Effect of Vaccination in the Computer Network for Distributed Attacks – A Dynamic Model

Yerra Shankar Rao[1], Hemraj Saini[2](✉), Geetanjali Rathee[2](✉), and Tarini Charan Panda[3]

[1] Department of Mathematics, Gandhi Institute of Excellent Technocrats, Bhubaneswar 752054, Odisha, India
sankar.math1@gmail.com

[2] Department of Computer Science and Engineering, Jaypee University of Information Technology, Wakanghat 173234, Himachal Pradesh, India
hemraj1977@yahoo.co.in,
geetanjali.rathee123@gmail.com

[3] Department of Mathematics, Revenshaw University, Cuttack 753003, Odisha, India
tc_panda@yahoo.co.in

Abstract. In this reviewed endeavour, a mathematical model is formulated to assess the spread of a distributed attack over a computer network for critical targeted resources. In this paper a mathematical model is formulated, the two sources susceptible, vaccinated, infected, recovered nanonodes in the target population (e-$S_tV_tI_tR_t$) and susceptible, infected, susceptible nanonodes in the attacking population (e-SIS) epidemic model generated in order to propagate malicious object in the network. Further the analysis of the model has been concentrated upon the basic reproduction number. Where threshold value has effectively examined the stability of the network system. This work is verified for both asymptotical stable, that is the basic reproduction number less than on when the infection free equilibrium express the stability and basic reproduction number is more than one when endemic equilibrium is stable. A very general recognized control mechanism is regarded as vaccination strategy, which is deployed in order to defend the malicious object in the computer network. Finally we examine the effect of vaccination on performance of the controlling strategy of malicious objects in the network. The simulated result produced has become compatible with the overall theoretical analysis.

Keywords: Reproduction number · Stability · Vaccination · Malicious objects · DDoS attack

1 Introduction

In the Modern society the ever growing dependence on computer network is accompanied by ever growing concern about the network vulnerability to information attacks and dependability of existing network security system. Many organizations are well recognized to threats to the society. The attacking agents are like worm, virus, etc. Recently our society has witnessed drastic changes catalyses by cyber world. Presently

© Springer Nature Singapore Pte Ltd. 2019
M. Singh et al. (Eds.): ICACDS 2019, CCIS 1046, pp. 175–184, 2019.
https://doi.org/10.1007/978-981-13-9942-8_17

it is threaten by malevolent things, like worm, viruses etc. Frequent use of electronic mails, floppy disk and internet is facilitating in propagation of spiteful virus in the network. Consider the contagious trait; malicious objects spread their tentacles in many ways. To counter the propagation and its dangerous impact, can observe the positive and negative the characteristic of those harmful objects. There are different types of internet based attack, out of which DDoS attack is dangerous and continuous in the cyber security domain. These type of attack is operated by consuming the resources like memory, network bandwidth [19, 20] etc. paralyzing the target sources and consequently which can no longer provide its service to users. The DDoS operates through the host computer systems to attack the target computers. In 2004 for the first time DDoS attack called Cabir, emerged. It used Bluetooth channel of cell phone to infect other phone by running the Symbian Operating System. It is capable of spreading through infected of mobile phones. It drains out the battery of affected devices by intensive scanning operations and blocking the wireless channels. They have not breached in security as it carries a malicious payload. However security threats over Bluetooth DDoS attack [1, 2] cannot rule out. The moment a DDoS attack affects the cell phone placing bough calls, sending spam mails and taking confidential information stored on the cello phone would be easily. DDoS attack might get upper hand over large number of cell phone in which embed Zombie. The wireless botnets can be used as a deterrent against the DDoS attack on base station, cellular switch, and exact IP address or emergence phone numbers.

Several attempts have been made mathematically to understand and analyze such attacks. It has been verified that the epidemic models are useful methods for understanding the transmission of virus malicious affected network in cyber space domain. The malicious objects can disseminate throughout the network rapidly and they pose serious threat. Continuous quarantine method can immunized against DDoS attack. The term vaccination means to compelled termination of infection. From the physiological aspect, vaccination is supposed to be employing in order to lessen the contamination [3, 4] of human ailments e.g. H1N1, Leprosy, Measles, and Smallpox etc. This perception prominently installed in the cyber domain [24, 28–30]. In particular the highest contaminated nodes are separated out from the system domain till the rehabilitation here.

