Optimal Control Analysis of Cyberattacks in Software-Defined Networking

By

B. O. S. BIAOU [1], A. O. Oluwatope [2] and B. S. Ogundare [3]

[1, 2] Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria.

[3] Department of Mathematics, Obafemi Awolowo University, Ile-Ife, Nigeria.

International Conference and Advanced Workshop on Modelling and Simulation of Complex Systems

May 27-31, 2024 – OAU Campus, Ile-Ife, Nigeria

Presentation Outline

- Introduction
- State-of-the-art
- Epidemic Modeling of VIS System
- Solutions and Stabilities Analysis of the Model
- VIS Model Simulation
- Results and Discussions
- Conclusion
- References

Introduction

- Networking which is basically, the use of computer networks to communicate with other devices digitally happens to be nowadays a crucial part of the live of human being.
- Then, data transmission in a high speed is the most requested by every internet user.

Introduction

- SDN is a ground-breaking networking model developed to give a new life of visibility and revolution in networking.
- Hence, the success of the SDN is based on the separation of the control plane and data plane, which is responsible for the flexibility, agility and ease manageability of the network.

Introduction

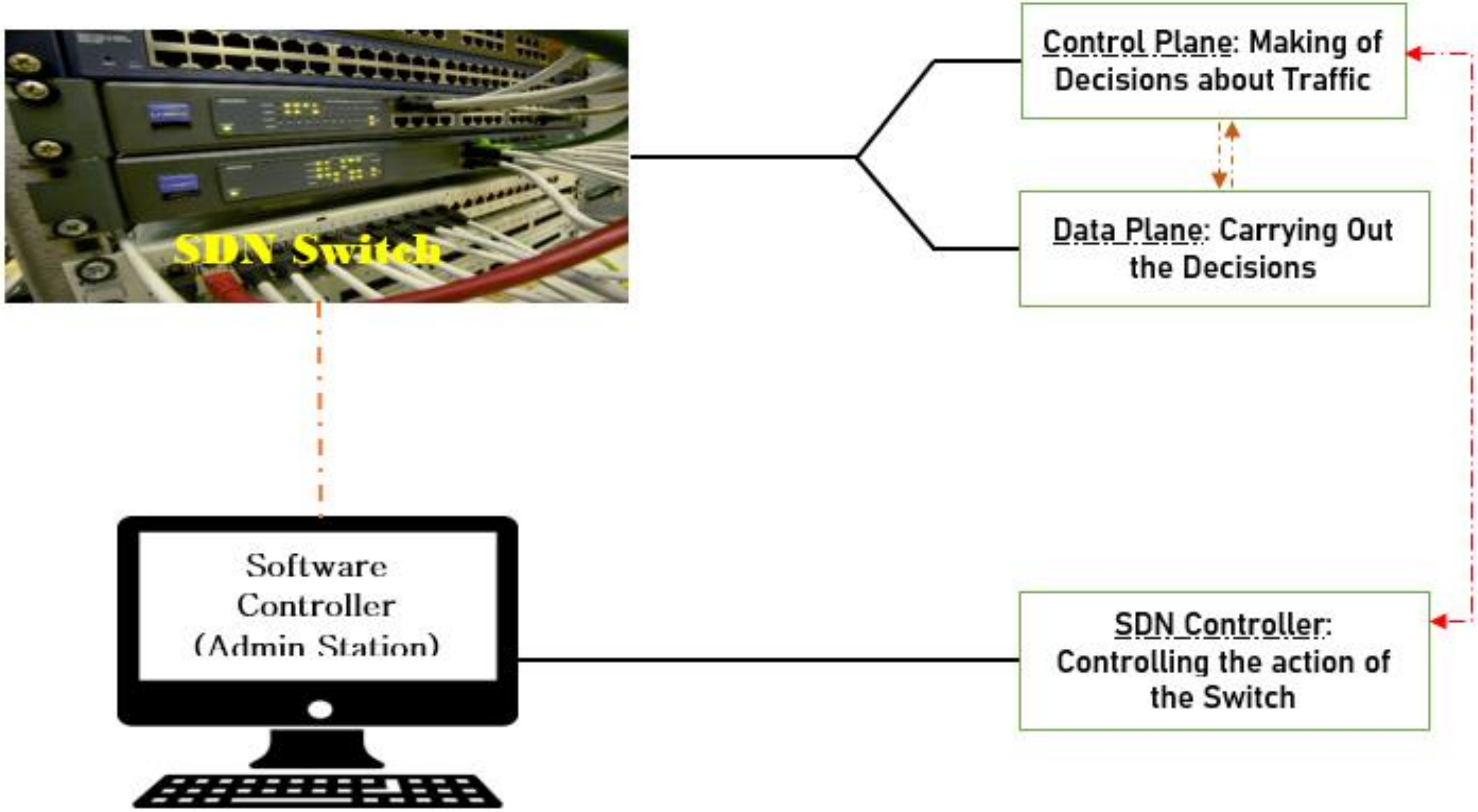


Figure 1: Typical SDN Functioning

Introduction

- Many types of cyberattacks such as SQL Injection Attacks, malware, Botnet, DDoS, 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.

Introduction

- 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 the target infrastructure for online services.

