IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 11 March 2023, accepted 3 April 2023, date of publication 6 April 2023, date of current version 12 April 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3264978

RESEARCH ARTICLE

Analysis of Delay-Aware Worm Propagation Model in Wireless IoT Systems With Ratio-Dependent Functional Response

V. MADHUSUDANAN[1], R. GEETHA[2], B. S. N. MURTHY[3], NHU-NGOC DAO[4], (Senior Member, IEEE), AND SUNGRAE CHO[5]

[1]Department of Mathematics, S.A. Engineering College, Chennai 600077, India
[2]Department of Computer Science and Engineering, S.A. Engineering College, Chennai 600077, India
[3]Department of Mathematics, Aditya College of Engineering and Technology, Surampalem 533437, India
[4]Faculty of Computer Science, Ho Chi Minh City Open University, Ho Chi Minh City 70000, Vietnam
[5]School of Computer Science and Engineering, Chung-Ang University, Seoul 06974, South Korea

Corresponding authors: Nhu-Ngoc Dao (ngoc.dn@ou.edu.vn) and Sungrae Cho (srcho@cau.ac.kr)

This work was supported by the Ministry of Science and ICT (MSIT), South Korea, under the Information Technology Research Center (ITRC) Support Program by the Institute for Information Communications (IITP) under Grant IITP-2023-RS-2022-00156353.

ABSTRACT This article presents a delayed susceptibility, exposure, infectivity, recovery, and vaccination (SEIRV) model with nonlinear incidence and ratio-dependent functional responses. Model limitations and local stability analyses were examined with strict consideration of delay awareness. In addition, the presence of Hopf bifurcations with delay as a bifurcation parameter was investigated along with feature distributions with appropriate constraints. Numerical simulations are presented to verify the proposed theoretical results. In particular, if the latency exceeds the threshold, worm propagation in the system may become out of control. We demonstrated that the propagation characteristics of worms can easily be predicted and eliminated if the delay values are below a suitable threshold. Finally, we conclude that worm propagation is controllable by shifting the presence of Hopf bifurcations.

INDEX TERMS Epidemic model, local stability, wireless internet of things (IoT), worm propagation.

I. INTRODUCTION

Wireless Internet of things (IoT) networks play an essential role in many application areas, such as patient health monitoring, military applications, disaster management, intrusion detection, and automotive applications [1], [2]. However, IoT devices are considered weakly defended and targeted by worms due to their limited origin in physical resources. Many attackers make IoT devices hot targets due to their limited defense capabilities. In particular, worms can replicate and propagate without manual intervention, deceiving other nodes into taking their sources from the network. Wireless communication technologies may allow malicious code to propagate directly from device to device [3], [4]. Fundamental parallels exist between the induction of software-spawn worms in wireless IoT networks and the spread of epidemics in human populations. In wireless IoT networks, crude epidemiological models were used by intellectuals to study the spread of the worm. Similarly, the Chameleon, Cabir, and Mabir worms make economics and transportation important. Significant and sufficient measures must be taken within the network to manage worm generation.

A. RELATED WORK

An epidemic model was used to study the behavior of the malicious object and control the spread of the worm within the network. An epidemic model was proposed in several studies [5], [6], [7] that deal with time delay and investigate the dynamic features of worm prevalence. To effectively manage worm intrusions, it is vital to understand the dynamics of worm propagation in wireless IoT networks. In existing studies, disease models have proven valuable in

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Arafatur Rahman.

explaining aspects of worm spread. Researchers in recent years [8], [9] have studied worms in wireless IoT networks because of the correlation between the spread of worms through wireless devices and the spread of traditional worms over the internet. Vogue models are used extensively to characterize worm reproduction. In this context, Mishra and Keshi proposed a susceptibility-exposure-infection-recovery-vulnerability using the vaccination compartment (SEIRS-V) model [10]. In [11], Mishra et al. proposed the susceptible-infected-quarantine-recovered-susceptible (SIQRS) model, recognizing the implications of quarantine scenarios. Based on the results of [10], Mishra and Tyagi [12] proposed the susceptible-exposed-infectious-quarantine-recovered with vaccination (SEIQR-V) model in wireless IoT networks to determine the potential threat of worm propagation. Feng et al. [13] proposed an improved susceptible-infected-recovered-susceptible (SIRS) prevalence model for classifying the effects of communication radius and assigned density and focused on the model stability to reduce the spread of worms. Subsequently, analyzing the strength of the model, Ojha et al. [14] extended the model by Feng et al. [13] to build a modified SIQRS worm propagation model with the introduction of compartment separation.

Other mathematical models also describe the mobility of malicious code in the case of wireless IoT networks [15], [16]. The SIRS worm propagation model in wireless IoT networks proposed by Feng et al. [13] was extended by Ojha et al. in [14]. Ojha et al. included the exposed class to propose the SEIRS worm propagation model. In [17], Upadhyay and Kumari proposed an energy-efficient electronic epidemic model by analyzing the linear stability with delay, where a Hopf bifurcation analysis was performed. Their results proved that packet delivery delays are the reason for chaotic dynamics and reveal a means of controlling the propagation of threatening signals. Signes-Pont et al. [18] modified the SEIRS malware propagation for mobile communication devices. They focused on well-defined inter-node communication patterns specifying local traces indicating infected connections. In addition, López et al. [19] presented the use of prevalent techniques to analyze the propagation of jamming attacks that can affect various communication layers of all nodes in various wireless IoT networks. On the other hand, Huang et al. [20] focused on the bifurcation problem of a fractional-order bidirectional associative memory neural network (FOBAMNN) with four different delays. This model calculated quantitatively the significant values of the Hopf bifurcation for various delays. It is recognized that the stability of the developed FOBAMNN with multiple delays can be obtained considerably if lower control delays are chosen, and Hopf bifurcation occurs when the control delay exceeds a critical value. For further study, [21] reports innovative results on the stability and bifurcation of a delayed quaternion-valued fractional neural network (FOQVNN). The analyses show that the amplitude of the branch oscillations increases with increasing time delay. It can be seen that the bifurcation phenomenon occurs earlier as the order increases. In [22], [23], Xu et al. discussed the stability and existence of the Hopf bifurcations for fractional-order BAM neural networks with and without leakage delays. A stability condition and a sufficient criterion for the existence of Hopf bifurcations of fractional-order BAM neural networks with delays (leakage delays) are established. In addition, [24] investigated Hopf bifurcation problems for fractional order quaternary numerical neural networks with leaky delays. The authors derived delay-influenced bifurcation conditions for eight real-valued networks using stability criteria and bifurcation theory for fractional-order differential dynamic systems.

B. CONTRIBUTIONS AND PAPER ORGANIZATION

Distinguished from aforementioned studies, we use open simulations and experiments to examine the accuracy of the susceptibility, exposure, infectivity, recovery, and vaccination (SEIRV) model for calculating the spread of destructive attacks in this paper. The worm propagation model was considered with a nonlinear incidence. Moreover, the proposed model focuses on periods of inactivity and interaction-induced time delays as ratio-dependent functional responses. Then, we investigate the viral balance to examine the local stability, applying the properties of the Hopf bifurcation. The numerical simulations support the theoretical conclusions.

