible (SEI2RS) model with a consideration of a saturated incidence rate and treatment has been introduced and analyzed.
- The impact of time delay on the transient immunity interval of restored nodes in the malware propagation model has been investigated. By using the time delay associated with the transitory immunity interval of recovered nodes as the bifurcation parameter, we derive a comprehensive set of appropriate conditions to assess the local stability of the malware-existence equilibrium and determine Hopf bifurcation. The center manifold theorem and normal form theory are employed to support the analysis.
- Numerical simulations demonstrate the efficiency of the proposed immunization strategy or control scheme in recovering infected nodes in both low and highly infected areas. Consequently, the threshold for Hopf bifurcation is reached, leading to the attainment of a stable state in cyber-physical systems. This, in turn, results in a reduction of harm and disturbance caused by malicious software to cyber-physical systems.

Table 1 gives the relative investigation of the proposed model with the current models in irresistible infection diseases.

The rest of this paper is structured as follows. Section 2 provides the delayed SEI2RS malware propagation in the cyber–physical model. Section 3 provides the basic reproduction number and calculates its equilibria. Section 4 investigates the model's stability along with an analysis of Hopf bifurcation. In Section 5, we determine the direction of the Hopf bifurcation and assess the stability of periodic solutions

within the CPS, employing the center manifold and normal form theories. Section 6 presents the simulation results used to test the hypothesis proposed in Section 2. Section 7 offers concluding remarks and outlines recommendations for the future.

Table 1: Comparison of proposed model with some existing models

Reference No	Type of Delay Model	Number of Compartments
Zhang et al. [14]	Saturated Incidence rate	5(Susceptible-Affected-Infected-Suspended-Recovered)
Madhusudanan, V. et al. [15]	Ratio dependent functional response	5(Susceptible-Exposed-Infected-Recovered-Vaccinated)
Nwoyoke et al. [16]	Holling Type-III incidence function	5(Susceptible-Exposed-Infected-Vaccinated-Recovered)
Yu and Wan [36]	General incidence rate	5(Susceptible-Exposed-Low Infected-High infected-Recovered)
Our proposed model	Ratio dependent functional response	5(Susceptible-Exposed-Low Infected-High infected-Recovered)

2. Delayed SEI2RS malware propagation in Cyber-Physical Systems

Numerous studies concerning cyber-physical network models often assume a bilinear infection rate. However, the topology of the underlying network system significantly affects the propagation of cyber-physical malware. To address this issue, we have incorporated the ratio-dependent functional response into the CPS, acknowledging its significant impact on malware propagation. Time delays also play a pivotal role in the spread of malware in cyber-physical networks. These delays can lead to stability loss and trigger Hopf bifurcations, resulting in periodic solutions. Interestingly, this cyclic behavioral phenomenon contrasts with the typical epidemiological viewpoint, where such cyclic patterns are considered undesirable.

To enhance comprehension and tackle these complexities, we developed a novel delay model for analyzing malware propagation in CPSs. Table 1 summarizes the parameters employed in our cyber-physical model, and Figure 1 presents a schematic representation of each group within the CPS. Through the integration of these elements, our research sheds light on the dynamics of malware propagation within the context of cyber-physical networks.

$$\left.\begin{aligned}
\frac{dS(t)}{dt} &= \nu - \frac{\eta_2 S(t) I_1(t)}{S + I_1 + c_1} - \frac{\eta_1 S(t) I_2(t)}{S + I_2 + c_2} + \varepsilon R(t) - \nu S(t), \\
\frac{dE(t)}{dt} &= \frac{\eta_2 S(t) I_1(t)}{S + I_1 + c_1} + \frac{\eta_1 S(t) I_2(t)}{S + I_2 + c_2} - \alpha E(t-\tau) - \beta E(t) - \nu E(t), \\
\frac{dI_1(t)}{dt} &= \alpha E(t-\tau) - \frac{\gamma I_1(t-\tau)}{I_1(t-\tau) + a} - \nu I_1(t), \\
\frac{dI_2(t)}{dt} &= \beta E(t) - \delta I_2(t) - \nu I_2(t), \\
\frac{dR(t)}{dt} &= \frac{\gamma I_1(t-\tau)}{I_1(t-\tau) + a} + \delta I_2(t) - \varepsilon R(t) - \nu R(t).
\end{aligned}\right\} \quad (1)$$

Table 1: Parameters description in SEI2RS malware propagation model in cyber–physical systems

Parameter	Description of the Parameters	Values
ν	New entry and exit nodes	0.01
η_2	Low infection rate of susceptible nodes	0.7
η_1	High infection rate of susceptible nodes	0.2
ε	Transition rate from recovered to susceptible nodes	0.08
α	Transition rate from exposed to low infected node	0.8
β	Transition rate from exposed to high infected node	0.1
γ	Recovery rate of low infected node	0.3
δ	Recovery rate of high infected rate	0.1
c_1	Half saturation constant for susceptible to low infected node	0.01
c_2	Half saturation constant for susceptible to high infected node	0.02
a	Half saturation constant for low infected nodes	0.8

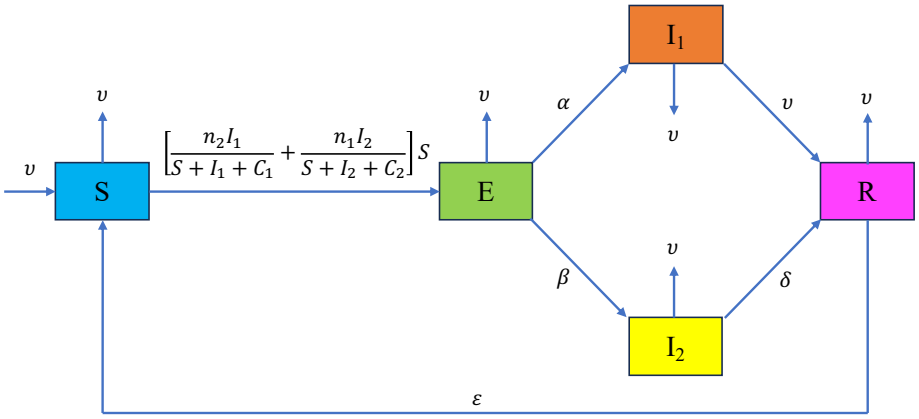


Fig. 3. A schematic representation of the propagation of malware in a cyber-physical system.

3. Malware propagation in Cyber-Physical Systems

The possible steady states of the system (1) are

(i) Malware-free equilibrium point in CPS $(p_0)=(1,0,0,0,0)$

(ii) Malware-present equilibrium point in CPS (p_1)

where $p_1=(S^*,E^*,I_1^*,I_2^*,R^*)$ and

$$S^*=\frac{(1+c_1)(1+c_2)(\alpha+\beta+\nu)(\delta+\nu)(\gamma+a\nu)}{a\eta_2\alpha(\delta+\nu)(1+c_2)+\eta_1\beta(\gamma+a\nu)(1+c_1)},$$

$$\mathrm{E}^{*}=\frac{\nu\left(a\eta_2\alpha\left(\delta+\nu\right)\left(1+c_2\right)+\eta_1\beta\left(\gamma+a\nu\right)\left(1+c_1\right)-\left(\alpha+\beta+\nu\right)\left(\delta+\nu\right)\left(\gamma+a\nu\right)\left(1+c_1\right)\left(1+c_2\right)\right)}{\left(a\eta_2\alpha\left(\delta+\nu\right)\left(1+c_2\right)+\eta_1\beta\left(\gamma+a\nu\right)\left(1+c_1\right)\right)\left(\alpha+\beta+\nu-\varepsilon\left(\xi+\psi\right)\right)},$$

$$\mathrm{I}_2^{*}=\frac{\beta E^{*}}{\delta+\gamma},\ R^{*}=\left[\frac{\gamma I_1^{*}}{I_1^{*}+a}+\frac{\delta\beta E^{*}}{\delta+\nu}\right]\frac{1}{\varepsilon+\nu}\ \text{and}\ \mathrm{I}_1^{*2}+a_1 I_1^{*}+a_2=0$$

$$\text{with}\ \xi=\frac{\alpha\gamma}{\left(\gamma+a\nu\right)\left(\varepsilon+\nu\right)};\psi=\frac{\beta\delta}{\left(\varepsilon+\nu\right)\left(\delta+\nu\right)};a_1=\frac{\gamma+a\nu-\alpha E^{*}}{\nu};a_2=-\frac{a\alpha E^{*}}{\nu}.$$

We use the next-generation matrix method [26] to obtain the basic reproduction number of the system. Accordingly, let $\Im=\left(E,I_1,I_2\right)$ and let F and V represent the Jacobian matrix of f and v at the malware-free equilibrium point $\left(p_o\right)$ respectively. We have

$$F=\begin{bmatrix}0 & \dfrac{\eta_2 S\left(S+c_1\right)}{\left(S+I_1+c_1\right)^2} & \dfrac{\eta_1 S\left(S+c_1\right)}{\left(S+I_1+c_1\right)^2}\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix};V=\begin{bmatrix}\alpha+\beta+\nu & 0 & 0\\ -\alpha & \dfrac{\gamma a}{\left(I_1+a\right)^2}+\nu & 0\\ -\beta & 0 & \delta+\nu\end{bmatrix}$$

$$FV^{-1}=\begin{bmatrix}\dfrac{\eta_2\alpha}{\left(1+c_1\right)\left(\alpha+\beta+\nu\right)\left(\frac{\gamma}{a}+\nu\right)}+\dfrac{\eta_1\beta}{\left(1+c_2\right)\left(\alpha+\beta+\nu\right)\left(\delta+\nu\right)} & \dfrac{\eta_2}{\left(1+c_1\right)\left(\frac{\gamma}{a}+\nu\right)} & \dfrac{\eta_1}{\left(1+c_1\right)\left(\delta+\nu\right)}\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}$$

Therefore, $R_0=\rho\left[\ FV^{-1}\ \right]=\dfrac{a\eta_2\alpha\left(\delta+\nu\right)\left(1+c_2\right)+\eta_1\beta\left(1+c_1\right)\left(\gamma+a\nu\right)}{\left(\alpha+\beta+\nu\right)\left(1+c_1\right)\left(1+c_2\right)\left(\gamma+a\nu\right)\left(\delta+\nu\right)}$