Introduction

- (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

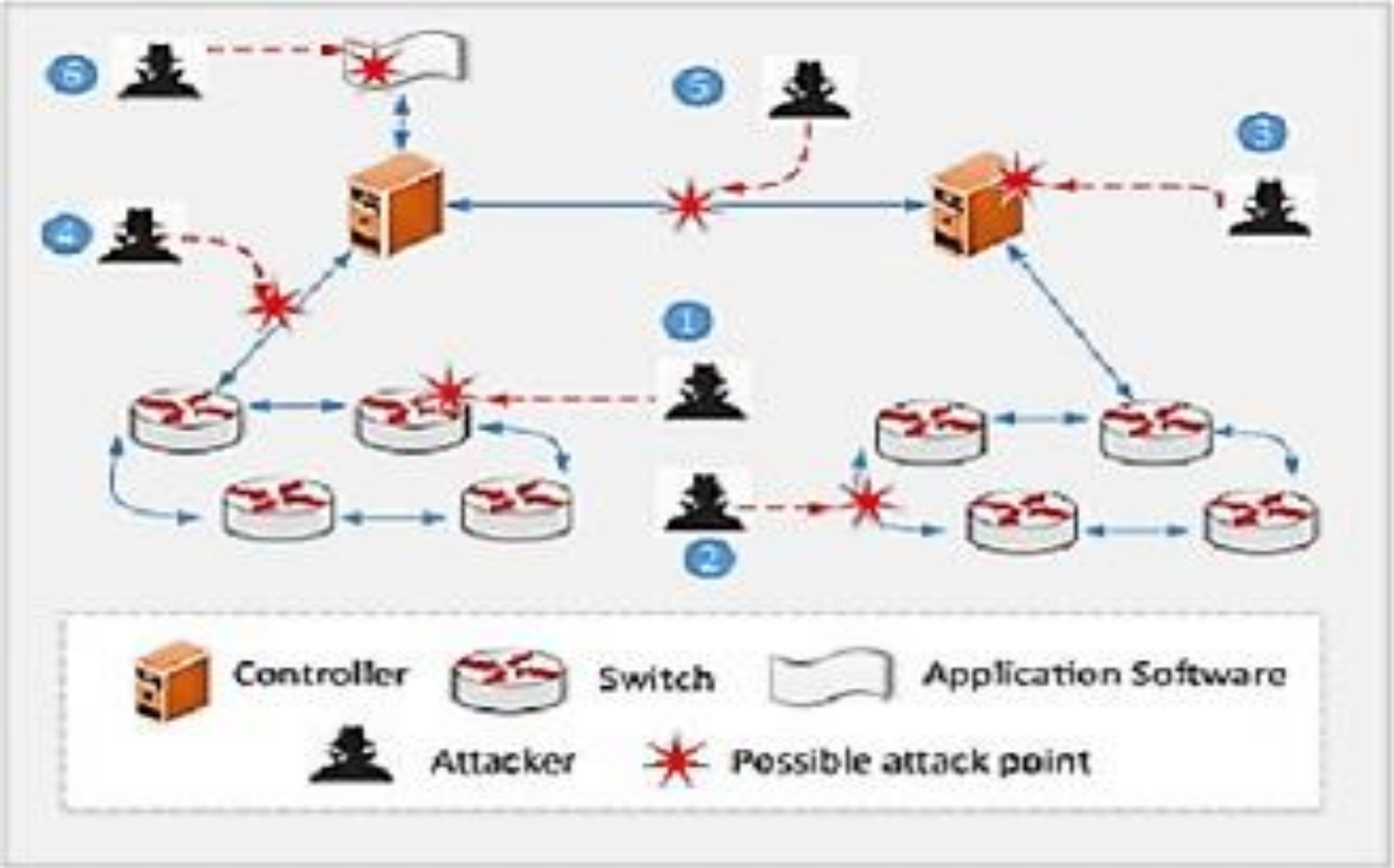


Figure 2: Cyberattacks in SDN Paradigm

State-of-the-art

- 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), (Hosseini et al. , 2014), (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.

State-of-the-art

- Some shortcomings in the existing epidemic models have being applied to analyse cyberattacks in SDN.
- The shortcomings include the close-population of nodes, the failure to consider the possibility of a node leaving the network for other reasons unconnected to the attacks and the failure to consider major parameters and assumptions related to network environment.

State-of-the-art

- The SEIR model in (Androulidakis et al. , 2016) (Yan and Liu , 2006), (Sirijampa et al. , 2018) and (Ajbar and Algahtani , 2020) was proposed to demonstrate how quickly the malware spread over the networks.
- Yet, the authors assumed a close-population of nodes, that is, new nodes joining the network during the instance of analysis is not permitted.

Epidemic Modeling of VIS System

- Hence, the infection of nodes behaves in a similar way as human epidemic such as the novel COVID-19.
- (V) Vulnerable class of nodes.
- (I) Infected class of nodes.
- (S) Secured class of nodes