This work is organized as follows. Section II provides the delayed mathematical model with a suitable explanation and discusses the boundedness (II-A) and equilibrium analysis (II-B). Next, Section III addresses the local stability analysis in the presence and absence of delay. Then, Section IV introduces the computer simulations to facilitate the hypothetical outcomes. Finally, Section V summarizes the paper with concluding remarks.

II. MATHEMATICAL MODEL

Most mentioned wireless communication network models assume a bilinear infection rate. In particular, wireless worm propagation can be dramatically affected by the topology of the underlying network system. From this perspective, we integrate the ratio-dependent functional response into the wireless IoT networks. Time delays play an essential role in worm propagation from wireless IoT networks because time delays can cause a loss of stability and induce Hopf bifurcations and periodic solutions. Hopf bifurcation results indicate that worm propagation changes from equilibrium to limited cycles in wireless IoT networks. This phenomenon is unexpected because cyclic behavior is unpleasant from an epidemiological viewpoint. With this idea in mind, we developed the following delay model for worm propagation in wireless IoT networks. The symbol definitions are summarized in Table 1.

$$S'(t) = A - \delta_0 S - \frac{\alpha S^2 I}{S^2 + cI^2} + \eta V - \mu S \tag{1}$$

$$E'(t) = \frac{\alpha S^2 I}{S^2 + cI^2} - \delta_0 E - \delta_1 E(t-\tau) \tag{2}$$

TABLE 1. Description of parameters.

Parameters	Descriptions
A	New IoT devices
α	Contact rate of susceptible IoT devices
β	Treatment rate of IoT devices
η	Immunity rate of IoT devices
μ	Vaccination rate of IoT devices
a	Half saturation constant rate for infected devices
c	Half saturation constant rate for susceptible devices
δ_0	Natural mortality rate of each IoT device
δ_1	Infection rate of exposed IoT devices
δ_2	Recovery rate of infected IoT devices
δ_3	Detached rate of infected IoT devices
S	Susceptible IoT devices
E	Exposed IoT devices
I	Infected IoT devices
R	Recovered IoT devices
V	Vaccinated IoT devices
τ	Time delay

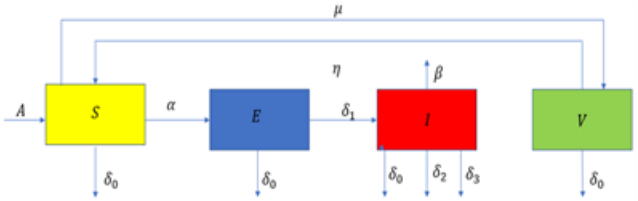


FIGURE 1. Schematic diagram of the SEIV worm propagation model in a wireless IoT network system.

$$I'(t) = \delta_1 E(t-\tau) - (\delta_0 + \delta_5 + \delta_3)I - \frac{\beta I}{I+a} \tag{3}$$

$$R'(t) = \delta_2 I - \delta_0 R + \frac{\beta I}{I+a} \tag{4}$$

$$V'(t) = \mu S - (\delta_0 + \eta)V. \tag{5}$$

Eliminating class R does not affect the elements of S, V, E, and I classes; therefore, we examine the accompanying modified framework as follows:

$$S'(t) = A - \delta_0 S - \frac{\alpha S^2 I}{S^2 + cI^2} + \eta V - \mu S \tag{6}$$

$$E'(t) = \frac{\alpha S^2 I}{S^2 + cI^2} - \delta_0 E - \delta_1 E(t-\tau) \tag{7}$$

$$I'(t) = \delta_1 E(t-\tau) - (\delta_0 + \delta_5 + \delta_3)I - \frac{\beta I}{I+a} \tag{8}$$

$$V'(t) = \mu S - (\delta_0 + \eta)V. \tag{9}$$

The SEIV worm propagation model in a wireless IoT network system is depicted in Fig. 1.

A. BOUNDEDNESS ANALYSIS

We let

$$N = S + E + I + V. \tag{10}$$

Then, differentiating ((10)) on both sides, we obtain

$$\begin{aligned}\frac{dN}{dt} &= \frac{dS}{dt} + \frac{dE}{dt} + \frac{dI}{dt} + \frac{dV}{dt} \\ &= A - \delta_0 (S + E + I + V) - (\delta_2 + \delta_3) I - \frac{\beta I}{I+a} \\ &= A - \delta_0 N - \left(\delta_2 + \delta_3 + \frac{\beta}{I+a}\right) I.\end{aligned}$$

Therefore,

$$\frac{dN}{dt} + \delta_0 N \le A.$$

Hence,

$$N(t) \le N_0 e^{-\delta_0 t} + \frac{A}{\delta_0}\left(1 - e^{-\delta_0 t}\right).$$

Thus, we assume that the initial value is

$$N_0 = S_0 + E_0 + I_0 + V_0 = \frac{A}{\delta_0}.$$

To have nodes with a constant size, we have

$$S(t) + E(t) + I(t) + V(t) = N = \frac{A}{\delta_0}.$$

The nodes $(S(t) + E(t) + I(t) + V(t))$ remain in the network and are related and represented in the set

$$\Omega = \left\{(S, E, I, V) \in {R_+}^4 / 0 \le S + E + I + V \le \frac{A}{\delta_0}\right\},$$

where

$$(S(0), E(0), I(0), V(0)) \in {R_+}^4,$$

which is a positively invariant region. Using $V(t) = \frac{A}{\delta_0} - S(t) - E(t) - I(t)$, we can eliminate $v(t)$, which provides a scaled-down three-dimensional model:

$$\begin{aligned}\frac{dS}{dt} &= A - \delta_0 S - \frac{\alpha S^2 I}{S^2 + cI^2} - \mu S \\ &\quad + \eta\left[\frac{A}{\delta_0} - S(t) - E(t) - I(t)\right] \\ \frac{dE}{dt} &= \frac{\alpha S^2 I}{S^2 + cI^2} - \delta_0 E - \delta_1 E \\ \frac{dI}{dt} &= \delta_1 E - (\delta_0 + \delta_5 + \delta_3)I - \frac{\beta I}{I+a}.\end{aligned}$$

We let $N_1 = S + E + I$, and from the above-reduced model, we have

$$\begin{aligned}\frac{dN_1}{dt} &= \frac{dS}{dt} + \frac{dE}{dt} + \frac{dI}{dt} \\ \frac{dN_1}{dt} &= \frac{A}{\delta_0}(\delta_0 + \eta) - (\delta_0 + \eta) N_1 \\ \frac{dN_1}{dt} &+ (\delta_0 + \eta) N_1 = \frac{A}{\delta_0}(\delta_0 + \eta) - \left(\delta_2 + \delta_3 + \frac{\beta}{I+a}\right).\end{aligned}$$

