A Survey of the Security and DDoS Attacks in the Software Defined Network

Abdoulkarim Tahirou(✉) and Karim Konate

Université Cheikh Anta Diop UCAD, Dakar, Senegal
{abdoul.tahiroudjambeidou,karim.konate}@ucad.edu.sn

Abstract. The Software Defined Network (SDN) is a new network paradigm aimed at making it easier to manage and operate computer networks. SDN is becoming more and more emerging because of the ease and flexibility it offers to companies working in CLOUD and TELECOM. Unlike the traditional network where the control plane and the data plane are integrated together, the SDN network separates the two planes and then makes the network more agile and scalable through programming. In SDN, all network management logic relies on the controller. The OPENFLOW protocol is one of the most widely used protocols in SDN. It offers an opportunity for researchers and industries to develop their own ideas on innovative network protocols or solutions. However, SDN is still immature and has many security holes. Most of its vulnerabilities are related to the fact that the architecture is based on software but also the centralized nature of the controller. Indeed, all the security problems encountered in traditional networks remain valid in SDN, but Distributed Denial of Service (DoS/DDoS) attacks remain the heaviest on SDN, linked to the separation of the control plane from the data plane. On one hand, this paper focuses on the various security threats from to DDoS attacks that weigh on the controller and transfer equipment. On the other hand, it reviews the existing solutions of DDoS attacks on the controller and data plane. Finally, it introduces our research plan in the field.

Keywords: Software Defined Network · Security · DoS · DDos · Control plane · Data plane · Application plane · OpenFlow

1 Introduction

IT has evolved exponentially through the Cloud, Internet of Things (IoT), Big Data, virtualization, block chain, etc. The number of devices connected to the internet has increased considerably, to more than 74,44 billion devices in 2025 [1]. In addition, modern applications make further demands on the availability of bandwidth. Despite this, traditional computer networks have remained static for decades. This is because its network architectures operate hierarchically and vertically [2]. The design, evaluation and deployment of a protocol can take 5 to 10 years in today's networks [3] as the IPV4 to IPV6 transition takes place. The difficulty of updating existing network security policies lies in the CLI command line [4]. These limitations have resulted in a lack of flexibility and agility in traditional networks.

M. Ben Ahmed et al. (Eds.): SCA 2022, LNNS 629, pp. 426–441, 2023.
https://doi.org/10.1007/978-3-031-26852-6_40

The SDN was born in this context to overcome the monotony of traditional networks. SDN is a network architecture where the control plane is dissociated from the transfer plane and is directly programmable. All the intelligence of the SDN network is logically centralized on the software controller. The router and switches become simple packet transfer devices. The SDN has lots of strengths but also still faces security issues. Indeed, the centralized nature of the controller, its programmability, the decoupling of the control from the data planet and the lack of intelligence of the SDN transfer equipment [5] amplify its vulnerability and introduce new security flaws [6]. Research in the field of performance, virtualization, loadbalacing and the network supervision has been carried out in the SDN. One of the broadest fields of research concerns SDN security in general and more specifically DoS/DDoS attacks, to assure the transition between traditional network and the SDN.

Most of the DoS/DDoS attacks perpetrated in the SDN network are issues out on the controller, or on the transfer equipment [7]. This paper presents security in the SDN network in general and more specifically in DoS/DDoS attacks. We will focus on the different types of DoS/DDoS attack on the SDN communication layers and interfaces. This document is organized as follows: Sect. 2 presents the SDN network; Sect. 3 describes security in SDN. Section 4 classifies the modus operandi and different types of DoS/DDoS attacks. Section 5 discusses the different security threats and the corresponding mitigation mechanisms. Section 6 proposes the contribution of the authors and opens the perspectives of research in the field.

2 Presentation of the SDN Architecture

The SDN architecture has three main layers which are the Infrastructure, Control, and Application.

