Mathematical Model on Distributed Denial of Service Attack in the Computer Network

YERRA SHANKAR RAO[1], ASWIN KUMAR RAUTA[2*], SATYA NARAYAN KUND[3],
BHAGIRATHI SETHI[4], JANGYADATTA BEHERA[5]
[1]Department of Mathematics, NIST (Autonomous) College,
Berhampur - 761008, Odisha,
INDIA

[2]Department of Mathematics, SKCG (Autonomous) College,
Paralakhemundi-761200, Odisha,
INDIA

[3]Controller of Examinations, Berhampur University,
Berhampur -760007, Odisha,
INDIA

[4]Department of Mathematics, Khemundi Degree College,
Digapahandi- 761012, Odisha,
INDIA

[5]Department of Mathematics, Roland Engineering College,
Berhampur- 761008, Odisha,
INDIA

**Corresponding Author*

Abstract: - In this paper, an electronic- epidemic two-folded mathematical model is formulated with help of non-linear ordinary differential equations. Distributed Denial of Service (DDoS) attacks in the computer network are studied. The modeling of both attacking nodes and targeting nodes is performed. Botnet based malicious devices and their threats on computer networks are addressed using appropriate parameters. The basic reproduction numbers for both the attacking and the targeting population are calculated and interpreted. Local and global stability analysis is carried out for the infection-free and endemic equilibrium points. Differential equations are solved with the help of the Runge-Kutta 4th order numerical method and graphs are analyzed using MATLAB software. Simulation shows that the success or failure depends on the number of initially infected computers in the attacking group. The proposed model exhibits the phenomenon of backward bifurcation for different values of transmission parameters. This model gives the theoretical base for controlling and predicting the DDoS attack. This shows the way to minimize the attack in the network. This study will be helpful to identify the botnet devices and run the latest version of antivirus in the network to protect against DDoS attacks from attacking sources. The application of this study is to ascertain online crime and locate the attacking nodes in the field of online transactions of real-life problems that involve the internet and computer networking systems. Moreover, our model can play an important role in policy-making against the distributed attack.

Key-Words: - Basic Reproduction Number, Bifurcation, Cyber-Crime, DDoS attack, Eigen Value, Malware, Mathematical Modeling, Simulation, Stability Analysis, Virus.

Received: July 23, 2022. Revised: September 15, 2023. Accepted: November 8, 2023. Published: December 31, 2023.