From the above equation, in the absence of a virus (i.e., $I = 0$, $N_1 \to \frac{A}{\delta_0}(\delta_0 + \eta)$), due to the spread of the virus in the computer network N_1, it follows that

$$N_1 \in \left(0, \frac{A}{\delta_0}(\delta_0 + \eta)\right).$$

As Ω is a positively invariant region for the original model, the following is also a positively invariant region for the above model:

$$\Omega = \left\{(S, E, I) : S \ge 0, E \ge 0, I \ge 0, S + E + I \le \frac{A}{\delta_0}(\delta_0 + \eta)\right\}. \tag{11}$$

$$
\begin{aligned}
\Gamma_0 =& c\alpha^2\delta_1^2k^2l^2 - c\alpha\delta_1k^3l^3,\\
\Gamma_1 =& ac\alpha^2\delta_1^2k^2l^2 - ac\alpha\delta_1k^3l^3 - c\alpha\beta\delta_1k^3l^2 + 2ac\alpha^2\delta_1^2k^2 - 2ac\alpha\delta_1k^3,\\
\Gamma_2 =& A^2c\alpha^2\delta_1^2 - A^2c\alpha\delta_1 + c\alpha^2\delta_1^2k^2l^2a^2 - c\alpha\delta_1k^3l^3a^2 + 2c\alpha^2\delta_1^2a^2k^2 - 2c\alpha\delta_1a^2k^3l - 2ac\alpha\delta_1k^3\beta - m^2c^2\alpha\delta_1kl,\\
\Gamma_3 =& A^2ac\alpha^2\delta_1^2 - A^2ackl\alpha\delta_1 + 2aA^2c\alpha^2\delta_1^2 - 2aA^2c\alpha\delta_1kl + ca^3\alpha^2\delta_1^2k^2l^2 - ca^3\alpha\delta_1k^3l^3 - c\alpha\beta\delta_1k^3l^2a^2 - 2Akl\alpha^2{\delta_1}^2\\
&- 2Ak^3l^3\alpha\delta_1 + 4A\alpha\delta_1k^2l^2 - m^2c^2\alpha\delta_1kal - m^2c^2\alpha\beta\delta_1k,\\
\Gamma_4 =& A^2a^2c\alpha^2\delta_1^2 - A^2a^2c\alpha\delta_1kl - 2A^2a^2c\alpha\delta_1kl - 2A^2ack\alpha\beta\delta_1 - 4aAkl\alpha^2\delta_1^2 + 4aAk^3l^3 + 8Aa\alpha\delta_1k^2l^2 + 4A\alpha\beta k^2l\delta_1\\
&- 4A\beta k^3l^2 + 2aAk^3l^3 - 4A\alpha\delta_1k^2l^2 + 2Ak\beta\alpha^2\delta_1^2 + 2A\beta k^3l^2 - 4A\beta\alpha\delta_1k^2l,\\
\Gamma_5 =& A^2a^3c\alpha^2\delta_1^2 - A^2a^3klc\alpha\delta_1 - A^2c\alpha\delta_1a^2\beta k - 2Akla^2\alpha^2\delta_1^2 - 2Ak^3l^3a^2 - 2\beta^2Ak^3l + 4Ak^2l^2a^2\alpha\delta_1 - 4Ak^3l^2a\\
&+ 4aA\beta k^2l\alpha\delta_1 + 4Akl\alpha^2\delta_1^2a^2 + 4Aa^2k^3l^3 + 4Aa\beta k^3l^2 + 4Aak\beta\alpha^2\delta_1^2 - 4Aak^2l\alpha\beta\delta_1 + 4A\beta ak^3l^2\\
&- 8Aa\alpha\delta_1k^2\beta l + 4A\beta^2k^3l - 4A\beta^2k^2\alpha\delta_1,\\
\Gamma_6 =& 2a^2A^2c\alpha^2\delta_1^2 + 2Akl\alpha^2\delta_1^2a^3 + 2Ak^3l^3a^3 + 2Ak^3l\beta^2a - 4\alpha\delta_1Ak^2l^2a^3 - 4\alpha\delta_1k^2l^2a^2 + 4aA\beta k^3l^2 - 4A\beta k^2la^2\alpha\delta_1\\
&+ 2Ak\beta\alpha^2\delta_1^2a^2 + 2Ak^3l^2\beta a^2 + 2Ak^3\beta^3 - 4A\alpha\delta_1k^2l\beta a + 4Ak^3\beta^2la - 4A\beta k^2\alpha\delta_1a,\\
k =& \delta_0 + \delta_1,\\
l =& \delta_0 + \delta_2 + \delta_3,\\
m =& \frac{{\delta_0}^2(\delta_0 + \eta + \mu)^2}{(\delta_0 + \eta)^2}.
\end{aligned}
$$

FIGURE 2. $\Gamma_0, \ldots, \Gamma_6$ formulas.

Theorem 1: All the nonnegative solutions of the model system ((1)–(5)) that initiate in

$$\Omega = \left\{ (S, E, I) : S \geq 0, E \geq 0, I \geq 0, S + E + I \leq \frac{A}{\delta_0}(\delta_0 + \eta) \right\}$$

are uniformly bound.

B. EQUILIBRIUM ANALYSIS

In this section, we discuss the presence of the infection-free harmony and the endemic balance of the model framework ((6)–(9)). The endemic equilibrium points of ((6)–(9)) are (12)–(14), as shown at the bottom of the page, where I^* is the positive root of the following equation:

$$\Gamma_0 I^6 + \Gamma_1 I^5 + \Gamma_2 I^4 + \Gamma_3 I^3 + \Gamma_4 I^2 + \Gamma_5 I + \Gamma_6 = 0, \tag{15}$$

where $\Gamma_0, \ldots, \Gamma_6$ are provided in Fig. 2.

III. DELAY-AWARE LOCAL STABILITY ANALYSIS

The Jacobian matrix of the system ((6)–(9)) at the endemic equilibrium point D^*, $J(D_*)$ is

$$\begin{vmatrix} \lambda - a_{11} & 0 & a_{13} & a_{14} \\ a_{21} & \lambda - a_{22} - b_{22} - e^{-\lambda\tau} & a_{23} & 0 \\ 0 & b_{32} - e^{-\lambda\tau} & \lambda - a_{33} & 0 \\ a_{41} & 0 & 0 & \lambda - a_{44} \end{vmatrix},$$

where

$$
\begin{aligned}
a_{11} &= -\left[\delta_0 + \mu - \frac{2\alpha {I_*}^3 S_*}{\left({S_*}^2 + c{I_*}^2\right)^2}\right],\\
a_{13} &= \frac{-\alpha {S_*}^2\left({S_*}^2 - c{I_*}^2\right)}{\left({S_*}^2 + c{I_*}^2\right)^2},\\
a_{14} &= \eta,\\
a_{21} &= \frac{2\alpha c {I_*}^3 S_*}{\left({S_*}^2 + c{I_*}^2\right)^2},\\
b_{22} &= -\delta_1,
\end{aligned}
$$