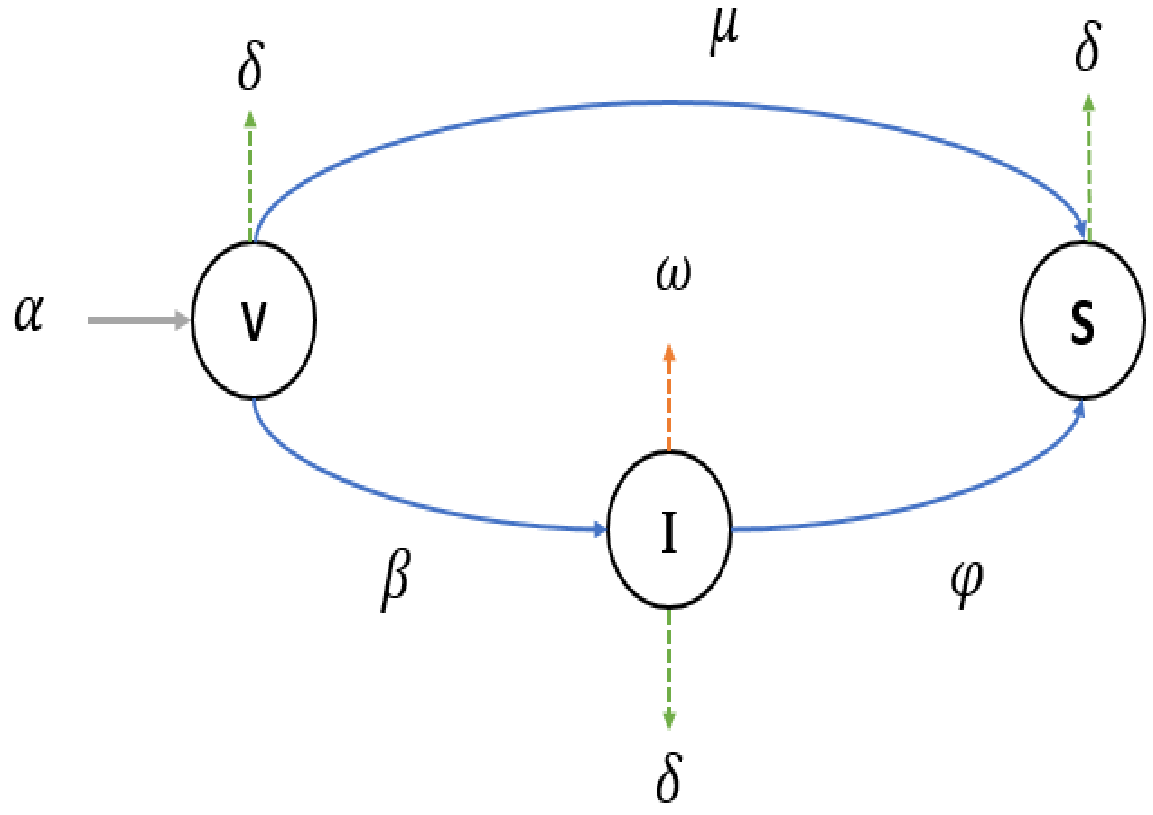


Figure 3: Representation of the Proposed VIS Model.

Solutions and Stabilities Analysis of the Model

- Matching ODE for the proposed VIS epidemic model.

$$\begin{cases} \dfrac{dV}{dt} = \alpha - \beta V I - \mu V - \delta V \\ \dfrac{dI}{dt} = \beta V I - \varphi I - \delta I - \omega I \\ \dfrac{dS}{dt} = \varphi I + \mu V - \delta S \end{cases} \qquad (1)$$

$$(V, I, S) \in \mathbb{R}^3, \begin{cases} V > 0 \\ I \geq 0 \\ S \geq 0 \end{cases}$$

- Equilibria point of VIS model.

- Every equation in the system (1) will be equal to zero.

$$\begin{cases} \alpha - \beta V I - \mu V - \delta V = 0 \\ \beta V I - \varphi I - \delta I - \omega I = 0 \\ \varphi I + \mu V - \delta S = 0 \end{cases} \qquad (2)$$

Solutions and Stabilities Analysis of the Model

- Attack-free Equilibrium.
- At a point where there is no attack in the integration of SDN and 5G, that particular stage is epidemically called attack-free equilibrium point.

$$\begin{cases} \alpha - \beta V^0 I^0 - \mu V^0 - \delta V^0 = 0 \\ \beta V^0 I^0 - \varphi I^0 - \delta I^0 - \omega I^0 = 0 \\ \varphi I^0 + \mu V^0 - \delta S^0 = 0 \end{cases} \quad (3)$$

- By solving the system (3), the VIS model will be free from attack at (V^0, I^0, S^0).

$$\begin{cases} V^0 = \dfrac{\alpha}{\mu + \delta} \\ I^0 = 0 \\ S^0 = \dfrac{\mu\alpha}{\delta(\mu + \delta)} \end{cases} \quad (4)$$

Solutions and Stabilities Analysis of the Model

- Local Stability of DDoS-free Equilibrium.

$$\begin{cases} \frac{dV}{dt} = \alpha - \beta VI - \mu V - \delta V = 0 \\ \frac{dI}{dt} = \beta VI - \varphi I - \delta I - \omega I = 0 \\ \frac{dS}{dt} = \varphi I + \mu V - \delta S = 0 \end{cases} \quad (5)$$

- "**J**" is set as the Jacobian Matrix of the system (5) equation.

$$J^{\bullet} = \begin{pmatrix} -\beta I^{0} - \mu - \delta & -\beta V^{0} & 0 \\ \beta I^{0} & \beta V^{0} - \varphi - \delta - \omega & 0 \\ \mu & \varphi & -\delta \end{pmatrix} \quad (6)$$

- The system (7) is gotten by considering the equation (4).

$$J^{\bullet} = \begin{pmatrix} -\mu - \delta & -\frac{\beta\alpha}{\mu+\delta} & 0 \\ 0 & \frac{\beta\alpha}{\mu+\delta} - \varphi - \delta - \omega & 0 \\ \mu & \varphi & -\delta \end{pmatrix} \quad (7)$$

- With the (3×3) Jacobian matrix, three eigenvalues are obtained after solving the determinant of $|J^{\cdot} - I\psi| = 0$.

$$\begin{cases} \psi_1 = -\delta \\ \psi_2 = -\mu - \delta \\ \psi_3 = \frac{\beta\alpha - (\mu+\delta)(\varphi+\delta+\omega)}{\mu+\delta} \end{cases} \quad (8)$$

Solutions and Stabilities Analysis of the Model

- BRN is found from ψ_3, the eigenvalue that is not obviously negative out of the three.

$$\frac{\beta\alpha - (\mu+\delta)(\varphi+\delta+\omega)}{\mu+\delta} < 0 \qquad (9)$$

$$\frac{\beta\alpha}{(\mu+\delta)(\varphi+\delta+\omega)} < 1 \qquad (10)$$

$$R_0(V,I,S) = \frac{\beta\alpha}{(\mu+\delta)(\varphi+\delta+\omega)}),\ (\mu+\delta)(\varphi+\delta+\omega) \neq 0 \qquad (11)$$

- The attack decreases and will probably dies out when $R_0 < 1$.
- The attack is stable without any new infectious node in the system when $R_0 = 1$.
- The attack increases in the system when $R_0 > 1$.