1 Introduction

The computer connects every person in the world, controlling their daily business through internet networking or browsing. The development of internet technology has thrown a number of challenges in the form of necessity in day-to-day life. Digital technology has brought a big change in the society. But, it is being the heaven of crimes using computer networks by the trained intelligentsia. The new type of such crime called cybercrime. It is a current research topic for the investigators. Many researchers have studied, [1], [2], [3], [4], [5], [6], [7], [8], this new crime using mathematical modeling. Among different types of internet-based crimes, the Denial of Service (DoS) attack is one of them. This attack is a very critical and continuous threat to cyber security. DoS is a cyber-attack in which cybercriminals search network resources or an IP address or machine from thousands of hosts infected with malware to make it unavailable to the intended users by interrupting the services indefinitely. It is done by notification of superficial requests when the computer of the user is turned on in an attempt to prevent some or all legal services from being fulfilled or slow down the system to hamper the services. When the DoS attack originates from many different sources, it is called a Distributed Denial of Service (DDoS) attack. So, it is difficult to locate the error and may not be possible to block the source of the attack. The DoS attacks are targeted by consuming resources, and forcing a computer to reset. e.g., network bandwidth, CPU cycles memory, etc. so that the network does not work properly that leads to the site. If someone uses the same connection for internal software, employees notice slowness issues. The TTL (time to live) on a ping request timed out and the victim's server responds with service outages. DDoS attacks can last as long as 24 hours and the cost of business is minimized while the user remains under attack. In this attack different kits like Stacheldraht, Trinoo, Mstream, Tribe Flood Network (TFN), etc. are launched to other computers by DDoS attackers. DDoS attacks are performed in two ways; (i) the crafted packets are sent to crash a system that causes a reboot or freezing of some operating system. (ii) Exhausted the resources like operating system, data structures, computing power, network bandwidth etc. of the targeted computer. Due to DDoS attacks, the quality of service is disabled or interrupted to the intended users. It is tedious work to deal with the second form of attack rather than the first form of attack. A botnet is the usual medium of DDoS attacks. Intelligent criminals make a network of computers called BOTNET to launch an effective DDoS attack. The people who control a botnet are called botnet owners or botnet masters. The software applications that are programmed to run automatically according to their instruction without users needing to start them are known as zombies or bots. The source of the botnet is called the control server. The most effective methods to control, respond, and prevent the spread of DDoS attacks are updating the operating system, data mining, firewall, auto patching, etc. To reduce transmission of botnet infective nodes, buy more bandwidth, build redundancy into your infrastructure, configure your network hardware against DDoS attacks, deploy anti-DDoS hardware and software modules, and deploy a DDoS protection appliance and DNS servers. The visitor's information could be stolen using the attacks. They are often used to make 'political' statements against the targeted organization or just as a form of malicious vandalism. For example, the criminals demand a ransom amount from the website owners to stop the attack. So, it is an emerging attention for the researchers to investigate and locate the attacking sources. Many authors have presented their investigation reports in this regard for locating the attacking node and providing the security system to the network, [9], [10], [11], [12]. The connection to the internet increases the complexity of interconnected networks. Mathematical modeling is used as a tool to identify and understand the problem of DDoS attacks. In order to provide better defense mechanisms, many researchers have used epidemic models. Dynamic models for infectious diseases are mostly based on compartment structures that were initially proposed for several areas of Mathematical Biology, [13], [14], [15]. It was developed later by many other mathematicians in the modeling of cybercrimes or computer related malicious objects. These epidemic models are dynamic in nature. Therefore, transmission of malicious objects is epidemic in nature. So, many mathematical models have been developed that specify the comprehensible view of attacking behavior as well as the spread of the malware objects in the network, [16], [17], [18], [19], [20], [21], [22], [23]. The use of vaccination and quarantine effects were studied for the DDoS attack and spread of malware in the computer network, [24], [25], [26], [27], [28]. Presently, this type of cybercrime is a new, global issue and draws serious attention. But currently, less study has been conducted in this field. Therefore, we have developed this model to formulate the attacking

nodes and targeted nodes for finding the basic reproduction number, and investigated the stability analysis to control DDoS attacks through analysis, simulation, and interpretation of data obtained from different sources.

2 Formulation of Mathematical Model and Assumptions

The whole population is divided into two sections namely attacking and targeting populations. The entire targeted system is divided into four compartments: Susceptible (S_t), Exposed (E_t), Infected (I_t), and Recovered (R_t) classes. Similarly, the attacking nodes are divided into two classes Susceptible (S), and Infected (I). Once the malicious objects enter into the network, the susceptible nodes of the targeted group after some time become exposed (E_t) at the rate $\beta>0$, and then it gets infectious (I_t) at the rate $\alpha>0$. Again, after running the anti-malicious software at the rate $\gamma>0$, infected nodes get recovered (R_t). The rate at which the recovered population becomes susceptible is taken as $\varepsilon_t>0$. Each susceptible node for attacking and targeted nodes becomes infected at the rate $\beta>0$. The model takes essential dynamics in each of the attacking nodes born or dies at the rate $\mu>0$. The rate at which infected classes become susceptible in the attacking network is taken as 'ε'. Based on these assumptions we have developed an e-epidemic mode as shown in the schematic diagram.

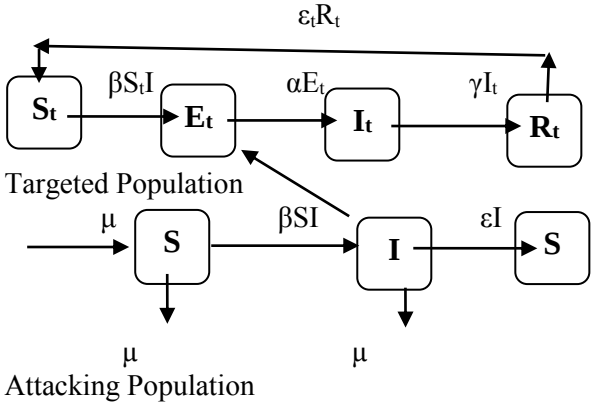

Fig. 1: Compartmental Model for Targeted Population and Attacking Population.