$$S^* = I^*\sqrt{\frac{c(\delta_0 + \delta_1)[(\delta_0 + \delta_2 + \delta_3)(I^* + a) + \beta]}{[\alpha\delta_1 - (\delta_0 + \delta_1)(\delta_0 + \delta_2 + \delta_3)](I^* + a) - \beta(\delta_0 + \delta_1)}} \tag{12}$$

$$E^* = \frac{(\delta_0 + \delta_1 + \delta_3)I^*}{\delta_1} + \frac{\beta I^*}{\delta_1(I^* + a)} \tag{13}$$

$$V^* = \frac{\mu S^*}{\delta_0 + \eta}, \tag{14}$$

$$
\begin{aligned}
a_{13} &= \frac{\alpha {S_*}^2 \left({S_*}^2 - c{I_*}^2\right)}{\left({S_*}^2 + c{I_*}^2\right)^2},\\
b_{32} &= -\delta_1,\\
a_{33} &= -\left(\delta_0 + \delta_2 + \delta_3\right) - \frac{\beta}{(I+\alpha)^2},\\
a_{41} &= \mu,\\
a_{44} &= -\left(\delta_0 + \eta\right).
\end{aligned}
$$

Thus, the characteristic equation of the system ((6)–(9)) at D^* is

$$
\begin{aligned}
&\lambda^4 + A_1\lambda^3 + A_2\lambda^2 + A_3\lambda + A_4\\
&\qquad + e^{-\lambda\tau}\left[B_1\lambda^3 + B_2\lambda^2 + B_3\lambda + B_4\right] = 0, \quad (16)
\end{aligned}
$$

where

$$
\begin{aligned}
A_1 =& -\left(a_{11} + a_{22} + a_{33} + a_{44}\right),\\
A_2 =& a_{11}\left(a_{33} + a_{44}\right) + a_{22}\left(a_{11} + a_{33}\right)\\
&+ a_{44}\left(a_{33} + a_{22}\right) - a_{14}a_{41},\\
A_3 =& -\begin{pmatrix} a_{11}a_{33}a_{44} + a_{11}a_{33}a_{22} + a_{11}a_{22}a_{44} + a_{22}a_{33}a_{44}\\ -a_{22}a_{41}a_{14} - a_{33}a_{41}a_{14}\end{pmatrix},\\
A_4 =& a_{11}a_{22}a_{33}a_{44} + a_{11}a_{33}a_{44}b_{22} - a_{14}a_{22}a_{33}a_{41},\\
B_1 =& -b_{22},\\
B_2 =& b_{22}\left(a_{11} + a_{33}\right) + a_{44}b_{22} - a_{23}b_{32},\\
B_3 =& \begin{pmatrix} a_{13}b_{32}a_{21} + a_{11}b_{32}a_{23} + a_{44}a_{23}b_{22} + a_{41}a_{14}b_{22}\\ -a_{11}a_{33}b_{22} - a_{11}b_{22}a_{44} - a_{33}b_{22}a_{44}\end{pmatrix},\\
B_4 =& \begin{pmatrix} a_{23}a_{41}a_{14}b_{32} - b_{32}a_{33}a_{41}a_{14} - a_{21}a_{13}a_{44}b_{32}\\ -a_{11}a_{44}a_{23}b_{32}\end{pmatrix}.
\end{aligned}
$$

A. IN THE CASE OF THE ABSENCE OF DELAY

Inputting $\tau = 0$ into (16), we have

$$
\begin{aligned}
&\lambda^4 + \left(A_1 + B_1\right)\lambda^3 + \left(A_2 + B_2\right)\lambda^2\\
&\qquad + \left(A_3 + B_3\right)\lambda + \left(A_4 + B_4\right) = 0. \quad (17)
\end{aligned}
$$

From the expression of A_1 and B_1, we have

$$
A_1 + B_1 = a_{11} + a_{22} + a_{33} + a_{44} + b_{22} > 0.
$$

Thus, given the Routh–Hurwitz criteria

$$
\det_1 = A_1 + B_1 > 0, \quad (18)
$$

$$
\det_2 = \begin{pmatrix} A_1 + B_1 & 1\\ A_3 + B_3 & A_2 + B_2\end{pmatrix} > 0, \quad (19)
$$

$$
\det_3 = \begin{pmatrix} A_1 + B_1 & 1 & 0\\ A_3 + B_3 & A_2 + B_2 & A_1 + B_1\\ 0 & A_4 + B_4 & A_3 + B_3\end{pmatrix} > 0, \quad (20)
$$

$$
\det_4 = \begin{pmatrix} A_1 + B_1 & 1 & 0 & 0\\ A_3 + B_3 & A_2 + B_2 & A_1 + B_1 & 1\\ 0 & A_4 + B_4 & A_3 + B_3 & A_2 + B_2\\ 0 & 0 & 0 & A_4 + B_4\end{pmatrix} > 0. \quad (21)
$$

Thus, if conditions (18)–(21) hold, D^* is locally asymptotically stable in the absence of delay.

B. IN THE CASE OF THE PRESENCE OF DELAY

By inputting $\lambda = i\omega$, $\omega > 0$, in (16), we obtain

$$
\begin{aligned}
&\left[(i\omega)^4 + A_1(i\omega)^3 + A_2(i\omega)^2 + A_3(i\omega) + A_4\right]\\
&\quad + e^{-i\omega\tau}\left[B_1(i\omega)^3 + B_2(i\omega)^2 + B_3(i\omega) + B_4\right] = 0. \quad (22)
\end{aligned}
$$

By equating the real and imaginary parts, we attain

$$
\begin{aligned}
&\cos\omega\tau\left(B_4 - B_2\omega^2\right) + \sin\omega\tau\left(B_3\omega - B_1\omega^3\right)\\
&\qquad = A_2\omega^2 - \omega^4 - A_4, \quad (23)\\
&\cos\omega\tau\left(B_3\omega - B_1\omega^3\right) - \sin\omega\tau\left(B_4 - B_2\omega^2\right)\\
&\qquad = A_1\omega^3 - A_3\omega. \quad (24)
\end{aligned}
$$

Squaring and adding (23) and (24) results in

$$
\omega^8 + P_1\omega^6 + P_2\omega^4 + P_3\omega^2 + P_4 = 0, \quad (25)
$$

where

$$
\begin{aligned}
P_1 &= {A_1}^2 - {B_1}^2 - 2A_2,\\
P_2 &= {A_2}^2 - 2A_3A_1 - {B_2}^2 + 2B_1B_3,\\
P_3 &= {A_3}^2 - 2A_4A_2 - {B_3}^2 + 2B_4B_2,\\
P_4 &= {A_4}^2 - {B_4}^2.
\end{aligned}
$$

Now, by assuming $\omega^2 = u$, (25) becomes

$$
u^4 + P_1u^3 + P_2u^2 + P_3u + P_4 = 0. \quad (26)
$$

We define the function as follows:

$$
f(u) = u^4 + P_1u^3 + P_2u^2 + P_3u + P_4 = 0. \quad (27)
$$

In addition, $\lim_{u\to\infty} f(u) = \infty$. Thus, if $P_4 < 0$, (27) has at least one positive root.

