Preprints of Control Conference Africa 2024
Balaclava, Mauritius, 16-17 September 2024

Transcritical and Hopf Bifurcation Analysis of Cyberattacks in Software-Defined Networking

B. O. S. Biaou * **A. O. Oluwatope** † **B. S. Ogundare** ‡

* *Comnet Laboratory, Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria (e-mail: bsbiaou@pg-student.oauife.edu.ng).*
† *Comnet Laboratory, Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria (e-mail: aoluwato@oauife.edu.ng)*
‡ *Department of Mathematics, Obafemi Awolowo University, Ile-Ife, Nigeria (e-mail: bogunda@oauife.edu.ng)*

Abstract: This research work examines the dynamics of cyberattacks using the lenses of transcritical and Hopf bifurcations in Software-Defined Networking (SDN) systems. The motivation of this research is to determine the bifurcation points that are crucial to evaluate the different movements of the cyberattacks in the network system. The bifurcation points can then be used to create an effective mitigation plans for better security of SDN. We examine the circumstances surrounding these bifurcations and how they affect the resilience and stability of SDN systems. The efficiency of these tactics is illustrated by numerical modeling in Anaconda, which adds to the understanding of the dynamics of cyberattacks in SDN systems, especially with regard to transcritical and Hopf bifurcations.

Keywords: Transcritical and Hopf Bifurcation, Cyberattacks and Software-Defined Networking.

1. INTRODUCTION

The rapid propagation of many Cyberattacks presents a serious danger to the flexibility of services via networks. Many types of cyberattacks such as SQL Injection Attacks, malware, Botnet, Distributed Denial of Service (DDoS), Cross-Site Scripting (XSS), Probe, User-to-Root attack (U2R), Zero-Day Exploits, Web attack and many more are disrupting the emerging technologies such as IoT, SDN, 5G technology, Edge computing, Blockchain, quantum computing, Cloud Computing, Big Data, AI and machine learning.

The primary goal of any cyberattack is to disrupt the operation of systems, networks, or services (Alasali and Dakkak, 2023). The Cyberattackers attempt to bring down a target infrastructure by exploiting security vulnerability inherent in the information and communication infrastructure for online services. Their soul aim is to overwhelm the online services' processors with traffics, and eventually render them unavailable to legitimate users (Acarali et al., 2022). By upsetting services, attackers have the potential to cause financial losses, reputation damage, and operational disruptions to any computer infrastructure (Abhishta et al., 2020). The SDN is a computing infrastructure that uses software-based application programming interfaces (APIs) or controllers to interconnect with fundamental hardware structure and direct traffic on a network. Fundamentally, Software-Defined Networking (SDN) divides the control plane of the network from the data plane, enabling centralized network management and dynamic network setup using software (Biaou et al., 2022). As the SDN is separated into three levels, there may be a need for regular communication between entities that may be dispersed throughout the network. As a result, SDN offers attackers more potential sites of attack than conventional networks as illustrated in Figure 1 (Shu et al., 2016). In the figure, the authors have highlighted six possible attack points in the SDN architecture as listed below.

(1) The SDN switch (2) The links between SDN switches (3) The SDN Controller (4) The links between the controller and the switches (5) The links between controllers (6) The application software.

We attempt to investigate cyberattacks in SDN using a variant of the epidemic model known as VIS based on four additional assumptions. They are i.) the possibility that a node may depart from SDN networks for reasons unrelated to cyberattacks; ii.) the model allows nodes to join or leave the network at any time, representing an open-population system. iii.) The model classifies all nodes as susceptible, infected, or secured. iv.) The model incorporates the rate at which nodes may disconnect from the system.