Using the schematic diagram in Figure 1, the rate of change of each class size is given by the set of ordinary differential equations (ODEs):

The targeted classes have the following ODEs

$$\begin{aligned}\frac{dS_t}{dt} &= -\beta S_t I + \varepsilon_t R_t \\ \frac{dE_t}{dt} &= \beta S_t I - \alpha E_t \\ \frac{dI_t}{dt} &= \alpha E_t - \gamma I_t \\ \frac{dR_t}{dt} &= \gamma I_t - \varepsilon_t R_t\end{aligned} \tag{1}$$

The attacking classes are governed by the following ODEs.

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

Here, the entire population of targeted compartment is assumed as one unit i.e., $S_t(t) + E_t(t) + I_t(t) + R_t(t) = 1$ .The entire population of attacking class is also assumed as one unit i.e., $S + I = 1$

The reduced form of above equations is;

$$\begin{aligned}\frac{dS_t}{dt} &= -\beta S_t I + \varepsilon_t(1 - S_t - E_t - I_t) \\ \frac{dE_t}{dt} &= \beta S_t I - \alpha E_t \\ \frac{dI_t}{dt} &= \alpha E_t - \gamma I_t \\ \frac{dI}{dt} &= \beta(1 - I - \varepsilon - \mu)I\end{aligned} \tag{3}$$

Where, $S_t \geq 0, E_t \geq 0, I_t \geq 0,$
$I \geq 0, S_t + E_t + I_t \leq 1$ and $I \leq 1$

3 Calculation and Interpretation of Basic Reproduction Number and Equilibrium Points

Basic reproduction number is an important threshold quantity that play a significant role in epidemiology. It is defined as the average number of secondary infections in a susceptible class produced by a single infectious device during the whole infection period. Two basic reproduction numbers are derived for two types of populations.
The basic reproduction number of the targeted population is derived as;

$$R_{0t} = \frac{\beta}{(\alpha + \gamma)} \tag{4}$$

Similarly, the basic reproduction number of the attacking population is calculated as;

$$R_{0a} = \frac{\beta}{(\varepsilon + \mu)} \tag{5}$$

The single basic reproduction number for the entire system is defined as the geometric mean of equations (4) and (5) which is,

$$R_0 = \sqrt{\frac{\beta^2}{(\varepsilon + \mu)(\alpha + \gamma)}} \tag{6}$$

In this article, it is observed that the basic reproduction number for the attacking population determines the overall risk of the attack on the targeted group. The basic reproduction number of the targeting population determines the effectiveness of attack and infection of the system.

Theorem-1:
System (2) is infection-free equilibrium in the region and admits the endemic equilibrium in the given region.

Proof
Consider the right-hand side of equations with zero to obtain the attack-free equilibrium points.

$$\begin{aligned} -\beta S_t I + \varepsilon_t (1 - S_t - E_t - I_t) &= 0 \\ \beta S_t I - \alpha E_t &= 0 \\ \alpha E_t - \gamma I_t &= 0 \\ \beta(1 - I) I - \varepsilon I - \mu I &= 0 \end{aligned} \tag{7}$$

For, attack free, we get I=0, E=0, R=0.

Therefore, S=S_0

After solving the above equations simultaneously, we get the endemic equilibrium point for the attack to be persisting.

$$\begin{aligned} S_t^* &= \frac{\alpha\gamma\varepsilon}{\alpha\beta\gamma + \beta\varepsilon\gamma + \alpha\beta\varepsilon - \alpha\gamma\mu - \varepsilon^2\mu - \varepsilon\mu\gamma - \alpha\mu\varepsilon} \\ E_t^* &= \frac{\gamma\varepsilon(\beta - \mu - \varepsilon)}{\alpha\beta\gamma + \beta\varepsilon\gamma + \alpha\beta\varepsilon - \alpha\gamma\mu - \varepsilon^2\mu - \varepsilon\mu\gamma - \alpha\mu\varepsilon} \\ I_t^* &= \frac{\alpha\varepsilon(\beta - \mu - \varepsilon)}{\alpha\beta\gamma + \beta\varepsilon\gamma + \alpha\beta\varepsilon - \alpha\gamma\mu - \varepsilon^2\mu - \varepsilon\mu\gamma - \alpha\mu\varepsilon} \\ I^* &= \frac{\beta - \varepsilon - \mu}{\beta} \end{aligned} \tag{8}$$

Theorem-2
The system (6) is locally asymptotically stable at attacking free equilibrium in the given region if $R_{0a} \le 1$ and it is unstable when $R_{0a} > 1$.

