International Journal of Applied Sciences and Smart Technologies

Volume 5, Issue 2, pages 271-302

p-ISSN 2655-8564, e-ISSN 2685-9432

A Detailed Review on The Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks in Software Defined Networks (SDNs) and Defense Strategies

Elvis Tamakloe[1, *], Benjamin Kommey [1], Emmanuel Akowuah [1], Daniel Opoku [1]

[1]*Faculty of Electrical and Computer Engineering, Kwame Nkrumah University of Science and Technology, PMB UPO, 00233, Ghana*
[*]*Corresponding Author: tamakloe.elvis@gmail.com*

(Received 15-05-2023; Revised 26-05-2023; Accepted 22-06-2023)

Abstract

The development of Software Defined Networking (SDN) has altered the landscape of computer networking in recent years. Its scalable architecture has become a blueprint for the design of several advanced future networks. To achieve improve and efficient monitoring, control and management capabilities of the network, software defined networks differentiate or decouple the control logic from the data forwarding plane. As a result of this, logical control is solely centralized in the controller. Due to the centralized nature, SDNs are exposed to several vulnerabilities such as Spoofing, Flooding, and primarily Denial of Service (DoS) and Distributed Denial of Service (DDoS) among other attacks. In effect, the performance of SDN degrades based on these attacks. This paper presents a comprehensive review of several DoS and DDoS defense/mitigation strategies and classifies them into distinct classes with regards to the methodologies employed. Furthermore, based on the discussions raised, suggestions have been made to enhance current mitigation strategies accordingly.

Keywords: Centralized controller, Software Defined Network (SDN), Denial of Service (DoS) attack, Distributed Denial of Service (DDoS) attack, Network security, Mitigation strategies

1 Introduction

Conventional networking infrastructures have great complexity with regards to monitoring, control, and management. That is, managing network devices in conventional networks poses a tremendous challenge since the configuration of this type of network is

This work is licensed under a Creative Commons Attribution 4.0 International License

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

based on organizational or supervisory policies. In conventional networks, logic control and data forwarding are tightly coupled together [1, 2]. This design architecture inhibits flexibility, increases operational cost, and retards innovation irrespective of certain initial benefits. Therefore, it implies that conventional networks are thus difficult to maintain [3] and cannot serve as the base for developing other emerging technologies like Internet of Things (IoT), Cloud, Big Data and many more since adequate bandwidth, adaptability and good manageability are required. Due to the paradigm shifts in networking architectures over the years, the impact of SDN since its development has adapted to meet current networking demands. By decoupling the control plane or logic and the data plane [4-6] in SDN architecture as depicted in Fig.1, network scalability, flexibility, and other security features are realized to enhance better network performance and management.

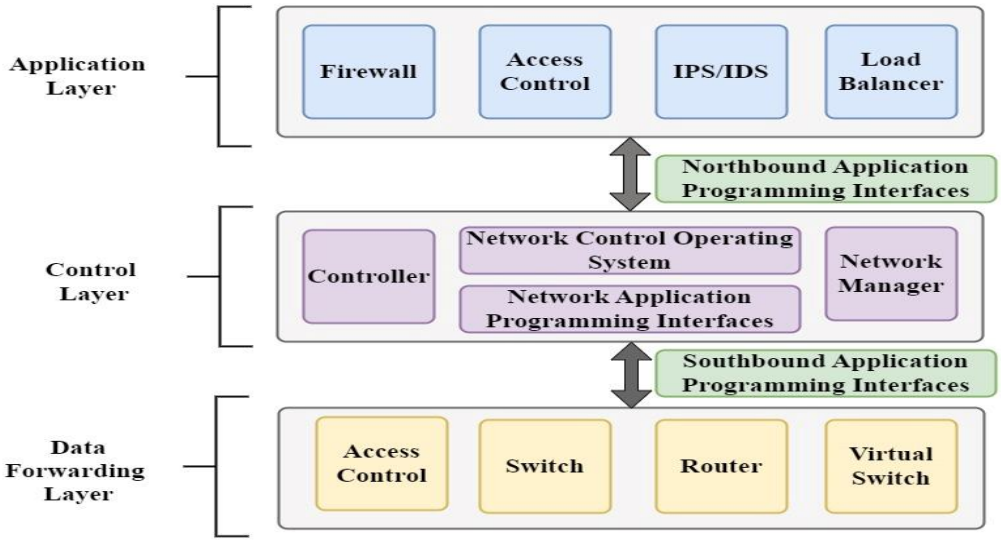


Figure 1. SDN architectural layers.

This design performs a vital task in relation to extensive and high-performance computer systems [7]. Based on this architecture, the critical network functions such as intrusion detection and routing amongst other functions are essentially handled by the linked control and application layer. In the controller, there exist an installed operating system (OS) which maps the entire network to a variety of applications and services realized in the application layer. The implementation of SDN application enables network operators or administrators to have greater control, automation, and optimization over the network [8]. A few protocols have been proposed for SDN however, the OpenFlow (OF)

Volume 5, Issue 2, pages 127-158
p-ISSN 2655-8564, e-ISSN 2685-9432

is the most used and standardized protocol which coordinates the control plane and the data plane via a southbound interface (control channel) [9, 10]. Switches enabled with OF have flow tables for storing flow rules for data forwarding. This implies that the switch compares the packet header with flow table's flow rules upon the arrival of a packet. Howbeit, in cases whereby no flow rule exists next to the data packet header, a table-miss results, and the data packet is transferred to the controller as a Packet-In message. This message is then processed by the controller and subsequently, a flow rule with the appropriate actions is sent towards the switch [11]. Therefore, it means that the switch's flow table comprise of data forwarding rules transmitted by the controller via the control channel. Additionally, it is imperative to note that the status of these rules is temporal since limited time is assigned to them after their installation. Thus, they are taken off from the flow table after this limited duration. Many recognized industry players in the network market like Hewlett-Packard (HP), Computer Information System Company (CISCO) etc., are integrating OF in the development of its switches. Although many advantages such as scalability, flexibility and manageability of the network have been drawn from implementing SDN, the decoupling of the control and data plane exposes the network to several or different attacks (conventional and modern) [12, 13]. In reference to these security issues DoS attacks or its distributed variant (DDoS) poses the most threat to the network in contrast to the other attacks. This implies that a successful DoS or DDoS attack has the tendency or ability to entirely disrupt the network by disabling the controller or switch [14, 15]. Hence, crippling both the control plane and data plane. In these attacks, switches are unable to appropriately transmit packets as required which results in network failure and subsequently, a system collapse. Therefore, this paper presents a detailed description of DoS and DDoS attacks on SDN infrastructure components, reviews a variety of techniques adopted to solve these attacks and provides a comprehensive study of these mitigation techniques as well as their benefits and limitations. Outlined in sections (2-6) are the most relevant areas that present a complete insight and in-depth analysis of DoS and DDoS attacks in SDN, and strategies developed to curb these attacks.

International Journal of Applied Sciences and Smart Technologies

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

2 Operation of the SDN architecture

The SDN architecture as illustrated in Fig.1 consist of three distinct and decoupled layers namely, the Application, Control and Data Forwarding layer. These respective layers contain certain vital components that allows for coordination. For instance, the application and control layer components coordinate via the Northbound API whilst the Southbound API facilitates communication between both the control and data forwarding layer. This implies that OpenFlow protocols are the most ubiquitous form of Southbound API [16] readily available to facilitate this particular form of interaction. The description of the three SDN layers together with the respective functionalities are as follows:

A. The Application Layer

It contains several applications (access control, firewall, load balancer, etc.) which via the northbound API, interact with the control layer in order to carry out expected tasks. The performance of these applications is independent of one another. Hence, they can be enabled or disabled based on requirements and network configuration by the administrator. In this regard, installing new applications are easy to perform and already existing applications can equally be uninstalled without affecting the operation of the SDN.