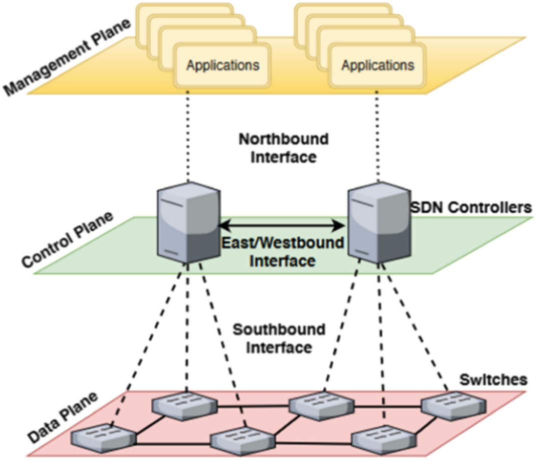

Fig. 1. Layered view of SDN architecture

2.1 Infrastructure Layer or Data Transfer Layer

The data layer is made up of various network devices that form the underlying network to carry traffic. Switches or routers and are linked by either physically wired or wireless media. Each switch is a simple packet transfer device, which has one or more flow tables within it. Each switch flow table contains a set of flow entries with packet routing rules [2].

2.2 Control Layer

The control layer is the intelligent part of the SDN network [3], because it maintains the entire structure of the network. All network management decisions are made by one or more controllers on the SDN network. The interaction between the controller and the deployed switches is called the southbound interface. The OpenFlow protocol is the most widely used between the control and transfer layer. This protocol was proposed by researchers at CleanState at Stanford University because of its flexibility and programmability. Its success is due to the support of certain technology giants such as Microsoft and Google [9], who quickly adopted it in their datacenters. A consortium called ONF has been set up for the standardization of the OpenFlow protocol [10]. On the opposite side, we have the Northbound API [11], which links the communication of business applications to the controller. There are two other interfaces in the case of a multi-controller network called Eastbound and Westbound respectively. Since the controller is the brain of the SDN network, its centralized nature creates a single point of failure in the network. To avoid network downtime most recent controller implementations offer the possibility of having multiple and distributed controllers such as NOX, POX [12], FLOODLIGHT [13], OPENDAYLIGHT [14].

2.3 Application Layer

It is the layer where all innovative network applications are developed. These applications can be used in the field of security, network load balancing, quality of service, etc. [15]. The application layer communicates with the control layer through the Northbound interface.

3 Generality on SDN Security

DDoS attacks are increasing continuously with sophisticated characteristics. These attacks concern all digital services with heterogeneous devices (computers, phones, cameras, etc.). This motivates researchers and equipment manufacturers namely CISCO, IBM, DELL, HUAWEI to focus more on this question. According to Yao et al. [16], there are three types of security issues: SDN intrusion, denial of service, and application trust management. A network intrusion is any action aimed at compromising the availability, integrity and confidentiality of any network resource or service [17]. There are other types of security issues in SDN. Those are applications, developed by third parties which make the application layer vulnerable. According to Li et al. [18], the security challenges in the SDN architecture based on OpenFlow are security issues on switches, controllers, applications and communications interfaces.

Table 1. The various security issues by layer and interface.

SDN Vulnerabilities	Attack target
Application Layer	**Application**
	Unauthenticated access to applications; Fraudulent rule insertion; Policy Application
Application-Controller Infterface	**Application-Controller Interface**
	Unauthenticated access to applications; Fraudulent rule insertion; Policy Application
Control layer	**Controller**
	Unauthorized and Unauthenticated access to controller; Modification of flow rules; Insertion of fraudulent rules; Hijacking of controllers; Saturation of the Controller-Switch communication; Saturation of the Controller-Switch communication
Controller-Data Interface	**Controller-Data Interface**
	Unauthorized access to the controller; Modification of flow rules; Hijacking of controllers; Controller-Switch link saturation
Data Layer	**Data**
	Unauthorized access to the controller; flow rule discovery; Discovery of transfer rules; Modification of flow rules to modify packets; controller hijacking

3.1 Fields of Attack in the Architecture of SDN

In the SDN all layers and interfaces can be attacked. There are six DDoS attack points according to Shu et al. [19].

- **Attacks on SDN switches:** A SDN switch is typically a separate device made up of related hardware and software, which are vulnerable to DDoS attacks. An example of a vulnerability is the small size of the SDN switch flow table and the resources of CPU, memory CAM/TCAM (Ternary Content Address Memory) [20].
- **Attacks on links between SDN switches:** the Packets transmitted between SDN switches are not encrypted and may contain sensitive user information. These packets can be intercepted by attackers easily, especially when the links between switches are wireless [21].
- **Attacks on the SDN controller:** all network management is done at the level of the controller, so it constitutes a potential target for attackers. Any attack on the control layer will have a direct impact on the operation of the SDN. Since each new flow is sent to the controller for decision, this leads to the saturation of the controller resources [20].
- **Attacks between SDN controller's links:** In a multi-controller environment, communication between different controllers is necessary to maintain the consistent state of

the entire SDN. In the event of an attack, packets can be intercepted via the Eastbound and Westbound APIs.