In this paper, the VIS is modeled in an open-populated epidemic framework to analyse the conditions for the equilibrium points at attacks-free and attacks-prone. Conversely, the circumstances surrounding the transcritical and Hopf bifurcations are analysed. Finally, an analysis is conducted to determine the transcritical and Hopf bifurcations points

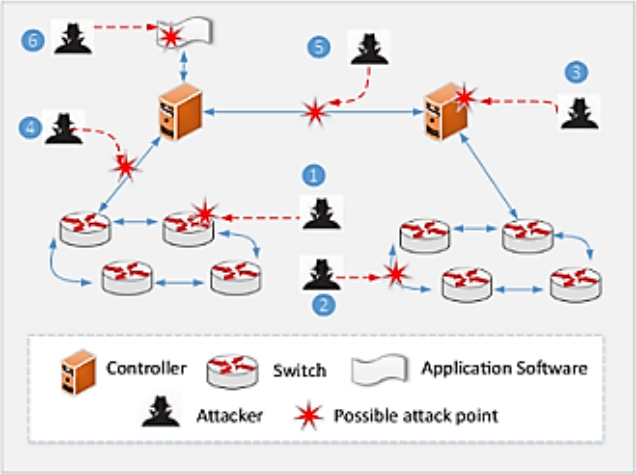

Figure 1. Cyberattacks in SDN Paradigm (Shu et al., 2016)

that are crucial to evaluate the different movements of the cyberattacks in SDN.

2. REVIEW OF RELATED WORKS

Several related works have been consecrated to different types of cyberattacks including epidemic approach ((Wang et al., 2017), (Nashat et al., 2021), (Mahboubi et al., 2017), (Mishra and Saini, 2017), (Yerra et al., 2017), (Androulidakis et al., 2016) and (Yan and Liu, 2006)). That being said, each of these strategies has addressed the impacts of the cyberattacks in networks. However, some shortcomings have been found in the existing epidemic models which have been applied to analyse cyberattacks in Software-Defined Networking (SDN). The shortcomings include the close-population of nodes, the failure to consider the possibility of a node leaving the network for reasons unrelated to the attacks and the failure to consider major parameters and assumptions related to network environment. Therefore, there is still the need to review analysis of cyberattacks in SDN using the redesigned epidemic model. In this research work, we have redesigned an existing epidemic framework founded on the model assumptions listed in the introduction section. Thus, in order to address the propagation of cyberattacks in a network, a number of previous publications have taken the epidemic approach into consideration such as SIS (susceptible, infected, susceptible), SEIR (susceptible, exposed, infected, recovered) and SEIRS (susceptible, exposed, infected, recovered, susceptible).

The authors in the papers (Mishra and Saini, 2017) and (Yerra et al., 2017) developed a SEIRS model to analyse the rate of attacks in a computer network. Yet, this model did not account for the possibility of nodes leaving the network for reasons unrelated to the attacks. The SEIR model in (Androulidakis et al., 2016) and (Ajbar and Algahtani, 2020) was suggested to demonstrate the rapid spread of the attacks over networks. However, the authors considered a closed-population, meaning no new nodes could join the network during the analysis period. Even though, the hopf bifurcation was evaluated in (Ajbar and Algahtani, 2020) respectively. The reviews (Wang et al., 2017), (Nashat et al., 2021), and (Mahboubi et al., 2017) engaged a SIS epidemic model to examine the movement of attacks in networks. Although, the SIS is most used, it is inadequate as it has not consider the real case circumstances in networks in which all the connected devices could be categorised as susceptible, infected and secured. The SIR model for Hopf bifurcation evaluation was proposed in (Wang and Chen (2016), Balamuralitharan and Radha (2018) and Ireri et al., 2020). The common limitation is based on failure to consider major parameters and assumptions in network environment. The SEIRV developed in (Mahata et al., 2022) introduced the concept of vaccination with the evaluation of the Hopf bifurcation analysis in epidemic fields.