B. The Control Layer

This layer comprises of the centralized controller which has an embedded operating system (OS) that controls the entire SDN network. Here in this layer, the application layer's specifications are interpreted downwards to the data forwarding layer thus, providing an overview of the network. In relation to distributed software defined networks it is important to note that the coordination of the different controllers via the Westbound and Eastbound interfaces are made possible in this very layer. Aside the controller, the control layer houses other components like the network OS, APIs, and the network manager to facilitate a more efficient interaction and control of the network.

C. The Data Forwarding Layer

It is considered as one of the major blocks of the SDN architect since it is comprising of many essential devices like routers, switches, access control and virtual switch that supports the operation of the SDN network. Alternatively referred to as the

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

network infrastructure layer, the data forwarding layer employs devices that can be connected in several topologies as well as to hosts and servers. Thus, to be able to obtain flow rule to ensure data forwarding, every device in this very layer is linked to the controller via an exclusive connection. As illustrated in Fig.2, a simplified tree topology based SDN architecture is presented.

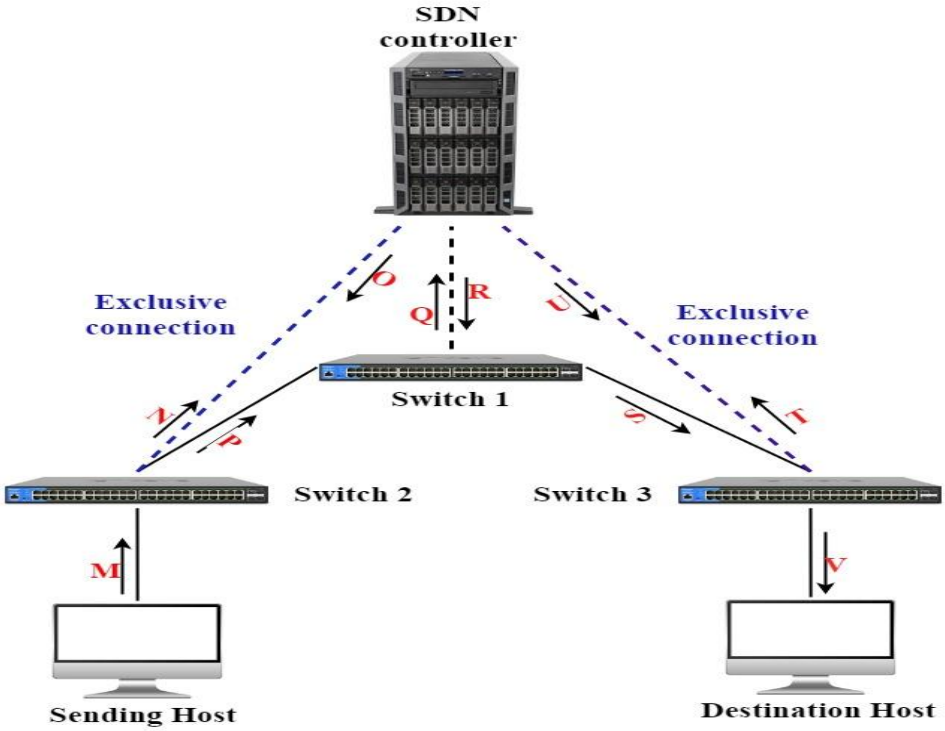


Figure 2. Simplified SDN architecture.

This simplified architecture consists mainly of a SDN controller, switches, the sending and destination or receiving host. To ensure a successful delivery of data from the sending host to the destination host, provided no flow rules are installed, it implies that a data packet must be first sent to switch 2 as indicated by process M. Afterwards, a packet-in message is then sent from switch 2 to the controller (process N). It is important to note that this is dependent on the network configuration, an exclusive connection (link) as well as the open flow version [6]. In responds, the controller delivers a packet-out message back to switch 2 (process O). Based on the feedback response from the controller, data packets are transferred from switch 2 to switch 1 for further actions. Upon the arrival of the data packets in switch 1, a similar activity (between switch 2 and controller) is carried out again with the controller to enquire with regards to the

Volume 5, Issue 2, pages 127-158
p-ISSN 2655-8564, e-ISSN 2685-9432

destination of the data packet. This is indicated by the process Q and R. The controller's response from switch 1 subsequently allows for data packets to be transferred to switch 3 (process S). The data packets are thereafter sent from switch 3 to the controller and back from the controller to switch 3 as shown by process T and U respectively. The data packets then received by the destination host via switch 3 as depicted by process V. Hence, to install the flow rules, all the processes (M, N, O, P, Q, R, S, T, U, V) must be successfully completed to guarantee the reception of data packets by the destination host from the sending host. Immediately these flow rules are installed, subsequent data packet deliveries are undertaken via only process M, P, S, and V as well as through all the respective switches. However, in the event of a role reversal (whereby the destination host becomes the sender, and the sending host becomes the destination host) a new flow rule must be installed. Therefore, the movement of data packets would be in the opposite direction.

3 DoS and DDoS attacks in SDN

The centralized nature of the SDN network, exposes it to certain severe attacks and security threats. Notable amongst these are Denial of Service and its distributed variant (DDoS) [17, 18]. A Denial-of-Service attack is a system-to-system security threat that occurs when data packets are flooded towards a targeted system (destination like server, web application etc.) in a manner that new flow rules are required for every data packet involved. The goal of this kind of attack is to overwhelm the processing ability of the targeted system in order to make its resources unavailable. The severity of this attack grows on much larger scale with DDoS when spoofed packets containing arbitrary addresses (sending and destination addresses) are sent by multiple systems to a targeted system in such a way that resources of the network are made inaccessible to authorized users. Furthermore, DoS attacks and its variants can be launched to consume especially bandwidth and other vital network resources. The repercussion of these attacks on the SDN infrastructure is mostly costly as its effect extends to the application, control, and data forwarding layer as a result of their evolving nature.

International Journal of Applied Sciences and Smart Technologies

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

Table I. Summarized comparison between DoS and DDoS in SDN

Denial of Service (DoS)	**Distributed Denial of Service (DDoS)**
It originates from a single source to overwhelm targeted resources	It emanates from multiple sources to inflict damage.
Rate of attack is slow	Rate of attack is very fast
Less traffic volumes are forwarded to targeted resources	Much larger traffic volumes are forwarded since it is a coordinated attack.
It is relatively easier to detect and trace the origin of attack	It is complex to detect and trace due to many disguised attack origins.

4 The Taxonomy of DoS and DDoS attacks

To provide solutions to the aforementioned attacks upon their detection, it is essential to classify them into respective groups so as to easily identify and efficiently administer the most appropriate mitigation technique or strategy to aid in combatting these attacks.