Solutions and Stabilities Analysis of the Model

- The Hopf bifurcation around the endemic point E2 is satisfied by the $\delta^* = \frac{\beta+\alpha}{I^*+S^*}$
- The adequate condition for the system to have a hopf bifurcation at E2 given by $T(\delta^*) = 0$
- The Jacobian matrix is obtained by solving the determinant of $|J^0 - I\psi| = 0$.

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

Solutions and Stabilities Analysis of the Model

- The eigenvalues is presented in equation (21) below

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

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

Results and Discussions

- Figure 3 presents the graphical representation of the three classes of nodes (V, I, S).

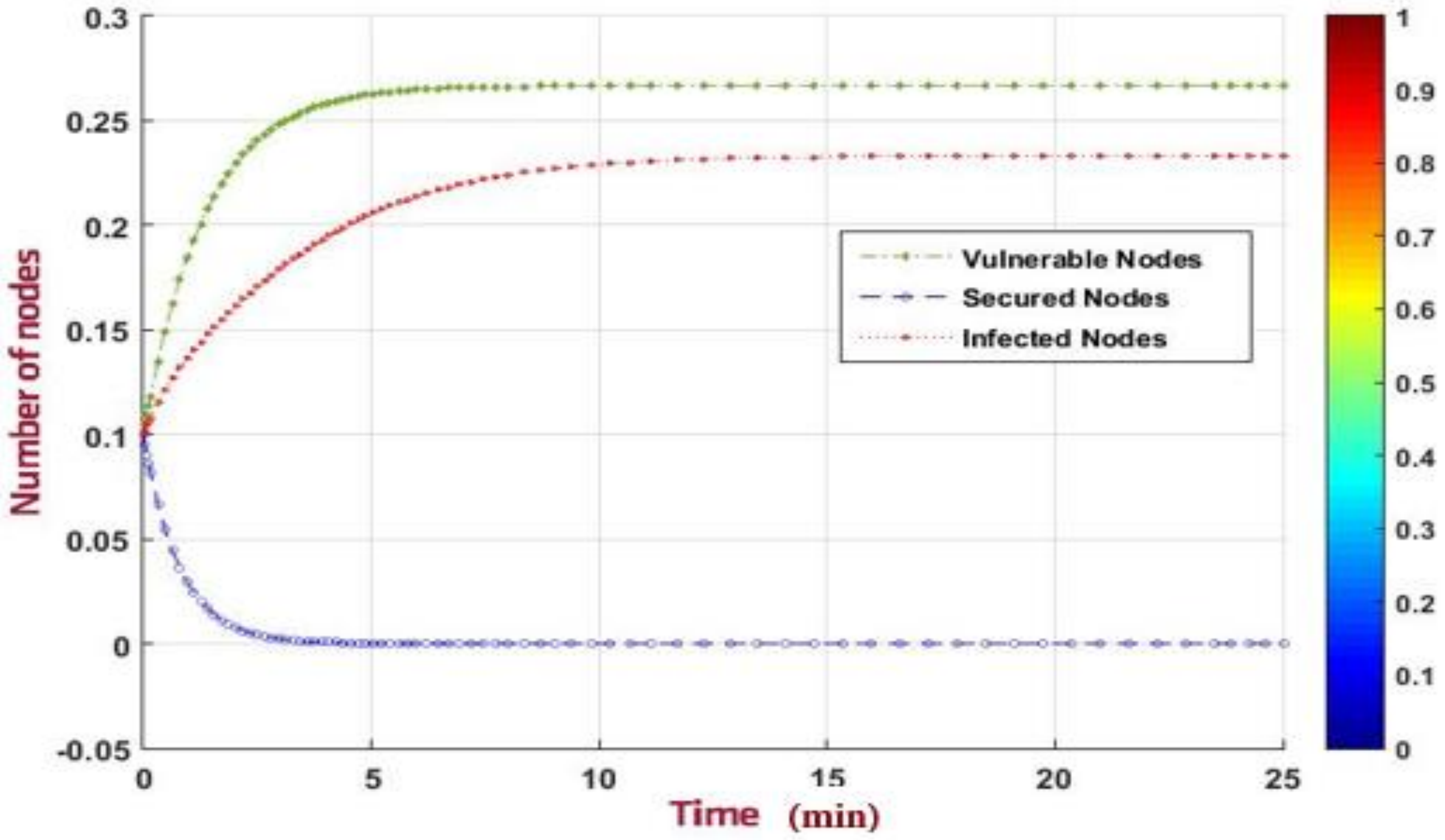
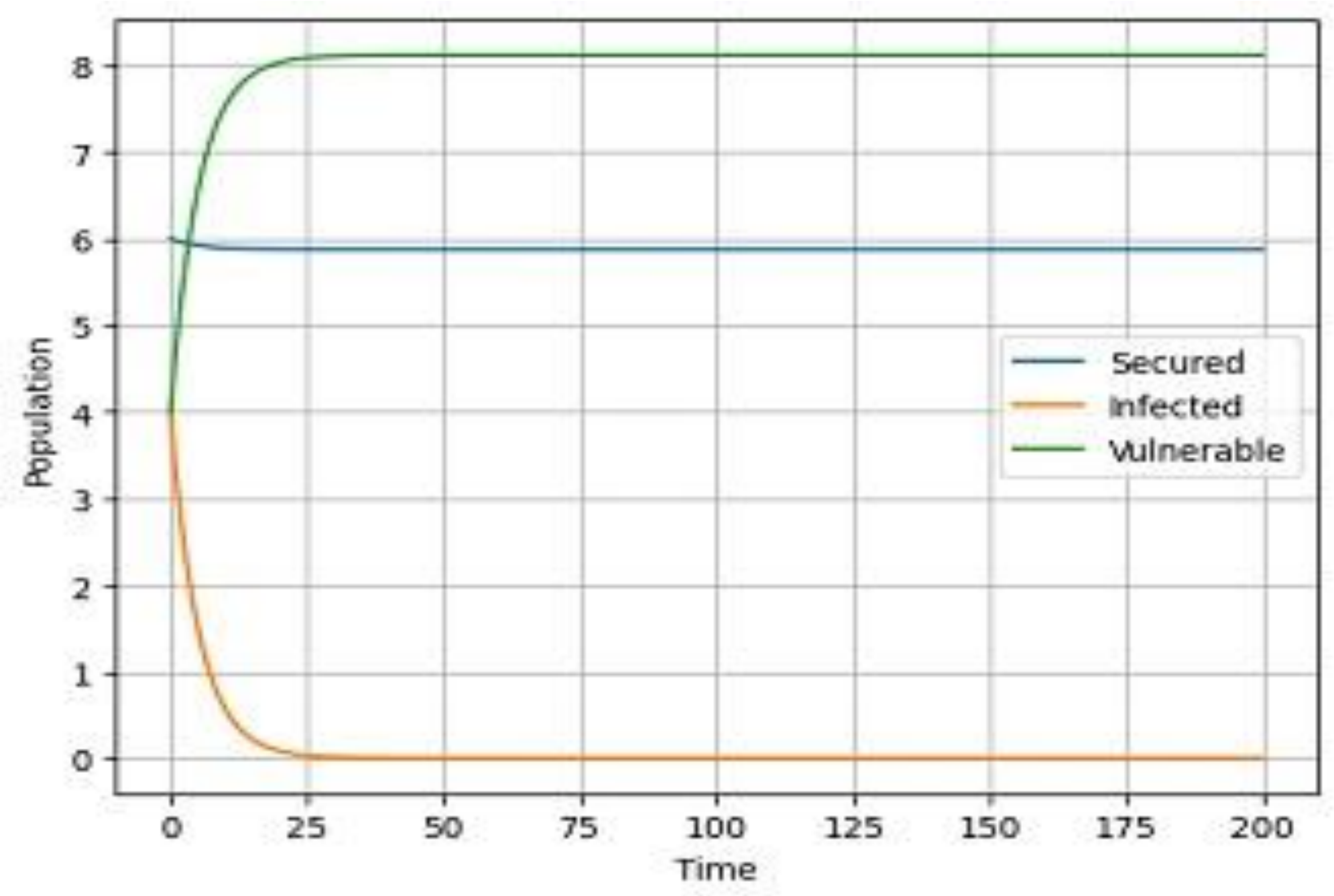