- **Attacks between Controller and links:** SDN centralizes all network intelligence on the controller. All new transfer rules are inserted into the switches by the controller via the Southbound API [19]. Data packets that contain these rules can be modified or tampered with by a malicious attacker who listens on the link between the controller and the switch.
- **Attacks on SDN applications:** It constitutes the added value in SDN, because it allows the development of innovative applications of the network. When applications solicit the controller through the Northbound malicious code can be embedded in the controller. The lack of a security mechanisms to ensure a relationship of trust between controllers and applications is at the root of these kinds of attacks [19].

3.2 Discussions on SDN Security

The SDN network offers more flexibility and programmability compared to the one in traditional network but the security issue in the SDN is almost identical to traditional network. We can have several types of attacks in SDN (see Table 1). The data layer is presented as the weakest link of the SDN chain in terms of security. There are many Southbound API solutions like OpenFlow, Open vSwitch Database Management Protocol (OVSDB), Path Computation Element Protocol (PCEP), Interface to the Routing System (I2RS) that exist [18]. However, not all these APIs are reliable and address security concerns. Several types of attacks can occur at this level, compromising switches or hosts. According to Dayal et al. [22] these are mainly denial of service, Man in the Middle (MIM), data modification, repudiation and side channel attacks.

4 Overview of DoS/DDoS Attacks in the SDN Security

A DDoS attack aims to make a server, service unavailable to legitimate users [4]. We will speak of a distributed DoS attack, any attack that is carried out remotely from several sources consisting of several hundred or even thousands of devices [23]. According to Saman et al. [24], the DDoS attack aims to disrupt the connectivity of legitimate users by depleting network resources. In this section, we describe the classification of DDoS attacks on the different layers and interfaces.

4.1 DDoS Security Threats on the Infrastructure Layer

This consists of networking devices that control the forwarding and data processing capabilities for the network. The attack against SDN data plane takes place at two levels, either on the CAM/TCAM memory of the switch by its overload on the one hand, and on the other hand, the saturation of its flow table. In the process of the Openflow switches, each new flow without correspondence in the flow table is sent to the controller for decision. The new rules can be inserted in the flow table via the interface southbound. In the event of a DDoS attack, the attacker can easily fill the flow table with new flow and saturate the switch. In addition, if the switch memory is saturated, instead of sending just the packet header, the entire packet will be sent to the controller [25].

4.1.1 Detection Mechanisms and Threats Against DDoS Attacks on the Infrastructure Layer

Several detection and defense mechanisms against DDoS attacks have been developed by researchers and industry. According to R. Swami et al. [4], these mechanisms can be classified into three main categories which are mechanism based on statistics, Machine Learning, or specific applications. Statistics-based detection mechanisms are statistical analyzes, which collect, and exploit data samples based on network traffic in order to make a decision on DDoS attacks. The work of several authors [26, 27] are algorithms based on statistics such as entropy, chi-square, which are used to detect DDoS attacks in the SDN.

These statistical techniques commonly used in the work are based on adaptive correlation analysis, standard deviation, probability, and entropy measures. Network features such as source IP address, destination IP address, and port numbers are used to calculate entropy with predefined thresholds to identify the presence or absence of DDoS attacks [28]. Another technique based on machine learning are used recent years due to their effectiveness in detecting DDoS attacks in SDN. These algorithms can be used to detect malicious traffic from legitimate traffic in the SDN. The algorithms used are artificial neural networks [41], Bayesian networks [42], self-organizing map (SOM) [29],and fuzzy logic [30, 31]. Other techniques use the intrinsic characteristics of SDN with specific applications for detection and defense against DDoS attacks.