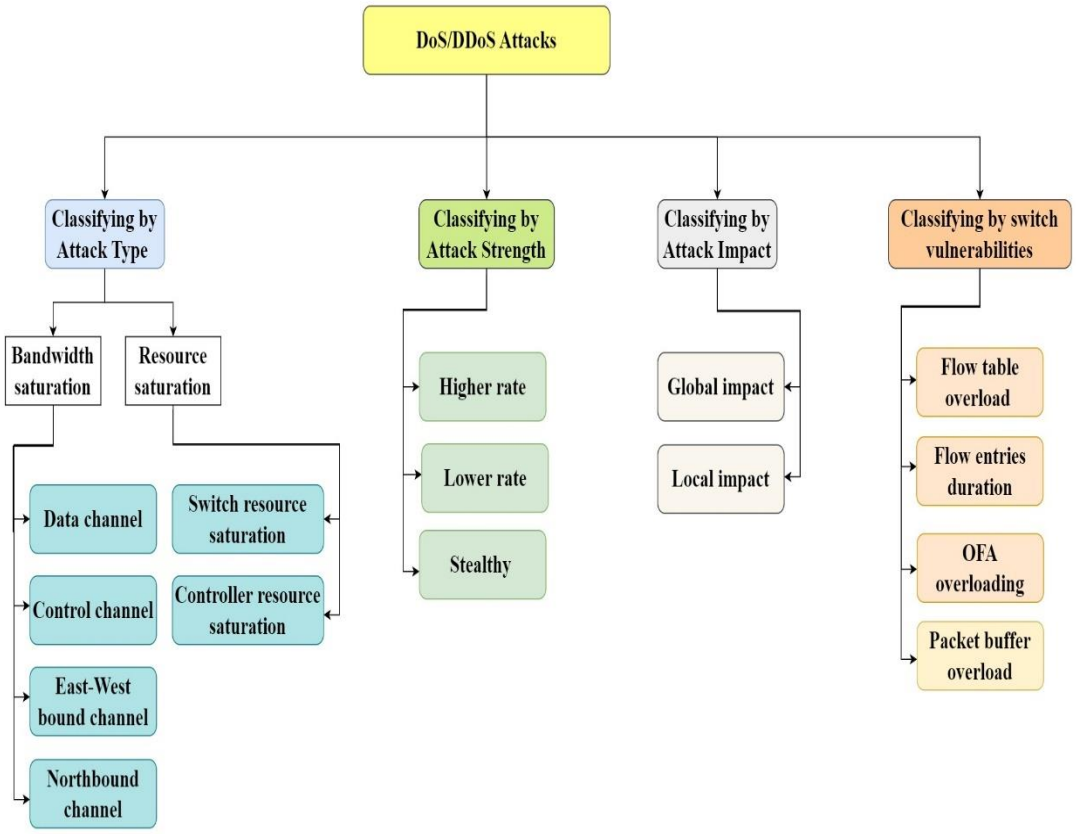


Figure 3. Taxonomy of DoS/DDoS attacks in SDN architecture.

Volume 5, Issue 2, pages 127-158
p-ISSN 2655-8564, e-ISSN 2685-9432

A variety of classifications of the denial of service and its distributed variant is presented in Fig.3 based on the attack type, strength, impact, and vulnerabilities of the OpenFlow data forwarding switches.

A. Classifying by Attack Type

The category of DoS/DDoS attacks which primarily seeks to exploit the different interfaces (channels or APIs) in SDNs [19-22] by solely forwarding enormous size of spoofed data packets with the intention to flood and consume channel bandwidth is termed as Bandwidth saturation attacks. As opposed to bandwidth saturation, resource saturation attacks mainly aim at overwhelming the resources (physical memory/RAM, processor/CPU) of the devices (controllers, switches etc.) in the SDN network. Subsequently, successful launch of these attacks results in high latency, total degradation of the quality of service (QoS) and unavailability of service to authorized users [23].

B. Classifying by Attack Strength

In reference to the transmission rate of the attack data packets forwarded towards the target SDN network, DoS/DDoS attacks can again be categorized based on strength. This implies that, given DoS/DDoS attacks with higher attack strength compared with the target network, a successful launch causes heavy damage to the switch's resource and simultaneously congesting the southbound API (control channel). More so, with regards to attacks possessing lower attack strength than the target SDN, a sizeable amount of the bandwidth that has been apportioned to authorized users is hijacked. This type of attacks is difficult to detect and are capable of remaining untraceable and active. A typical illustration is the attack employing mobile botnet [24]. In Stealthy attacks, attack flows are made to last in the flow table for a short idle_timeout value. This makes such attacks undetectable since these flow entries quickly expire in the switch before the networks defensive mechanisms are triggered. Thus, it imposes a long-term effect (financial loss) on the network.

C. Classifying by Attack Impact

There are mainly two classes of the impact of DoS/DDoS attacks on different target modules. These include the local and global impact. The impact of an attack is termed local provided the whole network experiences no malfunction. That is, only hosts that are

Volume 5, Issue 2, pages 127-158
p-ISSN 2655-8564, e-ISSN 2685-9432

connected directly or indirectly to the switches in worst-case scenario are affected. This type of impacts is mostly undetectable in the network and causes a long-term effect on the network. Conversely, the impact of an attack is defined as global when the whole network is prone to entirely fail, malfunction and collapse upon its successful launch. Therefore, this implies that, authorized users of the network are can neither send nor receive data in this regard [25-27].

D. Classifying by Switch Vulnerabilities

The quest to provide scalability and control in SDN, has resulted in the exposure of the OpenFlow switches in the network to be targeted by DoS/DDoS attacks. These include flow table overloading, target buffer overflow, altering of flow entries duration and open flow agent (OFA) overloading. It is imperative to note that OpenFlow switches have limited memory and processing capabilities [28]. When a target switch is flooded with data packets (having several addresses) by an immediate host, the flow table is searched for each data packet and subsequently forwarded to the controller which installs flow rules against the respective packets. However, due to the enormous amount of data packets, the flow table is bound to overflow. Thus, in this situation, the controller can therefore, not assign new flow rules due to the limited capacity which leads to packet drops. Additionally, overloading of the OFA potentially results due to these aforementioned points. In the event of a target buffer overflow, forwarding of a complete packet causes successive and extensive use of the controller's resources [29]. This in effect increases latency and response time as well as magnifies the rate of packet loss [30]. Hence, DoS/DDoS attacks exploits all these raised issues to inflict damage to the network. Furthermore, the timeout mechanisms (idle_timeout and hard_time) employed in flow entry durations provides an avenue for stealthy DDoS attacks which makes use of the minimal durations to send attack flows. Thus, crippling the SDN in a long term.

5 Mitigating strategies and probable challenges

Volume 5, Issue 2, pages 127-158
p-ISSN 2655-8564, e-ISSN 2685-9432

To curb or curtail the DoS/DDoS attacks in Software Defined Networks (SDNs), different detection and mitigation strategies have been developed to repel and safeguard the network against such threats [31-34]. These mitigation strategies can be grouped as follows:

A. Machine Learning Strategy

This type of mitigation technique is currently employed in most SDNs as one of the effective defense strategies to combat DoS/DDoS attacks. To safeguard the SDN network against the aforementioned attacks, in [35], an adversarial deep learning approach detection and defense was proposed. This approach employed a Generative Adversarial Network (GAN) framework to detect DDoS attacks and utilized adversarial training to make network system less sensitive to experimented adversarial attacks. The network traffic was sampled and analyzed every one second to achieve almost real-time results (detection response time). Although this approach delivered a performance score of about 95.54%, it was limited to only common and recent types of DDoS attacks. A Monte Carlo tree search (MCTS) algorithm was presented in [36] to generate adversarial examples of cross-site scripting (XSS) attacks. In this work, the algorithm is made to allow the generation model to proffer reward value that depicts the likelihood of the generative examples bypassing the detector. A generative adversarial network (GAN) framework was employed to optimize and increase the detection rate of these attacks. The percentage of improvement with respect to the accuracy was significant. However, rigorous training is required over several iterations to ensure an increase in the detection rate. In [37], a deep neural network model to safeguard against adversarial examples was proposed. In this regard, it is evident that different machine learning techniques can be used to safeguard software defined networks [38-40].

B. Policy and Resource Management Strategy

Providing protection against DoS/DDoS attacks requires adaptive policies that would render some degree of security for the network. In contrast to conventional networks which are managed based on static security policies, it is fundamentally advantageous to define dynamic security policies for SDN based on the system properties and network statistics. Thus, by configuring and managing the SDNs resources, DoS attacks are avoided. In [41],

Volume 5, Issue 2, pages 127-158
p-ISSN 2655-8564, e-ISSN 2685-9432

a two-level balancing solution composed of conventional and load balancing between servers and network devices respectively was proposed. This method employs Callophrys and efficiently distributes traffic between all alternative routes in the SDN network. In effect, this approach increases the survival time of the network during DDoS attacks. A software defined-internet of things (SD-IoT) algorithm was proposed in [42] to mitigate DDoS attacks. This algorithm efficiently gets the threshold value of the cosine similarity of the vectors of the packet-in rate and subsequently determines the occurrence of a DDoS attack based on the value. Hence, employing both the SD-IoT framework and algorithm enables the blockage and traceability of these attacks. Therefore, the use of policies and resource management mitigation strategies equally offer protection for SDNs against DoS/DDoS attacks [43-45].