4. Stability Analysis of Malware Propagation in Cyber-Physical System

The linearized system (1) becomes

$$\left.\begin{aligned}
&\frac{dS(t)}{dt}=a_{11}S(t)+a_{13}I_1(t)+\mathrm{a}_{14}\,I_2(t)+\mathrm{a}_{15}\,R(t),\\
&\frac{dE(t)}{dt}=a_{21}S(t)+\mathrm{a}_{22}\,E(t)+\mathrm{a}_{23}\,I_1(t)+a_{24}I_2(t)+\mathrm{b}_{22}\,E(t-\tau),\\
&\frac{dI_1(t)}{dt}=b_{32}E(t-\tau)+\mathrm{a}_{33}\,I_1(t)+\mathrm{b}_{33}\,I_1(t-\tau),\\
&\frac{dI_2(t)}{dt}=\mathrm{a}_{42}\,E(t)+a_{44}I_2(t),\\
&\frac{dR(t)}{dt}=b_{53}I_1(t-\tau)+a_{54}I_2(t)+\mathrm{a}_{55}\,R(t).
\end{aligned}\right\}\qquad(2)$$

The Jacobian matrix for the linearized system (2) is

$$J=\begin{pmatrix} a_{11}-\lambda & 0 & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22}-\lambda-b_{22}e^{-\lambda\tau} & a_{23} & a_{24} & 0 \\ 0 & b_{32}e^{-\lambda\tau} & a_{33}-\lambda-b_{33}e^{-\lambda\tau} & 0 & 0 \\ 0 & a_{42} & 0 & a_{44}-\lambda & 0 \\ 0 & 0 & b_{53}e^{-\lambda\tau} & a_{54} & a_{55}-\lambda \end{pmatrix} \tag{3}$$

with

$$a_{11}=-\frac{\eta_2 I_1^*(I_1^*+c_1)}{\left(S^*+I_1^*+c_1\right)^2}-\frac{\eta_1 I_2^*(I_2^*+c_2)}{\left(S^*+I_2^*+c_2\right)^2}-\nu, a_{13}=-\frac{\eta_2 S^*\left(S^*+c_1\right)}{\left(s^*+I_1^*+c_1\right)^2}, a_{14}=-\frac{\eta_1 S^*\left(S^*+c_2\right)}{\left(S^*+I_2^*+c_2\right)^2}, a_{15}=\varepsilon,$$

$$a_{21}=\frac{\eta_2 I_1^*(I_1^*+c_1)}{\left(S^*+I_1^*+c_1\right)^2}, a_{22}=-\left(\beta+\nu\right), a_{23}=\frac{\eta_2 S^*\left(S^*+c_1\right)}{\left(S^*+I_1^*+c_1\right)^2}, a_{24}=-\frac{\eta_1 S^*\left(S^*+c_2\right)}{\left(S^*+I_2^*+c_2\right)^2}, a_{33}=-\upsilon, a_{42}=\beta,$$

$$a_{44}=-(\delta+\upsilon), a_{54}=\delta, a_{55}=-(\varepsilon+\upsilon), b_{22}=-\alpha, b_{32}=\alpha, b_{33}=\frac{-\gamma c_3}{(I_1^*+a)^2}, b_{53}=\frac{\gamma c_3}{(I_1^*+a)^2}.$$

The Jacobian matrix characteristic equation (3) is given by

$$\left(\lambda^5+T_{11}\lambda^4+T_{12}\lambda^3+T_{13}\lambda^2+T_{14}\lambda+T_{15}\right)+e^{-\lambda\tau}\left(U_{11}\lambda^4+U_{12}\lambda^3+U_{13}\lambda^2+U_{14}\lambda+U_{15}\right)+e^{-2\lambda\tau}\left(V_{11}\lambda^3+V_{12}\lambda^2+V_{13}\lambda+V_{14}\right)=0, \tag{4}$$

where

$$T_{11}=-\left(a_{11}+a_{22}+a_{33}+a_{44}+a_{55}\right);$$

$$T_{12}=a_{11}a_{22}+a_{11}a_{33}+a_{11}a_{44}+a_{11}a_{55}+a_{22}a_{33}+a_{22}a_{44}+a_{22}a_{55}+a_{33}a_{44}+a_{33}a_{55}+a_{44}a_{55};$$

$$T_{13}=-(a_{11}a_{22}a_{33}+a_{11}a_{22}a_{44}+a_{11}a_{11}a_{55}+a_{11}a_{33}a_{44}+a_{11}a_{44}a_{55}+a_{22}a_{33}a_{44}+a_{11}a_{33}a_{55}+a_{22}a_{33}a_{55}+a_{22}a_{44}a_{55}+a_{33}a_{44}a_{55}+a_{14}a_{21}a_{42});$$

$$T_{14}=a_{11}a_{22}a_{33}a_{44}+a_{11}a_{22}a_{33}a_{55}+a_{14}a_{24}a_{33}a_{42}+a_{11}a_{22}a_{44}a_{55}+a_{11}a_{33}a_{44}a_{55}+a_{22}a_{33}a_{44}a_{55}+a_{14}a_{21}a_{42}a_{55};$$

$$T_{15}=a_{14}a_{21}a_{33}a_{42}a_{55}-a_{11}a_{22}a_{33}a_{44}a_{55};$$

$$U_{11}=-\left(b_{22}+b_{33}\right);$$

$$U_{12}=a_{11}b_{33}+a_{11}b_{22}+a_{22}b_{33}+a_{44}b_{33}+a_{55}b_{33}+a_{33}b_{22}+a_{44}b_{22}+a_{55}b_{22};$$

$$U_{13}=-(a_{11}a_{22}b_{33}+a_{11}a_{44}b_{33}+a_{11}a_{55}b_{33}+a_{11}a_{33}b_{22}+a_{22}a_{44}b_{33}+a_{22}a_{55}b_{33}+a_{44}a_{55}b_{33}+a_{33}a_{44}b_{22}+a_{33}a_{55}b_{22}+a_{44}a_{55}b_{2}-a_{13}a_{21}b_{32});$$

$$U_{14}=\begin{pmatrix} a_{11}a_{22}a_{44}b_{33}+a_{11}a_{22}b_{33}a_{55}+a_{11}a_{22}b_{33}a_{55}+a_{11}a_{33}a_{44}b_{22}+a_{11}a_{33}a_{55}b_{22}+a_{22}a_{44}a_{55}b_{33}+a_{33}a_{44}b_{22}a_{55}- \\ a_{13}a_{21}a_{44}b_{32}-b_{32}a_{13}a_{21}a_{55}-a_{14}a_{21}a_{42}b_{33} \end{pmatrix};$$

$$U_{15}=a_{11}a_{22}a_{44}a_{55}b_{33}+a_{11}a_{33}a_{44}a_{55}b_{22}-a_{13}a_{21}a_{44}a_{55}b_{32}+a_{14}a_{21}a_{42}a_{55}b_{33};$$

$$V_{11}=-b_{22}b_{33}; V_{12}=a_{11}b_{22}b_{33}+a_{44}b_{22}b_{33}+a_{55}b_{22}b_{33};$$

$$V_{13}=-a_{11}a_{44}b_{22}b_{33}-_{11}a_{55}b_{22}b_{33}-a_{44}a_{55}b_{22}b_{33}+a_{15}a_{21}b_{32}b_{53}; V_{14}=a_{11}a_{44}a_{55}b_{22}b_{33}-a_{15}a_{21}a_{44}b_{32}b_{53}.$$

Multiply $e^{\lambda\tau}$ on both sides of equation (4), then we have

$$\left(\lambda^5+T_{11}\lambda^4+T_{12}\lambda^3+T_{13}\lambda^2+T_{14}\lambda+T_{15}\right)e^{\lambda\tau}+\left(U_{11}\lambda^4+U_{12}\lambda^3+U_{13}\lambda^2+U_{14}\lambda+U_{15}\right)+e^{-\lambda\tau}\left(V_{11}\lambda^3+V_{12}\lambda^2+V_{13}\lambda+V_{14}\right)=0 \tag{5}$$

4.1 Stability analysis in the absence of delay

In the absence of delay, put $\tau = 0$ in equation (4), the characteristic equation (5) becomes

$$\lambda^5 + (T_{11} + U_{11} + \mathrm{V}_{11})\lambda^4 + (\mathrm{T}_{12} + U_{12} + \mathrm{V}_{12})\lambda^3 + (T_{13} + U_{13} + \mathrm{V}_{13})\lambda^2 + (T_{14} + U_{14} + \mathrm{V}_{14})\lambda + (T_{15} + U_{15}) = 0. \quad (6)$$

From equation (6),

$$T_{11} + U_{11} + V_{11} = (a_{11} + a_{22} + a_{33} + a_{44} + a_{55} + b_{22} + b_{33} + b_{22} + b_{33} + b_{22}b_{33}) > 0$$

The Routh-Hurwitz criteria provide a set of sufficient conditions that ensure all the roots of equation (5) have a negative real part. These conditions are expressed in a specific form to ascertain the stability of the system.

$$D_2 = \begin{vmatrix} T_{11} + U_{11} + V_{11} & 1 \\ T_{13} + U_{13} + V_{13} & T_{12} + U_{12} + V_{12} \end{vmatrix} > 0 \quad (7)$$

$$D_3 = \begin{vmatrix} T_{11} + U_{11} + V_{11} & 1 & 0 \\ T_{13} + U_{13} + V_{13} & T_{12} + U_{12} + V_{12} & T_{11} + U_{11} + V_{11} \\ 0 & T_{14} + U_{14} + V_{14} & T_{13} + U_{13} + V_{13} \end{vmatrix} > 0 \quad (8)$$

$$D_4 = \begin{vmatrix} T_{11} + U_{11} + V_{11} & 1 & 0 & 0 \\ T_{13} + U_{13} + V_{13} & T_{12} + U_{12} + V_{12} & T_{11} + U_{11} + V_{11} & 1 \\ T_{15} + U_{15} & T_{14} + U_{14} + V_{14} & T_{13} + U_{13} + V_{13} & T_{12} + U_{12} + V_{12} \\ 0 & 0 & T_{15} + U_{15} & T_{14} + U_{14} + V_{14} \end{vmatrix} > 0 \quad (9)$$

$$D_5 = \begin{vmatrix} T_{11} + U_{11} + V_{11} & 1 & 0 & 0 & 0 \\ T_{13} + U_{13} + V_{13} & T_{12} + U_{12} + V_{12} & T_{11} + U_{11} + V_{11} & 1 & 0 \\ T_{15} + U_{15} & T_{14} + U_{14} + V_{14} & T_{13} + U_{13} + V_{13} & T_2 + U_2 + V_2 & T_{11} + U_{11} + V_{11} \\ 0 & 0 & T_{15} + U_{15} & T_4 + U_4 + V_4 & T_{13} + U_{13} + V_{13} \\ 0 & 0 & 0 & 0 & T_{15} + U_{15} \end{vmatrix} > 0 \quad (10)$$

If conditions (7)-(10) are satisfied, the system is considered locally asymptotically stable in the absence of delay. These conditions play a crucial role in determining the stability of the system, ensuring that it converges towards equilibrium in its behavior.