According to Chen et al. [32], they proposed Flexprotect to protect data centers. They used the intrinsic features of SDN and NFV to protect the data center network from DDoS attacks. Two modules are offered by Flexprotect, the first one for detection and the second for mitigation, that are deployed separately in the system. A solution to defend against DDoS attacks with the monitoring tool named sFlow was proposed by Aizuddin et al. [33]. The proposed system used SDN features to support DDoS attacks against DNS amplification. It collects and processes header flows to check whether they originate from a DNS server. Zheng et al. [34] have implemented a solution to mitigate DDoS attacks by applying a real time adaptive correlation analysis called RADAR (Reinforcing Anti-DDoS Actions in Realtime). It consists of three main modules which are the collector, detector, and locator. RADAR can identify several types of attacks in real time, such as SYN flood, UDP flood and DNS amplification. The FlowTrApp tool [35] is an SDN-based DDoS defense mechanism for protecting data centers. FlowTrApp uses two parameters which are the rate and the duration of a flow. The characteristics of OpenFlow [36] are coupled with those of sFlow [37] for the collection of flow statistics. A tool called Woodpecker [38] is proposed by L. Wang et al. to detect and mitigate the type of DDoS flood attack using the characteristics of the SDN. Several selected ordinary switches are upgraded to SDN compatible switches. With the help of the global view provided by the SDN controller, Woodpecker locates the location of the bottleneck and identifies whether the congestion is really caused by link flooding. Woodpecker uses heuristic traffic engineering as an application on the controller to mitigate the impacts of the attack. The work of J. Liu et al. [39] focused on a modular tool called Floodlight Guard, which was implemented for detection and defense against DDoS attacks in SDN. FLGUARD applies dynamic IP address binding to solve the problem of IP address spoofing and uses the C-SVM algorithm to detect attacks. According to the authors Q. Niyaz et al. [40] their work is based on machine learning, the SAE (Stacked Autoencoder) to detect multi vector attacks in SDN. The packet headers are extracted classified in an unsupervised way by machine learning. SAE can detect DDoS attacks on control and data plane.

4.1.2 Summary Table of the Detection and Defense Mechanisms Against DDoS on the Infrastructure Layer

Security at the infrastructure layer is summarized as mentioned in the table below, DDoS attacks are the pure enemies of SDN. Because in the event of successful attacks on this layer, the entire network is crippled. This amplification of DDoS attacks on this layer could be explained by the non-intelligence of the switches. Several efforts are being deployed by researchers and industry to ensure the security of the SDN against DDoS attacks, but we mention some shortcomings in the work carried out.

Table 2. Detection and defense mechanisms against DDoS attacks on data layer

Ref.	Features	Intrusion	Target	Benefits	Limitations
[32]	FP-SYN, NFV, SDN, Snort, Pfsense	SYN-Flodding	Switch memory	Reduce traffic cost, bandwidth consumption	TCP-SYN DDOS only
[33]	SFlow, SDN	DNS amplification	Switch memory	Reduce controller response time	Only for DNS amplification
[34]	SDN, Adaptive correlation technique	Link flood, SYN flood, UDP/DNS amplification	Switch memory and control/data rate	Detects several types of DDoS attacks	Detection/defense mechanism for large network topologies
[35]	Openflow et Sflow-RT	DDoS ICMP-UDP Flood	Switch memory and control/data rate	Reduce controller load and false negatives	Too much information exchange with the controller
[38]	SDN, Openflow	Attack UDP flood	Bandwidth between controller and switches	Exact location of bottleneck Reduces and bandwidth usage	Use too much memory and CPU for controller resources
[39]	SDN, et SVM (Support Vector Machine)	Attack ICMP flood	Bandwidth between controller and switches	Flexibility, accuracy in DDoS Flooding attacks	Tool not tested in a real environment
[40]	SDN, SAE, Deep Learning	Attack TCP/UDP/ICMP flood	Controller memory Control/data link	Reduce controller, switch bandwidth	High memory and CPU controller resource usage

4.2 Security Threats at the Control Plane in SDN

Control plane security has a direct impact on the data and application layer. If one controller is compromised, the entire network, including switches, is affected. This is because when an Openflow switch can no longer receive forwarding rules from the controller, it will not know how to handle packets. Therefore, due to its important role, the controller is a key target for attackers. Hence the need to protect the control layer to preserve the security of SDN. There are several types of DDoS attack threats that still weigh heavily on the control layer. DDoS attacks generate an enormous amount of packets to overwhelm the resources of the controller in order to make network services or interface bandwidth unavailable to legitimate users [53]. In the SDN architecture, all packets management commands are concentrated on the controller. Most DDoS attacks on the controller try to saturate the controller with the arrival of new packets to increase the CPU workload and creat a botlneck between the control plane and the data plane. This separation of control over packet forwarding is one of the strengths of SDN [57], yet it is also one of the weaknesses of the SDN architecture.