3. MATHEMATICAL MODELING

3.1 Presentation of the Proposed Model

The epidemic model serves as a fundamental mathematical framework for analyzing the spread of viruses within a static community. In the context of the cyberattacks, a proposed framework denoted VIS (Vulnerable, Infected, and Secured) is proposed to elucidate the temporal dynamics of the cyberattacks propagation. The model comprises three distinct classes of nodes: vulnerable (**V**), representing nodes yet unaffected by cyberattacks; infected (**I**), denoting nodes currently under attack; and secured (**S**), indicating nodes that have recovered from previous attacks and vulnerable to future attacks.

Transitions between these compartments occur at varying rates: δ governs the transition from vulnerable to infected and φ dictates the shift from infected to secured. The VIS model is characterized by an open population rate (Y), allowing for unrestricted node input and output, with no migration from secured to vulnerable.

Furthermore, the disconnection rate (α) is uniform across all compartments, signifying the likelihood of node removal from the system. In the infected class, nodes face an additional disconnection rate (β) attributable to the attack's impact. The VIS epidemic model's schematic, elucidating the dynamics of the cyberattack propagation within SDN is presented in Figure 2.

3.2 Mathematical Model of VIS

The corresponding ordinary differential equations (ODEs) governing the proposed VIS epidemic model are depicted in system (1).

$$\begin{cases} \dfrac{dV}{dt} = Y - \delta V I - \alpha V \\ \dfrac{dI}{dt} = \delta V I - \varphi S - \beta I - \alpha I \\ \dfrac{dS}{dt} = \varphi I - \alpha S \end{cases} \tag{1}$$

Let (**T**) be the viable point for the proposed VIS. Then, (**T**) is given by

$T = \{(V, I, S) \in R^3 : V > 0, I \geq 0, S \geq 0\}$

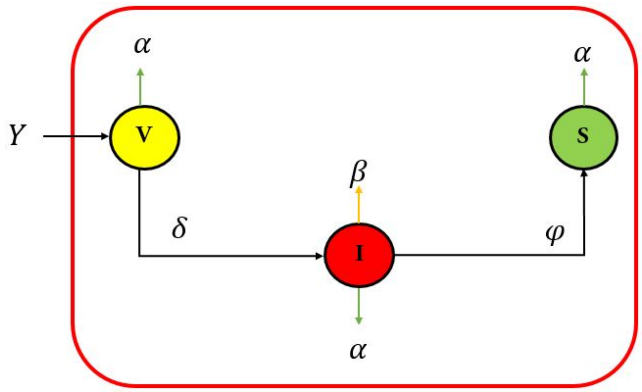

Figure 2. Proposed VIS Model

3.3 Equilibrium Points

Each equation in the system (1) will be equal to zero to determine the equilibrium points (**E**) of the model.

For $E = (V, I, S) \in \Omega$ and $\frac{dV}{dt} = \frac{dI}{dt} = \frac{dS}{dt} = 0$ We get:

$$\begin{cases} Y - \delta VI - \alpha V = 0 \\ \delta VI - \varphi S - \beta I - \alpha I = 0 \\ \varphi I - \alpha S = 0 \end{cases} \tag{2}$$

4. TRANSCRITICAL BIFURCATION OF THE MODEL

In this section, we determine the sufficient conditions for the transcritical bifurcation of the model. However, a transcritical bifurcation arises when the stability of the attack-free equilibrium point undergoes a shift as a parameter surpasses a critical threshold, leading to the interchange of stability between two separate equilibrium points.

4.1 Attacks-free Equilibrium

The attack-free equilibrium point is the location of non-appearance of attack in Software-Defined Networking.

Let E° represents the attack-free equilibrium $E^\circ(V^\circ, I^\circ, S^\circ)$ in R^3.

So,

$$\begin{cases} Y - \delta V^\circ I^\circ - \alpha V^\circ = 0 \\ \delta V^\circ I^\circ - \varphi S^\circ - \beta I^\circ - \alpha I^\circ = 0 \\ \varphi I^\circ - \alpha S^\circ = 0 \end{cases} \tag{3}$$

Without attack, we definitely have $I^\circ = 0$.