C. Deception, Blocking/Dropping Strategy

Creating unpredictable surfaces by altering the properties of the network system is another mechanism employed to guard against adversarial DoS/DDoS attacks. Blocking entails obstructing the port carrying the malicious host and extends to dropping such traffics. These strategies are, therefore, key to ensuring the safety and reliability of software defined networks. A DaMask architecture was presented in [46] as a control structure to enable efficient attack reactions in software defined networks and cloud-based computing. It embodies an anomaly detection module for matching flow packets with attack patterns and a mitigation module to facilitate in proffering the right solution upon detection of a DoS/DDoS attack. To surmount DoS attacks and it distributed variant, [47] suggested a distributed Firewall having Intrusion Prevention Security (IPS) capabilities. Here, incoming data packets are acted upon based on the firewall statistics and flow rules embedded in the switch. Detection of any malicious anomaly leads to the forwarding of packets to the controller for detailed analysis to be performed. If an attack is confirmed, the installed firewall rules immediately drop the malicious traffic. Several blocking strategies have been proposed in [48-50] to mitigate DoS/DDoS attacks in SDN infrastructure. Therefore, this strategy can be adopted to effectively safeguard the network against these attacks. However, it is imperative for the system to also distinguish clearly between false alarms (false cases of DoS/DDoS attacks) and real attacks to avoid blocking or dropping of legitimate users.

Volume 5, Issue 2, pages 127-158
p-ISSN 2655-8564, e-ISSN 2685-9432

D. Delaying and Collaborative Strategy

Safeguarding a software defined network against DoS/DDoS attacks can be achieved by an individual network or through a collaboration between multiple networks. More importantly, individual networks employ delaying as a strategy to mitigate denial of service attacks. In contrast to deception and blocking strategy, delaying approach keeps malicious traffics but under controlled circumstances. This implies that low trust-value is assigned to this type of traffic to allow some degree to communication with the network but at a very limited rate. Regardless of this mitigation approach, malicious traffic however consumes some amount of network resources in the long term. In relation to this subject, different works have been conducted to provide solutions to effectively optimize delay strategies to protect SDNs against the attack. In [51], every new and incoming data packet is assigned with a trust or priority value which is internet protocol based. Data packets are prioritized on mainly the trust value and are subsequently forwarded to the controller as packet headers. Thus, in this manner, DDoS attacks are well mitigated by efficiently utilizing the resource management switch. Other alternative methods have been proposed as FlowRanger in [52] to enable network controllers to effectively prioritize the mitigation solution. This is achieved with a trust management, queuing management and request scheduling modules to allocate to every flow request a trust or priority value, maintain numerous queues with several priority and employ weighted round-robin for processing queues respectively. In view of this, delaying can therefore be classified as an alternative measure to guard software defined networks against DoS/DDoS attacks [53-58]. Table II. presents an overview of the discussed mitigation strategies proposed in different related works for detection and safeguarding of the software defined network against DoS/DDoS attacks.

Table II. Overview of different DoS/DDoS mitigation strategies in SDN

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

Author	Type of mitigation strategy	Area of focus	Overview
[59]	Machine Learning	Control and Data Forwarding Layer	Presented a Woodpecker with an effective Heuristic algorithm for mitigating DDoS attacks (Link Flooding Attach)
[60]	Machine Learning	Control Layer	Proposed a deep learning approach to achieve greater detection accuracies of DDoS attacks in real time and with the aim to reduce SDNs resource dependency
[61]	Machine Learning	Application Layer	Suggested a blockchain framework known as Cochain-SC having an intra and inter-domain strategies to realize real time detection and mitigation of DDoS attacks.
[62]	Machine Learning	Control Layer	Developed a mitigation strategy based on the flow table's hit rate gradient (time feature) and adopted a real time detection and defense against DDoS attacks by employing a back propagation neural network.
[63]	Machine Learning	Application Layer	Presented a blockchain -based framework (Cochain-SC) with intra and inter-domain DDoS mitigation. The respective domains achieved real time detection and mitigation of illegitimate flows inside the domain as well as facilitate the collaborative among SDN-based domain peers.
[64]	Machine Learning	Data Forwarding Layer	Proposed an Ethereum blockchain which utilized smart contracts to defend SDN against DDoS attacks across several domains via detection algorithms and filter systems.
[65]	Policy and Resource Management	Control Layer	Presented a random route mutation (RRM) that puts together game theory and constraints satisfaction optimization to get the most preferred strategy for DoS/DDoS attack deterrence.
[66]	Policy and Resource Management	Data Forwarding Layer	Suggested an AVANT-GUARD to guard against resilient TCP SYN flood. Based on actuating triggers, the detection, response, and control of the traffic rate are thereby mitigated.

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

[67]	Policy and Resource Management	Control and Application Layer	Offered a Dossy application which operates in the application layer to curtail DoS attacks. This approach employed flow and packet-in analysis to deliver messages to detect and prevent DoS attacks in SDN
[68]	Policy and Resource Management	Control and Data Forwarding Layer	Presented a lightweight DoS detection and mitigation system known as FlowFence. It essentially comprises of switches and controller for detection of traffic congestion and bandwidth flows control respectively.
[69]	Policy and Resource Management	Control and Application Layer	Proposed a framework called FloodDefender to defend the controller against DDoS attacks. Mitigation is achieved by the utilization of packet-in message for attack detection, filtering of packets and efficient management of flow rules.
[70]	Policy and Resource Management	Control Layer	Suggested an SDNManager that mainly expects constant monitoring of flow information and future estimation of demands of bandwidth in the SDN. It therefore implies that, penalization of flows exceeding required estimates exist to facilitate mitigating the network against attacks.
[71]	Policy and Resource Management	Control Layer	Presented a mechanism to mitigate DDoS attacks by dropping packets dependent on the packet-in thresholds. In this regard, packets and bytes counts are the required parameters or statistics for the controller to ensure detection of such attacks.
[72]	Policy and Resource Management	Control Layer	Recommended an effective mechanism to guard against DDoS attacks by monitoring the fairness of packet-in messages or packet ratios and distribution of hosts.
[73]	Policy and Resource Management	Control and Data Forwarding Layer	Addressed low-rate DoS attacks by installing and monitoring flow rules on respective switches to facilitate detection of low-rate TCP attacks. Thus, reduction in bandwidth and mitigation on ingress switches were proposed as a solution to this type of attack via constant monitoring.
[74]	Blocking and dropping	Control Layer	Proposed the implementation of SLICOT in the controller to safeguard SDN against TCP SYN flooding attacks. This was

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

			achieved by installing provisional forwarding rules in TCP handshaking processes and after request validations. Thus, its capability of detecting and blocking malicious requests that would potential jeopardize the SDN.
[75]	Blocking and Dropping	Application and Data Forwarding Layer	Presented an architecture that employs OpenFlow and sFlow to detect and mitigate DoS attacks. Detection of anomalies are done with an entropy-based algorithm and dependent on sampled data from the sFlow. Hence, alteration of the flow table and its entries ensures the safety of SDN by blocking malicious traffic.
[76]	Blocking and Dropping	Control Layer	Suggested a vital framework called NIMBUS for detecting DoS/DDoS attacks by thoroughly analyzing traffics. This implies that malicious traffic is blacklisted or rate limits applied with auto scalable VMs to ensure effective mitigation.
[77]	Blocking and Dropping	Control Layer	Presented a link flooding attacks (LFA)Defender which explores or inspects the SDN to recognize probable target links, reroute traffics in events of congestion and blocks harmful traffics. This provides the requisite flexibility and economic efficiency.
[78]	Blocking and Dropping	Control Layer	Proposed an architecture referred to as RADAR to enable detection of DDoS attacks by utilizing adaptive correlation analysis. Thus, by employing a port-based max-min fairness approach, malicious traffics are dropped via analysis
[79]	Blocking and Dropping	Data Forwarding Layer	Incorporated the data plane in the defense mechanism to eliminate dependency on the network controller in the control layer. In this regard, detection of DoS/DDoS attacks is made by propagating alarm across the SDN using probe packets. As a result, mitigation measures (traffic dropping, IP obfuscation) were adopted to handle these malicious traffics. A typical example is with respect to FastFlex.

