Mathematical Analysis of DDoS Attacks in SDN-Based 5G

B. O. S. BIAOU[1(✉)], A. O. Oluwatope[1], and B. S. Ogundare[2]

[1] Comnet Laboratory, Department of Computer Science and Engineering, OAU, Ile-Ife, Nigeria
bsbiaou@pg-student.oauife.edu.ng
[2] Department of Mathematics, Obafemi Awolowo University, Ile-Ife, Nigeria

Abstract. Data transmission in a high speed is the most requested by every internet user. Fortunately, the implementation of the fifth-generation (5G) cellular network was carried out by Verizon in 2019 to ameliorate and overcome some challenges of the 4G cellular networks. Software-defined networking (SDN) as a good networking prototype of the hour extremely welcomed the 5G to render the full performance of itself. Unluckily, the best integration of SDN and 5G is seriously being confronted the Distributed Denial of Service (DDoS) attacks day in and day out. The goal of this paper is to analyse the DDoS attacks in the SDN-based 5G technology. Hence, a proposed VIS (Vulnerable-Infected-Secured) epidemic model is provided to investigate the security issues posed by DDoS attacks in SDN-based 5G. In this paper, the mathematical formulation for the epidemic VIS model was developed. The equilibria points, DDoS-free equilibrium, basic reproduction number and stabilities of DDoS-free equilibria were provided in MATLAB.

Keywords: SDN · 5G · DDoS · VIS epidemic model. · SDN-based 5G

1 Introduction

5G telecom is picking up impressive speed from numerous areas like business, industry, IoT, e-Health, smart cities, scholarly community and academic [1,2]. In the middle of 2021, the Global Mobile Equipment Suppliers Association (GSA) reported more than 800 5G devices by May and reach 822 after a month. In addition, it has reported that about 443 telecom administrators in 70 Nations invested in 5G [3]. With the spring of 5G, IDC projects the number of connected IoT tools per minute at 152,200 by 2025 [4]. Likewise, SDN allows network administrators to handle network services through the abstraction of lower-level functionality. [5] recognized SDN as an emerges and powerful new technology that provides global visibility of the network by decoupling the control logic from the forwarding devices and the abstraction of network services in SDN

R. A. Saeed et al. (Eds.): AFRICOMM 2022, LNICST 499, pp. 87–100, 2023.
https://doi.org/10.1007/978-3-031-34896-9_7

architecture provides more flexibility for network administrators to execute various applications.

DDoS attack is one of the most dangerous attacks that smashes the industries, the businesses and the private systems every day. The principal resolution of the DDoS attacks is to interrupt the services by flooding superfluous massive traffic over the network. The three major processes using by DDoS to attack are either on volume based-attack (in bits per second) or on protocol attacks (in packets per second) or on application layer attacks (in requests per second).

The main goal of this research is to analyse mathematical-based the DDoS attacks in SDN-enabled 5G. Hence, the infection of nodes behaves in a similar way as human epidemic such as the novel COVID-19. In SDN-enabled 5G, a single centralized controller can manage multiples forwarding nodes which could lead to a faster propagation process of the DDoS attack. Therefore, an epidemic model could be adapted to the SDN-enabled 5G since the forwarding nodes and the controllers themselves can be infected in order to become part of a botnet which later could be used to perform the DDoS attacks.

Consequently, the clear overview on the join area of 5G and SDN will be presented including the security issues and the damages of the DDoS in SDN-enabled 5G. Moreover, VIS model will be designed with the mathematical formulations to evaluate the proposed VIS epidemic model. Furthermore, the solutions and the stabilities of the model will be analysed at the local and global asymptotic stabilities. Finally, the results for the numerical simulations of the proposed model will be carried out using MATLAB.

This manuscript is systematically arranged in seven sections. Section one and two express clearly the introduction and the state-of-the-art respectively while the section three presents the mathematical modelling of the VIS model. Section four is based on the solutions and the stabilities of the system. The VIS model is simulated in the section five following by the discussions in section six while the manuscript is concluded in the last section seven.

2 Conceptualization of Related Works

In an Accenture review of 2,600 5G consumers, 35% of them voiced out about the security of 5G, whereas 62% considered 5G as an open door to more attacks [6]. The author in [7] presented 5G as a wide area of research. Even though, the transition from 4G to 5G SA can extraordinarily boost the quantity of mobile devices and the data rate, at the same time, it can rise up the DDoS treats. The more devices are connected the more the network is exposed to treats. Besides, the multitude of links among the devices in 5G can be the significant security issues [8]. The author in [9] presented a DDoS attacks detection in 5G networks using statistical and higher-order statistical features while the paper [10] presented DDoS detection and mitigation mechanisms in 5G Mobile Technologies.