Solving from (23) and (24), we find

$$
\cos\omega t = \frac{s_1\omega^6 + s_2\omega^4 + s_3\omega^2 + s_4}{s_5\omega^6 + s_6\omega^4 + s_7\omega^2 + s_8}, \quad (28)
$$

where

$$
\begin{aligned}
s_1 &= B_2 - A_1B_1,\\
s_2 &= A_3A_1 + A_1B_3 - A_2B_2 - B_4,\\
s_3 &= A_4B_2 + A_2B_4 - A_3B_3,\\
s_4 &= -A_4B_4,\\
s_5 &= B_1,\\
s_6 &= B_2^2 - 2B_1B_3,\\
s_7 &= B_3^2 - 2B_4B_2,\\
s_8 &= B_4^2.
\end{aligned}
$$

Thus, corresponding to $\lambda = i\omega_0$, where $n = 0, 1, 2, \ldots$, there exists

$$
\tau_{0n} = \frac{1}{\omega_0}\cos^{-1}\left[\frac{s_1\omega^6 + s_2\omega^4 + s_3\omega^2 + s_4}{s_5\omega^6 + s_6\omega^4 + s_7\omega^2 + s_8}\right] + \frac{2n\pi}{\omega_0}. \quad (29)
$$

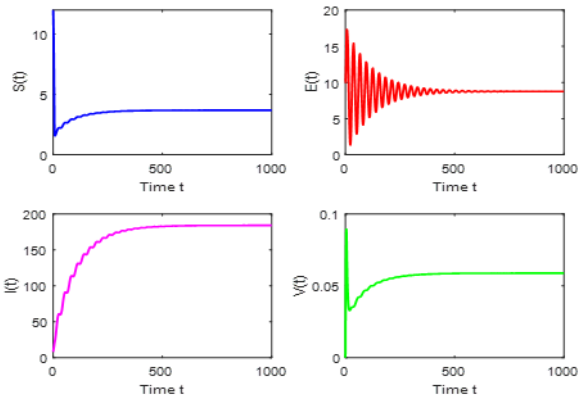


FIGURE 3. Time series analysis of susceptible, exposed, infected, and vaccinated IoT devices in the absence of delay.

Differentiating (16) with respect to τ provides

$$\left(\frac{d\lambda}{d\tau}\right)^{-1} = -\frac{4\lambda^3 + 3A_1\lambda^2 + 2A_2\lambda + A_3}{\lambda(\lambda^4 + A_1\lambda^3 + A_2\lambda^2 + A_3\lambda + A_4)} + \frac{3B_1\lambda^2 + 2B_2\lambda + B_3}{\lambda\left(B_1\lambda^3 + B_2\lambda^2 + B_3\lambda + B_4\right)} - \frac{\tau}{\lambda}$$

$$= -\frac{4\lambda^4 + 3A_1\lambda^3 + 2A_2\lambda^2 + A_3\lambda}{\lambda^2(\lambda^4 + A_1\lambda^3 + A_2\lambda^2 + A_3\lambda + A_4)} + \frac{3B_1\lambda^3 + 2B_2\lambda^2 + B_3\lambda}{\lambda^2\left(B_1\lambda^3 + B_2\lambda^2 + B_3\lambda + B_4\right)} - \frac{\tau}{\lambda}.$$

$$\left(\frac{d\lambda}{d\tau}\right)^{-1} = -\left(\frac{3\lambda^4 + 2A_1\lambda^3 + A_2\lambda^2 - A_4}{\lambda^2(\lambda^4 + A_1\lambda^3 + A_2\lambda^2 + A_3\lambda + A_4)}\right) + \frac{2B_1\lambda^3 + B_2\lambda^2 - B_4}{\lambda^2\left(B_1\lambda^3 + B_2\lambda^2 + B_3\lambda + B_4\right)} - \frac{\tau}{\lambda}.$$

Next,

$$\left(\frac{d\lambda}{d\tau}\right)^{-1} = \left[\frac{(3{\omega_0}^4 - A_2{\omega_0}^2 - A_4) - i2A_1{\omega_0}^3}{{\omega_0}^2({\omega_0}^4 - A_2{\omega_0}^2 + A_4) + i(A_3\omega_0 - A_1{\omega_0}^3)}\right] + \left[\frac{({B_2}{\omega_0}^2 + B_4) + i2B_1{\omega_0}^3}{{\omega_0}^2(B_4 - B_2{\omega_0}^2) + i(B_3\omega_0 - B_1{\omega_0}^3)}\right] - \frac{i\tau}{\omega_0}.$$

$$\mathrm{Re}\left(\frac{d\lambda}{d\tau}\right)^{-1} = \frac{(3{\omega_0}^4 - A_2{\omega_0}^2 - A_4)({\omega_0}^4 - A_2{\omega_0}^2 + A_4)}{{\omega_0}^2({\omega_0}^4 - A_2{\omega_0}^2 + A_4)^2 + (A_3\omega_0 - A_1{\omega_0}^3)^2} + \frac{2A_1{\omega_0}^3(A_3\omega_0 - A_1{\omega_0}^3)}{{\omega_0}^2({\omega_0}^4 - A_2{\omega_0}^2 + A_4)^2 + (A_3\omega_0 - A_1{\omega_0}^3)^2} + \left[\frac{({B_4}^2 - {B_2}^2{\omega_0}^4) + 2B_1{\omega_0}^3(B_3\omega_0 - B_1{\omega_0}^3)}{{\omega_0}^2(B_4 - B_2{\omega_0}^2)^2 + (B_3\omega_0 - B_1{\omega_0}^3)^2}\right].$$

$$\mathrm{Re}\left(\frac{d\lambda}{d\tau}\right)^{-1} > 0.$$

Therefore, the transverse ability conditions hold; hence, Hopf bifurcation occurs at $\tau = \tau_0$.

Theorem 2: If D^* exists with the conditions (18)–(21) and $u = \omega^2$ is a positive root of (27), then $\tau = \tau_0$ exists such that

- D^* is locally asymptotically stable for $0 \le \tau < \tau_0$,
- D^* is unstable for $\tau > \tau_0$, and

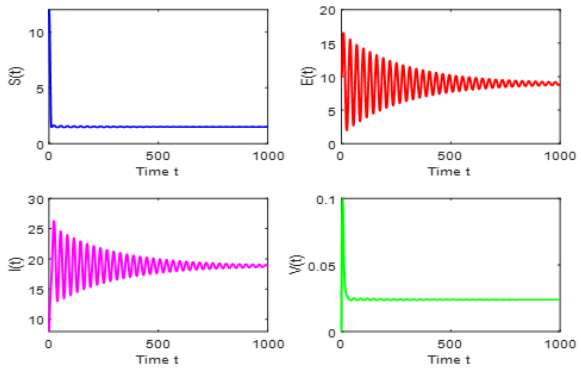


FIGURE 4. Time series analysis of susceptible, exposed, infected, and vaccinated IoT devices with $\tau = 7.96$.