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

[80]	Blocking and Dropping	Data Forwarding Layer	Proposed a policy enforcement engine known as Poseidon to defend DDoS attacks. This utilized modularized defense primitives to throttle denial of service attacks and its distributed variant in SDN
[81]	Blocking and Dropping	Application and Data Forwarding Layer	Introduced a new security plane along with the data plane. Imperatively, this is parallel to the control plane. Pyretic is used by switches in the data plane to forward packets to detection engines. To throttle DDoS attacks, these engines forward the right rules to the controller for insertion into switches. Hence, effective for safeguarding SDN against malicious attacks.
[82]	Blocking and Dropping	Application and Data Forwarding Layer	Proposed a transparent intrusion detection system (TIDS) which offers a distributed and scalable remedy against DDoS attacks. To achieve detection of intruders and mitigating low-level DoS attacks, a polling processor is employed to perform analysis on flows, recognize anomalies and forward modified requests of flows to realize the blocking of malicious addresses.
[83]	Delaying and Collaborative Strategy	Control Layer	DrawBridge was proposed to facilitate between ISPs and hosts an end-to-end effective/reliable communication. Implemented in SDN as a controller, it forwards flow rules to switches in the ISP and interacts with other controllers in the ISP upstream. Thus, it enables filtering of malicious DDoS traffics via thorough verification, processing and deployment of flow rules.
[84]	Delaying and Collaborative Strategy	Control Layer	Developed an SDN controller-to-controller based protocol for collaborative defense against DDoS attacks. This protocol enables secure interaction and exchange of attack information between established SDN controllers. Thus, this allows for effective monitoring, alert of malicious paths and filtering of traffics close to the source attack
[85]	Delaying and Collaborative Strategy	Application and Control Layer	Proposed a FireCol architecture as an effective solution against flooding DDoS attacks based on early detection. The

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

			architecture incorporates intrusion prevention systems (IPSs) for creating virtual shield rings around hosts. This imperatively ensures the exchange of vital traffic information to safeguard end users and the entire network's infrastructure.
[86]	Deception and Moving Target Strategy	Control Layer	Proposed a smart moving target defense linked proactive and reactive virtual machine migration scheme. This scheme improves or optimizes the migration frequency to reduce resource wastage and curb attack impacts. In this regard, protection against DDoS attacks is improved by employing false reality pretense to repel malicious attacks and study attack patterns.
[87]	Deception and Moving Target Strategy	Control Layer	Presented a controller placement camouflage solution to effectively alter the attack surface in moving target defense. A stochastic game (Zero-Sum) is used to lead the MTD solution between the system defender and attacker. Thus, this technique enables real time risk evaluation of network vulnerabilities based in a Bayesian Attack Graph and constantly shifts the location of the SDN controller.
[88]	Deception and Moving Target Strategy	Control Layer	Introduced an agile architectural framework to exploit SDN and NFV by applying moving target defense and network forensics techniques. Interested traffics are stored by the VCP framework and forwarded to the SDN controller for thorough analysis. Route mutation was employed to guard against DDoS attacks by obfuscating the network's topology information. Thus, an effective MTD strategy for protecting SDN although much storage of traffic data is required.
[89]	Deception and Moving Target Strategy	Control Later	Addressed protection against DDoS attacks by leveraging MTD security in SDN enabled cloud infrastructure. Reduction in frequency and selection of location of target mobility across heterogeneous VM based on the probability of the attack was the focal point for subsequent framework

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

			development. This proved effective based on low success rate of attacks.
[90]	Deception and Moving Target Strategy	Control Layer	Developed an SDN-based MTD system known as CHAOS to obfuscate the attack surfaces to enhance the uncertain and unpredictable nature of the environment. This is best achieved with the proposed Chaos Tower Obfuscation algorithm. Therefore, this offers several degrees of obfuscation for hosts thus, enabling the realization of moving target defense in SDN controller based networks.

Upon reviewing DoS/DDoS attacks, its effects on the SDN architecture (layers) and several mitigation strategies adopted to guard networks against them, it is vital to find an optimal and robust security that guarantees protection for legitimate users from all forms of vulnerabilities. Practically, this is very essential for integration on other modern networks or frameworks like the SDN-IoT networks [91-93], smart grid security networks [94-100], industrial networks [101-105], enterprise networks [106-109], backbone networks [110-115], 5G networks [116-118], and software defined network optical networks (SDON) [119, 120]. Therefore, future works can incorporate certain combinations of the reviewed mitigation or defense strategies with modules capable of:

1. Efficiently detecting real-time attacks with optimal response time
2. Effective processing of data packets
3. Adding extra traffics to enable effective verification
4. Ensuring the long-term reliability of the SDN

Hence, it is worth noting that, the quantity and quality of network traffics are essential parameters for thorough examination and assessment of the discussed defense or mitigation strategies in SDN.

6 Conclusions

The scalability, control, and manageability of SDNs offer network developers a flexible platform to fabricate and run self-made protocols without changing existing hardware in the network. This dynamism had made it a preferred choice with regards to current and future network developments. Considering the drawbacks in reference to

security in SDNs, this paper presented a detailed review of potential mitigation strategies to tackle most well-known DoS and DDoS attacks. Furthermore, based on the discussed methods, it is thus essential to enhance current mitigation strategies more collaboratively to ensure faster and efficient attack detection, maximum security, reliability and longevity to SDN infrastructures.

References

[1] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F.De Turck and R. Boutaba, Network Function Virtualization: State-of-the-Art and Research Challenges. IEEE Communications Surveys & Tutorials, 18(1) (2016) 236-262.

[2] D. Kreutz, F.M.V. Ramos, P.E. Verissimo, C.E. Rothenberg, S. Azodolmolky, and S. Uhlig, Software-Defined Networking: A Comprehensive Survey. Proceeding of the IEEE, 103(1) (2015) 14-76.

[3] R. Masoudi, and A. Ghaffari, Software defined networks: A survey. Journal of Network and Computer Applications, 67 (2016) 1-25. 2016.

[4] X. Zhang, L.Cui, K. Wei, F.P. Tso, Y. Ji, W. Jia, A survey on stateful data plane in software defined networks. Computer Networks. 184, (2021) 107597.

[5] Q. Waseem, W.I.S.W. Din, A. Aminuddin, M.H. Mohammed, R.F.A. Aziza, Software-Defined Networking (SDN): A Review. 5th International Conference on Information and Communications Technology, (2022) 30-35.

[6] M. Imran, M.H. Durad, F.A. Khan, and A. Derhab, Toward an optimal solution against Denial of Service attacks in Software Defined Networks. Future Generation Computer Systems 92, (2019) 444-453.

[7] Q. Yan, F.R. Yu, Q. Gong, and J. Li, Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey. Some Reseach Issues, and Challenges. IEEE Communications Surveys & Tutorials, 18 (1) (2016) 602-622.

[8] I. Ahmad, S. Namal, M. Ylianttila,and A. Gurtov, Security in software defined networks: A survey. IEEE Communications Surveys & Tutorials, 17(4) (2015) 2317-2346.

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

[9] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 38(2) (2008) 69-74.

[10] K. Alghamdi, and R. Braun, Software Defined Network (SDN) and OpenFlow Protocol in 5G Network.Communications and Networks 12 (2020) 28-40.

[11] K. Rowan, V. Kotronis, and P. Smith, Openflow: A security analysis. 21st IEEE International Conference on Network Protocols, IEEE. (2013).

[12] A. Izzat, and D. Xu, Security of software defined networks: A survey. Computer Security, 53 (2015) 79-108.

[13] M.D. Firoozjaei, J.P. Jeong, H. Ko, H. Kim, Security challenges with network functions visualization. Future Generation Computer Systems, 67 (2017) 315-324.

[14] H. Beitollahi, and G. Deconinck, Analyzing well-known countermeasures against distributed denial of service attacks. Computer Communication, 35(11) (2012) 1312-1332.

[15] A. Shameli-Sendi, M. Pourzandi, M. Fekih-Ahmed, and M. Cheriet, Taxonomy of Distributed Denial of Service mitigation approaches for cloud computing. Journal of Network and Computer Applications, 58 (2015) 165-179.