Nevertheless, according to the researchers, DDoS in SDN can be caused by the centralized control [11], the limited size of flow tables in switches [12], the separation of planes [13] and even the single point of failure [14].

Although, the SDN-enabled 5G has modernized wireless networks but with numerous treats as presented in Fig. 1 required tremendous exploration [15].

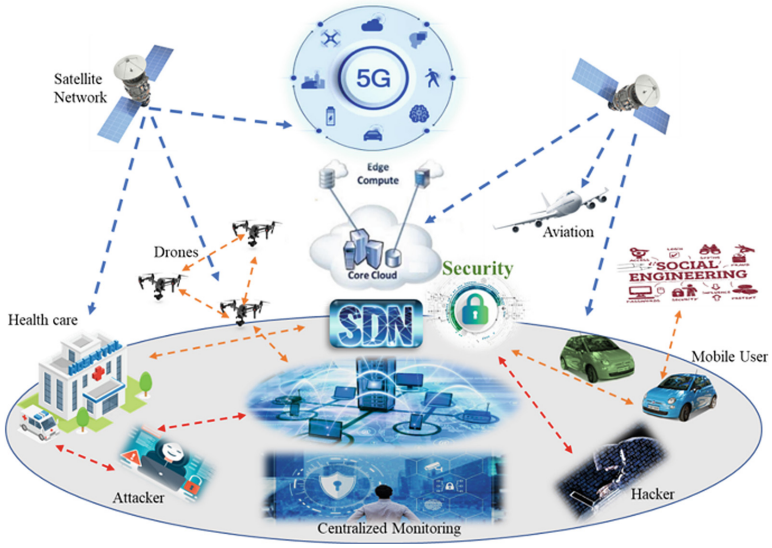

Fig. 1. Paradigm of SDN-enabled 5G [15].

Figure 1 illustrates the overall view of the integration of SDN and 5G. Henceforth, several opportunities including edge computing, satellite network, health care, drones, aviation, mobile and many of others are took-off with the achievement of the SDN-enabled 5G. On the other hand, several challenges such as threats and attacks had outstretched in the paradigm of 5G and SDN.

The delivery of QoS in the high level of the SDN for 5G networks are more perplex and represents a genuine issue that should be tended to [16]. Furthermore, the bit error speed caused by the network congestion and latencies in the SDN-based 5G is raised in [17]. Hence, Researches demonstrated that each of the layer of the SDN-enabled 5G including the connection between the layers are all exposed to threats and the DDoS attacks as showed in Fig. 2. [18] proposed a new method to equalize the processing burden among the dispersed controllers in SDN-based 5G networks.

In Fig. 2, displays the architectural of the SD-based 5G and the security issued related to it. The application layer including its services communicates with the control layer, which is responsible for the management of the entire traffic flow through the northbound interface (NBI). The southbound interface (SBI) connects the control layer to the infrastructure layer. In addition, the figure presents the security issues even at each level of the architecture including the two interfaces (NBI and SBI).