4.2 Stability analysis in the presence of delay

For $\tau > 0$, put $\lambda = i\eta (\eta > 0)$ be the root of equation (6). Then

$$\left[\left(\eta^4 T_{11} - \eta^2 T_{13} + T_{15}\right) + \left(V_{14} - V_{12}\eta^2\right)\right]\cos\eta\tau + \left[\left(\eta V_{13} - \eta^3 V_{11}\right) - \left(\eta^5 - \eta^3 T_{12} + \eta T_{14}\right)\right]\sin\eta\tau = \eta^2 U_{13} - \eta^4 U_{11} - U_{15} \quad (11)$$

$$\left[\left(\eta^5 - \eta^3 T_{12} + \eta T_{14}\right) + \left(\eta V_{13} - \eta^3 V_{11}\right)\right]\cos\eta\tau + \left[\left(\eta^4 T_{11} - \eta^2 T_{13} + T_{15}\right) - \left(V_{14} - V_{12}\eta^2\right)\right]\sin\eta\tau = \eta^3 U_{12} - \eta U_{14} \quad (12)$$

Thus,

$$\cos\eta\tau = \frac{P_0\eta^8 + P_1\eta^6 + P_2\eta^4 + P_3\eta^2 + P_4}{\eta^{10} + Q_0\eta^8 + Q_1\eta^6 + Q_2\eta^4 + Q_3\eta^2 + Q_4}, \quad (13)$$

$$\sin\eta\tau = \frac{R_0\eta^8 + R_1\eta^6 + R_2\eta^4 + R_3\eta^2 + R_4}{\eta^{10} + Q_0\eta^8 + Q_1\eta^6 + Q_2\eta^4 + Q_3\eta^2 + Q_4}, \tag{14}$$

where

$P_0 = U_{12} - U_{11}U_{11}; P_1 = U_{11}T_{13} - U_{11}V_{12} + U_{13}T_{11} + V_{11}U_{12} - T_{12}U_{12};$

$P_2 = T_{12}U_{14} + U_{12}T_{14} - U_{12}V_{13} - V_{11}U_{14} + V_{14}U_{11} - U_{11}T_{15} + V_{12}U_{13} - T_{13}U_{13} - T_{11}U_{15};$

$P_3 = U_{13}T_{15} - w_{12}U_{15} + T_{13}U_{15} - T_{14}U_{14} + V_{13}U_{14}; P_4 = V_{14}U_{15} - T_{15}U_{15}; R_0 = \eta^9;$

$R_1 = T_{11}U_{12} - U_{13} - T_{12}U_{11} - V_{11}U_{11}; R_2 = U_{15} + T_{12}U_{13} + T_{14}U_{11} + V_{13}U_{11} + V_{11}U_{13} - T_{13}U_{12} - U_{12}V_{12};$

$R_3 = T_{13}U_{14} + U_{12}T_{15} + V_{14}U_{12} + V_{12}U_{14} - T_{12}U_{15} - T_{14}U_{13} - V_{13}U_{13} - V_{11}U_{15};$

$R_4 = T_{14}U_{15} + w_{13}U_{15} - T_{15}U_{14} - w_{14}U_{14}; Q_0 = T_{11}^2 - 2T_{12}; Q_1 = T_{12}^2 + 2T_{14} - V_{11}^2 - 2T_{11}T_{13};$

$Q_2 = T_{13}^2 + 2T_{11}T_{15} - V_{12}^2 - 2T_{12}T_{14} + 2V_{11}V_{13}; Q_3 = T_{14} - 2T_{13}T_{15} + 2V_{12}V_{14} + T_{14} - V_{13}^2; Q_4 = T_{15}^2 - V_{14}^2.$

Therefore, we obtain

$$\eta^{20} + S_1\eta^{18} + S_2\eta^{16} + S_3\eta^{14} + S_4\eta^{12} + S_5\eta^{10} + S_6\eta^8 + S_7\eta^6 + S_8\eta^4 + S_9\eta^2 + S_{10} = 0 \tag{15}$$

Let $\eta^2 = \vartheta$, then equation (15) becomes

$$\vartheta^{10} + S_1\vartheta^9 + S_2\vartheta^8 + S_3\vartheta^7 + S_4\vartheta^6 + S_5\vartheta^5 + S_6\vartheta^4 + S_7\vartheta^3 + S_8\vartheta^4 + S_9\vartheta + S_{10} = 0 \tag{16}$$

where

$S_1 = 2L_0 - R_0^2\ ; S_2 = 2Q_0Q_1 + 2Q_1 - P_0^2 - 2R_0R_1; S_3 = 2Q_2 - 2P_0P_1 - 2R_0R_2;$

$S_4 = Q_1^2 + 2Q_0Q_2 + 2Q_3 - P_1^2 - 2P_0P_2 - 2R_0R_3;$

$S_5 = 2Q_4 + 2Q_0Q_3 + 2Q_1Q_2 - 2P_0P_2 - 2P_1P_3 - R_2^2 - 2R_0R_4 - 2R_1R_3;$

$S_6 = Q_2^2 + 2Q_0Q_4 + 2Q_1Q_3 - P_2 - 2P_0P_4 - 2P_1P_3 - 2R_1R_4 - 2R_2R_3;$

$S_7 = 2Q_2Q_3 + 2Q_1Q_4 - N_3^2 - 2P_1P_4 - 2P_2P_3 - 2R_2R_4; S_8 = 2Q_2Q_4 + Q_3^2 - P_3^2 - 2P_2P_4 - 2R_3R_4.$

$S_9 = 2Q_3Q_4 - 2P_3P_4 - R_4^2;\ S_{10} = Q_4^2 - P_4^2;$

Now, we have equation (13), which has at least one positive root η_0. Thus, from equation (13), we have

$$\tau_0 = \frac{1}{\eta_0}\cos^{-1}\left(\frac{L_0\eta^8 + L_1\eta^6 + L_2\eta^4 + L_3\eta^2 + L_4}{\eta^{10} + M_0\eta^8 + M_1\eta^6 + M_2\eta^4 + M_3\eta^2 + M_4}\right) \tag{17}$$

Differentiating equation (5) with respect to τ, we obtain

$$\left(5\lambda^4 + 4\lambda^3T_{11} + 3\lambda^2T_{12} + 2\lambda T_{13} + T_{14}\right)e^{\lambda\tau} + \left(3\lambda^2V_{11} + 2\lambda V_{12} + V_{13}\right)e^{-\lambda\tau} +$$

$$\left[\frac{d\lambda}{d\tau}\right]^{-1} = \frac{\left(4\lambda^3U_{11} + 3\lambda^2U_{12} + 2\lambda U_{13} + U_{14}\right)}{\lambda\left(e^{-\lambda\tau}\left(\lambda^3V_{11} + \lambda^2V_{12} + \lambda V_{13} + V_{14}\right) - e^{\lambda\tau}\left(\lambda^5 + \lambda^4T_{11} + \lambda^3T_{12} + \lambda^2T_{14} + T_{15}\right)\right)} - \frac{\tau}{\lambda}$$

Thus, we get

$$\mathrm{Re}\left[\frac{d\lambda}{d\tau}\right]^{-1}_{\tau=\tau_0} = \frac{A_r B_r + A_q B_q}{B_r^2 + B_q^2} \tag{18}$$

where

$$A_r = \left(5\eta_0^4 - 3\eta_0^2 T_{12} + T_{14} + V_{13} - 3\eta_0^2 V_{11}\right)\cos\eta_0\tau + \left(2\eta_0 V_{12} + 4\eta_0^3 T_{11} - 2\eta_0 T_{11}\right)\sin\eta_0\tau + U_{14} - 3\eta_0^2 U_{12};$$

$$B_r = \left(\eta_0 T_{14} - \eta_0^3 T_{12} + \eta_0^5 + \eta_0^3 V_{11} - \eta_0 V_{13}\right)\cos\eta_0\tau + \left(V_{14} - \eta_0^2 V_{12} + T_{15} - \eta_0^2 T_{13} + \eta_0^4 T_{11}\right)\sin\eta_0\tau;$$

$$A_q = \left(2\eta_0 V_{12} + 2\eta_0 T_{11} - 4\eta_0^3 T_{11}\right)\cos\eta_0\tau + \left(5\eta_0^4 - 3\eta_0^2 T_{12} + T_{14} + V_{13} - 3\eta_0^2 w_{11}\right)\sin\eta_0\tau + 2\eta_0 V_{13} - 4\eta_0^3 V_{11};$$

$$B_q = \left(V_{14} - \eta_0^2 V_{12} - T_{15} + \eta_0^2 T_{13} - \eta_0^4 T_{11}\right)\cos\eta_0\tau + \left(\eta_0 T_{14} - \eta_0^3 T_{12} + \eta_0^5 - \eta_0^3 V_{11} + \eta_0 V_{13}\right)\cos\eta_0\tau;$$

The transversality condition holds if $C_2 : A_r B_r + A_q B_q \neq 0$. We have the following result.

Theorem 1: Let an endemic equilibrium point $\left(S^*, E^*, I_1^*, I_2^*, R^*\right)$of system (1) exist, and let conditions $\left(C_1\right)$ and $\left(C_2\right)$ be satisfied. Then it is locally asymptotically stable at $\tau \in \left[0, \tau_0\right)$and unstable for $\tau > \tau_0$. Furthermore, system (1) undergoes Hopf bifurcation at $\left(S^*, E^*, I_1^*, I_2^*, R^*\right)$ when $\tau = \tau_0$ and a family of periodic solutions bifurcates from $\left(S^*, E^*, I_1^*, I_2^*, R^*\right)$ near $\tau = \tau_0$.

Assuming the existence of an endemic equilibrium point $\left(S^*, E^*, I_1^*, I_2^*, R^*\right)$ of system (1) and fulfillment of conditions $\left(C_1\right)$ and $\left(C_2\right)$, the equilibrium point is deemed locally asymptotically stable at $\tau \in \left[0, \tau_0\right)$ and unstable for $\tau > \tau_0$. Moreover, the system (1) experiences a Hopf bifurcation at $\left(S^*, E^*, I_1^*, I_2^*, R^*\right)$ when $\tau = \tau_0$, giving rise to a family of periodic solutions that bifurcate from $\left(S^*, E^*, I_1^*, I_2^*, R^*\right)$, the vicinity of $\tau = \tau_0$. These findings shed light on the dynamic behavior of system (1) and its susceptibility to undergo significant changes under specific conditions and parameter values.