[16] J. Suárez-Varela, and P. Barlet-Ros, Flow monitoring in Software Defined Networks: Finding the accuracy/performance tradeoffs. Computer Networks, 135 (2018) 289-301.

[17] M.B. Jiménez, D. Fernández, J.E. Rivadeneira, L. Bellido, and A. Cárdenas, A Survey of the Main Security Issues and Solutions for the SDN Architecture. IEEE Access, 9 (2021) 122016-122038.

[18] J.F. Balarezo, S. Wang, K.G. Chavez, A. Al-Hourani, and S. Kandeepan, "A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual network." Engineering Science and Technology, an International Journal , 31 (2022) 1-15.

[19] C. Hu, K. Hou, H. Li, R. Wang, P. Zheng, P. Zhang, and H. Wang, SoftRing: TAming the reactive model for software defined networks. 2017 IEEE 25th International Conference on Network Protocols, ICNP, IEEE, (2017) 1-10.

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

[20] K. Kalkan, G. Gür, and F. Alagöz, SDNScore: A statistical defense mechanism against DDoS attacks in SDN environment. Computers and Communication (ISCC), 2017 IEEE Symposium, IEEE , (2017) 669-675.

[21] M. Alsaeedi, M.M. Mohammad, and A.A. Al-Roubaiey, Toward adaptive and scalable OpenFlow-SDN flow control: A survey. IEEE Access, 7 (2019) 107346-107379.

[22] Z. Latif, K. Sharif, F. Li, M.M. Karim, S. Biswas, and Y. Wang, A comprehensive survey of interface protocols for software defined networks. Journal of Network and Computer Applications, 156 (2020).

[23] M.P. Singh, and A. Bhandari, New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges. Computer Communications, 154 (2020) 509-527.

[24] K. Ahmad, S.S.A. Ali, S.R. Bin, A. Muhammad, M.N. Rafidah, and S. Shahaboddin, Mobile botnet attacks-an emerging threat: Classification, review and open issues. KSII Transactions on Internet and Information System, 9 (4) (2015) 1471-1492.

[25] Y. Lui, B. Zhao, P. Zhao, P. Fan, and H. Liu, A survey: Typical security issues of software-defined networking. China Communication, 16 (7) (2019) 13-31.

[26] Y. Xiao, Zj. Fan, A. Nayak, and Cx. Tan, Discovery method for distributed denial-of-service attack behaviour in SDNs using a feature-pattern graph model. Frontiers of Information Technology and Electronic Engineering, 20 (2019) 1195-1208.

[27] S.Q.A. Shah, F.Z. Khan, and M. Ahmad, The impact and mitigation of ICMP based economic denial of sustainability attack in cloud computing environment using software defined network. Computer Networks, 187 (2021).

[28] M. Ayan, S. Misra, and I. Maity, Buffer size evaluation of openflow systems in software-defined networks. IEEE Systems Journal, 13 (2) (2019) 1359-1366.

[29] A. Mondal, S. Misra, and I. Maity, Buffer Size Evaluation of OpenFlow Systems in Software-Defined Networks. IEEE Systems Journal, 13(2) (2019) 1359-1366.

[30] Z. Guo, Y. Xu, R. Liu, A. Gushchin, Ky. Chen, A. Walid, and H.J. Chao, Balacing flow table occupancy and link utilization in software-defined networks. Future Generation Computer Systems, 89 (2018) 213-223.

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

[31] R. Swami, M. Dave, and V. Ranga, Software-defined Networking-based DDoS Defense Mechanisms. ACM Computing Surveys, 52(2) (2019) 1-36.

[32] A. Shaghaghi, M.A. Kaafar, R. Buyya, and S. Jha, Software-defined network (SDN) data plane security: Issues, solution, and future directions. Handbook of Computer Networks and Cyber Security. Springer, (2020) 341-387.

[33] I. Farris, T. Taleb, Y. Khettab, and J. Song, A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems. IEEE Communications Surveys & Tutorials, 21(1) (2019) 812-837.

[34] D.B. Rawat, and S.R. Reddy, Software Defined Networking Architecture, Security and Energy Efficient: A Survey. IEEE Communications Surveys & Tutorials, 19(1) (2017) 325-346.

[35] M.P. Novaes, L.F. Carvalho, J. Lloret, and M.L. Proença Jr,. Adversarial Deep Learning approach detection and defense against DDoS attacks in SDN environments. Future Generation Computer Systems, 125 (2021) 156-167.

[36] X. Zhang, Y. Zhou, S. Pei, J. Zhuge, and Chen, Adversarial Examples Detection for XSS Attacks Based on Generative Adversarial Networks. IEEE Access, 8 (2020) 10989-10996.

[37] K. Groose, N. Papernot, P. Manoharan, M. Backes, and P. McDaniel, Adversarial Examples for Malware Detection. S.N. Foley, D. Gollmann, E. Snekkenes (Eds.) Computer Security - ESORICS 2017, Springer International Publishing, Cham, (2017) 62-79.

[38] T.E. Ali, Y.-W. Chong, and S. Manickam, Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review. Applied Sciences, 13(5) (2023) 3183. 2023

[39] T.V. Phan, T.M.R. Gias, S.T. Islam, T.T. Huong, N.H. Thanh, and T. Bauschert, Q-MIND: Defeating Stealthy DoS Attacks in SDN with a Machine-Learning Based Defence Framework. 2019. IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, (2019) 1-6.

[40] M.A. Albahar, Recurrent Neural Network Model Based on a New Regularization Technique for Real-Time Intrusion Detection in SDN Environment. Hindawi; Security and Communication Networks, (2019) 1-9.

[41] M. Belyaev, and S. Gaivoronski, Towards load balancing in SDN-networking during DDoS-attacks. 2014 International Science and Technology Conference (Modern Networking Technologies)(MoNeTeC), Moscow, Russia, (2014) 1-6.

[42] D. Yin, L. Zhang, and K. Yang, A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework. IEEE Access, 6 (2018) 24694-24705.

[43] R. Kandoi, and M. Antikainen, Denial-of-service attacks in OpenFlow SDN networks. 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, Canada, (2015) 1322-1326.

[44] S. Shin, and G. Gu, Attacking software-defined networks: a first feasibility study. Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, (2013) 165-166.

[45] L. Dridi, and M.F. Zhani, SDN-Guard: DoS Attacks Mitigation in SDN Networks. 2016 5th IEEE International Conference on Cloud Networking (Cloudnet), Pisa, Italy, (2016) 212-217.

[46] B. Wang, Y. Zheng, W. Lou, and Y.T. Hou, DDoS attack protection in the era of cloud computing and Software-Defined Networking. Computer Networks, 81 (2015) 308-319.

[47] P. Rengaraju, V.R. Ramanan, and C.-H. Lung, Detection and preventing of DoS attacks in Software-Defined Cloud networks. 2017 IEEE Conference on Dependable and Secure Computing, Taipei, (2017), 217-223.

[48] S. Fichera, L. Galluccio, S.C. Grancagnolo, G. Morabito, and S. Palazzo, OPERETTA: An Openflow-based Remedy to Mitigate TCP SYNFLOOD Attacks against web servers. Computer Networks, 92, (2015) 89-100.

[49] L.F. Carvalho, T. Abrão, Ld. S. Mendes, and M.L. Proença Jr, An ecosystem for anomaly detection and mitigation in software-defined networking. Experts Systems with Applications, 104 (2018) 121-133.

[50] M. Ambrosin, M. Conti, F. De Gaspari, and R. Poovendran, LineSwitch: Tackling Control Plane Saturation Attacks in Software-Defined Networking. IEEE/ACM Transactions on Networking, 25(2) (2017) 1206-1219.

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

[51] A. Shoeb, and T. Chithralekha, Resource management of switches and controller during saturation time to avoid DDoS in SDN. 2016 IEEE International Conference on Engineering and Technology (ICETECH), Coimbatoree, India, (2016) 152-156.

[52] W. Lei, and C. Fung, FlowRanger: A request prioritizing algorithm for controller DoS attacks in Software Defined Networks. 2015 IEEE International Conference on Communication (ICC), London, UK, (2015) 5254-5259.