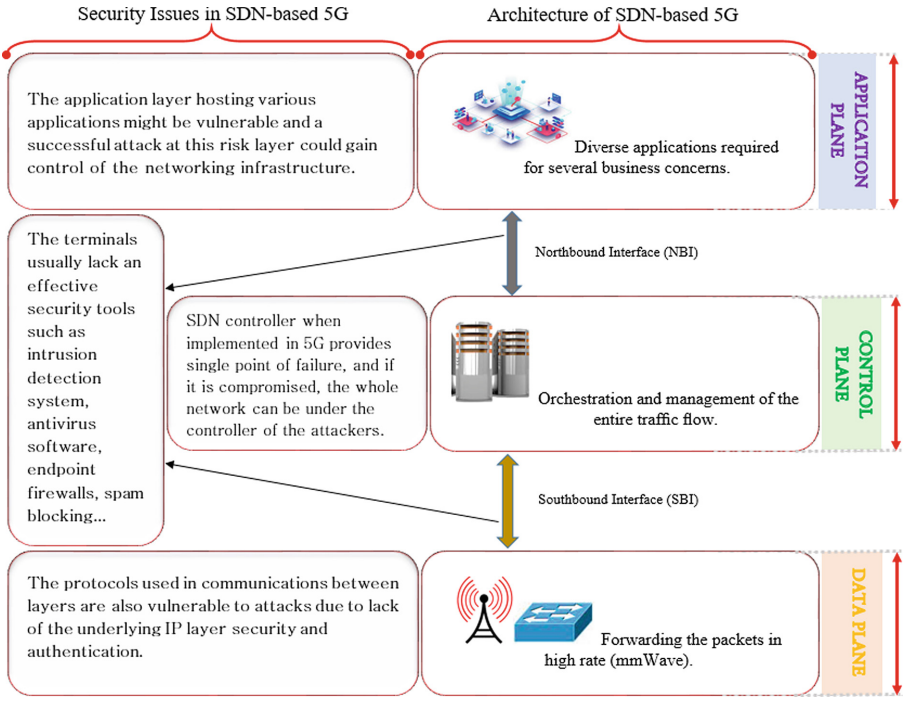

Fig. 2. SDN-based 5G: Architecture and Security Issues.

3 Mathematical Modeling of VIS System

3.1 Presentation of VIS Model

The Epidemic model is known as the greatest illustrative mathematical analysis for investigation on viruses or infections in a static society [19].

The spread of the DDoS attack over time is analysed by a proposed epidemic model VIS (Vulnerable, Infected, and Secured). The fraction of vulnerable class of nodes (**V**) are the class that has never been attacked by DDoS while the infected class of nodes (**I**) has been attacked by DDoS and the secured class of nodes (**S**) has recovered from the attack. A node can migrate from one compartment to another by different transmission rates (the rate β from **V** to **I**, the rate μ from **V** to **S** and the rate φ from **I** to **S**).

A node in vulnerable class of nodes can move directly to secured class of nodes without being infected. The proposed VIS epidemic model is built in an open population rate (α) of free input and output of node into the system where their will not be the migration of the node from secured to vulnerable.

The rate transition (δ) for any node to be disconnected from the system in this VIS model is equal while in infected class, a node can be disconnected with the rate ω due to the DDoS attack in the system.

Hence, the illustration of the proposed VIS epidemic model of the DDoS attack in SDN-based 5G technology is presented in Fig. 3.

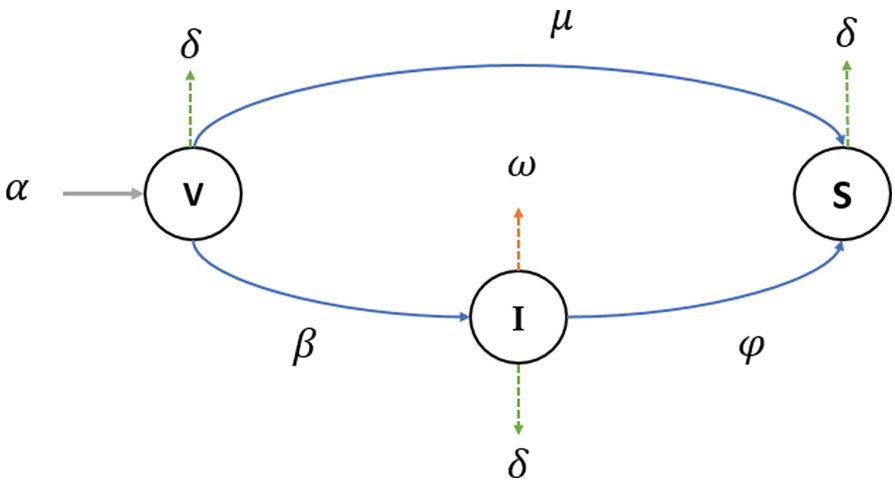

Fig. 3. Representation of the Proposed VIS Model.

3.2 Mathematical Model of VIS

The matching ordinary differential equations (ODE) for the proposed VIS epidemic model are presented in the system (1).

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

In the system (1), (**U**) represents the viable point for the model VIS. So, (**U**) is given by

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

4 Solutions and Stabilities Analysis of the Model

The proposed VIS model will be mathematically analysed at the local and global equilibrium in this section.

4.1 Equilibrium Points

Every equation in the system (1) will be equal to zero for proper finding of the equilibria points (**E**) of VIS model.