2 Nomenclatures

S_t: Susceptible compartments of target population
I_t: Infected compartments of target population
V_t: Vaccinated compartment of target population
R_t: Recovered compartments of target populations
S: Susceptible nodes from the attacking population
I: Infected nodes from the attacking population
β: Probability of transmission infection rate from susceptible
γ: The rate coefficients from vaccinated to infected class of target population
ε: The rate coefficients from infected to recovered class in target population.
σ: The rate of coefficients from recovered to susceptible class in target population.
α: The rate coefficients from infected to susceptible class in attacking population

3 Mathematical Model and Assumptions

Consider the entire population of nodes is divided in two sections like attacking population and target population [5, 6]. The preliminary object of the attacker is to find more and more sensitive nodes then it unleash attack the precise target population. As the total number of the target population remains constant, the loss of any nodes due to DDoS attack is considered to be replaced instantly by the supporting nodes. The target population remains constant. The vulnerable hosts work on dual approach: one for attacking target and secondly looking for new hosts to begin the attack [7–10]. The susceptible hosts do not recover permanently and it revolt to susceptible. Whereas the target resource of susceptible compartments will move to vaccination compartment with the help of screening or scanning then moves to infected compartments and after treatment of anti malicious object goes to recovery compartments. As soon as these recovered compartments again start net-surfing or receive suspicions emails or other malware factors are accessed, it again becomes susceptible. The repercussion of such attack on critical infrastructure is anticipated. Therefore the target hosts must have much stronger defence mechanism.

Based on assumption we can total population can categorized in to two groups i.e. attacking population and target population. The target population can be divided in to susceptible, vaccinated, infected, and recovered. As well as the attacking population

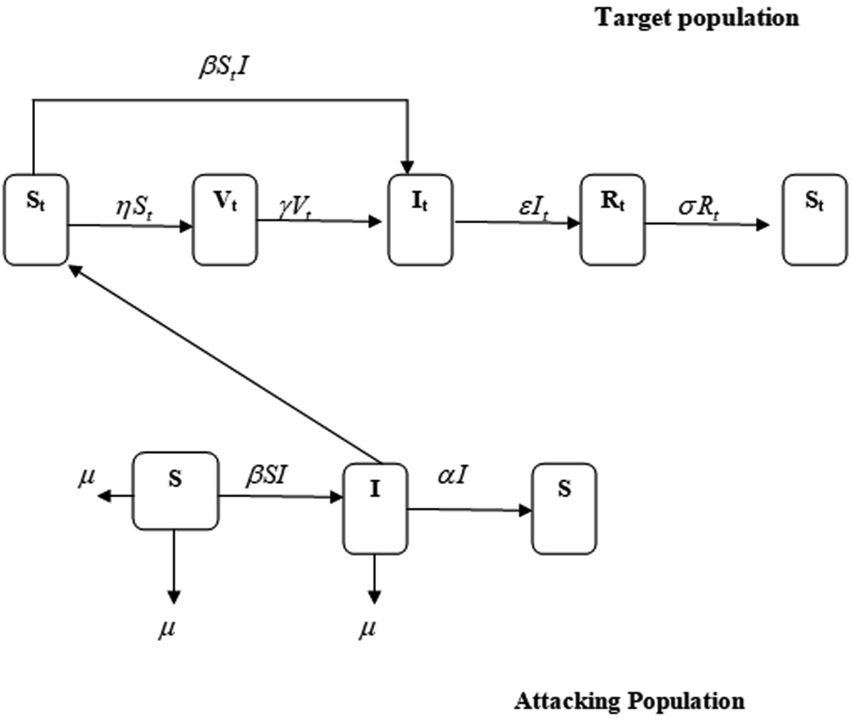

Fig. 1. Schematic diagram for flow of malicious objects in Target/Attacking population

can be categorized into two i.e. either susceptible or infected. The new nodes added in to network is susceptible. Death rate other than attack of malicious objects is constants. The natural death of the nodes as they are once susceptible to any malicious objects decreases. The infectious nodes recover from infection without immunity back to susceptible compartment. Our assumption on transmission of malicious objects in computer network is depicted in Fig. 1.