Proof
Linearization of the system (3) around the infection free equilibrium point (1, 0,0,0), the Jacobian Matrix is $J_{IFE} = \begin{pmatrix} -\varepsilon_t & -\varepsilon_t & -\varepsilon_t & 0 \\ 0 & -\alpha & 0 & 0 \\ 0 & \alpha & -\gamma & 0 \\ 0 & 0 & 0 & \beta - \varepsilon - \mu \end{pmatrix}$

Therefore, the characteristic roots are given by,

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

when $\beta \le (\varepsilon + \mu) \Rightarrow \frac{\beta}{(\varepsilon + \mu)} \le 1$, i.e. $R_{0a} \le 1$.

As all the eigen values have negative real parts at infection free equilibrium point, so by Routh-Hurwitz criteria, the system is locally asymptotically stable for $R_{0a} \le 1$ and is unstable when $R_{0a} > 1$ i.e. $\beta > (\varepsilon + \mu)$.

Theorem-3
The system is local asymptotically stable at the endemic equilibrium point when $R_{0a} > 1$.

Proof:
Linearization of (3) at the endemic equilibrium, we get the following Jacobian Matrix

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

One of the Eigen values is given by

$$\begin{aligned} \lambda_1 &= -2\beta I^* + \beta - (\varepsilon + \mu) \\ &= -(2\beta I^* - (\beta - \varepsilon - \mu)) \end{aligned}$$

If $\beta > \varepsilon + \mu$ or $R_{0a} > 1$,i.e., $-(\beta - \varepsilon - \mu) < 0$,then λ_1 is negative.
Other eigen values are also determined from the following cubic equation;

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

Where, $A = \alpha + \gamma + \beta I^* + \varepsilon_t > 0$

$$B = \alpha\beta I^* + \gamma\beta I^* + \alpha\varepsilon_t + \varepsilon_t\gamma + \varepsilon_t\beta I^* + \alpha\gamma > 0$$

$$C = \alpha\beta\gamma I^* + \alpha\varepsilon_t\gamma + \varepsilon_t\beta I^*\gamma - \alpha\beta I^* > 0$$

Therefore, AB>C
Again, as per Routh-Hurwitz stability criteria, the system is local asymptotically stable.

4 Global Stabilities for Infection-Free Equilibrium

Theorem-4
The system is globally asymptotically stable for $R_{oa} < 1$ and is unstable when $R_{oa}>1$ at the infection-free equilibrium point.

Proof: Consider a Lyapunov function, [29], [30], [31], as

$$V = E_t + I_t + I$$

$$\frac{dV}{dt} = \beta S_t I - \alpha E_t + \alpha E_t - \gamma I_t + \beta(1-I)I - (\varepsilon+\mu)I$$

$$= \beta S_t I - \gamma I_t + \beta(1-I)I - (\varepsilon+\mu)I$$

$$= \beta S_t I - \gamma I_t + (\beta - \varepsilon - \mu)I - I^2$$

$$= \beta S_t I - \gamma I_t - I^2 + \frac{1}{(\varepsilon+\mu)}(\frac{\beta}{\varepsilon+\mu} - 1)I$$

$$= \beta S_t I - \gamma I_t - I^2 + \frac{1}{(\varepsilon+\mu)}(R_{0a} - 1)I$$

If $R_{0a} \le 1$, then $\frac{dV}{dt} \le 0$

Using LaSalle's maximum invariant principle, it is globally asymptotically stable at the infection-free equilibrium point for $R_{0a} \le 1$.