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

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

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

We initially obtain

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

In absence of attack, $I^\circ = 0$.

Consequently, the system (3) become

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

Therefore, the VIS model is free from attack at

$$E^\bullet = (V^\circ, I^\circ, S^\circ) = \left(\frac{\alpha}{\mu + \delta}, 0, \frac{\mu\alpha}{\delta(\mu + \delta)}\right) \tag{5}$$

4.3 Local Stability of DDoS-Free Equilibrium

In this section, we find out the adequate conditions for the local stability of the attack-free equilibria of the model.

We have

$$\begin{cases} \dfrac{dV}{dt} = \alpha - \beta V I - \mu V - \delta V = 0 \\ \dfrac{dI}{dt} = \beta V I - \varphi I - \delta I - \omega I = 0 \\ \dfrac{dS}{dt} = \varphi I + \mu V - \delta S = 0 \end{cases} \tag{6}$$

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

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

By considering the equation (5), we get

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

With the 3×3 Jacobian matrix, three eigenvalues will be obtained after solving the determinant of $|J^{\circ} - I\psi| = 0$.

Then,

$$\begin{cases} \psi_1 = -\delta \\ \psi_2 = -\mu - \delta \\ \psi_3 = \dfrac{\beta\alpha - (\mu+\delta)(\varphi+\delta+\omega)}{\mu+\delta} \end{cases} \tag{7}$$

Therefore, the three eigenvalues are
$\psi_1 = -\delta, \psi_2 = -\mu - \delta$ and $\psi_3 = \frac{\beta\alpha-(\mu+\delta)(\varphi+\delta+\omega)}{\mu+\delta}$

4.4 Basic Reproduction Number (BRN)

BRN is found from the eigenvalue that is not obviously negative out of the three eigenvalues (ψ_1, ψ_2 and ψ_3). So, in this case, the BRN will be determined from ψ_3.

We establish

$$\frac{\beta\alpha - (\mu+\delta)(\varphi+\delta+\omega)}{\mu+\delta} < 0 \tag{8}$$

Then,

$$\frac{\beta\alpha}{(\mu+\delta)(\varphi+\delta+\omega)} < 1 \tag{9}$$

By definition, the BRN is given by

$$R_0(V, I, S) = \frac{\beta\alpha}{(\mu+\delta)(\varphi+\delta+\omega)}, (\mu+\delta)(\varphi+\delta+\omega) \neq 0 \tag{10}$$

Remark

The proposed VIS model can be analysed based on the value of the basic reproduction number as follow.

- 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 $R_0 > 1$.

4.5 Global Stability of DDoS-Free Equilibria

Theorem 1

From (E°) in the system (3), the attack is globally free if $R_0 \leqslant 1$ in (Ω).

Proof

Let $(R_0 < 1)$, there will be a small $(\lambda_0 > 0)$ such that

$$\beta(\frac{\alpha}{\mu+\delta} + \lambda_0) - (\varphi+\delta+\omega) < 0 \tag{11}$$

From the system (1), we get

$$\frac{dV(t)}{dt} = \alpha - (\mu+\delta)V \tag{12}$$

For $(t_0 > 0)$,

$$V(t) \leqslant \frac{\alpha}{\mu+\delta}, (\forall t \geqslant t_0) \tag{13}$$

From the equation (13), and the second equation in the system (1), we obtain

$$\frac{dI(t)}{dt} \leqslant \beta(\frac{\alpha}{\mu+\delta} + \lambda_0)I - (\varphi+\delta+\omega)I \tag{14}$$

$$= [\beta(\frac{\alpha}{\mu+\delta} + \lambda_0) - (\varphi+\delta+\omega)]I(t) \tag{15}$$

From the Eqs. (11) and (15), we obtained

$$\lim_{t\to\infty} I(t) = 0 \tag{16}$$

From the equation (16) and the first equation in the system (1), we get

$$\frac{dV(t)}{dt} = \alpha - (\mu+\delta)V \tag{17}$$

From Equation (17), we get

$$\lim_{t\to\infty} V(t) = \frac{\alpha}{\mu+\delta} \tag{18}$$

By considering Eqs. (18), (16) and the third equation in the system (1), it follows tat $S(t)$ is asymptotic to the following system

$$\frac{dS(t)}{dt} = \delta S \frac{\mu\alpha}{\mu+\delta} \tag{19}$$

Then, by the theory for asymptotically autonomous semi flows

$$\lim_{t\to\infty} S(t) = \frac{\mu\alpha}{\delta(\mu+\delta)} \tag{20}$$

By considering all the Eqs. (16), (18) and (20), the prove is concluded.