Therefore, the system (3) can be written

$$\begin{cases} V^\circ = \dfrac{Y}{\alpha} \\ I^\circ = 0 \\ S^\circ = 0 \end{cases} \tag{4}$$

Consequently, the proposed VIS is without attack at

$$E^\bullet = (V^\circ, I^\circ, S^\circ) = (\frac{Y}{\alpha}, 0, 0) \tag{5}$$

4.2 Eigenvalues of the Attacks-free equilibrium

When a linear transformation is applied to a vector, the scalar values are known as eigenvalues. The eigenvalues therefore, indicate the scaling factor that causes the vector to be expanded or contracted.

So, for

$$\begin{cases} \dfrac{dV}{dt} = Y - \alpha V - \delta VI = 0 \\ \dfrac{dI}{dt} = \delta IV - (\beta I + \alpha)I - \varphi S = 0 \\ \dfrac{dS}{dt} = \varphi I - \alpha S = 0 \end{cases} \tag{6}$$

Let J be the Jacobian Matrix of the system (6).

$$J^\bullet = \begin{pmatrix} -\alpha & -\delta V^\circ & 0 \\ \delta I^\circ & -(\beta + \alpha) & -\varphi \\ 0 & \varphi & -\alpha \end{pmatrix}$$

The Jacobian matrix is obtained by solving the determinant of $|J^\circ - I\psi| = 0$.

$$\begin{cases} -\alpha - \psi_V = 0 \\ -(\beta + \alpha) - \psi_I = 0 \\ -\alpha - \psi_S = 0 \end{cases} \tag{7}$$

Then,

$$\begin{cases} \psi_V = -\alpha \\ \psi_I = -(\beta + \alpha) \\ \psi_S = -\alpha \end{cases} \tag{8}$$

Therefore, the three eigenvalues are listed below.

$\psi_V = -\alpha, \psi_I = -(\beta + \alpha)$ and $\psi_S = -\alpha$

4.3 Eigen Vector of the Attacks-free equilibrium

The Eigenvectors are nonzero vectors that correspond to certain eigenvalues and stay in the same direction but can be expanded or shortened by a linear transformation.

So, from the above obtained Jacobian matrix, we get

$$\begin{pmatrix} -\alpha & -\delta V^\circ & 0 \\ \delta I^\circ & -(\beta + \alpha) & -\varphi \\ 0 & \varphi & -\alpha \end{pmatrix} \begin{pmatrix} T_V \\ T_I \\ T_S \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Then,

$$\begin{cases} -\alpha T_V - \delta V^{\circ} T_I = 0 \\ \delta I^{\circ} T_V - (\beta+\alpha) T_I - \varphi T_S = 0 \\ \varphi T_I - \alpha T_S = 0 \end{cases} \tag{9}$$

Hence,

$$\begin{cases} T_V = \dfrac{-\delta V^{\circ} T_I}{\alpha} \\ T_I = \dfrac{\delta I^{\circ} T_V - \varphi T_S}{\beta+\alpha} \\ T_S = \dfrac{\varphi T_I}{\alpha} \end{cases} \tag{10}$$

Let $T_S = \Psi$. Then $\varphi T_I = \alpha\Psi$.

By replacing $T_S = \Psi$ in the equation (10), we get

$$\begin{cases} T_V = \dfrac{-\delta V^{\circ}\Psi}{\varphi} \\ T_I = \dfrac{\alpha\Psi}{\varphi} \\ T_S = \Psi \end{cases} \tag{11}$$

Then, the eigenvector is:

$$W^{\circ}(w_V, w_I, w_S) = \Psi \begin{pmatrix} \frac{-\delta V^{\circ}}{\varphi} \\ \frac{\alpha}{\varphi} \\ 1 \end{pmatrix}$$

Where

$w_V = \frac{-\delta V^{\circ}\Psi}{\varphi}$, $w_I = \frac{\alpha\Psi}{\varphi}$ and $w_S = \Psi$

4.4 Attacks-Prone Equilibrium

Here, we determine the necessary conditions for the model's endemic equilibrium where $I^* \neq 0$.