For the Target population the mathematical model can express as

$$\begin{aligned}
\frac{dS_t}{dt} &= -\beta S_t I - \eta S_t + \sigma R_t \\
\frac{dV_t}{dt} &= \eta S_t - \gamma V_t \\
\frac{dI_t}{dt} &= \beta S_t I + \gamma V - \varepsilon I_t \\
\frac{dR_t}{dt} &= \varepsilon I_t - \sigma R_t
\end{aligned} \tag{1}$$

In similarly for the Attacking population the mathematical model as

$$\begin{aligned}
\frac{dS}{dt} &= \mu - \beta SI - \mu S + \alpha I \\
\frac{dI}{dt} &= \beta SI - \mu I - \alpha I
\end{aligned} \tag{2}$$

Where $S_t + V_t + I_t + R_t = 1$ and $S + I = 1$

The above system of equation can be represented as

$$\begin{aligned}
\frac{dS_t}{dt} &= -\beta S_t I - \eta S_t + \sigma(1 - S_t - V_t - I_t) \\
\frac{dV_t}{dt} &= \eta S_t - \gamma V_t \\
\frac{dI_t}{dt} &= \beta S_t I + \gamma V - \varepsilon I_t \\
\frac{dI}{dt} &= \beta(1 - I)I - \mu I - \alpha I
\end{aligned} \tag{3}$$

When adding all the equations in the model (2) & (3) we have $S_t + V_t + I_t \leq 1$, $I \leq 1$. This inequality satisfies the condition $\lim \sup_{t \to \infty} S_t + V_t + I_t \leq 1, and\, I \leq 1$. Thus system (3) is defined on the closed, positive invariant set.

That can further represented as $D = \{(S_t, I_t, V_t, I) : S_t > 0, V_t > 0, I_t > 0, S_t + V_t + I_t \leq 1 : I \leq 1\}$.

As a results we discuss the stability of the model (3) on the set D.

4 Basic Reproduction Number ($\mathbf{R_0}$)

It is the one of the theoretical foundation of the mathematical epidemiology as well as technological epidemiology. It permits for the classification of e- dynamic model. The stability of the system as well as eradication of the malicious objects depends on basic reproduction number. It gives the behaviour of the model stability and prediction of malicious object spread to some extent [21, 23, 25–27].

So, basic reproduction number can play the vital role in both biological as well as technological attack. So it is defined as the t during its life time a single malicious objects affected computer can produce total susceptible class caused by secondary infection. This can approach by Jones. Here it is calculated by two populations

Basic reproduction number for the target population

$$R_{0t} = \frac{\beta}{\varepsilon}$$

Similarly for the attacking population

$$R_{0a} = \frac{\beta}{(\mu + \alpha)}$$

In the epidemiology the value of basic reproduction can be calculated by taking the geometric mean of the attacking and target population reproduction number. Which can expressed as

$$R_0 = \sqrt{\frac{\beta^2}{\varepsilon(\alpha + \mu)}}$$

5 Stability Analysis

The positive invariant set D has two possible equilibriums. First the infection free equilibrium and second is the endemic equilibrium [11–18]. In this section we discuss the locally stability for infection free equilibrium and endemic equilibrium.

For the infection free equilibrium - $(S_t = 1, I_t = 0, V_t = 0, I = 0)$.

On the set D, endemic equilibrium $(S_t^*, V_t^*, I_t^*, I^*)$ can be achieved by considering all the equation of the system to zero.

$$\begin{aligned} &-\beta S_t I - \eta S_t + \sigma(1 - S_t - V_t - I_t) = 0 \\ &\eta S_t - \gamma V_t = 0 \\ &\beta S_t I + \gamma V - \varepsilon I_t = 0 \\ &\beta(1 - I)I - \mu I - \alpha I = 0 \end{aligned} \tag{4}$$

Solving simultaneously the above equations we have for the endemic state $(S_t^*, V_t^*, I_t^*, I^*)$

$$
\begin{aligned}
S_t^* &= \frac{\varepsilon\gamma\sigma}{[\eta\gamma\sigma - \varepsilon\sigma\eta - (\beta+\eta) - (\mu+\alpha+\sigma)\varepsilon\gamma]}\\
V_t^* &= \frac{\varepsilon\eta\sigma}{\eta\gamma\sigma - \varepsilon\sigma\eta - (\beta+\eta) - (\mu+\alpha+\sigma)\varepsilon\gamma}\\
I_t^* &= \frac{\eta\gamma\sigma}{[\eta\gamma\sigma - \varepsilon\sigma\eta - (\beta+\eta) - (\mu+\alpha+\sigma)\varepsilon\gamma]}\\
I^* &= \frac{\beta-\mu-\alpha}{\beta}
\end{aligned}
$$

Theorem 1
The infection free equilibrium is locally asymptotically locally stable in the region D if $R_{0a} \le 1$. And it is unstable if $R_{0a} > 1$.