5. Direction of Hopf bifurcation and its stability

Theorem 2:

(i) If $\wp_1 > 0\left(\wp_1 < 0\right)$then the Hopf-bifurcation is supercritical (subcritical),

(ii) (ii) If $\wp_2 < 0\left(\wp_2 > 0\right)$then the bifurcation periodic solutions are stable(unstable),

(iii) (iii) If $\wp_3 > 0\left(\wp_3 < 0\right)$ then the bifurcating periodic solutions increase(decrease).

Proof:

Let $\tau = \tau_0 + \theta$, $v_1 = S(\tau t)$, $v_2 = E(\tau t)$, $v_3 = I_1(\tau t)$, $v_4 = I_2(\tau t)$, $v_5 = R(\tau t)$, $\theta \in R$ $\mathrm{M}_\theta : \mathbb{C} \to \Re^4$ and $\mathrm{H} : \Re \times \mathbb{C} \to \Re^5$, so that the system (1) is transformed into a functional differential equation in $\mathbb{C} = \mathbb{C}\left([-1,0], \Re^5\right)$ as

$$v^1(t) = \mathrm{M}_\theta(v_t) + \mathrm{H}(\theta, v_t) \tag{19}$$

where

$$\mathrm{M}_\theta(\xi) = (\tau_0 + \theta)\left(k_1\xi(0) + k_2\xi(-1)\right) \tag{20}$$

With $k_1 = \begin{bmatrix} a_{11} & 0 & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & 0 \\ 0 & 0 & a_{33} & 0 & 0 \\ 0 & a_{42} & 0 & a_{44} & 0 \\ 0 & 0 & 0 & a_{54} & a_{55} \end{bmatrix}$; $k_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & b_{22} & 0 & 0 & 0 \\ 0 & b_{32} & b_{33} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & b_{53} & 0 & 0 \end{bmatrix}$; and

$$\mathrm{H}(\theta, \xi) = (\tau_0 + \theta)\begin{bmatrix} -\eta_2\xi_1(0)\xi_3(0) - \eta_1\xi_1(0)\xi_4(0) \\ \eta_2\xi_1(0)\xi_3(0) + \eta_1\xi_1(0)\xi_4(0) \\ 0 \\ 0 \\ 0 \end{bmatrix}. \tag{21}$$

Based on the Riesz representation theorem, it can be inferred that there exists a function $\mathrm{N}(\theta, \kappa)$ that satisfies

$$\mathrm{M}_\theta(\xi) = \int_{-1}^{0} \xi(\theta) d\mathrm{N}(\theta, \kappa), \text{ for } \xi \in \mathbb{C} \tag{22}$$

From equation (20), we set

$$\mathrm{N}(\theta, \kappa) = (\tau_0 + \theta)\left(k_1\Omega(\theta) + k_2\Omega(\theta + 1)\right) \tag{23}$$

where $\Omega(\theta)$ is the Dirac-Delta function.

Define

$$\mathrm{P}(\kappa)\xi = \begin{cases} \dfrac{d\xi(\theta)}{d\theta}, & -1 \le \theta < 0 \\ \displaystyle\int_{-1}^{0} \xi(\theta) d\mathrm{N}(\theta, \kappa), & \theta = 0 \end{cases} \tag{24}$$

and

$$[\![\ (\kappa)\xi = \begin{cases} 0, & -1 \le \theta < 0 \\ \mathrm{H}(\theta, \kappa), & \theta = 0 \end{cases} \tag{25}$$

Thus, system (19) yields

$$v^1(t) = \mathrm{P}(\kappa)v_t + [\![\ (\kappa)v_t \tag{26}$$

For $\sigma \in c^1\left([0,1], \left(R^5\right)\right)$,

$$\mathrm{P}^{*}(\sigma)=\begin{cases}-\dfrac{d\sigma(s)}{ds}, & 0<s\le 1\\ \int_{-1}^{0}\sigma(-s)d\mathrm{N}^{T}(\mathrm{s},0), & \mathrm{s}=0\end{cases} \tag{27}$$

and $\langle\sigma,\xi\rangle=\bar{\sigma}(0).\xi(0)-\int_{\theta=-1}^{0}\int_{\psi=0}^{\theta}\bar{\sigma}(\psi-\theta)d\mathrm{N}(\theta)\xi(\psi)d\psi$. (28)

Let $\sigma(\theta)=(1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)^{T}e^{i\tau_0\omega_0\theta}$ be the eigen vector of $\mathrm{P}(0)$ related to $i\tau_0\omega_0$ and $\sigma^{*}(\theta)=\mathbb{Z}(1,\sigma_2^{*},\sigma_3^{*},\sigma_4^{*},\sigma_5^{*})e^{i\tau_0\omega_0\theta}$ be the eigen vector of $\mathrm{P}^{*}(0)$ related to $-i\tau_0\omega_0$. According to equation (23) and equation (28), through simple calculation, one has

$$\sigma_2=\frac{a_{21}\left(i\omega_0-a_{33}-b_{33}e^{-i\omega_0\tau_0}\right)}{\left(i\omega_0-a_{22}-b_{22}e^{-i\omega_0\tau_0}\right)\left(i\omega_0-a_{33}-b_{33}e^{-i\omega_0\tau_0}\right)-a_{23}b_{32}e^{-i\omega_0\tau_0}};$$

$$\sigma_3=\frac{b_{32}e^{-i\omega_0\tau_0}}{i\omega_0-a_{33}-b_{33}e^{-i\omega_0\tau_0}}\sigma_2;\sigma_4=\frac{a_{42}\sigma_2}{i\omega_0-a_{44}};\sigma_5=\frac{b_{53}e^{-i\omega_0\tau_0}+a_{54}\sigma_4}{i\omega_0-a_{55}};$$

$$\sigma_2^{*}=-\frac{(a_{11}+i\omega_0)}{a_{21}};\sigma_3^{*}=-\frac{\left(a_{13}+a_{23}\sigma_2^{*}+b_{53}e^{i\omega_0\tau_0}\sigma_5^{*}\right)}{a_{33}+b_{33}e^{i\omega_0\tau_0}+i\omega_0};\sigma_3^{*}=-\frac{\left(a_{14}+a_{24}\sigma_2^{*}+b_{54}\sigma_5^{*}\right)}{a_{11}+i\omega_0};\sigma_5^{*}=-\frac{a_{15}}{a_{15}+i\omega_0};$$

According to equation (28), one has

$$\bar{\chi}=\left(1+\sigma_2\bar{\sigma}_2^{*}+\sigma_3\bar{\sigma}_3^{*}+\sigma_4\bar{\sigma}_4^{*}+\sigma_5\bar{\sigma}_5^{*}+\alpha\sigma_2\left(1-\bar{\sigma}_2^{*}\right)e^{-i\omega_0\tau_0}+\alpha\sigma_3\left(1-\bar{\sigma}_3^{*}\right)e^{-i\omega_0\tau_0}\right)^{-1} \tag{29}$$

According to the computation process in [27, 28], we obtain the values of w_{20},w_{11},w_{02}, and w_{21}.

Therefore

$$w_{20}=2\omega_0\bar{\chi}\left(\eta_2\sigma_3+\eta_1\sigma_4\right);w_{11}=\omega_0\bar{\chi}\left(\bar{\sigma}_2^{*}-1\right)\left(\eta_2\left(\sigma_3+\bar{\sigma}_3\right)+\eta_1\left(\sigma_4+\bar{\sigma}_4\right)\right);$$

$$w_{02}=2\omega_0\bar{\chi}\left(\bar{\sigma}_2^{*}-1\right)\left(\eta_2\bar{\sigma}_3+\eta_1\bar{\sigma}_4\right);$$

$$w_{21}=2\omega_0\bar{\chi}\left(\bar{\sigma}_2^{*}-1\right)\begin{pmatrix}\eta_2\left(\Upsilon_{11}^{(1)}(0)\sigma_3+\frac{1}{2}\Upsilon_{20}^{(1)}(0)\bar{\sigma}_3+\Upsilon_{11}^{(3)}(0)+\frac{1}{2}w_{20}^{(3)}(0)\right)+\\ \eta_1\left(\Upsilon_{11}^{(1)}(0)\sigma_4+\frac{1}{2}\Upsilon_{20}^{(1)}(0)\bar{\sigma}_4+\Upsilon_{11}^{(4)}(0)+\frac{1}{2}\Upsilon_{20}^{(4)}(0)\right)\end{pmatrix}.$$

where

$$\Upsilon_{20}(\theta)=-\frac{iw_{20}}{\tau_0\omega_0}\sigma(0)+i\frac{w_{02}}{3\tau_0\omega_0}\bar{\sigma}(0)+\Phi_1e^{2i\tau_0\omega_0};$$

$$\delta_{11}(\psi)=-\frac{iw_{11}}{\tau_0\omega_0}\sigma(0)+\frac{i\bar{w}_{11}}{\tau_0\omega_0}\sigma(0)+\Phi_2;$$

and $\Phi_1=\left(\Phi_1^{(1)},\Phi_1^{(2)},\Phi_1^{(3)},\Phi_1^{(4)},\Phi_1^{(5)}\right)\in R^5$, $\Phi_2=\left(\Phi_2^{(1)},\Phi_2^{(2)},\Phi_2^{(3)},\Phi_2^{(4)},\Phi_2^{(5)}\right)^{T}\in R^5$ are described in the following form

$$\Phi_1^{(1)}=\frac{2}{\Upsilon_{20}}\begin{bmatrix} -\eta_2\sigma_3-\eta_1\sigma_4 & 0 & -a_{13} & -a_{14} & -a_{15} \\ \eta_2\sigma_3+\eta_1\sigma_4 & 2i\omega_0-a_{22}-b_{22}e^{-2i\tau_0\omega_0} & -a_{23} & -a_{24} & 0 \\ 0 & 0 & 2i\omega_0-a_{33}-b_{33}e^{-2i\tau_0\omega_0} & 0 & 0 \\ 0 & -a_{42} & 0 & 2ij_0-a_{44}-b_{33}e^{-2ij_0\xi_0} & 0 \\ 0 & -a_{52} & 0 & -a_{54} & 2ij_0-a_{55} \end{bmatrix};$$