We have

$$\begin{cases} Y - \delta V^* I^* - \alpha V^* = 0 \\ \delta V^* I^* - \varphi S^* - \beta I^* - \alpha I^* = 0 \\ \varphi I^* - \alpha S^* = 0 \end{cases} \tag{12}$$

Then,

$$\begin{cases} V^* = \dfrac{\alpha(\delta Y - \varphi^2 - \alpha\beta - \alpha^2)}{\delta(\varphi^2 + \alpha\beta + \alpha)} \\ I^* = \dfrac{\varphi(\delta Y - \varphi^2 - \alpha\beta - \alpha^2)}{\delta(\varphi^2 + \alpha\beta + \alpha)} \\ S^* = \dfrac{Y(\varphi^2 + \alpha\beta + \alpha)}{\beta\alpha^2 + \alpha\delta Y - \alpha\beta} \end{cases} \tag{13}$$

Thereafter,

$$\begin{cases} V^* = \dfrac{Y}{\delta I^* + \alpha} \\ I^* = \dfrac{\varphi(\delta Y - \varphi^2 - \alpha\beta - \alpha^2)}{\delta(\varphi^2 + \alpha\beta + \alpha)} \\ S^* = \dfrac{\varphi I^*}{\alpha} \end{cases} \tag{14}$$

Therefore, the model is prone of attacks at

$E^* = (V^*, I^*, S^*)$

$$E^* = \left(\frac{Y}{\delta I^* + \alpha}, \frac{\varphi(\delta Y - \varphi^2 - \alpha\beta - \alpha^2)}{\delta(\varphi^2 + \alpha\beta + \alpha)}, \frac{\varphi I^*}{\alpha}\right) \tag{15}$$

4.5 Eigen Vector of the Attacks-prone equilibrium

The eigenvector of the attacks-prone equilibrium point is determined by the transposition of the Jacobian matrix (J^T) such as:

$$\begin{pmatrix} -\alpha & \delta I^* & 0 \\ -\delta V^* & -(\beta+\alpha) & \varphi \\ 0 & -\varphi & -\alpha \end{pmatrix} \begin{pmatrix} h_V \\ h_I \\ h_S \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Then,

$$\begin{cases} -\alpha h_V + \delta I^* h_I = 0 \\ -\delta V^* h_V - (\beta+\alpha) h_I + \varphi h_S = 0 \\ -\varphi h_I - \alpha h_S = 0 \end{cases} \tag{16}$$

Therefore,

$$\begin{cases} h_V = \dfrac{\delta I^* h_I}{\alpha} \\ h_I = \dfrac{-\alpha h_S}{\varphi} \\ h_S = \dfrac{\delta V^* h_V + (\beta+\alpha) h_I}{\varphi} \end{cases} \tag{17}$$

Let $h_I = \Phi$. Then $-\alpha h_S = \varphi\Phi$.

By replacing $h_I = \Phi$ into the equation (17), we get,

$$\begin{cases} h_V = \dfrac{\delta I^*\Phi}{\alpha} \\ h_I = \Phi \\ h_S = \dfrac{\varphi\Phi}{\alpha} \end{cases} \tag{18}$$

Then, the eigen vector is:

$$W^{\circ}(h_V, h_I, h_S) = \Phi \begin{pmatrix} \frac{\delta I^*}{\alpha} \\ 1 \\ \frac{\varphi}{\alpha} \end{pmatrix}$$

Where $h_V = \frac{\delta I^*\Phi}{\alpha}$, $h_I = \Phi$ and $h_S = \frac{\varphi\Phi}{\alpha}$

Thereafter, to determine either the transcritical bifurcation occurs at disease free equilibrium, the system (1) can be written as in a vector form $\frac{dX}{dt} = f(x)$