Figure 4: General Stability of the VIS Model.

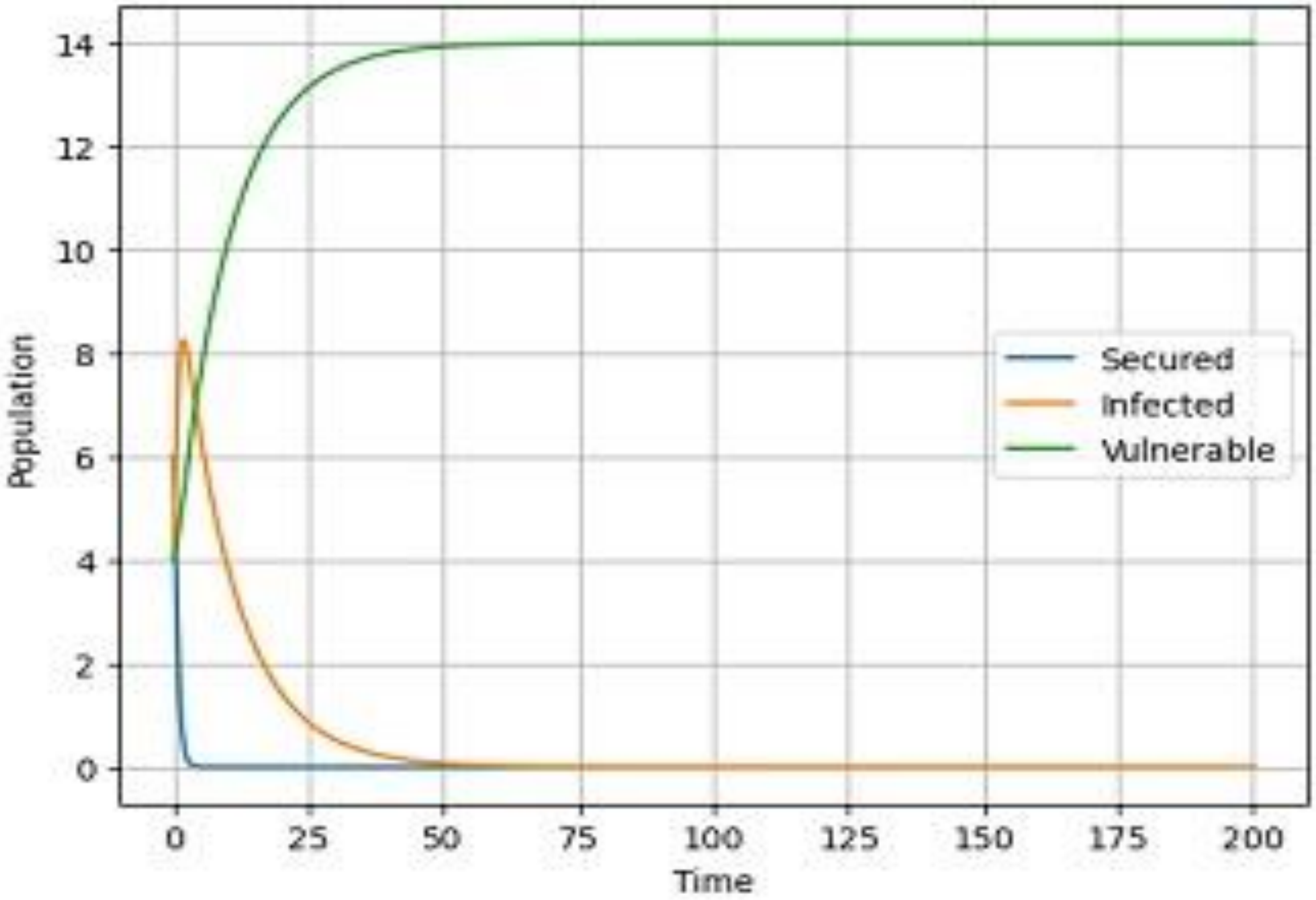
Results and Discussions

- Figure 5: Bifurcation Occurs at the Attacks-Free Equilibrium Point With $\beta = 0.03$

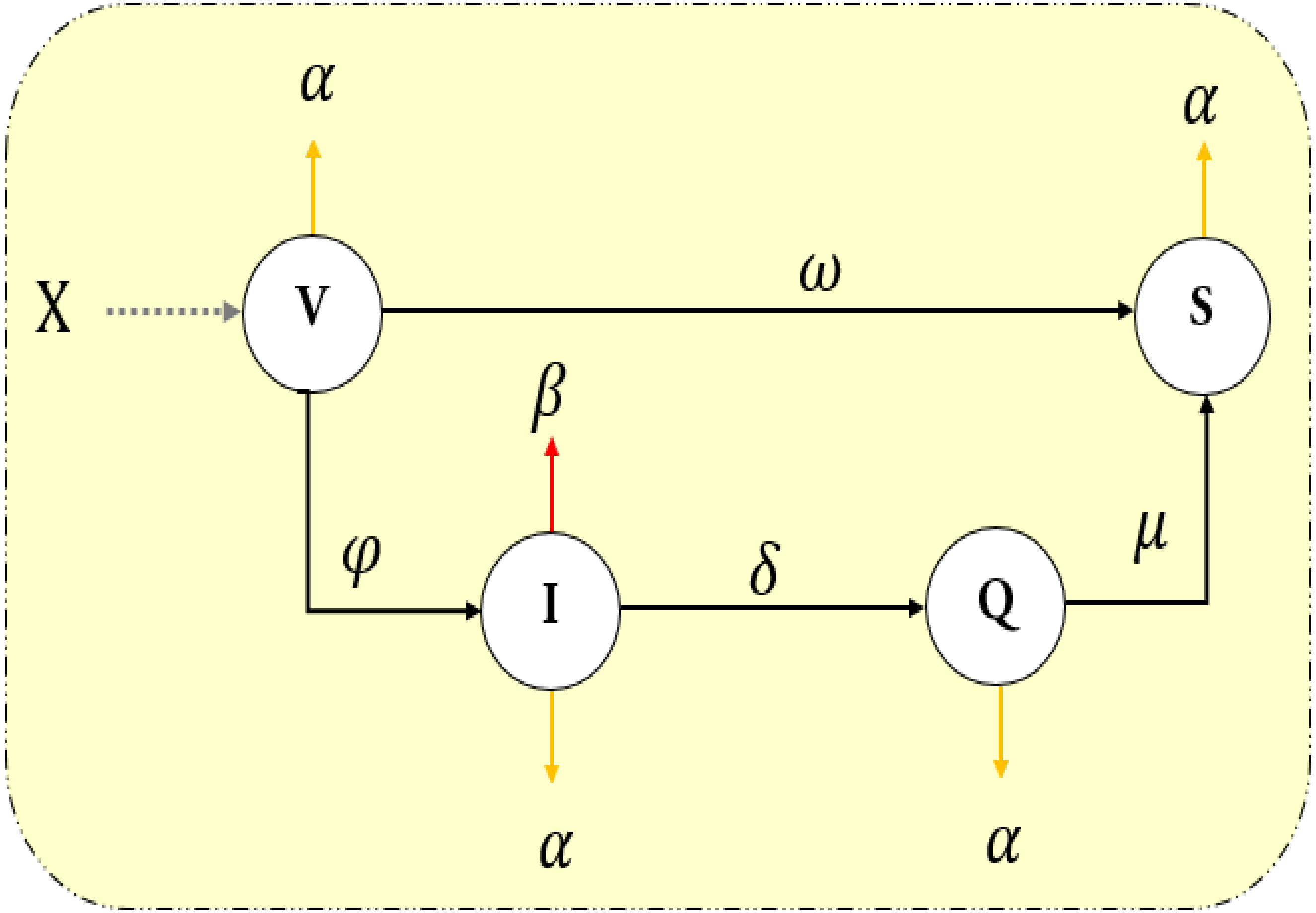


Results and Discussions

- Figure 6: Bifurcation Occurs at the Attacks-Free Equilibrium Point With $\beta = 0.2$