4.2.1 Security Threat Detection Mechanisms Against DDoS Attacks on the Control Layer

The control plane is the most critical in the SDN architecture, as all the intelligence of the network is focused on it. Several tools have been developed to protect this plane against DoS/DDoS attacks in order to avoid its downtime. A tool called DBA (DDoS Application Blocking) has been proposed by Lim et al. [53], which consists of blocking DDoS attacks from the abnormal traffic. The architecture requires communication between the DDoS blocking application running on the SDN controller and the server to be protected. The other exchanges are carried out through the standard interfaces of Openflow. L. Dridi et al. [58] focuses on the development of an effective tool called SDNGUARD. This tool helps to protect SDN networks from DDoS attacks simultaneously and mitigate DoS impact on SDN controller and bandwidth between data layer and switch control. SDNGUARD also dynamically manages flow routes, rule entry delays, and aggregate flow rule entries. This tool performs well in protecting switch controller and bandwidth during DDoS attacks. To solve the bottleneck problem between the data plane and the control plane, the authors of [59] introduce Avant-Guard, an extension of the Openflow data plane called “connection migration”. The purpose of this connection migration is to add intelligence to the switches in the data plane, in order to prevent the TCP based DDoS attacks. The objective of the Avant-Guard is to reduce the spoofing of IP addresses, by effectively delete a quantity of data to be transferred to the control plane during a DDoS attack.

FloodDefender [60] is an effective, protocol independent defense tool for SDN / Openflow networks that helps mitigate DDoS attacks. It sits between the control plane and the other controller applications, and can protect both the data layer, memory and CPU resources of the control plane using three new techniques that are: “table engineering-miss”, “packet filtering”, and finally “management of the flow rule”. According to Celyn et al. [24], they implemented a tool for intrusion detection and prevention against certain types of TCP-based DoS attacks in the SDN network. Two connection techniques were used for IPDS namely CB-TRW (Credit-Based Threshold Random Walk) and RL (Rate Limiting), a port scanning detection technique that the authors call Port Bingo (PB), and a QoS technique that relies on throughput statistics to mitigate DoS attacks.

4.2.2 Summary of the Table of the Mechanisms for Detecting and Defending Threats Against DDoS Attacks on the Control Layer (See Table 3)

In the SDN network, the controller is the intelligent part of the SDN. All network management décisions are made by the controller. This makes the controller a potential point of attack. In addition, in the case of an SDN network with a single controller, the latter is a single point of failure of the network. These attacks are mainly focused on saturating the resources of the controller. Another DDoS attack angle on the control layer is the saturation of the bandwidth of the Openflow channel that links the data layer to the controller. Several techniques are used to ensure the security of the controller against DDoS attacks, mainly detection and defense mechanisms. These mechanisms used are IDS, IPS and NIDS tools, for the detection and mitigation of DDoS attacks. Other techniques are used to strengthen the detection and mitigation of DDoS attacks on the controller and interfaces (Table 4).

Table 3. Different sources of SDN attacks on the SDN control and data layer

Réf.	Features	Intrusion	Target	Benefits	Limitations
[41]	SDN, Openflow	Http-Floo	Controller memory; control/data bandwidth	Reduces traffic costs and bandwidth consumption	Only handles TCP-SYN attacks
[42]	SDN, OpenFlow	DoS Flood	Saturation link Control and Data plan	Controller memory and CPU protection Control/data bandwidth reduction	Additional hardware to store data
[43]	SDN, Openflow, connection migration	All DoS Flood	Saturation link Data to Control	two modules used connection migration and trigger for statistics	Adding modules to SDN architecture, Controller overload
[44]	SDN, Openflow	ICMP spoof, IP, UDP/TCP flood	bandwidth and memory saturation of the controller	Detects several types of attacks	Controller overload, not tested to scale

(*continued*)

Table 3. (*continued*)

Réf.	Features	Intrusion	Target	Benefits	Limitations
[45]	SDN, Openflow, Snort, Wireshark, TCP-replay CB-TRW, Rate Limit and port scan	DoS TCP, UDP ICMP	Controller to switch bandwidth	Creation of rules to counter the attack	Controller overload, To many false positives
[46]	SDN, Openflow	TCP/UDP/ICMP flood DoS attack	Bandwidth controller and switch	Allows to protect the controller saturation	Adding additional hardware as a cache to the data plane
[47]	SDN, Openflow	TCP, UDP	Bandwidth between controller and switch	Controller overload, control-data link saturation reduction	Packet loss between controller and data plane