$X = (V, I, S)$ and $f(f_1, f_2, f_3)^T$ with $f_i = i = 1, 2, 3$ then determine $\frac{df}{d\delta} = f_\delta$

We obtain

$$f_\delta = \begin{pmatrix} -VI \\ VI \\ 0 \end{pmatrix}$$

Then, at the attacks-free equilibrium point, we obtain:

$$f_\delta(E^\circ, \delta) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$h^T.f_\delta(E^\circ, \delta) = 0$

$$Df_\delta(E^\circ, \delta) = \begin{pmatrix} 0 & -V^\circ & 0 \\ 0 & V^\circ & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$h^T.[Df_\delta(E^\circ, \delta).Z] = \Omega \neq 0$

Where

$$\Omega = \Phi \begin{pmatrix} \frac{\delta I^*}{\alpha} \\ 1 \\ \frac{\varphi}{\alpha} \end{pmatrix}^T . \begin{pmatrix} 0 & -V^\circ & 0 \\ 0 & V^\circ & 0 \\ 0 & 0 & 0 \end{pmatrix} .Z$$

The transcritical bifurcation has occurred in disease-free equilibrium when the parameter δ passes over the bifurcation value δ^*, according to the Sotomayor Theorem (Balamuralitharan and Radha, 2018).

5. HOPF BIFURCATION ANALYSIS

The Hopf bifurcation around the endemic point E_2 is satisfied by the system at $\delta^* = \frac{\beta+\alpha}{I^*+S^*}$

The adequate condition for the system to have a Hopf bifurcation at (E_2) given by $T(\delta^*) = 0$

$\frac{dT}{d\delta} \neq 0$ at $\delta = \delta^*$

From the equation,

$$\begin{cases} Y - \delta V_2 I_2 - \alpha V_2 = 0 \\ \delta V_2 I_2 - (\beta + \alpha) I_2 - \varphi S_2 = 0 \\ \varphi I_2 - \alpha S_2 = 0 \end{cases} \tag{19}$$

The Jacobian matrix of the system at attacks-prone equilibrium point can be calculated as

$$J(E_2) = \begin{pmatrix} -(\delta I_2 + \alpha) & -\delta V_2 & 0 \\ \delta I_2 & \delta V_2 - (\beta + \alpha) & -\varphi \\ 0 & \varphi & -\alpha \end{pmatrix}$$

The eigenvalues are obtained by solving the determinant of $|J^\circ - I\psi| = 0$.

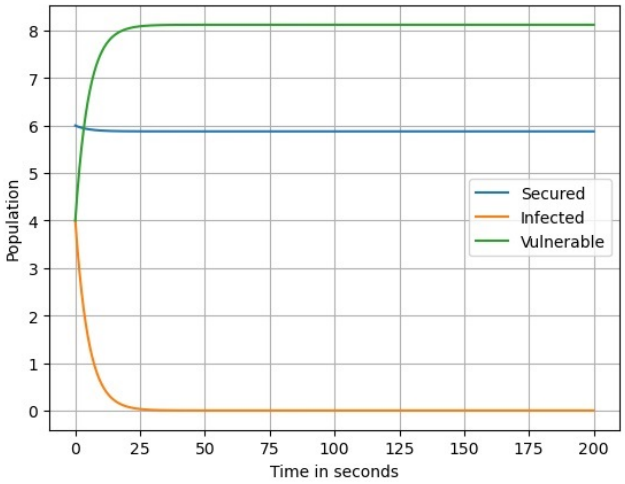

Figure 3. Transcritical Bifurcation Occurs at the Attacks-Free Equilibrium Point With $\beta = 0.03$

$$\begin{cases} -(\delta I_2 + \alpha) - \psi_V = 0 \\ \delta V_2 - (\beta + \alpha) - \psi_I = 0 \\ -\alpha - \psi_S = 0 \end{cases} \tag{20}$$

Then, the three eigenvalues is presented in equation (21) below:

$$\begin{cases} \psi_V = -(\delta I_2 + \alpha) \\ \psi_I = \delta V_2 - (\beta + \alpha) \\ \psi_S = -\alpha \end{cases} \tag{21}$$

Therefore, for $\alpha > 0$ the eigenvalue ψ_S is negative while the root of the remaining two eigenvalues are complex conjugate. Consequently, the condition for the Hopf bifurcation is satisfied at $\delta = \delta^*$.