$$\Phi_1^{(2)}=\frac{2}{\Upsilon_{20}}\begin{bmatrix} 2i\omega_0-a_{11} & -\eta_2\sigma_3-\eta_1\sigma_4 & -a_{13} & -a_{14} & -a_{15} \\ -a_{21} & \eta_2\sigma_3+\eta_1\sigma_4 & -a_{23} & 0 & 0 \\ 0 & 0 & 2i\omega_0-a_{33}-b_{33}e^{-2i\tau_0\omega_0} & 0 & 0 \\ 0 & 0 & 0 & 2i\omega_0-a_{44} & 0 \\ 0 & 0 & -b_{33}e^{-2i\tau_0\omega_0} & -a_{54} & 2i\omega_0-a_{55} \end{bmatrix};$$

$$\Phi_1^{(3)}=\frac{2}{\Upsilon_{20}}\begin{bmatrix} 2i\omega_0-a_{11} & 0 & -\eta_2\sigma_3-\eta_1\sigma_4 & -a_{14} & -a_{15} \\ -a_{21} & 2i\omega_0-a_{22}-b_{22}e^{-2ij_0\xi_0} & \eta_2\sigma_3+\eta_1\sigma_4 & -a_{24} & 0 \\ 0 & -b_{32}e^{-2i\tau_0\omega_0} & 0 & 0 & -a_{35} \\ 0 & -a_{42} & 0 & 2i\omega_0-a_{44} & 0 \\ 0 & 0 & 0 & -a_{54} & 2i\omega_0-a_{55} \end{bmatrix};$$

$$\Phi_1^{(4)}=\frac{2}{\Upsilon_{20}}\begin{bmatrix} 2i\omega_0-a_{11} & 0 & -a_{13} & -\eta_2\sigma_3-\eta_1\sigma_4 & -a_{15} \\ -a_{21} & 2i\omega_0-a_{22}-b_{22}e^{-2ij_0\xi_0} & -a_{23} & \eta_2\sigma_3+\eta_1\sigma_4 & 0 \\ 0 & -b_{32}e^{-2i\tau_0\omega_0} & 2ij_0-a_{33}-b_{33}e^{-2i\tau_0\xi_0} & 0 & 0 \\ 0 & -a_{42} & -a_{43} & 0 & 0 \\ 0 & 0 & 0 & 0 & 2i\omega_0-a_{55} \end{bmatrix};$$

$$\Phi_1^{(5)}=\frac{2}{\Upsilon_{20}}\begin{bmatrix} 2i\omega_0-a_{11} & 0 & -a_{13} & -a_{14} & -\eta_2\sigma_3-\eta_1\sigma_4 \\ -a_{21} & 2i\omega_0-a_{22}-b_{22}e^{-2i\tau_0\omega_0} & -a_{23} & -a_{24} & \eta_2\sigma_3+\eta_1\sigma_4 \\ 0 & -b_{32}e^{-2i\tau_0\omega_0} & 2i\omega_0-a_{33}-b_{33}e^{-2i\tau_0\omega_0} & -a_{34} & 0 \\ 0 & -a_{42} & 0 & 2i\omega_0-a_{44} & 0 \\ 0 & 0 & b_{53}e^{-2i\tau_0\omega_0} & -a_{54} & 0 \end{bmatrix};$$

$$\Phi_2^{(1)}=-\frac{2}{\Upsilon_{11}}\begin{bmatrix} -\eta_2\left(\sigma_3+\bar{\sigma}_3\right)-\eta_1\left(\sigma_4+\bar{\sigma}_4\right) & 0 & a_{13} & a_{14} & a_{15} \\ \eta_2\left(\sigma_3+\bar{\sigma}_3\right)+\eta_1\left(\sigma_4+\bar{\sigma}_4\right) & a_{22}+b_{22} & a_{23} & a_{24} & 0 \\ 0 & 0 & a_{33}+b_{33} & 0 & a_{35} \\ 0 & a_{42} & 0 & a_{44} & 0 \\ 0 & 0 & b_{53} & a_{54} & a_{55} \end{bmatrix};$$

$$\Phi_2^{(2)}=-\frac{2}{\Upsilon_{11}}\begin{bmatrix} a_{11} & -\eta_2\left(\sigma_3+\bar{\sigma}_3\right)-\eta_1\left(\sigma_4+\bar{\sigma}_4\right) & a_{13} & a_{14} & a_{15} \\ a_{21} & \eta_2\left(\sigma_3+\bar{\sigma}_3\right)+\eta_1\left(\sigma_4+\bar{\sigma}_4\right) & a_{23} & a_{24} & 0 \\ 0 & b_{32} & & & a_{33}+b_{33} \\ 0 & a_{42} & 0 & a_{44} & 0 \\ 0 & 0 & b_{53} & a_{54} & a_{55} \end{bmatrix};$$

$$\Phi_2^{(3)}=-\frac{2}{\Upsilon_{11}}\begin{bmatrix} a_{11} & 0 & -\eta_2\left(\sigma_3+\bar{\sigma}_3\right)-\eta_1\left(\sigma_4+\bar{\sigma}_4\right) & a_{14} & a_{15} \\ a_{21} & a_{22}+b_{22} & \eta_2\left(\sigma_3+\bar{\sigma}_3\right)+\eta_1\left(\sigma_4+\bar{\sigma}_4\right) & a_{24} & 0 \\ 0 & b_{32} & 0 & 0 & 0 \\ 0 & a_{42} & 0 & a_{44} & 0 \\ 0 & 0 & 0 & a_{54} & a_{35} \end{bmatrix};$$

$$\Phi_2^{(4)}=-\frac{2}{\Upsilon_{11}}\begin{bmatrix} a_{11} & 0 & 0 & -\eta_2\left(\sigma_3+\bar{\sigma}_3\right)-\eta_1\left(\sigma_4+\bar{\sigma}_4\right) & a_{15} \\ a_{21} & a_{22}+b_{22} & a_{23} & \eta_2\left(\sigma_3+\bar{\sigma}_3\right)+\eta_1\left(\sigma_4+\bar{\sigma}_4\right) & 0 \\ 0 & b_{32} & a_{33}+b_{33} & 0 & 0 \\ 0 & a_{42} & 0 & 0 & 0 \\ 0 & 0 & b_{53} & 0 & a_{55} \end{bmatrix};$$

$$\Phi_2^{(5)}=-\frac{2}{\Upsilon_{11}}\begin{bmatrix} a_{11} & 0 & a_{13} & a_{14} & -\eta_2\left(\sigma_3+\bar{\sigma}_3\right)-\eta_1\left(\sigma_4+\bar{\sigma}_4\right) \\ a_{21} & a_{22}+b_{22} & a_{23} & a_{24} & \eta_2\left(\sigma_3+\bar{\sigma}_3\right)+\eta_1\left(\sigma_4+\bar{\sigma}_4\right) \\ a_{31} & b_{32} & a_{33}+b_{33} & 0 & 0 \\ a_{41} & a_{42} & 0 & a_{44} & 0 \\ 0 & 0 & 0 & a_{54} & 0 \end{bmatrix};$$

And

$$\Upsilon_{20}=\begin{bmatrix} 2i\omega_0-a_{11} & 0 & -a_{13} & -a_{14} & -a_{15} \\ -a_{21} & 2i\omega_0-a_{22}-b_{22}e^{-2i\tau_0\omega_0} & -a_{23} & -a_{24} & 0 \\ 0 & -b_{32}e^{-2i\tau_0\omega_0} & 2i\omega_0-a_{33}-b_{33}e^{-2i\tau_0\omega_0} & 0 & 0 \\ 0 & 0 & 0 & 2i\omega_0-a_{44} & 0 \\ 0 & 0 & -b_{33}e^{-2i\tau_0\omega_0} & -a_{54} & 2i\omega_0-a_{55} \end{bmatrix};$$

$$\delta_{11}=\begin{bmatrix} a_{11} & 0 & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22}+b_{22} & a_{23} & a_{24} & 0 \\ 0 & b_{32} & a_{33}+b_{33} & 0 & 0 \\ 0 & 0 & 0 & a_{44} & 0 \\ 0 & 0 & b_{53} & a_{54} & a_{55} \end{bmatrix}.$$

Then, we have

$$\Im(0)=\frac{i}{2\tau_0\omega_0}\left[w_{11}w_{20}-2\left|w_{11}\right|^2-\frac{\left|w_{02}\right|^2}{3}\right]+\frac{w_{21}}{2}; \tag{30}$$

$$\wp_1 = -\frac{\mathrm{Re}\{\Im(0)\}}{\mathrm{Re}\{\lambda^1(\omega_0)\}}; \tag{31}$$

$$\wp_2 = 2\,\mathrm{Re}\{\Im(0)\}; \tag{32}$$

$$\wp_3 = -\frac{\mathrm{Im}\{\Im(0)\} + \wp_1\,\mathrm{Im}\{\lambda^1(\tau_0)\}}{\tau_0\omega_0}. \tag{33}$$

6.Numerical Simulations and analysis

Numerical simulations are accomplished to show the malware spreading in cyber physical system and to validate the findings of the analysis.

$$\left.\begin{aligned}
\frac{dS(t)}{dt} &= 0.01 - \frac{0.7S(t)I_1(t)}{S+I_1+0.01} - \frac{0.2S(t)I_2(t)}{S+I_2+0.02} + 0.08R(t) - 0.01S(t)\\
\frac{dE(t)}{dt} &= \frac{0.7S(t)I_1(t)}{S+I_1+0.01} + \frac{0.2S(t)I_2(t)}{S+I_2+0.02} - 0.8E(t-\tau) - 0.1E(t) - 0.01E(t)\\
\frac{dI_1(t)}{dt} &= 0.8E(t-\tau) - \frac{0.3I_1(t-\tau)}{I_1(t-\tau)+0.8} - 0.01I_1(t)\\
\frac{dI_2(t)}{dt} &= 0.1E(t) - 0.1I_2(t) - 0.01I_2(t)\\
\frac{dR(t)}{dt} &= \frac{0.3I_1(t-\tau)}{I_1(t-\tau)+0.8} + 0.1I_2(t) - 0.08R(t) - 0.01R(t)
\end{aligned}\right\} \tag{34}$$

Through a series of calculations, we determined that the malware-existence equilibrium is uniquely given by (0.4996, 0.2317, 1.1067, 0.2104, 3.2910), and the elementary reproduction number (R_0) = 1.18262>1 and the malware presence equilibrium point p_1(0.4996, 0.2317, 1.1067, 0.2104, 3.2910). It can be confirmed that the system (34) is locally asymptotically stable when $\tau = 0$. This can be shown in Fig 4. For $\tau \neq 0$ by some computations with the aid of MATLAB platform, we obtain $\tau_0 = 16.55$, $\eta_0 = 2.583$. Upon setting the parameters to their respective values and initializing the system with the values p_1(S*, E*, I_1*, I_2*, R*) = p_1(0.4996, 0.2317, 1.1067, 0.2104, 3.2910), it can be observed from Figure 5(a) that the model (34) demonstrates local asymptotic stability. This achievement was made possible through careful parameter selection. Under this scenario, the densities of exposed nodes, sensitive nodes and infected nodes with weak infected capacity, infected nodes with strong infected capacity, and recovered nodes gradually converge to a unique equilibrium state, referred to as p_1 (0.4996, 0.2317, 1.1067, 0.2104, 3.2910), which indicates the presence of malware. In addition, Figures 5(b-f) present phase plots depicting the dynamics of I_1-I_2-R, S-I_1-I_2, R-I_2-S, E-I_1-R, and E-R-S, that can be used to illustrate this stable phenomenon of system (34) with $\tau = 14.55$.