5 Numerical Simulation and Discussion

In this research, the differential equations are solved using Runge-Kutta 4th order method and numerical simulations are carried out by MATLAB software in support of theoretical analysis discussed in the previous section. Some parameters can be used for infection-free equilibrium. The basic reproduction number depends on the values of contact rate β. Further, it is seen that if we increase the contact rate β then increase the infection that leads to more infection of the network, and the system remains unstable. Thus, if the recovery rate is higher from the attack, then the system remains stable. The graphs are plotted for initial values of St=0.8585, E_t=0.4718, I_t=0.1415, S=0.1847, I=0.1888 when $R_{0a}>1$ and initial values S_t=1000, E_t=0.2773, I_t=0, S=0.1754, I=0 when $R_{0a}<1$. The interpretations of the numerical results are discussed below.

5.1 Dynamic Behaviour of Nodes with Respect to Times when $R_{0a}>1$

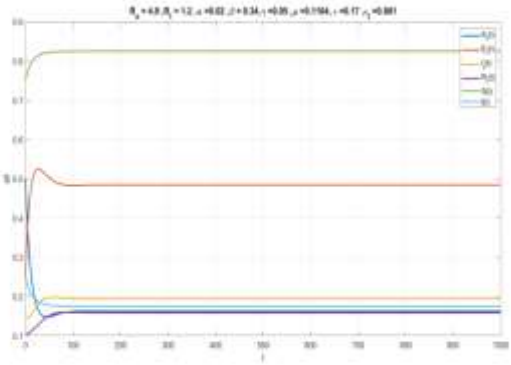

Fig. 2: All nodes versus time graph when R_a = 4.9, R_t=1.2.

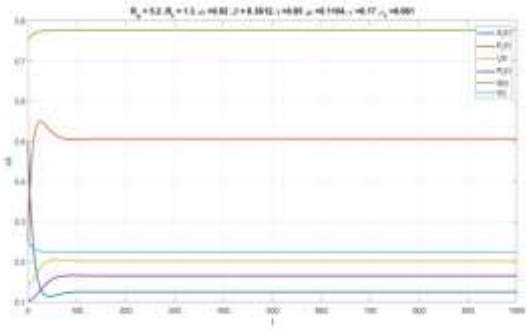

Fig. 3: All nodes versus time graph when R_a=5.2,R_t=1.3.

When the basic reproduction number $R_{0a} > 1$, then I increase to a peak and S decreases for time being then I decrease for endemicity. Figure 2 and Figure 3 explain that all the nodes S_t, E_t, I_t, R_t ,S and I approach to its steady state values as time goes to infinity for $R_{0a}>1$, due to being endemic in nature.

5.2 Dynamic Behaviour of Nodes with Respect to Times when $R_{0a}<1$

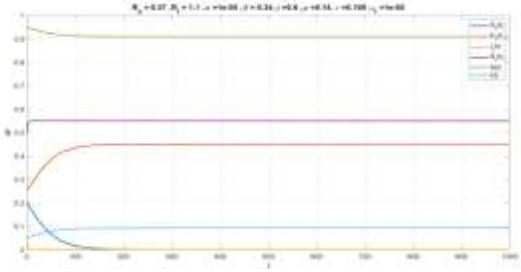

Fig. 4: All nodes versus time graph when R_a = 0.57, R_t=1.1.

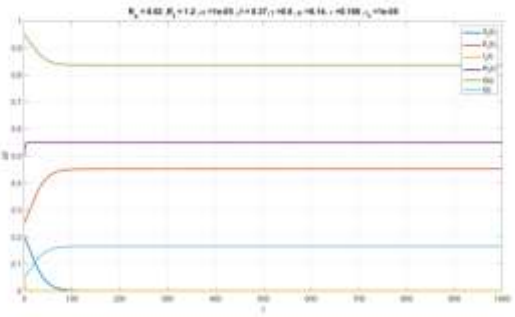

Fig. 5: All nodes versus time graph when R_a = 0.62, R_t =1.2.

When the basic reproduction number $R_{0a} \leq 1$ i.e. when an infective computer replaces itself with less than one new infective node, then the attack dies out. It indicates that the susceptible class goes to its full capacity because each system becomes susceptible when the attack will disappear. So, in Figure 4 and Figure 5; S_t E_t, I_t, R_t ,S and I approach to steady state as time goes to infinity for R_{0a}<1.