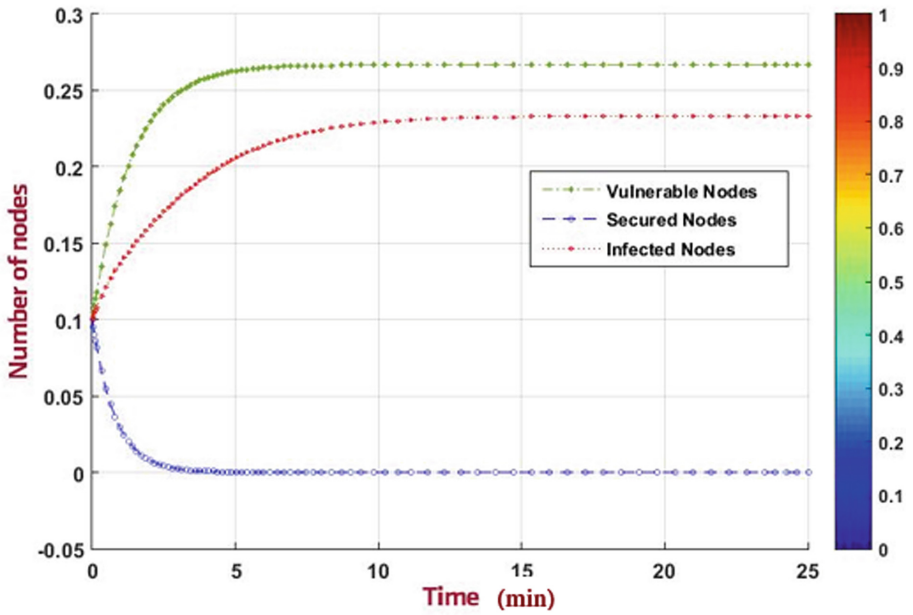

Fig. 4. General Stability of the VIS Model.

5 VIS Model Simulation

In this section, we evaluate the proposed VIS model to sustain the mathematical analysis of the DDoS attack in SDN-based 5G. The numerical simulations were carried out in Matlab.

However, the local stability of the attack free equilibrium as shown in Fig. 4 is considered over the unit time of 25 min with the following numerical

values: $V_0 = 0.1; I_0 = 0.1; S_0 = 0.1; \omega = 0.6; \delta = 0.2; \varphi = 0.4; \mu = 0.35; \beta = 0.15$ and $\alpha = 0.25$.

Nevertheless, we analyse each class of nodes (**V**, **I** and **S**) when we assume five different variations of the open population rate ($\alpha = 0.25, \alpha = 0.3, \alpha = 0.4, \alpha = 0.5$ and $\alpha = 0.7$) as shown in Figs. 5, 6, 7 and 8.

The variations of the open population rate (α) are related to the reality of SDN for 5G in term of Ultra-Reliable Low Latency Communication (URLLC) services that will increasingly affect the open population rate (α).

6 Discussion

Figure 4 presents the graphical representation of the three classes of nodes (**V**, **I** and **S**). Hence, the class **V** following by the class **I** increased over time while the class **S** decreased considerably over time. The gap observed between the three classes of nodes is significantly demonstrated the state of nodes when the DDoS attack occurred in any of the SDN-based 5G device.