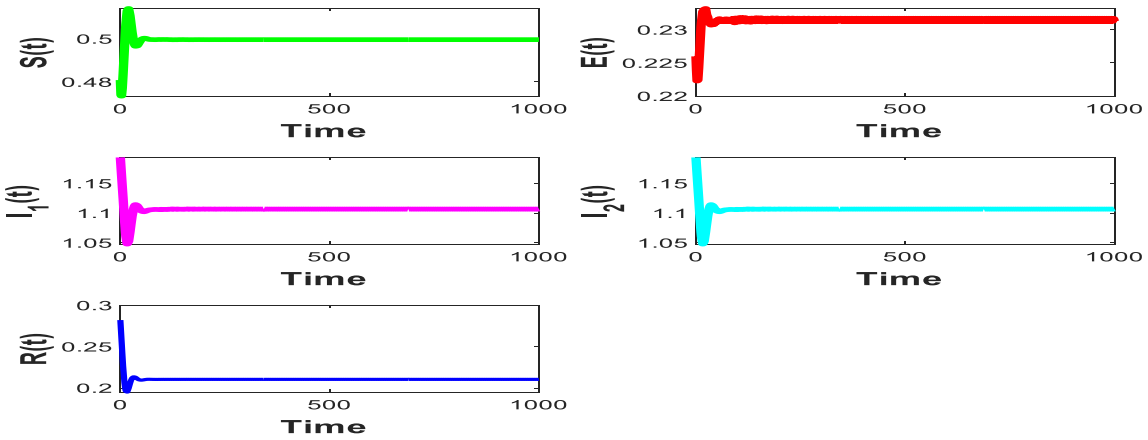
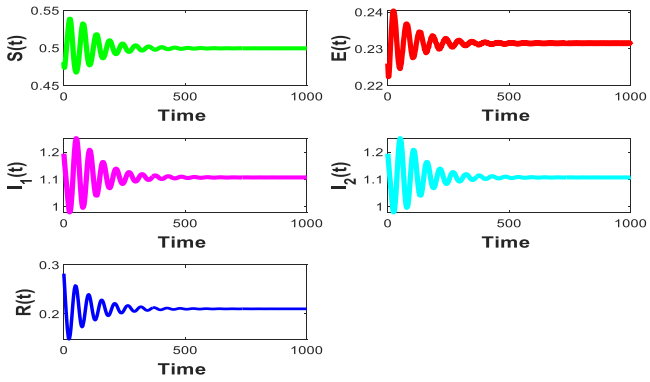
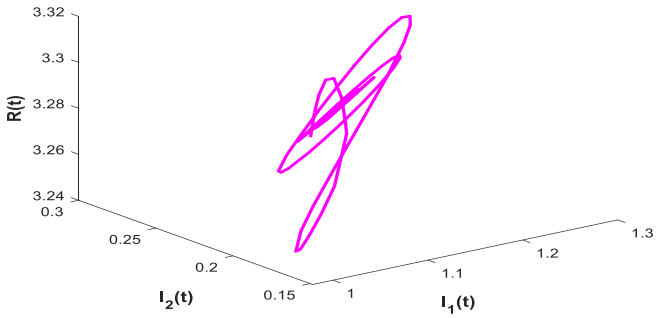


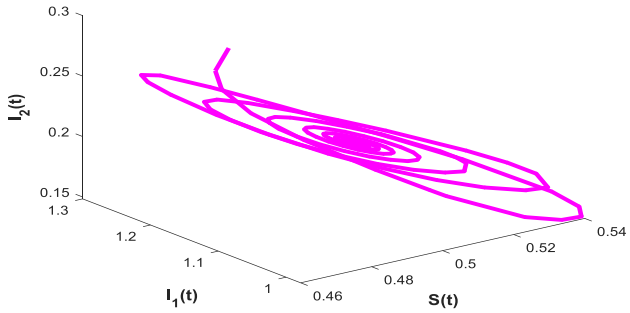
Fig 4. Time series plot of the nodes S-E-I_1-I_2-R for $\tau = 0$.



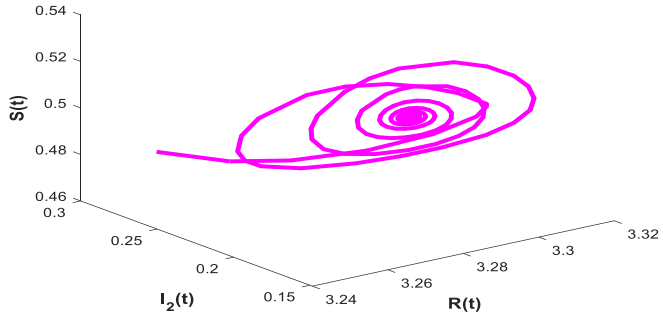
(a) Time series plot of the nodes S-E-I_1-I_2-R



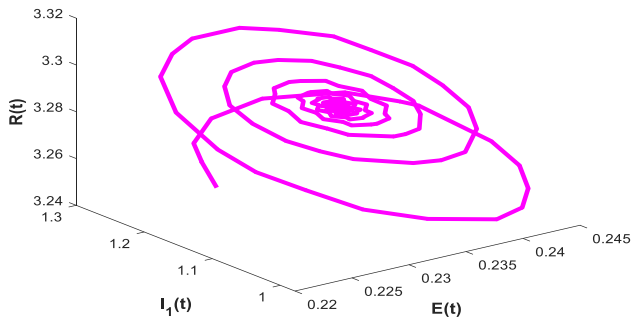
(b) Phase plot of I_1-I_2-R



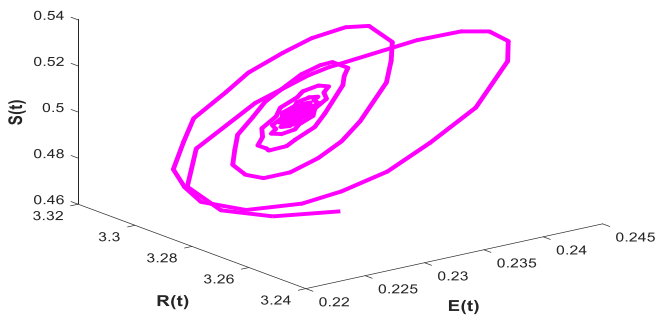
(c) Phase plot of S-I_1-I_2



(d) Phase plot of R-I_2-S



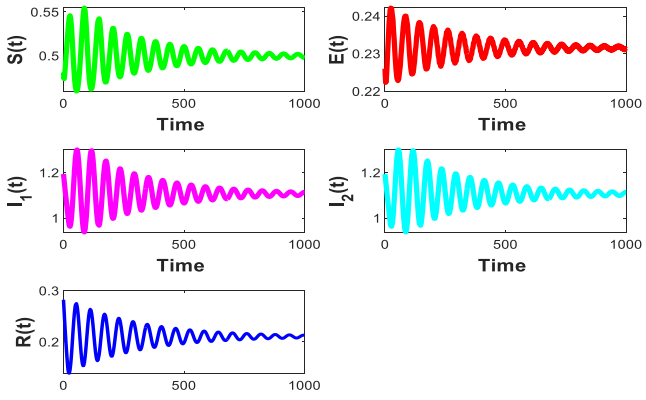
(e) Phase plot of E-I_1-R



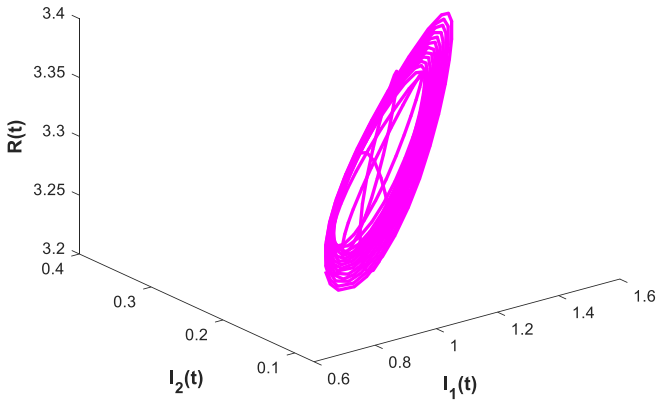
(f) Phase plot of E-R-S

Fig. 5. Node states for $\tau = 14.55 < 16.55$.

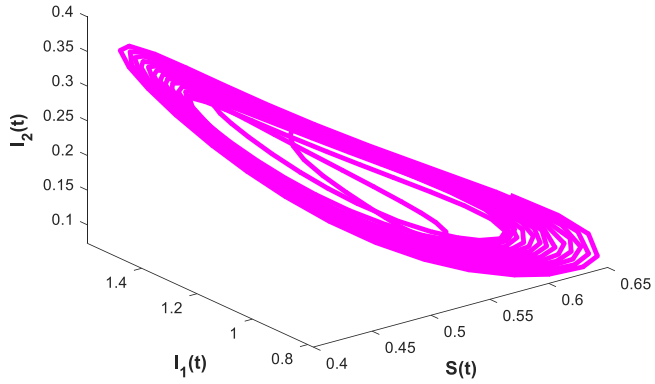
On the other hand, we fix $\tau = 18.55 > 16.55$ and choose the same initial value of densities of the nodes. When considering the values (S, E, I_1, I_2, R) = [0.4809, 0.2260, 1.1939, 0.2822, 3.2529], it is observed that the model (34) undergoes a loss of stability. Consequently, the densities of exposed nodes, susceptible and infected nodes with minimal infection capacity, infected nodes with high infection capacity, and recovered nodes exhibit periodic oscillations around the unique equilibrium state of malware existence, denoted as p_1(0.4996, 0.2317, 1.1067, 0.2104, 3.2910), as depicted in Figure 6(a). In addition, Figures 6(b-f) depict phase plots of I_1-I_2-R. S-I_1-I_2, R-I_2-S, E-I_1-R, and E-R-S stand as additional instances that can be used to illustrate this stable phenomenon of system (29) with $\tau = 18.55 > 16.55$.