Table 4. The various security issues by layers and interfaces

SDN	SDN Sources of DoS/DDoS attacks	Defense mechanisms
Data layer	Non-intelligent switch	Adding intelligence to switches
	Saturation of CAM/TCAM memory	CAM/TCAM memory protection
		Adding additional equipment
Controller-Data Interface	Bandwidth saturation between the contact layer and the data layer	Dynamic flow management
		Delegation of flow processing locally on the switches
		Connection migration
		Proactive analysis of flows
Controller Layer	Centralized control of the SDN network	Minimum processing on the packets by the switches before transfer to the controller
	Single point of failure (SPOF)	Adding multiple controllers in SDN networks
	Limited controller resources (CPU, RAM)	Adding NIDS to protect resources

4.3 Security Threats on the Application Layer

In the SDN architecture, the application layer is a critical point of DDoS attack. This is due to the variety of applications supported by this layer. A DDoS attack can occur either on different applications or on the Northbound API between the control plane and the application. The diversification of applications and their design by several stakeholders lead to a notorious security breach on the application layer, application can contain malicious code, which can spread throughout other applications.

4.3.1 Security Threat Detection Solutions Against DDoS Attacks on the Application Layer

Nowadays, computer applications are diverse and multiple in all areas. This exposes the SDN network to face DDoS attacks from them. Thus, several studies have been carried out in the context of securing SDN applications. The FLOVER [48] is a model verification system that verifies the global disconnection policies instantiated in OpenFlow network do not violate the network security policy. Another tool VERICON [49] is a system which verifies that the SDN network is indeed properly configured. Adel et al. have proposed an OrchSec tool [50], an orchestrator module developed in the application layer which uses the functionalities of the Openflow controller (redirects or blocks packets) and SFlow-RT for monitoring. It aims to improve network security by reducing overloads on SDN controllers by decoupling the control and monitoring functions. Another technique using WILDCARD, to access the information level by sampling a packet and keep its visibility on the Openflow network has been proposed by Sajad et al. FleXam [51]. Flexam collects network statistics efficiently.

5 Panoply of Open Issues on the Control Layer, Data Layer, and Southbound Interface in SDN

The SDN network presents a lot of openness in terms of vulnerabilities for attackers in general and more specifically for DDoS attacks. This is how several researches are carried out or underway to mitigate DDoS attacks in SDN. Most of these DDoS attacks happen on the control plane, the bandwidth of the interface between the controller and the switches.. Most of the research for the detection and mitigation of DDoS attacks has been carried out for the control layer, data and their link interface. It is clear that these DDoS attacks are constantly being improved by attackers in order to bypass detection and defense measures. The most widespread attacks are above all TCP, ICMP, UDP floods (see Tables 2 and 3).

6 Contribution of This Document and Future Research Perspectives

In this paper we have seen the security challenges that abounds in the SDN network in general and more specifically against DoS/DDoS attacks. We have reviewed the security issues by layer and by interfaces between layers. Most detection mechanisms use the intrinsic characteristics of the openflow based SDN in order to collect statistics and information based on the openflow protocol. Once a certain number of conditions are met, mitigation tools such as IDS, NIDS or IPS are mobilized to mitigate attacks. Our future research will focus on the detection and mitigation of DDoS attacks in the two SDN layers as well as the link interface between them.

7 Conclusion

SDN is the latest trend in computer networking, its adoption as a new paradigm is shaking up the habits of traditional networking. The separation of the control plane from the data plane is the most interesting advantage of the SDN. The centralization of control makes it possible to better secure the SDN from different types of attacks, in general and to bring innovations in its management through network programming. In this article we have reviewed the architecture of the SDN network and DDoS attack. This showed that the separation of the control plane from the data plane, which is one of the biggest strengh of the SDN, can also be at the same time, the biggest weakness of the SDN. In recent years, several researchers have initiated research with a particular focus on fighting DDoS attacks, but much research remains to be done in this area. In this paper we have focused on the two planes of the SDN architecture namely the control plane and the data plane. We have noticed that most DDoS attacks take place on these two planes on the one hand, and on the other hand between the communication interface between these two planes.