[53] S. Padmaja, and V. Vetriselvi, Mitigation of switch-Dos in software defined network. 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, (2016) 1-5.

[54] P. Bera, A. Saha, and S.K. Setua, Denial of service attack in software defined network. 2016 5th International Conference on Computer Science and Network Technology (ICCSNT), Changchun, China, (2016) 497-501.

[55] Q. Yan, Q. Gong, and F.R. Yu, Effective software-defined networking controller scheduling method to mitigate DDoS attacks. Electronics Letters, 53(7) (2017) 469-471.

[56] H. Wang, L. Xu, and G. Gu, Flood Guard: A DoS Attack Prevention Extension in Software-Defined Networks. 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Rio de Janeiro, Brazil, (2015) 239-250.

[57] M. Kuerban, Y. Tian, Q. Yang, Y. Jia, B. Huebert and D. Poss, FlowSec: DOS Attack Mitigation Strategy on SDN Controller. 2016 IEEE International Conference on Networking, Architecture and Storage (NAS), Long Beach, CA, USA, (2016) 1-2.

[58] K. Hong, Y. Kim, H. Choi, and J. Park, SDN-Assisted Slow HTTP DDoS Attack Defense Method. IEEE Communication Letters, 22(4) (2018) 688-691.

[59] L. Wang, Q. Li, Y. Jiang, and J. Wu, Towards mitigating link flooding attack via incremental SDN development. IEEE Symposium on Computers and Communication, ISCC, (2016) 397-402.

[60] C. Li, Y. Wu, X. Yuan, Z. Sun, W. Wang, X. Li, L. Gong, Detection and defense of DDoS attack-based on deep learning in OpenFlow-based SDN. International Journal of Communication Systems, 31(5) (2018) e3497.

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

[61] Z.A. El Houda, A.S. Hafid, L. Khoukhi, Cochain-SC: An Intra- and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using SDN and Smart Contract. IEEE Access, 7 (2019) 98893-98907.

[62] J. Cui, J. He, Y. Xu, H. Zhong, TDDAD: Time-based detection and defense scheme against DDoS attack on SDN controller. Australasian Conference on Information Security and Privacy. Springer. (2018) 649-665.

[63] Z.A. El Houda, A. Hafid, and L. Khoukhi, Co-IoT: A Collaborative DDoS Mitigation Scheme in IoT Environment Based on Blockchain Using SDN. 2019 IEEE Global Communication Conference (GLOBECOM), Waikoloa, HI, USA. (2019) 1-6.

[64] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, A blockchain-based architecture for collaborative DDoS mitigation with smart contracts. IFIP International Conference on Autonomous Infrastructure, Management and Security. Springer, Cham. (2017) 16-29.

[65] J.H. Jafarian, E.Al Shaer, and Q. Duan, Formal approach for route agility against persistent attackers. Lecture Notes in Computer Science, 8134 (2013) 237-254.

[66] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, AVANT-GUARD: Scalable and vigilant switch flow management in softare-defined networks. ACM SIGSAC Conference on Computer and Communications Security, (CCS), (2013) 413-424.

[67] Y.E. Oktian, S. Lee, and H. Lee, Mitigating denial of service (DoS) attacks in openflow networks. International Conference on Information and Communication Technology Convergence, (ICTC). (2014) 325-330.

[68] A.F.M. Piedrahita, S. Rueda, D.M.F. Mattos, and O.C.M.B. Duarte, Flowfence: A denial of service defense system for software defined networking. Global Information Infrastructure and Networking Symposium, GIIS. (2015) 1-6.

[69] G. Shang, P. Zhe, X. Bin, H. Aiqun, and R. Kui, Flooddefender: Protecting data and control plane resources under SDN-aimed DoS attacks. INFOCOM 2017-IEEE Conference on Computer Communication, (2017) 1-9.

[70] T. Wang, H. Chen, G. Cheng, and Y. Lu, SDNManager: A Safeguard Architecture for SDN DoS Attacks Based on Bandwidth Prediction. Network Security and Management in SDN, (2018).

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

[71] S. Wang, S. Chandrasekharan, K. Gomez, S. Kandeepan, A. Al-Hourani, M.R.Asghar, G. Russello, and P. Zanna, SECOD: SDN Secure Control and Data Plane Algorithm for Detecting and Defending Against DoS Attacks. NOMS 2018 IEEE/IFIP Network Operations and Management Symposium. IEEE. (2018) 1-5.

[72] N. Goksel, and M. Demirci, DoS attack detection using packets statistics in SDN. International Symposium on Networks, Computers, and Communications, (ISNCC), IEEE. (2019) 1-6.

[73] R. Xie, M. Xu, J. Cao, and Q. Li, Softguard: Defend against the low-rate TCP attack in SDN. 2019 IEEE International Conference on Communication (ICC). (2019)1-6.

[74] R. Mohammadi, R. Javidan, and M. Conti, SLICOTS: An SDN-Based Lightweight Countermeasure for TCP SYN Flooding Attacks. IEEE Transactions on Network and Service Management, 14(2) (2017) 487-497.

[75] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, and V. Maglaris, Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. Computer Networks, 62 (2014) 122-136.

[76] R. Miao, M. Yu, and N. Jain, NIMBUS: Cloud-scale attack detection and mitigation. ACM SIGCOMM Computer Communications. Rev.44. (2014) 121-122.

[77] J. Wang, R. Wen, J. Li, F. Yan, B. Zhao, and F. Yu, Detecting and Mitigating Target Link-Flooding Attacks Using SDN. IEEE Transactions on Dependable and Secure Computing. 16(6) (2019) 944-956.

[78] J. Zheng, Q. Li, G. Gu, J. Cao, D.K.Y. Yau, and J. Wu, Realtime DDoS Defense Using COTS SDN Switches via Adaptive Correlation Analysis. IEEE Transactions on Information Forensics and Security, 13(7) (2018) 1838-1853.

[79] J. Xing, W. Wu, and A. Chen, Architecting Programmable Data Plane Defense into the Network with FastFlex. HotNets ′19: Proceedings of the 18th ACM Workshop on Hot Topics in Networks. (2019) 161-169.

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

[80] M. Zhang, G. Li, S. Wang, C. Liu, A. Chen, H. Hu, G. Gu, Q. Li, M. Xu, and J. Wu, Poseidon: Mitigating Volumetric DDoS Attacks with Programmable Switches. Network and Distributed Systems Security (NDSS) Symposium 2020. (2020) 1-18.

[81] A. Hussein, I.H. Elhajj, A. Chehab, and A. Kayssi, SDN security plane: An architecture for resilient security services. IEEE International Conference on Cloud Engineering Workshop. (IC2EW), (2016) 54-59.

[82] O. Joldzic, Z. Djuric, and P. Vuletic, A transparent and scalable anomaly-based DoS detection method. Computer Networks, 104 (2016) 27-42.

[83] J. Li, S. Berg, M. Zhang, P. Reiher, and T. Wei, Drawbridge: software-defined DDoS-resistant traffic engineering. SIGCOMM '14: Proceedings of the 2014 ACM conference on SIGCOMM, (2014) 591-592.

[84] S. Hammed, and H.A. Khan, SDN Based Collaborative Scheme for Mitigation of DDoS Attacks. Future Internet, 10(3) (2018) 1-18.

[85] J. Francois, I. Aib, and R. Boutaba, FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks. IEEE/ACM Transactions on Networking, 20(6) (2012) 1828-1841.

[86] S. Debroy, P. Calyam, M. Nguyen, R.L. Neupane, B. Mukherjee, A.K. Eeralla, K. Salah, Frequency-Minimal Utility-Maximal Moving Target Defense Against DDoS in SDN-Based System. IEEE Transactions on Network and Service Management, 17(2) (2020) 890-903.

[87] M. Samir, M. Azab, and E. Samir, SD-CPC: SDN Controller Placement Camouflage based on Stochastic Game for Moving-target Defense. Computer Communications, 168 (2021) 75-92.