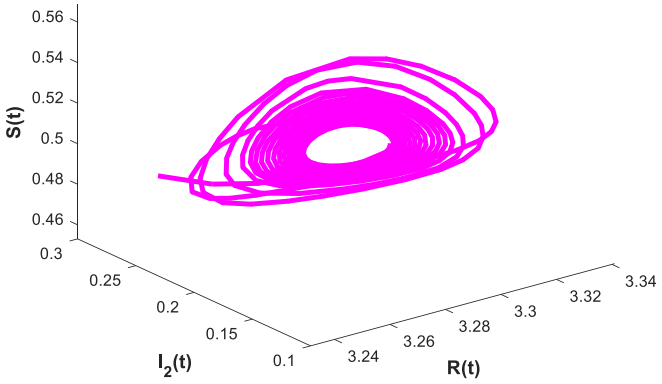
(a) Time series plot of the nodes S-E-I_1-I_2-R



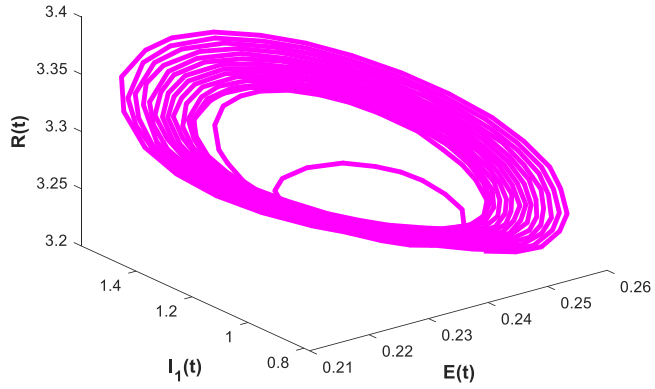
(b) Phase plot of I_1-I_2-R



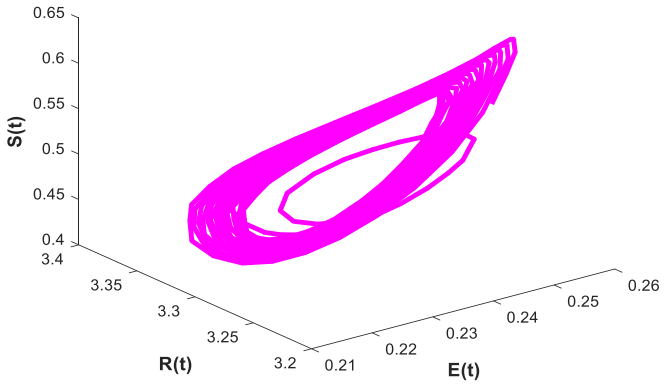
(c) Phase plot of S-I_1-I_2



(d) Phase plot of R-I_2-S



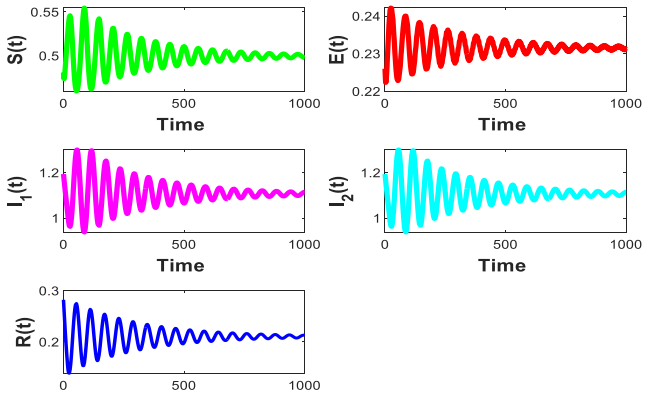
(e) Phase plot of E-I_1-R



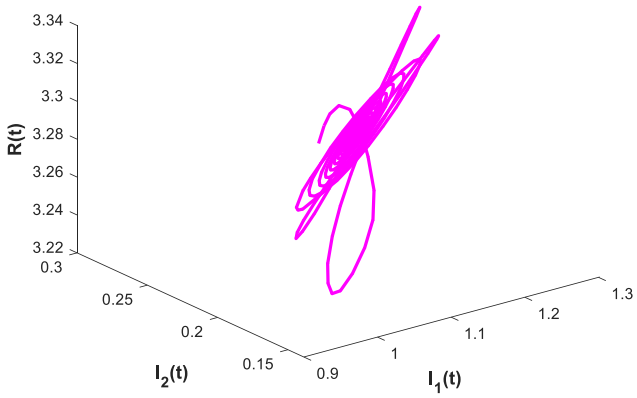
(f) Phase plot of E-R-S

Fig. 6. Node states for $\tau = 18.55 > 16.55$.

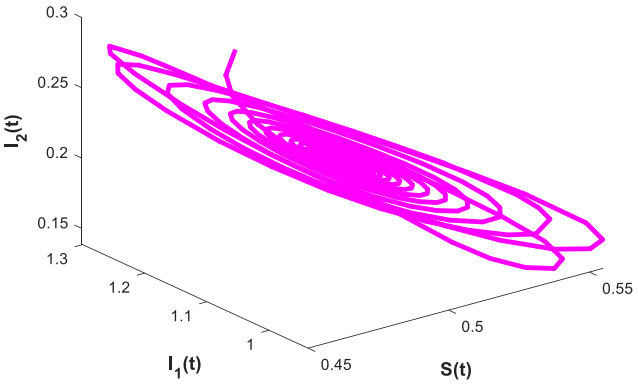
Furthermore, near the value of τ_0, the model (34) undergoes a Hopf bifurcation, leading to a transition from its stable state to a limit cycle. This behavior is exemplified in Figure 7. Additionally, providing further insights into the dynamics of the system during this bifurcation, illustrate phase plots of I_1-I_2-R, S-I_1-I_2, R-I_2-S, E-I_1-R, and E-R-S are instances that can be used to illustrate this stable phenomenon of system (34) with $\tau = \tau_0 = 16.55$.



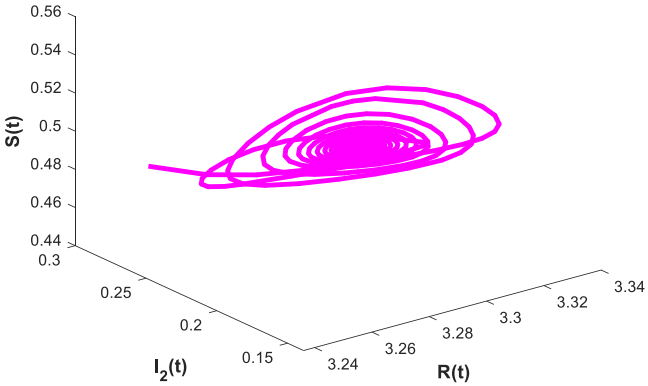
(a) Time series plot of the nodes S-E-I_1-I_2-R



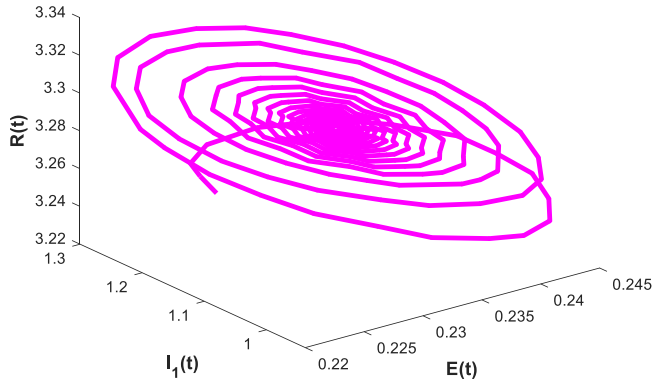
(b) Phase plot of I_1-I_2-R



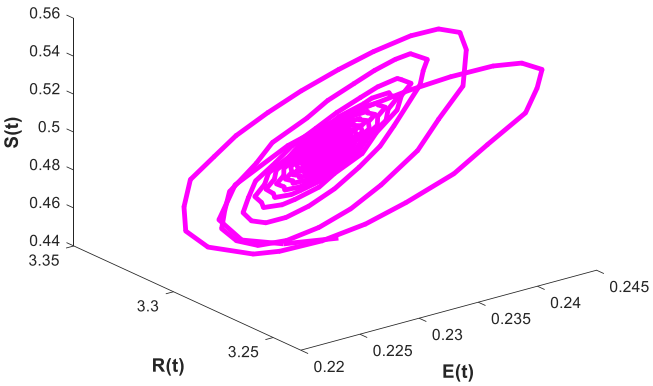
(c) Phase plot of S-I_1-I_2



(d) Phase plot of R-I_2-S



(e) Phase plot of E-I_1-R



(f) Phase plot of E-R-S

Fig. 7. Node states for $\tau = \tau_0 = 16.55$.

In addition, we obtain $\Im(0) = -1.612 - i0.1924$ by some complex computation with the help of MAT Lab software package. Thus, established on equation (30)-(33), we get $\wp_1 = 3.6437 > 0$, $\wp_2 = -1.2467 < 0$, $\wp_3 = 4.1372 > 0$. Consequently, drawing from Theorem 2, we can deduce that the Hopf bifurcation occurring at $\tau_0 = 16.55$ is of a supercritical nature. The resulting periodic solutions from the bifurcation are stable, and there is an increase in the period of these bifurcating periodic solutions.

Moreover, it is observed that as the delay parameter increases in model (34), the system undergoes a transition from a stable state to a chaotic state. In addition, when R_0 is greater than one, the number of infected nodes I_2 tends to increase more rapidly in comparison to infected nodes I_1 initially. Nonetheless, this difference eventually levels off. Therefore, to effectively manage the number of infected nodes, it is crucial to minimize R_0 as much as possible, ensuring that infected nodes remain in a stable state and facilitating better control of malware spread.