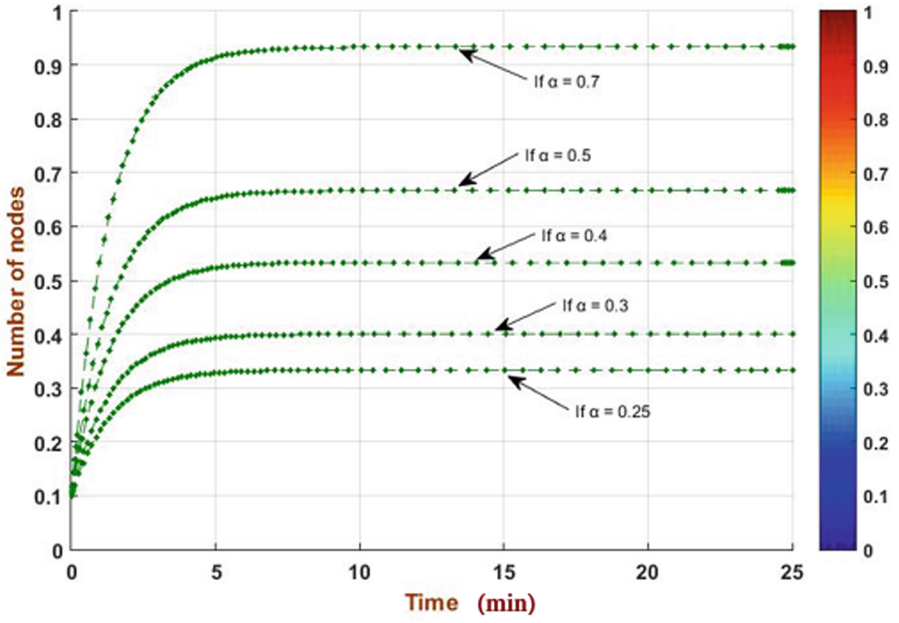

Fig. 5. General Stability of the Vulnerable Class when $\alpha = 0.25, \alpha = 0.3, \alpha = 0.4, \alpha = 0.5, \alpha = 0.7$.

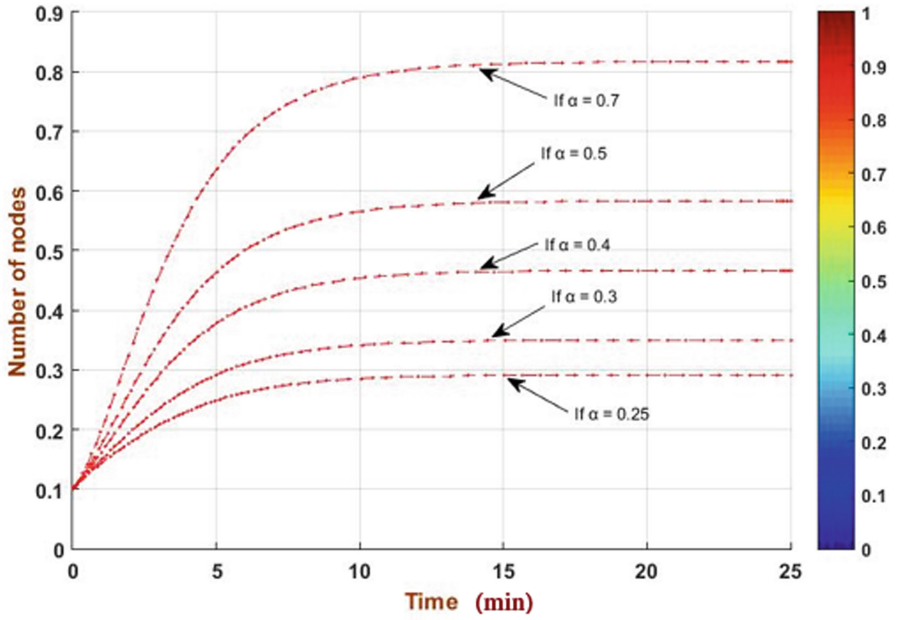

Fig. 6. General Stability of the Infected Class when $\alpha = 0.25, \alpha = 0.3, \alpha = 0.4, \alpha = 0.5, \alpha = 0.7$.