[88] A. Aydeger, N. Saputro, and K. Akkaya, A moving target defense and network forensics framework for ISP networks using SDN and NFV. Future Generation Computer Systems, 94 (2019) 496-509.

[89] S. Debroy, P. Calyam, M. Nguyen, A. Stage, and V. Georgiev, Frequency-minimal moving target defense using software-defined networking. 2016 International Conference on Computing, Networking and Communications (ICNC), Kauai, USA. (2016) 1-6.

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

[90] Y. Shi, H. Zhang, J. Wang, F. Xiao, J. Huang, D. Zha, H. Hu, F. Yan, and B. Zhao, CHAOS: An SDN-Based Moving Target Defense System. Hindawi: Security and Communication Networks, (2017) 1-11.

[91] K. Doshi, Y. Yilmaz, and S. Uludag, Timely Detection and Mitigation of Stealthy DDoS Attacks Via IoT Networks. IEEE Transactions on Dependable and Secure Computing, 18(5) (2021) 2164-2176.

[92] M.S. Ali, M. Vecchio, M. Pincheira, K. Doului, F. Antonelli, and M.H. Rehmani, Applications of Blockchains in the Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(2) (2018) 1676-1717.

[93] F.H. Pohrmen, R.K. Das, and G. Saha, Blockchain-based security aspects in heterogeneous Internet-of-Things networks: a survey. Transactions on Emerging Telecommunication Technologies, 30 (10) (2019) E3741.

[94] S. Demirci, and S. Sagiroglu, Software defined networking for improved security in smart grid system. 2018 7th International Conference on Renewable Energy Research and Applications, ICRERA, IEEE. (2018) 1021-1026.

[95] U. Ghosh, P. Chatterjee and S. Shetty, Securing SDN-enabled smart power grids: SDN-enabled smart grid security. Cyber-Physical Systems for Next-Generation Networks, IGI Global, (2018) 79-98.

[96] J. Kim, F. Filali, and Y.-B. Ko, Trends and Potentials of the Smart Grid Infrastructure: From ICT Sub-System to SDN-Enabled Smart Grid Architecture. Applied Sciences, 5(4) 706-727.

[97] H. Maziku, S. Shetty, and D.M. Nicol, Security risk assessment for SDN-enabled smart grids. Computer Communications, 133 (2019) 1-11.

[98] D. Ibdah, M. Kanai, N. Lachtar, N. Allan, and B. Al-Duwairi, On the security of SDN-enabled smartgrid systems. 2017 International Conference on Electrical and Computing Technologies and Applications, (ICECTA). Ras Al Khaimah, UAE. (2017) 1-5.

[99] X. Dong, H. Lin, R. Tan, R.K. Iyer and Z. Kalbarczyk, Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges. CPSS '15: Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, (2015) 61-68.

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

[100] R. Chaudhary, G.S. Aujla, S. Garg, N. Kumar, and J.J.P.C. Rodrigues, SDN-Enabled Multi-Attribute-Based Secure Communication for Smart Grid in IIoT Environment. IEEE Transactions on Industrial Informatics, 14(6) (2018) 2629-2640.

[101] N.E. Petroulakis, K. Fysarakis, I. Askoxylakis, and G. Spanoudakis, Reactive security for SDN/NFV-enabled industrial networks leveraging service function chaining. Transactions on Emerging Telecommunications Technologies, 29(7) (2017).

[102] F. Holik, and P. Dolezel, Industrial Network Protection by SDN-Based IPS with AI. ACIIDS 2020: Intelligent Information and Database Systems. Communications in Computer and Information Science, 1178 (2020) 192-203.

[103] M. Cheminod, L. Durante, L. Seno, F. Valenzano, and C. Zunino, Leveraging SDN to improve security in industrial networks. 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway. (2017) 1-7.

[104] D. Henneke, L. Wisniewski, and J. Jasperneite, Analysis of realizing of future industrial network by means of Software-Defined Networking (SDN). 2016 IEEE World Conference on Factory Communication Systems (WFCS), Aveiro, Portugal. (2016) 1-4.

[105] M. Singh, G.S. Aujla, A. Singh, N. Kumar, and S. Garg, Deep-Learning-Based Blockchain Framework for Secure Software-Defined Industrial Networks. IEEE Transactions on Industrial Informatics, 17(1) (2021) 606-616.

[106] C. Lorenz, D. Hock, J. Scherer, R. Durner, W. Kellerer, S. Gebert, N. Gray, and T. Zineer, An SDN/NFV-Enabled Enterprise Network Architecture Offering Fine-Grained Security Policy Enforccement. IEEE Communications Magazine, 55(3) (2017) 217-223.

[107] R. Alvizu, G. Maier, S. Troia, V.M. Nguyen, and A. Pattavina, SDN-based network orchestration for new dynamic Enterprise Networking services. 2017 19th International Conference on Transparent Optical Networking (ICTON), Girona, Spain. (2017) 1-4.

[108] J. Bailey, and S. Stuart, Faucet: Deploying SDN in the enterprise. Communications of the ACM, 60(1) (2017) 45-49.

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

[109] D. Levin, M. Canini, S. Schmid, and A. Feldmann, Incremental SDN Deployment in Enterprise Networks. ACM SIGCOMM Computer Communication Review, 43(4) (2013) 473-474.

[110] K. Poularakis, G. Iosifidis, and L. Tassiulas, SDN-Enabled Tactical Ad Hoc Networks: Extending Programmable Control to the Edge. IEEE Communications Magazine, 56(7) (2018) 132-138.

[111] Y. Wei, X. Zhang, L. Xie, and S. Leng, Energy-aware traffic engineering in hybrid SDN/IP backbone networks. Journal of Communications and Networks, 18(4) (2016) 559-566.

[112] B.R. Dawadi, D.B. Rawat, S.R. Joshi, and P. Manzoni. Towards Smart Networking with SDN Enabled IPv6 Network. arXiv preprint, (2022).

[113] E. Seve, J. Pesic, C. Delezoide, A. Giorgetti, A. Sgambelluri, N. Sambo, S. Bigo, and Y. Pointurier, Automated Fibre Type Identification in SDN-Enabled Optical Networks. Journal of Lightwave Technology, 37(7) (2019) 1724-1731.

[114] M. Birk, G. Choudhury, B. Cortez, A. Goddard, N. Padi, A. Raghuram, K. Tse, S. Tse, A. Wallace, and K. Xi, Evolving to an SDN-enabled isp backbone: key technologies and applications. IEEE Communication Magazine, 54(10) (2016) 129-135.

[115] X. Zhang, H. Wang, and H. Zhao, An SDN framework for UAV backbone network towards knowledge centric networking. IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) Honolulu. USA, (2018) 456-461.

[116] G. Kakkavas, A. Stamou, V. Karyotis, and S. Papavassiliou, Network Tomography for Efficient Monitoring in SDN-Enabled 5G Networks and Beyond: Challenges and Opportunities. IEEE Communications Magazine, 59(3) (2021) 70-76.

[117] X. Duan, X. Wang, Y. Liu, and K. Zheng, SDN Enabled Dual Cluster Head Selection and Adaptive Clustering in 5G-VANET. 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, Canada, (2016) 1-5.

[118] J. Liu, Y. Shi, L. Zhao, Y. Cao, W. Sun, and N. Kato, Joint Placement of Controllers and Gateways in SDN-Enabled 5G-Satellite Integrated Network. IEEE Journal on Selected Areas in Communications, 36(2) (2018) 221-232.

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

[119] A.S. Thyagaturu, A. Mercian, M.P. McGarry, M. Reisslein, and W. Kellerer, Software Defined Optical Networks (SDONs): A Comprehensive Survey. IEEE Communications Surveys & Tutorials, 18(4) (2016) 2738-2786.

[120] E. Guler, M. Karakus, and S. Uludag, SpectrumChain: An Efficient Spectrum Management Framework in Blockchain-Enabled Flexible SDON's. ICC 2022-IEEE International Conference on Communications, Seoul, Republic of Korea. (2022) 5744-5749.

Volume 5, Issue 2, pages 127-158

p-ISSN 2655-8564, e-ISSN 2685-9432

This page intentionally left blank