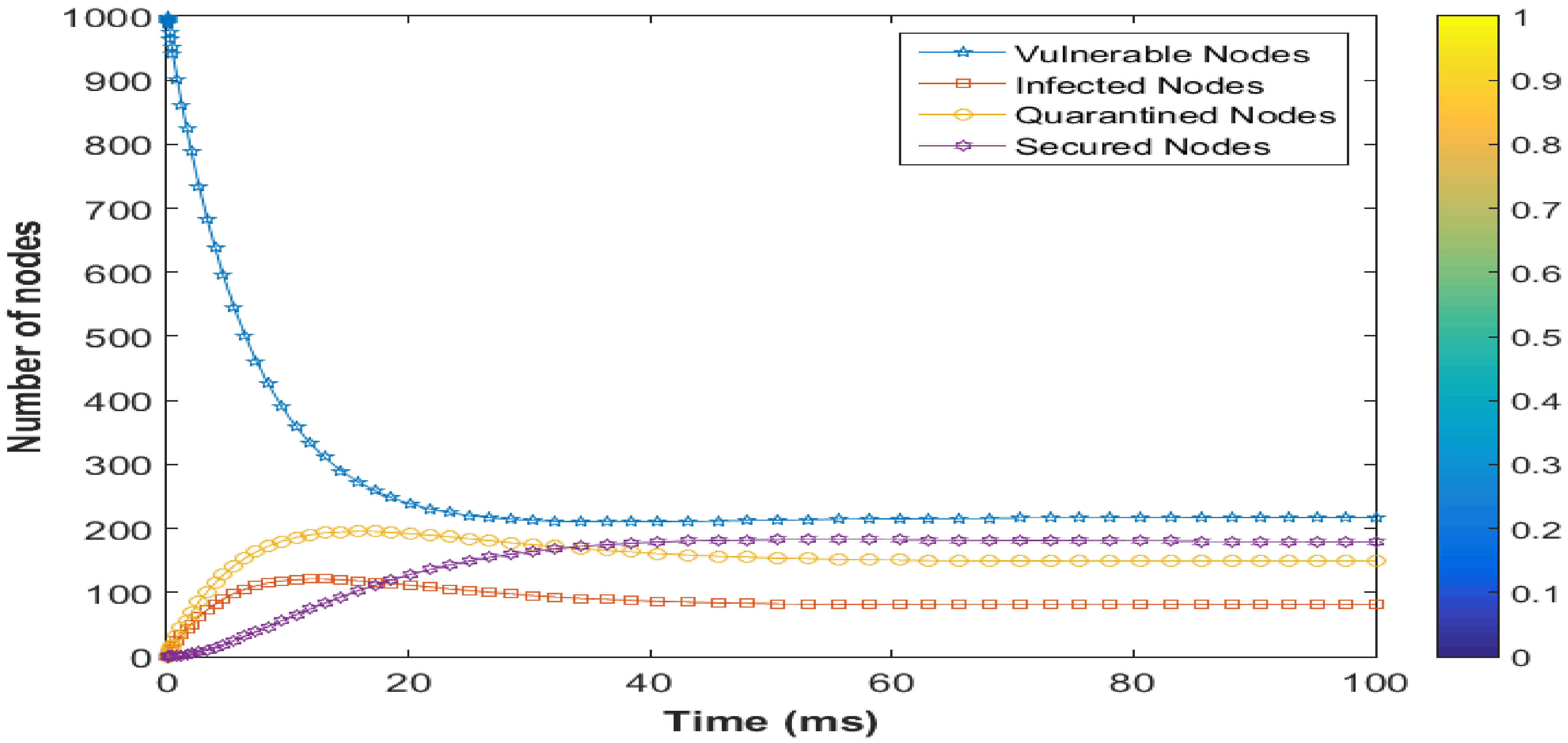


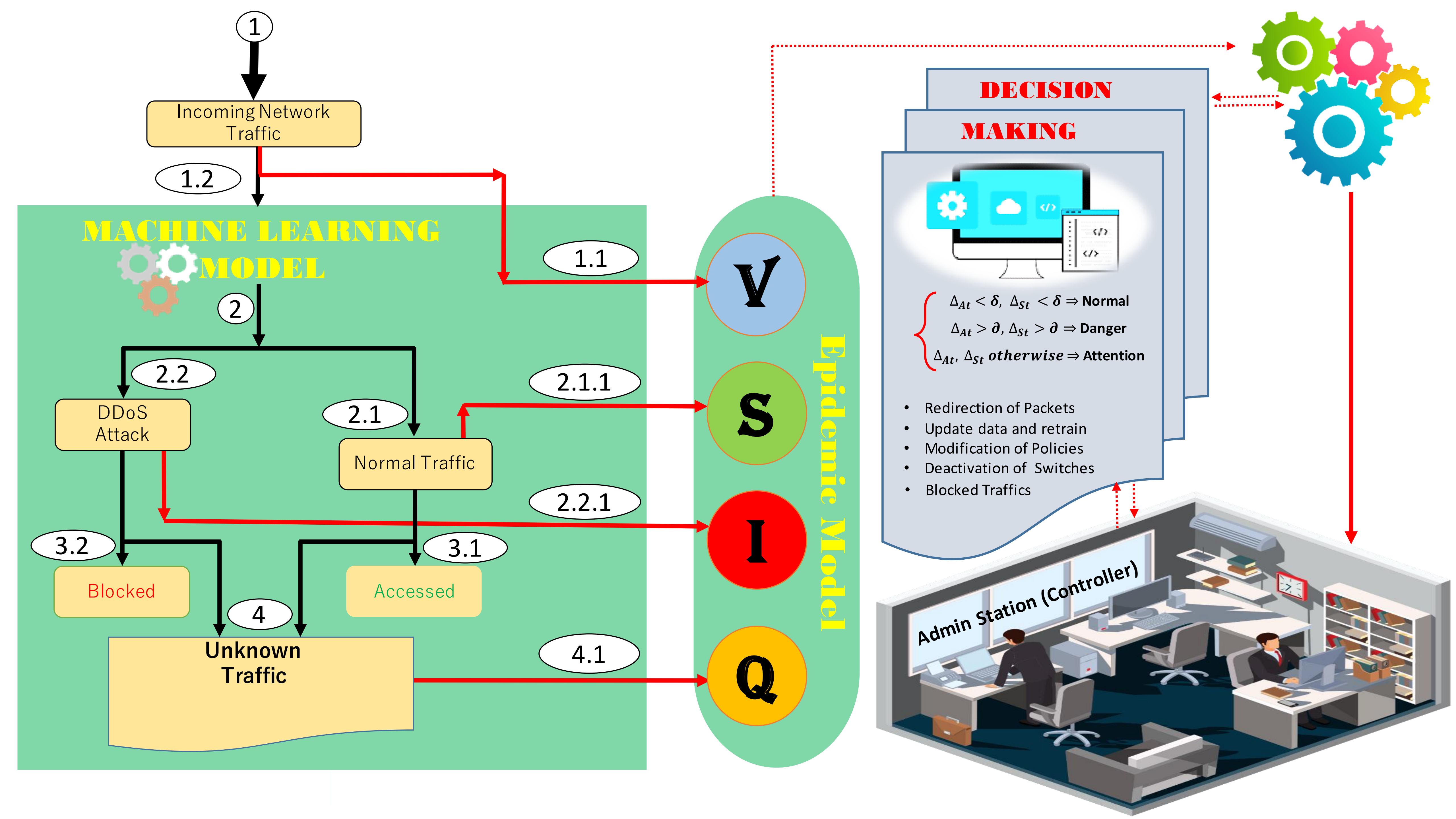
Optimal Control Analysis



$$
\begin{cases}
X - \varphi V I - \omega V - \alpha V = 0 \\
\varphi V I - \delta I - \alpha I - \beta I = 0 \\
\delta I - \mu Q - \alpha Q = 0 \\
\mu Q + \omega V - \alpha S = 0
\end{cases}
$$

Optimal Control Analysis





1
Incoming Network Traffic
1.2
1.1
MACHINE LEARNING MODEL
2
2.2
2.1
2.1.1
DDoS Attack
Normal Traffic
2.2.1
3.2
3.1
Blocked
Accessed
4
4.1
Unknown Traffic
V
S
I
Q
Epidemic Model
DECISION
MAKING
$\Delta_{At} < \delta,\ \Delta_{St} < \delta \Rightarrow$ Normal
$\Delta_{At} > \partial,\ \Delta_{St} > \partial \Rightarrow$ Danger
$\Delta_{At},\ \Delta_{St}$ *otherwise* $\Rightarrow$ Attention
• Redirection of Packets
• Update data and retrain
• Modification of Policies
• Deactivation of Switches
• Blocked Traffics
Admin Station (Controller)

Conclusion

- To evaluate the impact of control measures, the model is reformulated as an optimal control problem incorporating the quarantined class of nodes and mitigation strategies.

References

- Dahiya, D. (2022). DDoS Attacks Detection in 5G Networks: Hybrid Model with Statistical and Higher-Order Statistical Features. Cybernetics and Systems, 1-26.
- Wu, P., Yao, L., Lin, C., Wu, G., & Obaidat, M. S. (2018). Fmd: A DoS mitigation scheme based on flow migration in software - defined networking. International Journal of Communication Systems, 31(9), e3543.
- Kalkan, K., Gür, G., & Alagöz, F. (2017, July). SDNScore: A statistical defense mechanism against DDoS attacks in SDN environment. In 2017 IEEE Symposium on Computers and Communications (ISCC) (pp. 669-675). IEEE.