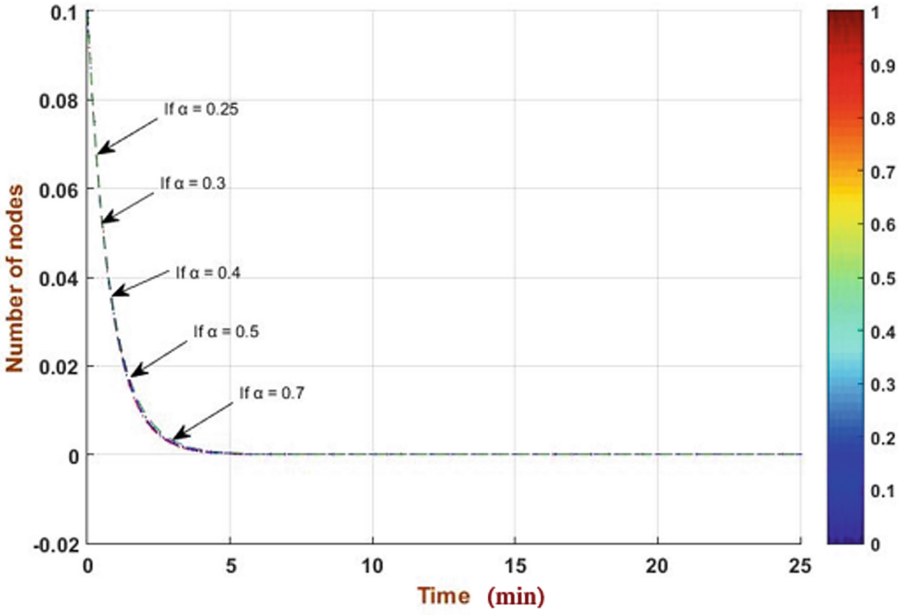

Fig. 7. General Stability of the Secured Class when $\alpha = 0.25, \alpha = 0.3, \alpha = 0.4, \alpha = 0.5, \alpha = 0.7$.

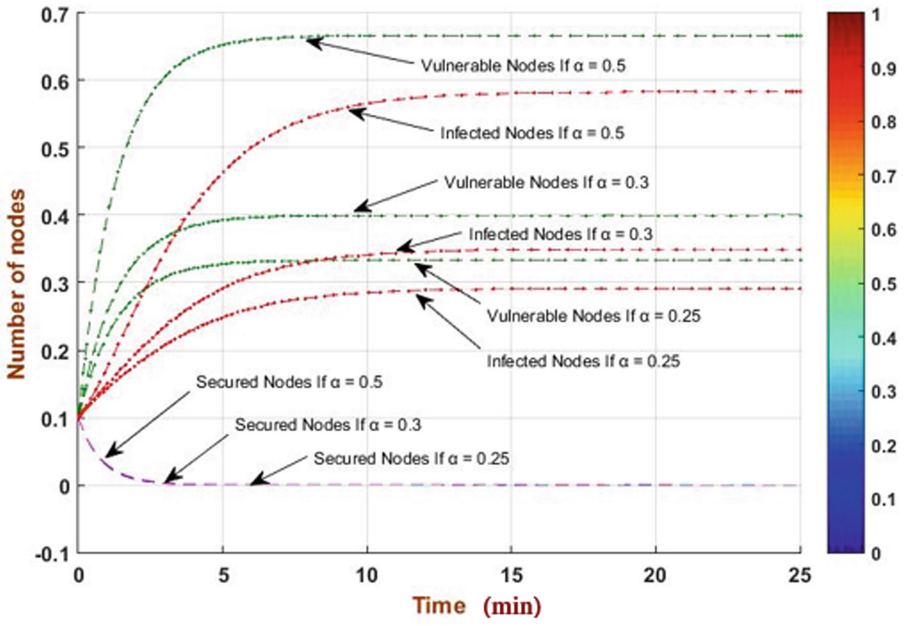

Fig. 8. General Stability of the VIS Model when $\alpha = 0.25, \alpha = 0.3, \alpha = 0.5$.

The Fig. 5 likewise the Fig. 6 show the gaps in which the number of vulnerable nodes and infected nodes respectively increases five times as the five different variations of the open population rate ($\alpha = 0.25, \alpha = 0.3, \alpha = 0.4, \alpha = 0.5$ and $\alpha = 0.7$) were considered over time. Unlike the previous results showed in Figs. 5 and 6, Fig. 7 presents a different result where there is approximatively no gap between the number of secured nodes even though the five different variations of the open population rate ($\alpha = 0.25, \alpha = 0.3, \alpha = 0.4, \alpha = 0.5$ and $\alpha = 0.7$) were applied over time.

As well, Fig. 8 presents a general graphical view of the VIS model in three different variations of the open population rate ($\alpha = 0.25, \alpha = 0.3$ and $\alpha = 0.5$) over time. The result showed in Fig. 8 is the compile results of the Figs. 5, 6 and 7 to confirm the full analysis of the proposed VIS epidemic model in the paradigm of SDN-based 5G technology.

7 Conclusion

In this research, a VIS epidemic model to analyse the DDoS attacks related to the great security issues of the DDoS in the SDN-based 5G technology was proposed. The mathematical formulation of the proposed model was numerically analysed using MATLAB. Furthermore, it was demonstrated that the DDoS attacks disrupt atrociously the well being of the targeted SDN-based 5G resource.