As malware proliferates, the behaviors of CPS change and possess nonlinear traits, leading to the consideration of CPS behavior as a nonlinear dynamic system. Consequently, the impact of a malware attack on CPSs may manifest in destructive dynamic behaviors, including bifurcation and chaos. The emergence of bifurcation, for example, can instigate mutations in CPS stability, potentially leading to adverse effects. In practical terms, bifurcation might induce harmful phenomena in power networks, such as voltage fluctuations, with the potential for catastrophic consequences. Therefore, it is crucial to delve into the distribution of malware and its dynamic manifestations within CPSs to better understand and mitigate potential risks.

The widespread adoption of robust communication infrastructure has heightened our dependence on cyber-physical systems, shaping their pivotal role in both professional and everyday activities. The vulnerability of cyber-physical systems to disruptions upon encountering malware underscores the critical security challenges they face. To explore the dynamics of malware propagation in these systems, we refine a model incorporating delayed dissemination and varying infection rates. This model introduces time delays corresponding to the transient immunity intervals of exposed and low-infected nodes.

Comprehensive mathematical derivations have meticulously validated the phenomena of Hopf bifurcation and local stability. This analysis establishes a crucial threshold value, determining the manageability of malware spread in cyber-physical systems. Below this threshold, regulation is achievable, but surpassing it renders the spread uncontrollable. The outcomes of numerical simulations reveal that, under specific circumstances, the proposed model undergoes a transition from its initially stable state to a limit cycle. Notably, our numerical simulations shed light on the impact of various parameters on the model, emphasizing proactive measures for cyber-physical system users. Regular use of anti-malware software, coupled with timely updates, emerges as a pivotal strategy to effectively manage malware dissemination within these systems, as evidenced by our numerical findings.

7. Concluding Remarks

To scrutinize the propagation dynamics of malware in these systems, a model with deferred propagation, incorporating diverse infection rates, is reconceptualized in this paper. This reformulation introduces a time delay attributed to the transitory immunity interval of recovered nodes. Careful mathematical derivations have been made in order to confirm local stability and the demonstration of Hopf bifurcation. The identification of the critical threshold value signifies the point beneath which the propagation of malware in cyber-physical systems can be effectively controlled, while surpassing this threshold renders it uncontrollable. The results of numerical simulations reveal that, under specific conditions, the proposed model undergoes a transition from its optimal stable state to a limit cycle. The proposed theorem is then validated through simulation. Through numerical simulations assessing the impact of factors like, and on our model, it becomes evident that users within cyber-physical systems should routinely employ anti-software to eradicate malware and ensure timely updates to control the dissemination of malware effectively. To extend this study, future research will consider the proposed system on various practical cyber security measures and analyze the impact of various factors, such as network topology, system architecture, and user behaviors. In addition, the incorporation of machine learning and artificial intelligence techniques into the malware detection and control processes can be further investigated in future work.

References

[1] G. Dartmann, H. Song, A. Schmeink, Big data analytics for Cyber–Physical Systems: Machine learning for the Internet of Things, Elsevier, 2019.

[2] Y. Jiang, H. Song, R. Wang, M. Gu, J. Sun, L. Sha, Data-centered runtime verification of wireless medical cyber–physical system, IEEE Trans. Ind.Inf. 13 (4) (2016) 1900–1909.

[3] S. Tan, J.M. Guerrero, P. Xie, R. Han, J.C. Vasquez, Brief survey on attack detection methods for cyber–physical systems, IEEE Syst. J. 14 (4) (2020) 5329–5339.

[4] H. Song, D. Rawat, S. Jeschke, C. Brecher, Cyber-Physical Systems: Foundations, principles and applications, Academic Press, 2016, pp. 1–514.

[5] H. Song, G.A. Fink, S. Jeschke, Security and Privacy in Cyber–Physical Systems: Foundations, principles, and applications, John Wiley & Sons, 2021, pp. 1–472.

[6] H. Zhu, Y. Li, R. Li, J. Li, H. Song, Sed droid: An enhanced stacking ensemble of deep learning framework for android malware detection, IEEE Trans. Netw. Sci. Eng. 99 (2020) 1.

[7] S. Arshad, M.A. Shah, A. Wahid, A. Mehmood, H. Song, Sama droid: A novel 3-level hybrid malware detection model for android operating system, IEEE Access (2018) 1.

[8] S. Xu, Y. Xia, H.L. Shen, Analysis of malware-induced cyber attacks in cyber–physical power systems, IEEE Trans. Circuits Syst. II: Express Briefs 67 (12) (2020) 3482–3486.

[9] S. Muthu Krishnan, S. Muthu Kumar, V. Chinnadurai, Optimal control of malware spreading model with tracing and patching in wireless sensor networks, Wirel. Pers. Commun. 117 (3) (2021) 2061–2083.

[10] S. Shen, H. Zhou, S. Feng, J. Liu, Q. Cao, SNIRD: Disclosing rules of malware spread in heterogeneous wireless sensor networks, IEEE Access 7(2019) 92881–92892.

[11] A. Mahboubi, S. Camtepe, K. Ansari, Stochastic modeling of IoT botnet spread: A short survey on mobile malware spread modeling, IEEE Access 99 (2020)

[12] Verma R. Smart city healthcare Cyber Physical System: Characteristics technologies and challenges. Wirel. Pers. Commun. 2022;122:1413–33.

[13] Zheng Z, Zhang KT, Gao XQ. Human-cyber–physical system for production and operation decision optimization in smart steel plants. Sci China Technol Sci 2022;65:247–60. Results Phys. 40 (2022) 10585

[14] Z.Zhang, V.Madhusudanan, B.S.N.Murthy. Efect of Delay in SMS Worm Propagation in Mobile Network with Saturated Incidence Rate, Wireless Personal Communications 131 (1), 1-22,2023.

[15] V.Madhusudanan, R.Geetha, B.S.N.Murthy, NHU-NGOC Dao, Sungrae CHO. Analysis of Delay-Aware Worm Propagation Model in Wireless IoT Systems With Ratio-Dependent Functional Response, IEEE Access 11, 34968-34976,2023.

[16] CH.Nwokoye , V. Madhusudanan , MN. Srinivas, NN Mbeledogu . Delay Modeling time. External noise and multiple malware infections in wireless sensor networks. Egyptian Inf J http://dx.doi.org/10.1016/j.eij.2022.02.002, published online.

[17] L.Behera, Nonlinear System Analysis—Lyapunov Based Approach; Intelligent Control Lecture Series; CRC Press: Boca Raton, FL, USA, 2003.

[18] YY.Cheng , LA.Huo , LJ.Zhao . Stability analysis and optimal control of rumor spreading model under media coverage considering time delay and pulse vaccination. Chaos Solitons Fractals 157,2022.

[19] K.Hooshmandi, F.Bayat, MR.Jahed-Motlagh, AA. Jalali. Stability analysis and design of nonlinear sampled-data systems under aperiodic samplings. *Int. J. Robust Nonlinear Control* , *10*, 2679–2699,2018.

[20] Z.Liu, D.Huang, Y. Xing, C. Zhang,Z. Wu, X. Ji. New Trends in Nonlinear Control Systems and Applications. Abstr. Appl. Anal. 2015.

[21] M O. Ajayi. Modelling and Control of Actuated Lower Limb Exoskeletons: A Mathematical Application Using Central Pattern Generators and Nonlinear Feedback Control Techniques; HAL archives; Tshwane University of Technology: Pretoria, South Africa, 2016.

[22] Yao Y, Sheng C, Fu Q, Liu HX, Wang DJ. A propagation model with defensive measures for PLC-PC worms in industrial networks. Appl. Math. Model. 2019;69:696–713.

[23] Xiao X, Fu P, Li Q, Hu GW, Jiang Y. Modeling and validation of SMS worm propagation over social networks. J. Comput. Sci. 2017;21:132–9.

[24] Kumari S, Upadhyay RK. Exploring the behavior of malware propagation on mobile wireless sensor networks: Stability and control analysis. Math. Comput. Simul. 2021;190:246–69.

[25] Yu ZH, Gao HX, Wang D, Alnuaim AA, Firdausi M, Mostafa AM. SEI2RS malware propagation model considering two infection rates in cyber–physical systems. Physica A. 2022;597:127207.

[26] Madhusudanan V, Geetha R. Dynamics of epidemic computer virus spreading model with Delays. Wirel. Pers. Commun. 2020;115:2047–61.

[27] Farah E, Amine S, Allali K. Dynamics of a time-delayed two-strain epidemic model with general incidence rates. Chaos Solit. Fractals. 2021;153:111527.

[28] Xu CJ, Liao MX, Li PL, Yuan S. Impact of leakage delay on bifurcation in fractional-order complex-valued neural networks. Chaos Solit. Fractals. 2021;142:110535.

[29] Yang FF, Zhang ZZ. Hopf bifurcation analysis of SEIR-KS computer virus spreading model with two-delay. Results Phys. 2021;24:104090.

[30] Huang CD, Nie XB, Zhao X, Song QK, Tu ZW, Xiao M, et al. Novel bifurcation results for a delayed fractional-order quaternion-valued neural network. Neural Netw. 2019;117:67–93.

[31] Hassard BD, Kazarinoff ND, Wan YH. Theory And Applications of Hopf Bifurcation. Cambridge: Cambridge University Press; 1981.

[32] Zhang ZZ, Upadhyay RK. Dynamical analysis for a deterministic SVIRS epidemic model with Holling type II incidence rate and multiple delays. Results Phys. 2021;24:104181

[33] Hu Zhang, V. Madhusudanan, R. Geetha, M.N. Srinivas, ChukwuNonso H. Nwokoye ”Dynamic analysis of the e-SITR model for remote wireless sensor networks with noise and Sokol-Howell functional response”, Results in Phys., 38 (2022) 105643.

[34] Geetha, R., Madhusudanan, V. & Srinivas, M.N. Influence of clamor on the transmission of worms in remote sensor network. Wirel. Pers. Commun. 118, 461–473 (2021).

[35] Z.A.Zhang., S.Kunda., J.P.Tripathi., S.Bugalia. Stability and Hopf – bifurcation analysis of an SVEIR epidemic model with vaccination and multiple delays, Chaos, Solitons and Fractals, 131, 2020.

[36] Xiaodong Yu, Aying Wan,’Dynamical aspects of a delayed SEI2RS malware dissemination model in cyber–physical systems’’ Results in Physics,Volume 40 ,105851, 2022.

[37] Miguel López, Alberto Peinado, Andrés Ortiz, An extensive validation of a SIR epidemic model to study the propagation of jamming attacks against IoT wireless networks, Computer Networks, Volume 165, 106945, 2019.