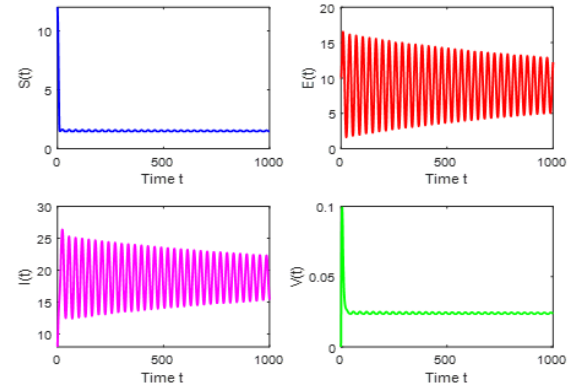


FIGURE 5. Time series analysis of susceptible, exposed, infected, and vaccinated IoT devices with $\tau = 8.243$.

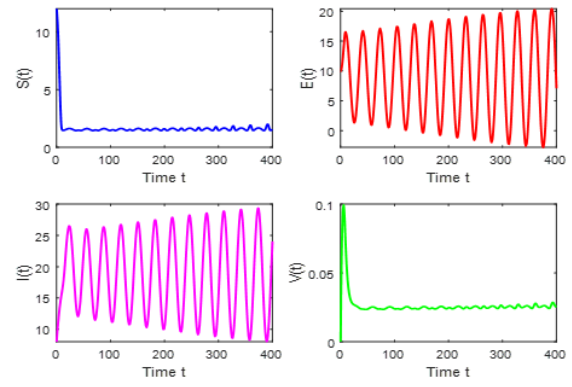


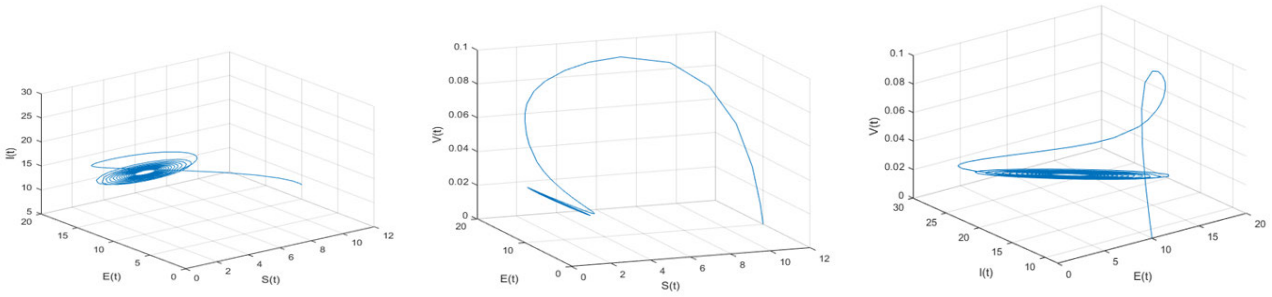
FIGURE 6. Time series analysis of susceptible, exposed, infected, and vaccinated IoT devices with $\tau = 8.5$.

- The system undergoes Hopf bifurcation around D^* at $\tau = \tau_0$, where τ_{0n}, where $n = 0, 1, 2, \ldots$, is equal to

$$\frac{1}{\omega_0}\cos^{-1}\left[\frac{s_1\omega^6 + s_2\omega^4 + s_3\omega^2 - s_4}{s_5\omega^6 + s_6\omega^4 + s_7\omega^2 + s_8}\right] + \frac{2n\pi}{\omega_0}.$$

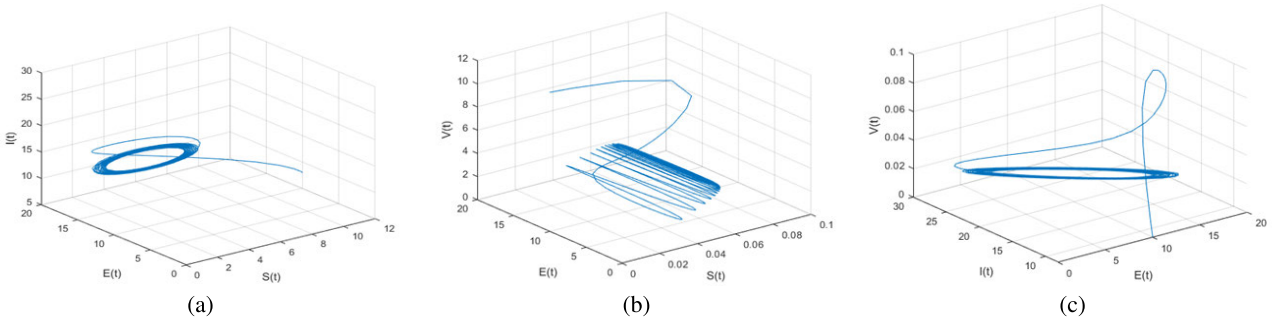
IV. NUMERICAL SIMULATIONS

In this section, we present numerical simulations using MATLAB software to validate the analytical results of this



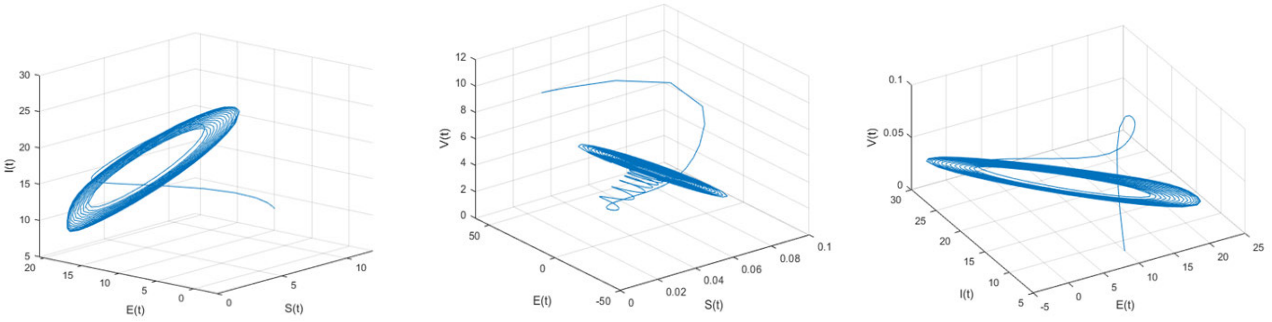
(a) (b) (c)

FIGURE 7. Phase portrait diagrams of devices with $\tau = 7.96$.



(a) (b) (c)

FIGURE 8. Phase portrait diagrams of devices with $\tau = 8.243$.