Proof: Linearization of the system (3) for $S_t = 1, I_t = 0, V_t = 0, I = 0$

$$
J_{IFE} = \begin{pmatrix} -\eta-\sigma & -\sigma & -\sigma & -\beta \\ 0 & -\gamma & 0 & 0 \\ 0 & 0 & -\varepsilon & 0 \\ 0 & 0 & 0 & \beta-\mu-\alpha \end{pmatrix}
$$

The Eigen values are

$$
\begin{aligned}
\lambda_1 &= -\eta-\sigma\\
\lambda_2 &= -\gamma\\
\lambda_3 &= -\varepsilon\\
\lambda_4 &= \beta-\mu-\alpha
\end{aligned}
$$

Here first three Eigen values are negative and fourth Eigen value is also negative if $\beta-\mu-\alpha < 0$. i.e.

$$
\begin{aligned}
&\beta < \mu+\alpha\\
&R_{0a} < 1
\end{aligned}
$$

Hence the infection free equilibrium is locally asymptotical stable in the region D.
While $R_{0a} > 1$, which means $\beta > \mu+\alpha$. So $\lambda_4 > 0$. Therefore the infection free equilibrium is unstable.

Theorem 2
For the endemic equilibrium is asymptotically stable in the region D when $R_{0a} > 1$.

Proof
Linearization of the model about the endemic equilibrium $(S_t^*, V_t^*, I_t^*, I^*)$

$$J_{EE} = \begin{pmatrix} -\beta I^* - \eta - \sigma & -\sigma & -\sigma & -\beta S_t^* \\ \eta & -\gamma & 0 & 0 \\ \beta I^* & \gamma & -\varepsilon & 0 \\ 0 & 0 & 0 & -2\beta I^* - \mu - \alpha \end{pmatrix}$$

Solving we get the Eigen values

$$\lambda_1 = -2\beta I^* - \mu - \alpha$$

The other three Eigen values can be obtained by solving

$$\lambda^3 + A\lambda^2 + B\lambda + C = 0$$

Where

$$\begin{aligned} A &= \beta I^* + \eta + \sigma + \gamma + \varepsilon \\ B &= \sigma\eta + (\beta I^* + \eta + \sigma)\gamma + (\beta I^* + \eta + \sigma)\varepsilon + \gamma\varepsilon - \sigma\beta I^* \\ C &= (\beta I^* + \eta + \sigma)\varepsilon\gamma + \sigma\eta\varepsilon + \sigma\eta\gamma - \sigma\gamma\beta I^* \end{aligned}$$

Where A, B and C are positive when $R_{0a} > 1$.

Furthermore $AB > C$.

Hence, by Routh-Hurtwitz condition [22] the endemic equilibrium is locally asymptotically stable.

6 Numerical Simulations

The Fig. 2 using the different parameter, we can obtained that the basic reproduction number for attacking population is below the unity the malicious object gradually eliminated. Which is agree with the Theorem 1. This figure also clearly explain that spread of malicious objects is depressive, which consists with the analysis of theory. Lastly the infected nodes will vanishes and reached the recovered level.

Similarly the Fig. 3 using the different parameters remains unchanged, we can seen that the basic reproduction number for attacking population is above the unity, the all the nodes are maintain positive values between the range. Which indicates the malicious objects does not vanish if the objects are initially present. Hence finally theses state reaches their endemic equilibrium point. It agrees with the Theorem 2. This is consistent and asymptotical stable. To reveal the effect of partial vaccination rate on infected nodes. So, we give the partial vaccination, which all the nodes get vaccinated. However, in the real world network, as a result, we expected the use of vaccination process, the rate of spread malicious objects slowly down and decrees the infected nodes in the network.

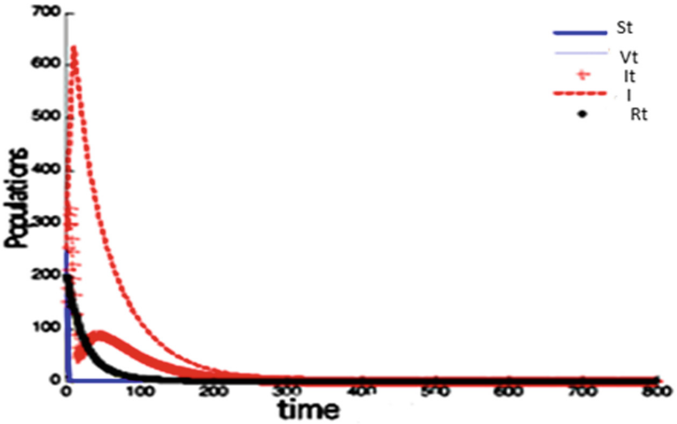

Fig. 2. Dynamic behaviour of the model for infection free equilibrium ($R_{0a} \leq 1$)