5.3 Effect of Susceptible Nodes with Infective Nodes of Targeting Population

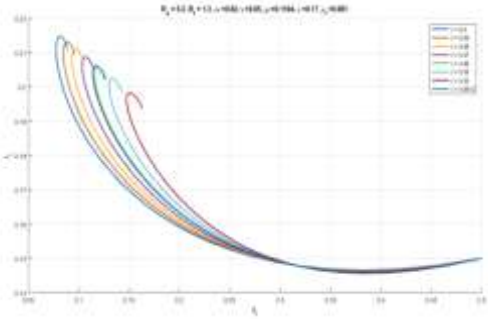

Fig. 6: Targeted susceptible node versus targeted infective node phase plane analysis graph when R_a =5.2, Rt=1.3.

If, the basic reproduction number $R_{0a} > 1$ i.e. the attack is persisting, infective class 'I' will increase first then decrease just as for an epidemic. Therefore, the susceptible class slowly starts to increase due to the installation of anti DDoS devices or new updated anti-malware software. As time evolutions, the susceptible class reaches large enough, and again due to new attacks every time, there is a possibility of a second smaller epidemic. Continuing in this process, we will get the path spirals approaching to the equilibrium point and trajectories that appear to be asymptotically stable to the endemic equilibrium point that is shown in Figure 6.

5.4 Bifurcation Diagram of the Model

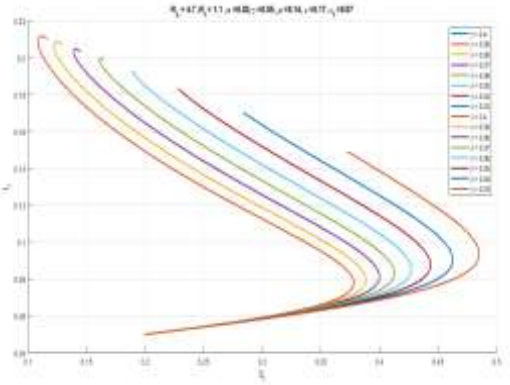

Fig. 7: Targeted susceptible node versus targeted infective node phase plane analysis graph when R_a =4.7, Rt=1. 1.

The model with DDoS protection appliances under certain conditions admit the backward bifurcation. A backward bifurcation is predicted when the targeted group is prevented from DDoS attack.

Figure 7 exhibits the coexistence of two stable equilibriums of model form $R_{0a} \leq 1$. If there is no recovery case then bifurcation is reversed. As infected computers are recovered every time due to protection against DDoS attack, that shows a backward bifurcation and sign of epidemic control.

6 Conclusion

In this study, we have presented a dynamic model to control DDoS attacks in the computer network by considering two sections. We started by showing a nonnegative solution to the model. We proved both infection free equilibrium points to be locally and globally asymptotically stable. It is observed that, if the basic reproduction number $R_{0a} > 1$ then attack would continue. Similarly, if $R_{0a} \leq 1$ then the attacking population would die out. The success and failure of the attack is demonstrated graphically. Due to the latent time between attacking susceptible and infectious nodes, the model is more appropriate for DDoS attacks. The attacking population of DDoS attacks is very high approximately, when antivirus software is not run at regular intervals of time. These simulated results supported by the theoretical approach show the malicious objects died out or persisted.

In the stability analysis of the model, it is shown that the attack dies out whenever R_0<1. Figure 2 to Figure 5 exhibit that the susceptible

class remains at a steady state as time continues. This indicates that the susceptible class is stable. It is also interpreted from the figures that the susceptible class, and recovered class remain the same if no new infected cases arise in the later stage. That is, as long as a new infected case does not occur, then the size of the susceptible compartment remains the same as the total population.

The future scope of this study may be the extension of the model by considering more parameters. This study may also be extended by including more compartments like quarantine compartments to ascertain the global cyber threat and provide security in the network. In addition to this, the model can be used for modeling of contagious diseases in the biological systems in real-life problems.

References:

[1] S.Siva Saravana Babu, G.Saravanakumar, Naveen V M, Ajitesh Kumar A S B, Koushik P H, Carolyne Sneha, & Bhuvaneswari. A DDoS Attack Categorization and Prediction Method Based on Machine Learning. *Journal of Population Therapeutics and Clinical Pharmacology*, *30*(9), 2023, 300–307. https://doi.org/10.47750/jptcp.2023.30.09.030.