(a) (b) (c)

FIGURE 9. Phase portrait diagrams of devices with $\tau = 8.5$.

paper. To ensure consistency, we used the values of several attributes in [25] and considered a concomitant anomalous instance of the framework with conditions for the existence of Hopf bifurcations. In particular, the simulation parameters are set up as follows: $A = 2, \alpha = 0.27, \beta = 0.03, \eta = 0.2, \mu = 0.003, c = 0.01, \delta_0 = 0.02, \delta_1 = 0.2, \delta_2 = 0.045$, and $\delta_3 = 0.03$.

Without delays, the intrinsic equilibrium points (1.506, 9.118, 19.16, and 0.023) are locally asymptotically stable, and the corresponding time series are illustrated in Fig. 3. Accordingly, when $\tau = 7.96 < \tau^*$, the intrinsic equilibrium points D^*(1.506, 9.118, 19.16, and 0.023) are locally asymptotically stable in the presence of delays, and the dynamic behavior of the time series is depicted in Fig. 4. The result suggests that the quantity of infected hosts remains relatively low and is predictable. There is still room for new approaches to worm eradication. Fig. 7 shows a projection of the phase portrait of the system as in S-E-I, S-E-V, and E-I-V spaces. In these cases, the spread of computer worms in wireless IoT networks can be easily controlled. The numerical simulation illustrates this property in Fig. 4. Every kind of host is considered stable.

When passes through the critical value, D^*(1.506, 9.118, 19.16, 0.023) will lose its stability and a Hopf bifurcation occurs. Here, a family of periodic solutions bifurcates from equilibrium, which is depicted by the 8.243 minutes long numerical simulation in Fig. 5, with other parameters remaining the same. However, if the time delay is increased until it

reaches the threshold of τ^*, D^* will no longer be stable, and a bifurcation will take place. When $\tau = 8.5 > \tau^*$, Fig. 6 depicts the susceptible, infected, and immunized hosts in the system. This plot graph makes it abundantly evident that the number of infected hosts will explode after a brief period of peace and recur repeatedly but not within the same period, making it difficult to anticipate the number of infected hosts and to build further worm-elimination measures.

Further increasing the delay value $\tau = 8.243 = \tau^*$ causes the framework to experience Hopf bifurcations at unique equilibrium points D^*(1.506, 9.118, 19.16, and 0.023) and bifurcation periods diverging from D^*(1.5006, 9.118, 19.16, and 0.023) are depicted in Fig. 8. The corresponding time series for this case is also provided in Fig. 5, where $\tau = 8.5 > 8.243$ and $\omega_0 = 0.6543$. From Theorem 2, we know the endemic equilibrium point D^*(1.5006, 9.118, 19.16, and 0.023) loses its stability, making it difficult to take measures to control the propagation of worms. The corresponding time series and phase portraits for S-E-I, S-E-V, and E-I-V are illustrated in Figs. 6 and 9.

To observe the impact of time delay, τ is set to a different value while the other parameters stay constancy. Infected hosts are depicted in Fig. 6 at the same coordinate with time delays of $\tau = 0.796$, 8.243, and8.5. The four curves initially overlap, indicating that time delay has no impact during the early stages of worm propagation. The curve starts oscillating as the time delay gets longer. The infecting process becomes unstable when the time delay crosses the threshold τ^*. In the meantime, it has been shown that the number of infected hosts is growing in amplitude and duration.

V. CONCLUDING REMARKS

The use of Internet technology continues to obfuscate the boundaries between the real world and the virtual one, and it is becoming more and more crucial in advancing the integration and penetration of the entire economic and social development. However, as Internet technology is used more widely, threats and difficulties also rise. Particularly, because of their limited battery life and memory space, wireless IoT networks face a serious challenge to network security. The application of wireless IoT networks is tremendously increasing in various domains. Since many domains are unattended in nature, this is more vulnerable towards malicious happenings that lead to various risks and challenges. Hence, there is needed to analyze the nature of the propagation of the malicious codes inside the network. To address this issue, we have investigated a SEIRV model with delay to understand the propagation worms in the network with nonlinear incident rate and ratio-dependent functional response. The results of the proposed model show that it is superior compared to the other models with respect to Hopf-bifurcation and local stability. We found that the nature of worm propagation can be easily controlled when the delay is within the threshold limit and it has been proved that this can be achieved by deferring the existence of Hopf-bifurcation. The future work of the Hopf bifurcation and its stability in wireless IoT fractional model has the potential to describe more complex dynamics than the integer model and can include easily the memory effects presented in many real-world problems.

REFERENCES

[1] R. Geetha, V. Madhusudhan, T. Padmavathy, and A. Lallithasree, "A light weight secure communication scheme for wireless sensor networks," *Wireless Pers. Commun.*, vol. 108, no. 3, pp. 1957–1976, Oct. 2019.

[2] R. Geetha, A. K. Suntheya, and G. U. Srikanth, "Cloud integrated IoT enabled sensor network security: Research issues and solutions," *Wireless Pers. Commun.*, vol. 113, no. 2, pp. 747–771, Jul. 2020.

[3] P. De, Y. Liu, and S. K. Das, "An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 8, no. 3, pp. 413–425, Mar. 2009.

[4] X. Xiao, P. Fu, C. Dou, Q. Li, G. Hu, and S. Xia, "Design and analysis of SEIQR worm propagation model in mobile internet," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 43, pp. 341–350, Feb. 2017.

[5] Q. Zhu, X. Yang, L.-X. Yang, and C. Zhang, "Optimal control of computer virus under a delayed model," *Appl. Math. Comput.*, vol. 218, no. 23, pp. 11613–11619, Aug. 2012.

[6] L. Feng, X. Liao, H. Li, and Q. Han, "Hopf bifurcation analysis of a delayed viral infection model in computer networks," *Math. Comput. Model.*, vol. 56, nos. 7–8, pp. 167–179, Oct. 2012.

[7] V. MadhuSudanan and R. Geetha, "Dynamics of epidemic computer virus spreading model with delays," *Wireless Pers. Commun.*, vol. 115, no. 3, pp. 2047–2061, Dec. 2020.

[8] R. Geetha, V. Madhusudanan, and M. N. Srinivas, "Influence of clamor on the transmission of worms in remote sensor network," *Wireless Pers. Commun.*, vol. 118, no. 1, pp. 461–473, May 2021.

[9] X. Wang and Y. Li, "An improved SIR model for analyzing the dynamics of worm propagation in wireless sensor networks," *Chin. J. Electron.*, vol. 18, no. 1, pp. 8–12, 2009.

[10] B. K. Mishra and N. Keshri, "Mathematical model on the transmission of worms in wireless sensor network," *Appl. Math. Model.*, vol. 37, no. 6, pp. 4103–4111, Mar. 2013.

[11] B. K. Mishra, S. K. Srivastava, and B. K. Mishra, "A quarantine model on the spreading behavior of worms in wireless sensor network," *Trans. IoT Cloud Comput.*, vol. 2, no. 1, pp. 1–12, 2014.