In order to simulate the behaviour of spread of the malicious objects the parameters in the experiments are practical values for dies the malicious object in the computer network in real life. Here by using the Range kutta fourth and fifth order to solve the system of ordinary differential equation with the help of MATLAB. Here by applying the MATLAB we can observe the behaviour of different nodes with respect to time. This simulated result agrees with the real life situation.

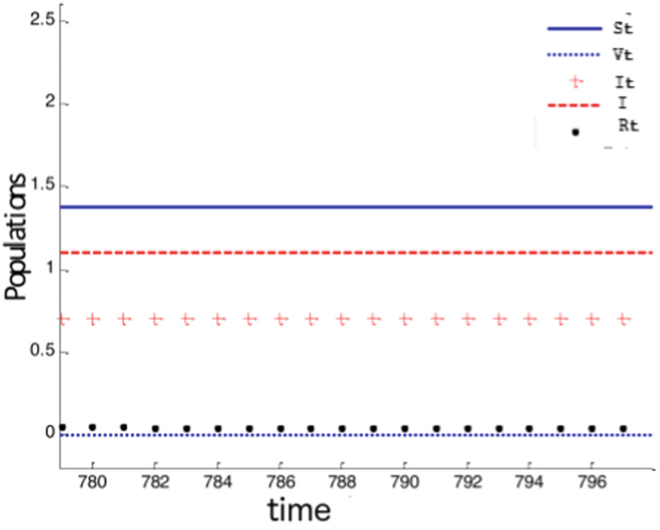

Fig. 3. Dynamic behaviour of the model for endemic equilibrium ($R_{0a} > 1$)

7 Conclusion

The aim of this work is to model the malicious object control in the network. It also finds out the particular workable means of controlling the spread of malicious object in the network. Here a dynamic two population e-epidemic model has been generated for the transmission of the malicious object in the network. The investigation over the dynamic behaviour of the specified model with partial immunizations has been systematically expressed. The derivation of the basic reproduction number which determines the worm extinguished has been solidified. Again the fact behind basic reproduction number is that it exclusively depends on the stability of the system. Considering the consequence of the analysis the infection free equilibrium as well as endemic equilibrium which are locally asymptotically stable have become confirmed. The defence measure i.e. vaccination (filter, scanning) against malicious object in the network has been successfully deployed. Latest version of antivirus with latest signature has made the DDoS attack minimum in the network. The numerical simulation results have optimistically explained the positive impact of increasing the security of DDoS attack. We imagine that our analysis can provide a quantity of close into malicious object counter measure. In the real world, the result can supportive to antivirus companies on related organization to make cost useful countermeasure to work well. Finally the foremost future endeavour will be verifying the model in scale free network. And it can be extended to time delay parameter.

References

1. Gan, C., Xiaofan, Y., Qingyi, Z., Li, H.: The spread of computer virus under external computers. Nonlinear Dyn. **73**(3), 1615–1620 (2013)
2. Gelenbe, E., Gellman, M., Loukas, G.: Defending networks against denial-of-service attacks. In: Unmanned/Unattended Sensors and Sensor Networks, vol. 5611, pp. 233–244. International Society for Optics and Photonics (2004)
3. Li, M.Y., Graef, J.R., Wang, L., Karsai, J.: Global dynamics of an SEIR model with a varying total population size. Math. Biosci. **160**, 191–213 (1999)
4. Kermac, W.O., McKendrick, A.G.: Contribution of mathematical theory to epidemic. Proc. R. Soc. Lond. Ser. Contain. Pap. Math. Phys. Character **14**(843), 94–122 (1933)
5. Haldar, K., Mishra, B.K.: A mathematical model for the distributed attack on the target resources in the computer network. Commun. Nonlinear Sci. Simul. **19**, 3149–3160 (2014)
6. Mishra, B.K., Haldar, K.: e-epidemic models on attack and defence of malicious objects in networks, theories and simulations of complex social system. In: Dabbaghian, V., Mago, V. (eds.) Theories and Simulations of Complex Social Systems. Intelligent System Reference Library, vol. 52, pp. 117–143. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-39149-1_9
7. Song, X., Chen, L.: Optimal harvesting and stability for two species competitive system with stage structure. Math. Biosci. **170**, 173–186 (2001)
8. Toutonji, O., Yoo, S.M.: Passive benign worm propagation modelling with dynamic quarantine defence. KSII Trans. Internet Inf. Syst. **3**(1), 96–107 (2009)
9. Mishra, B.K.: Jha, N: SEIORS model for the transmission of malicious objects in computer network. Appl. Math. Model. **34**, 710–715 (2010)