Besides, this manuscript enumerate clearly that the great advantages of SDN-based 5G technology are as high as the DDoS attacks are over-high in the great playground opened by the implementation of 5G technology. Consequently, the proposed VIS epidemic model laid down the problematic of the security issues of the DDoS attack in an environment where 5G technology is implemented as we refer to SDN-based 5G.

In the future, the research will look at the global stability of DDoS free equilibrium, the endemic equilibrium, the global hopf bifurcation and the optimal control analysis of the delayed VIS model. As well, it will implement the proposed VIS model in a real Telecom (5G) infrastructure under DDoS attacks.

Acknowledgement. The authors appreciate the support received from the Africa Centre of Excellence, ICT-Driven Knowledge Park (ACE OAK-Park), OAU, Ile-Ife in funding this research.

References

1. Santos, G.L., Endo, P.T., Sadok, D., Kelner, J.: When 5G meets deep learning: a systematic review. Algorithms **13**(9), 208 (2020)
2. Dutta, A., Hammad, E.: 5G security challenges and opportunities: a system approach. In: 2020 IEEE 3rd 5G World Forum (5GWF), pp. 109–114. IEEE (2020)
3. GSA: 794 organisations are deploying LTE or 5G Private Mobile Networks worldwide. Press Release published by Global mobile Suppliers Association, under 5G, Manufacturing, Market Research/Analysis, Small Cells, 15 Jun 2022. https://www.cambridgewireless.co.uk/news/2022/jun/15/gsa-794-organisations-are-deploying-lte-or-5g-priv/
4. Rosen, M.: Driving the digital agenda requires strategic architecture (2015)
5. Aujla, G.S., Singh, M., Bose, A., Kumar, N., Han, G., Buyya, R.: BlocksDN: blockchain-as-a-service for software defined networking in smart city applications. IEEE Netw. **34**(2), 83–91 (2020)
6. Accelerating the 5G future of business, 25 February 2020. https://www.accenture.com/us-en/insights/communications-media/accelerating-5g-future-business
7. Dzik, S.: COVID-19 convalescent plasma: now is the time for better science. Transfus. Med. Rev. **34**(3), 141 (2020)
8. Gündoğan, C., Amsüss, C., Schmidt, T.C., Wählisch, M.: Content object security in the internet of things: challenges, prospects, and emerging solutions. IEEE Trans. Netw. Serv. Manage. **19**(1), 538–553 (2021)
9. Dahiya, D.: DDoS attacks detection in 5G networks: hybrid model with statistical and higher-order statistical features. Cybern. Syst. (2022). https://doi.org/10.1080/01969722.2022.2122002
10. Dahiya, D.: DDoS attacks detection in 5G networks: hybrid model with statistical and higher-order statistical features. Cybern. Syst. 1–26 (2022)
11. Wu, P., Yao, L., Lin, C., Wu, G., Obaidat, M.S.: FMD: a DoS mitigation scheme based on flow migration in software-defined networking. Int. J. Commun. Syst. **31**(9), e3543 (2018)
12. Durner, R., Lorenz, C., Wiedemann, M., Kellerer, W.: 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, July 2017

13. Mohammadi, R., Javidan, R., Conti, M.: Slicots: an SDN-based lightweight countermeasure for TCP SYN flooding attacks. IEEE Trans. Netw. Serv. Manage. **14**(2), 487–497 (2017)
14. Wang, T., Chen, H., Qi, C.: MinDos: a priority-based SDN safe-guard architecture for DoS attacks. IEICE Trans. Inf. Syst. **101**(10), 2458–2464 (2018)
15. Kazmi, S.H.A., Qamar, F., Hassan, R., Nisar, K., Chowdhry, B.S.: Survey on Joint Paradigm of 5G and SDN Emerging Mobile Technologies: Architecture. Security, Challenges and Research Directions (2022)
16. Chen, M., Qian, Y., Mao, S., Tang, W., Yang, X.: Software-defined mobile networks security. Mob. Netw. Appl. **21**(5), 729–743 (2016)
17. Duan, X., Liu, Y., Wang, X.: SDN enabled 5G-VANET: adaptive vehicle clustering and beamformed transmission for aggregated traffic. IEEE Commun. Mag. **55**(7), 120–127 (2017)
18. Sheibani, M., Konur, S., Awan, I.: 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, August 2022
19. Yang, L., et al.: Analysis of psychological state and clinical psychological intervention model of patients with COVID-19. MedRxiv (2020)