[12] B. K. Mishra and I. Tyagi, "Defending against malicious threats in wireless sensor network: A mathematical model," *Int. J. Inf. Technol. Comput. Sci.*, vol. 6, no. 3, pp. 12–19, Feb. 2014.

[13] L. Feng, L. Song, Q. Zhao, and H. Wang, "Modeling and stability analysis of worm propagation in wireless sensor network," *Math. Problems Eng.*, vol. 2015, pp. 1–8, 2015.

[14] R. P. Ojha, P. K. Srivastava, and G. Sanyal, "Improving wireless sensor networks performance through epidemic model," *Int. J. Electron.*, vol. 106, no. 6, pp. 862–879, Jun. 2019.

[15] J. Liu and Z. Zhang, "Hopf bifurcation of a delayed worm model with two latent periods," *Adv. Difference Equ.*, vol. 2019, no. 1, pp. 1–27, Dec. 2019.

[16] Z. Zhang and T. Zhao, "Bifurcation analysis of an e-SEIARS model with multiple delays for point-to-group worm propagation," *Adv. Difference Equ.*, vol. 2019, no. 1, pp. 1–26, Dec. 2019.

[17] R. K. Upadhyay and S. Kumari, "Discrete and data packet delays as determinants of switching stability in wireless sensor networks," *Appl. Math. Model.*, vol. 72, pp. 513–536, Aug. 2019.

[18] M. T. Signes-Pont, A. Cortés-Castillo, H. Mora-Mora, and J. Szymanski, "Modelling the malware propagation in mobile computer devices," *Comput. Secur.*, vol. 79, pp. 80–93, Nov. 2018.

[19] M. López, A. Peinado, and A. Ortiz, "An extensive validation of a SIR epidemic model to study the propagation of jamming attacks against IoT wireless networks," *Comput. Netw.*, vol. 165, Dec. 2019, Art. no. 106945.

[20] C. Huang, J. Wang, X. Chen, and J. Cao, "Bifurcations in a fractional-order BAM neural network with four different delays," *Neural Netw.*, vol. 141, pp. 344–354, Sep. 2021.

[21] C. Huang, X. Nie, X. Zhao, Q. Song, Z. Tu, M. Xiao, and J. Cao, "Novel bifurcation results for a delayed fractional-order quaternion-valued neural network," *Neural Netw.*, vol. 117, pp. 67–93, Sep. 2019.

[22] C. Xu, M. Liao, P. Li, Y. Guo, and Z. Liu, "Bifurcation properties for fractional order delayed BAM neural networks," *Cognit. Comput.*, vol. 13, pp. 322–356, Jan. 2021.

[23] C. Xu, Z. Liu, M. Liao, and L. Yao, "Theoretical analysis and computer simulations of a fractional order bank data model incorporating two unequal time delays," *Exp. Syst. Appl.*, vol. 199, Aug. 2022, Art. no. 116859.
[24] C. Xu, Z. Liu, C. Aouiti, P. Li, L. Yao, and J. Yan, "New exploration on bifurcation for fractional-order quaternion-valued neural networks involving leakage delays," *Cognit. Neurodynamics*, vol. 16, no. 5, pp. 1233–1248, 2022.
[25] Y. Chu, W. Xia, and Z. Wang, "A delayed computer virus model with nonlinear incidence rate," *Syst. Sci. Control Eng.*, vol. 7, no. 1, pp. 389–406, Jan. 2019.

V. MADHUSUDANAN received the Ph.D. degree from Annamalai University, Chidambaram, in 2017. He has vast teaching and research experience in mathematics and computer science. He is currently an Associate Professor with the Department of Mathematics, S.A. Engineering College. He has published many papers in various reputable national and international journals. His research interests include mathematical modeling, computational intelligence, and control systems.

R. GEETHA received the B.E. degree in computer science and engineering from Madras University, in 1999, the M.E. degree in computer science and engineering from Anna University, in 2006, and the Ph.D. degree from the School of Computing and Information Technology, Vel Tech Rangarajan Dr. Sagunthala Research and Development Institute of Science and Technology, India, in 2017. She has more than 22 years of teaching experience. She is currently a Professor and the Department Head with the S.A. Engineering College. Her research interests include wireless networks and security schemes in wireless networks. She is the author/coauthor of several research papers in international conferences and journals. She is a Life Member of the Indian Society for Technical Education and a member of the Computer Society of India.

B. S. N. MURTHY received the Ph.D. degree in mathematics from JNTUK, Kakinada, in 2018. Since then, he has worked on mathematical modeling and published research papers in many international journals. He is currently a Professor with the Aditya College of Engineering and Technology (ACET), Surampalem, where he is also the Head of the Department of Humanities and Basic Sciences. His research interests include differential equations, delay differential equations, and computational dynamics.

NHU-NGOC DAO (Senior Member, IEEE) received the B.S. degree in electronics and telecommunications from the Posts and Telecommunications Institute of Technology, Hanoi, Vietnam, in 2009, and the M.S. and Ph.D. degrees in computer science from the School of Computer Science and Engineering, Chung-Ang University, Seoul, Republic of Korea, in 2016 and 2019, respectively. He was a Visiting Researcher with the University of Newcastle, NSW, Australia, in 2019, and a Postdoctoral Researcher with the Institute of Computer Science, University of Bern, Switzerland, from 2019 to 2020. He is currently a Lecturer with the Faculty of Computer Science, Ho Chi Minh City Open University (HCMOU), Ho Chi Minh City, Vietnam. His research interests include network softwarization, mobile cloudization, intelligent systems, and the Intelligence of Things. He currently serves as an Editor for *Scientific Reports*.

SUNGRAE CHO received the B.S. and M.S. degrees in electronics engineering from Korea University, Seoul, South Korea, in 1992 and 1994, respectively, and the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2002. He is currently a Professor with the School of Computer Science and Engineering, Chung-Ang University (CAU), Seoul. Before joining CAU, he was an Assistant Professor with the Department of Computer Sciences, Georgia Southern University, Statesboro, GA, USA, from 2003 to 2006, and a Senior Member of the Technical Staff with the Samsung Advanced Institute of Technology (SAIT), Kiheung, South Korea, in 2003. From 1994 to 1996, he was a Research Staff Member with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, South Korea. From 2012 to 2013, he held a visiting professorship with the National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA. His current research interests include wireless networking, ubiquitous computing, and ICT convergence. He has served numerous international conferences as an Organizing Committee Chair, such as the IEEE SECON, ICOIN, ICTC, ICUFN, TridentCom, and IEEE MASS, and a Program Committee Member for IEEE ICC, GLOBECOM, VTC, MobiApps, SENSORNETS, and WINSYS. He has been a Subject Editor of *IET Electronics Letter*, since 2018, and was an Area Editor of *Ad Hoc Networks Journal* (Elsevier), from 2012 to 2017.