10. Wang, L., Li, M.Y.: A criteria for stability of matrices. Math. Anal. Appl. **225**, 249–264 (1998)
11. Dagon, D., Zou, C., Lee, W.: Modelling bonnet propagation using time zones. In: Proceedings of 13th Network and Distributed System Security Symposium NDSS, vol. 6, pp. 2–13 (2006)
12. Bailey, N.: The mathematical theory of epidemic. Wiley, New York (1957)
13. LaSalle, J.: The Stability of Dynamical Systems. Regional to Conference Series in Applied Mathematics. SIAM, Philadelphia (1976)
14. Mishra, B.K., Pandey, S.K.: Dynamic model of worms with vertical transmission in computer network. Appl. Math. Comput. **217**, 8438–8446 (2011)
15. Rao, Y.S., Rauta, A.K., Saini, H., Panda, T.C.: Mathematical model for the cyber attack in the computer network. Int. J. Bus. Data Commun. Netw. **13**(1), 58–65 (2017). https://doi.org/10.4018/ijbdcn.2017010105
16. Nayak, P.K., Rao, Y.S., Panda, T.C.: Calculation of basic reproduction number by graph reduction method and stability analysis in SEIQRS E epidemic model in computer network. J. Eng. Appl. Sci. **12**(23), 7332–7338 (2017)
17. Rauta, A.K., Rao, Y.S., Panda, T.C., Saini, H.: A probabilistic approach using poisson process for detecting the existence of unknown computer virus in real time. Int. J. Eng. Sci. **4**, 47–51 (2015)
18. Rao, Y.S., Rauta, A.K., Saini, H., Panda, T.C.: Influence of educational qualification on different types of cyber crime: a statistical interpretation. Indian J. Sci. Technol. **9**(32), 1–7 (2016)
19. Saini, H., Rao, Y.S., Panda, T.C.: Cyber-crimes and their impacts: a review. Int. J. Eng. Res. Appl. **2**, 202–209 (2012)
20. Liu, X., Takeuchi, Y.: SVIR epidemic model with vaccination strategies. J. Theor. Biol. **253**, 1–11 (2008)
21. Driessche, P.V.D., Watmough, J.: Reproduction numbers and sub threshold endemic equilibria for compartmental models of diseases transmission. Math. Biosci. **180**, 29–48 (2002)
22. Routh-Hurwitz Criterion. http://web.abo.fi/fak/mnf/mate/kurser/dynsyst/2009/R-hcriteria.pdf
23. Kribs-Zaleta, C., Velasco-Hernandez, J.: A simple vaccination model with multiple endemic states. Math. Biosci. **164**, 183–201 (2000)
24. Gan, C., Yang, X., Liu, W., Zhu, Q., Zhang, X.: An epidemic model of computer viruses with vaccination and generalized nonlinear incidence rate. Appl. Math. Comput. **222**, 265–274 (2013)
25. Anwar, S.: Wireless nanosensor networks: a basic review. Int. J. Emerg. Technol. Adv. Eng. **5**(12), 151–154 (2015)
26. Mishra, B.K., Tyagi, I.: Defending against malicious threats in wireless sensor network: a mathematical model. Int. J. Inf. Technol. Comput. Sci. **6**, 12–19 (2014)
27. Peng, M., Mou, H.: A novel computer virus model and its stability. J. Netw. **9**, 367–374 (2014)
28. Yang, L.X., Yang, X., Tang, Y.Y.: A bi-virus competing spreading model with generic infection rates. IEEE Trans. Netw. Sci. Eng. **5**, 2–13 (2018)
29. Zheng, R., Lu, W., Xu, S.: Preventive and reactive cyber defense dynamics is globally stable. IEEE Trans. Netw. Sci. Eng. **5**, 156–170 (2018)
30. Yang, L.X., Li, P., Yang, X., Wu, Y., Tang, Y.Y.: On the competition of two conflicting messages. Nonlinear Dyn. **91**, 1853–1869 (2018)