[2] U, Rahamathullah and E, Karthikeyan, Distributed Denial of Service Attacks Prevention, Detection and Mitigation – A Review. *Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021*), Available at May-2021, http://dx.doi.org/10.2139/ssrn.3852902.

[3] X. Liu, J. Ren, H. He, B. Zhang, C. Song, and Y. Wang, ‘‘A Fast All-Packets Based DDoS Attack Detection Approach Based on Network Graph And Graph Kernel,’’ *J. Netw. Comput. Appl.*, vol. 185, Jul. 2021, Art. no. 103079.

[4] Yerra Shankar Rao, Ajit Kumar Keshri, Bimal Kumar Mishra, Tarini Charana Panda, Distributed Denial of Service Attack on Targeted Resources in a Computer Network for Critical Infrastructure: A Differential e-Epidemic Model, *Physica A: Statistical Mechanics and its Applications*, Volume 540, 2020, 123240, https://doi.org/10.1016/j.physa.2019.123240.

[5] Yerra Shankar Rao, Hemraj Saini, Geetanjali Rath , Tarini Charan Panda, Effect of Vaccination in the Computer Network for Distributed Attacks - *A Dynamic Model, Advances in Computing and Data Sciences*, 2019, pp. 175-184. Switzerland AG, Springer Nature.

[6] Z. Li, H. Jin, D. Zou, B. Yuan, Exploring New Opportunities to Defeat Low-Rate DDoS Attack in Container-Based Cloud Environment, *IEEE Transactions on Parallel and Distributed Systems* 31 (3) ,2020, 695–706, https://doi.org/10.1109/TPDS.2019.2942591.

[7] Zargar, S. T., Joshi, J., & Tipper, D. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials*, 15,2013 (4), 2046–2069.

[8] Zhang, Z., Si, F. Dynamics of a Delayed SEIRS-V Model on the Transmission of Worms in a Wireless Sensor Network. *Adv. Differential Equation*. 2014, -295.

[9] Mishra, B. K., & Jha, N., SEIQRS Model for the Transmission of Malicious Objects in a Computer Network. *Applied Mathematical Modelling*, 34 ,2010, 710–715.

[10] R. Biswas, S. Kim, J. Wu, Sampling Rate Distribution for Flow Monitoring and DDoS Detection in Datacentre, *IEEE Transactions on Information Forensics and Security* 16 2021 2524–2534, https://doi.org/10.1109/TIFS.2021.3054522.

[11] Yerra Shankar Rao, Rauta A.K., Saini Hemraj., Panda.,T.C., Mathematical Model for Cyber-attack in the Computer Network, *International Journal of Business Data Communications and networking*, 13(1)2017,58-65.

[12] S.J. Wang, Q.M. Liu, X.F. Yu, Y. Ma, Bifurcation Analysis of a Model for Network Worm Propagation with Time Delay, *Mathematical and Computer Modelling* 52(3–4),2010,435–447.

[13] Kermack, W. O., & McKendrick, A. G. Contributions of Mathematical Theory to Epidemics. *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, 115, 1927, 700–721.

[14] Kermack, W. O., & McKendrick, A. G. Contributions of Mathematical Theory to Epidemics, *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, 138,1932, 55–83.

[15] Kermack, W. O., & McKendrick, A. G. Contributions of Mathematical Theory to Epidemics. *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, 141, 1933, 94–122.

[16] Ahmad, A.; Abuhour, Y.; Alghanim, F. A Novel Model for Distributed Denial of Service Attack Analysis and Interactivity. *Symmetry* 2021, *13*, 2443. https://doi.org/10.3390/sym13122443.

[17] Bimal Kumar Mishra, Ajit Kumar Keshri, Dheeresh Kumar Mallick, and Binay Kumar Mishra, Mathematical Model on Distributed Denial of Service Attack Through Internet of Things in a Network, *Nonlinear Engineering* 2018, pp.1-10.

[18] C. Gan, X. Yang, W. Liu, Q. Zhu, J. Jin, L. He, Propagation of Computer Virus Both Across the Internet and External Computer: A Complex Network Approach, *Communication of Nonlinear Sci. Numer.Simul.,* 19(8), 2014, 2785–2792.