- Durner, R., Lorenz, C., Wiedemann, M., & Kellerer, W. (2017, July). Detecting and mitigating denial of service attacks against the data plane in software defined networks. In 2017 IEEE Conference on Network Softwarization (NetSoft) (pp. 1-6). IEEE.
- Mohammadi, R., Javidan, R., & Conti, M. (2017). Slicots: An sdn-based lightweight countermeasure for tcp syn flooding attacks. IEEE Transactions on Network and Service Management, 14(2), 487-497.
- Wang, T., Chen, H., & Qi, C. (2018). Mindos: A priority-based SDN safe-guard architecture for DoS attacks. IEICE TRANSACTIONS on Information and Systems, 101(10), 2458-2464.
- Kazmi, S. H. A., Qamar, F., Hassan, R., Nisar, K., & Chowdhry, B. S. (2022). Survey on Joint Paradigm of 5G and SDN Emerging Mobile Technologies: Architecture, Security, Challenges and Research Directions.

References

- Kazmi, S. H. A., Qamar, F., Hassan, R., Nisar, K., and Chowdhry, B. S. (2022). Survey on Joint Paradigm of 5G and SDN Emerging Mobile Technologies: Architecture, Security, Challenges and Research Directions
- , X., Liu, Y., & Wang, X. (2017). SDN enabled 5G-VANET: Adaptive vehicle clustering and beamformed transmission for aggregated traffic. IEEE Communications Magazine, 55(7), 120-127.
- Sheibani, M., Konur, S., & Awan, I. (2022, August). DDoS Attack Detection and Mitigation in Software-Defined Networking-Based 5G Mobile Networks with Multiple Controllers. In 2022 9th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 32-39). IEEE.
- Gaurav, A., Gupta, B. B., & Panigrahi, P. K. (2022). A novel approach for DDoS attacks detection in COVID-19 scenario for small entrepreneurs. Technological Forecasting and Social Change, 177, 121554.
- Yang, L., Wu, D., Hou, Y., Wang, X., Dai, N., Wang, G., … and Ruan, L. (2020). Analysis of psychological state and clinical psychological intervention model of patients with COVID-19. MedRxiv.

Thanks for listening