Since,

$\frac{dT}{d\delta} = S_2 \neq 0$

Consequently, the system at the parameter $\delta = \delta^*$ has a Hopf bifurcation around the attacks-prone equilibrium point (E_2).

6. NUMERICAL SIMULATIONS

In this section, we evaluate the VIS model to determine the critical parameter values at which a Hopf bifurcation occurs, as well as the circumstances in which the transcritical bifurcation of the attack-free equilibrium is stable or unstable. PYTHON was used to simulate numerically the transcritical and Hopf bifurcations of the attack-free equilibrium.

The assumed initial conditions for the simulation are listed as: $V_0 = 10; I = 4; R = 4; Y = 15; \delta = 0.1; \alpha = 0.001\varphi = 0.5$ and $\beta = 0.03$.

Figure 3 presents the transcritical bifurcation of the attack-free equilibrium at $\beta = 0.03$ while the Figure 4 presents the transcritical bifurcation of the attack-free equilibrium at $\beta = 0.2$.

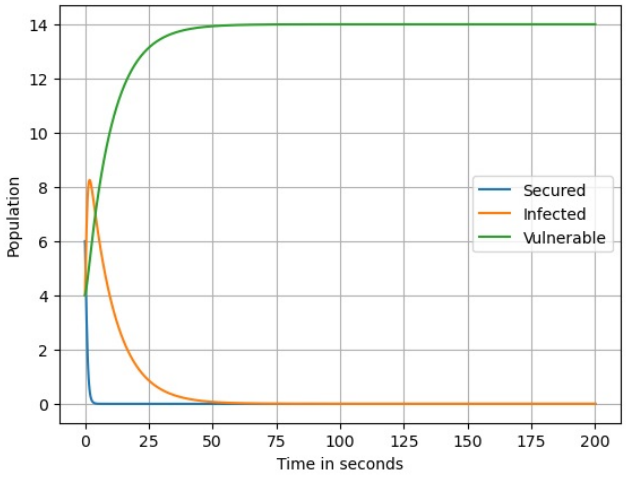

Figure 4. Transcritical Bifurcation Occurs at the Attacks-Free Equilibrium Point With $\beta = 0.2$

The transcritical bifurcation of the system (1) takes place close to the attack-free equilibrium point (E°), as shown by examining the graphical representation in Figure 3. The system (1) turn out to be unbalanced at the attacks-free equilibrium point as the infection rate rises, and its trajectory asymptotically moves closer to the attacks-prone equilibrium point.

By changing the infection rate from $\beta = 0.03$ to $\beta = 0.2$, the analysis of the graphical representation obtained from Figures 3 and Figure 4 respectively, demonstrate that the transcritical bifurcation occurs at the attacks-free equilibrium point. The system's trajectory then asymptotically approaches the attacks-prone equilibrium point.

Consequently, the Hopf bifurcation in the VIS model happens at the attacks-prone equilibrium point (E_2), and the system loses stability as the treatment rate increases.

7. CONCLUSION

This study has used transcritical and Hopf bifurcation analysis to clarify the intricate dynamics of cyberattacks inside Software-Defined Networking (SDN). Our findings provide evidence that the proposed VIS model exhibits a transcritical bifurcation and that the asymptotic behavior of the system approaches the attacks-prone equilibrium point from the attacks-free equilibrium point as the infection rate increases. Finding these bifurcation points is the important step in creating effective mitigation plans and strengthening the security of SDN. In the future, the optimal control of a delay VIS model and the Machine Learning model will be implemented to mitigate cyberattacks in SDN environments.