[19] C. Gan, X. Yang, Q. Zhu, J. Jin, L. He, The Spread of Computer Viruses Under the Effect of External Computers, *Nonlinear Dynamic*, 73, 2013, 1615–1620.

[20] J. P. Salle, The Stability of Dynamical System, *SIAM*, Philadelphia, PA , 1976.

[21] Juan Fernando Balarezo, Song Wang, Karina Gomez Chavez, Akram Al-Hourani, Sitham paranathan Kandeepan, A Survey on DoS/DDoS Attacks Mathematical Modeling for Traditional, *SDN and virtual networks, Engineering Science and Technology, an International Journal*, Volume 31, 2022, 101065, , https://doi.org/10.1016/j.jestch.2021.09.011.

[22] K. Mishra and K. Halder, e-Epidemic Models on the Attack and Defense of Malicious Objects in Networks, Theories and Simulations of Complex Social Systems, *Intelligent Systems Reference Library 52, Springer-Verlag Berlin Heidelberg*, 2014.

[23] K.S. Sahoo, B.K. Tripathy, K. Naik, S. Rama Subba Reddy, B. Balusamy, M. Khari, D. Burgos, An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks, *IEEE Access* 8 ,2020, https://doi.org/10.1109/ACCESS.2020.3009733.

[24] L. X. Yang, X. Yang, and Y. Y. Tang, A Bi-virus Competing Spreading Model with Generic Infection Rates, *IEEE Transactions on Network Science and Engineering*, 2017.

[25] L.X. Yang, X. Yang,Q. Zhu, L.We, A Computer Virus Model with Graded Cure Rates, *Nonlinear Anal. Real World* Appl. 14, 2013, 414–422.

[26] L.Yang, X.Yang, The Effect of Infected External Computers on the Spread of Viruses, A Compartment Model Study, *Physica A* 392, 2013, 6523–6525.

[27] Liu, X., Yang, X., & Lu, Y, To Filter or to Authorize: Network-Layer DoS Defense Against Multimillion-Node Botnets. *In ACM SIGCOMM computer communication review*, 38, 2008, (4), pp. 195–206). New York: ACM.

[28] Liu, Z.; Wang, Y.; Feng, F.; Liu, Y.; Li, Z.; Shan, Y., A DDoS Detection Method Based on Feature Engineering and Machine Learning in Software-Defined Networks. *Sensors* 2023, *23*, 6176. https://doi.org/10.3390/s23136176.

[29] A.M. Lyapunov, The General Problem of the Stability of Motion, *Taylor and Francis*, London, 1992.

[30] Korobeinikon,G.C. Wake, Lyapunov Functions and Global Stability for SIR, SIRS, and SIS Epidemiological Models, *Appl. Math. Lett*. 15 ,2002, 955–960.

[31] Korobeinikov, Lyapunov Functions and Global Properties for SEIR and SEIS Epidemic Models, *Math. Med. Biol*. 21, 2004, 75–83.

Nomenclatures:

St - Number of Susceptible Targeted nodes.
E_t - Number of Exposed Targeted nodes.
It - Number of Infected Targeted nodes.
R_t - Number of Recovered targeted nodes.
S - Number of Susceptible attacking nodes.
I - Number of Infected attacking nodes.
β - Rate of contact both attacking and targeted nodes.
α - Rate of contact from exposed to infected targeted nodes.
γ - Rate of recovered from infected to recovered in targeted nodes.
ε_t - Rate at which from recovered to Susceptible targeted nodes.
μ- Rate of death and newborn in attacking compartment.
ε - Infection rate in the attacking class.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

- Yerra Shankar Rao has carried out the formulation of the problem, derived the mathematical equations and proved the theorems.
- Aswin Kumar Rauta has executed the experiment, organized the manuscript, analyzed and interpreted the results. He has also acted as corresponding author.
- Satya Narayan Kund envisaged the theme of research and motivated for the investigation.
- Bhagirathi Sethi verified the calculated results and was responsible for the literature review.
- Jangyadatta Behera has implemented the computer software MATLAB for numerical simulation and plotted the graphs.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study

Conflict of Interest

The authors have no conflicts of interest to declare.