REFERENCES

A. Mahboubi, S. Camtepe, and H. Morarji, 2017. A study on formal methods to generalize heterogeneous mobile malware propagation and their impacts. *IEEE Access*, vol. 5, pp. 27740-27756.

Abhishta, A., Heeswijk, W. van, Junger, M., Nieuwenhuis, L. J. M., and Joosten, R., 2020. Why would we get attacked? An analysis of attacker's aims behind DDoS attacks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 11(2), 3–22.

Acarali, D., Rajesh Rao, K., Rajarajan, M., Chema, D., and Ginzburg, M., 2022. Modelling smart grid IT-OT dependencies for DDoS impact propagation. *Computers and Security*, 112, 102528.

Ajbar, A., and Alqahtani, R. T., 2020. Bifurcation analysis of a SEIR epidemic system with governmental action and individual reaction. *Advances in Difference Equations*, 2020, 1-14.

Alasali, T., and Dakkak, O., 2023. Exploring the Landscape of SDN-based DDoS Defense: A Holistic Examination of Detection and Mitigation Approaches, Research Gaps and Promising Avenues for Future Exploration. *International Journal of Advanced Natural Sciences and Engineering Researches*, 7(4), 327–349.

B. K. Mishra and D. K. Saini, 2007. SEIRS epidemic model with delay for transmission of malicious objects in computer network. *Applied Mathematics, and Computation*, vol. 188, no. 2, pp. 1476-1482.

Balamuralitharan, S., and Radha, M., 2018. Bifurcation analysis in SIR epidemic model with treatment. *In Journal of Physics: Conference Series*, Vol. 1000, No. 1, p. 012169. IOP Publishing.

BIAOU, B.O.S., Oluwatope, A.O. and Ogundare, B.S., 2022, December. Mathematical Analysis of DDoS Attacks in SDN-based 5G. In *International Conference on e-Infrastructure and e-Services for Developing Countries* (pp. 87-100). Cham: Springer Nature Switzerland.

I. Androulidakis, S. Huerta, V. Vlachos, and I. Santos, 2016. Epidemic model for malware targeting telephony networks. *In Proc. 23rd Int. Conf. Telecommun*, pp. 1-5.

Ireri, J., Pokhariyal, G., and Moindi, S., 2020. Hopf bifurcation analysis for a two species periodic chemostat model with discrete delays. *J. Adv. Math. Comput. Sci*, 35(3), 93-105.

Mahata, A., Paul, S., Mukherjee, S., and Roy, B., 2022. Stability analysis and Hopf bifurcation in fractional order SEIRV epidemic model with a time delay in infected individuals. *Partial Differential Equations in Applied Mathematics*, 5, 100282.

Nashat, D., Khairy, S. and Hassan, M.M., 2021. Detection of Application Layer DDoS Attack Based on SIS Epidemic Model. *IEEE Access*, 9, pp.159827-159832.

Shu, Z., Wan, J., Li, D., Lin, J., Vasilakos, A. V., and Imran, M., 2016. Security in software-defined networking: Threats and countermeasures. *Mobile Networks and Applications*, 21, 764-776.

Z. Wang, H. Hu, and C. Zhang, 2017. On achieving SDN controller diversity for improved network security using coloring algorithm. *In Proc. 3rd IEEE Int. Conf. Comput. Commun. (ICCC)*, pp. 12701275.

Yerra Shankar Rao, Aswin Kumar Rauta, Hemraj Saini and Tarini Charana Panda, 2017. Mathematical Model for Cyber Attack in Computer Network. *International Journal of Business Data Communications and Networking*, Volume 13, Issue 1.

Wang, W., and Chen, L., 2016. Stability and Hopf bifurcation analysis of an epidemic model by using the method of multiple scales. *Mathematical Problems in Engineering*, 2016.