In addition, most of the proposed detection and defense solutions to mitigate DDoS attacks in the SDN manage the rates of the inbound flows to determine the attack. Other solutions combine input streams with either NIDS, IDS, IPS, packet filtering, machine learning, or statistical tools to define the attack. Some proposed mitigation tools also make it possible to add a little intelligence at the level of data plane or use additional equipment for the detection of DDoS attacks.

In this context we will propose a tool, which can use the intrinsic characteristics of SDN, Openflow protocol and sFlow for the detection and mitigation of DDoS attacks. The combination of SDN and sFlow makes this possible whitout the need for additional equipment, just the intrinsic characteristics of SDN.

References

1. «IoT : nombre d'appareils connectés dans le monde 2015–2025», *Statista.* https://fr.statista.com/statistiques/584481/internet-des-objets-nombre-d-appareils-connectes-dans-le-monde--2020/ (consulté le 4 mars 2022)
2. Nunes, B.A.A., Mendonca, M., Nguyen, X.-N., Obraczka, K., Turletti, T.: A survey of software-defined networking: past, present, and future of programmable networks. IEEE Commun. Surv. Tutorials **16**(3), 1617–1634 (2014). https://doi.org/10.1109/SURV.2014.012214.00180
3. Kreutz, D., Ramos, F.M.V., Esteves Verissimo, P., Esteve Rothenberg, C., Azodolmolky, S., Uhlig, S.: Software-defined networking: a comprehensive survey. Proc. IEEE **103**(1), 14–76 (2015). https://doi.org/10.1109/JPROC.2014.2371999

4. Swami, R., Dave, M., Ranga, V.: Software-defined networking-based DDoS defense mechanisms. ACM Comput. Surv. **52**(2), 1–36, avr. 2019. https://doi.org/10.1145/3301614
5. Devi, B.S.K., Subbulakshmi, T.: A comparative analysis of security methods for DDoS attacks in the cloud computing environment. Indian J. Sci. Technol. **9**(34) (2016). https://doi.org/10.17485/ijst/2016/v9i34/93175
6. Liu, Y., Zhao, B., Zhao, P., Fan, P., Liu, H.: A survey: typical security issues of software-defined networking. China Commun. **16**(7), 13–31, juill. 2019. https://doi.org/10.23919/JCC.2019.07.002
7. Cui, J., He, J., Xu, Y., Zhong, H.: TDDAD: time-based detection and defense scheme against DDoS attack on SDN controller. In: Susilo, W., Yang, G. (eds.) ACISP 2018. LNCS, vol. 10946, pp. 649–665. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-93638-3_37
8. Latif, Z., Sharif, K., Li, F., Karim, M.M., Wang, Y.: A comprehensive survey of interface protocols for software defined networks. arXiv:1902.07913 [cs], févr. 2019, Consulté le: 28 mars 2022. [En ligne]. Disponible sur: http://arxiv.org/abs/1902.07913
9. Jain, S., et al.: B4: Experience with a Globally-Deployed Software Defined WAN, p. 12
10. SDN Technical Specifications|Open Networking Foundation. https://www.opennetworking.org/software-defined-standards/specifications/ (consulté le 27 mars 2019)
11. «What are SDN Northbound APIs (and SDN REST APIs)?», SDxCentral. https://www.sdxcentral.com/networking/sdn/definitions/north-bound-interfaces-api/ (consulté le 5 mars 2022)
12. Lunagariya, D., Goswami, B.: A comparative performance analysis of stellar SDN controllers using emulators. In: 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, févr. 2021, pp. 1–9. https://doi.org/10.1109/ICAECT49130.2021.9392391
13. Daha, M.Y., Zahid, M.S.M., Husain, K., Ousta, F.: Performance evaluation of software defined networks with single and multiple link failure scenario under floodlight controller. In: 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, févr. 2021, pp. 959–965 (2021). https://doi.org/10.1109/ICCCIS51004.2021.9397125
14. Xiaohua, Y., Canhui, H.: Design and implementation of OpenDayLight manager application. In: 2020 13th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), Chengdu, China, pp. 977–982, October 2020. https://doi.org/10.1109/CISP-BMEI51763.2020.9263553
15. Mubarakali, A., Alqahtani, A.S.: A survey: security threats and countermeasures in software defined networking. In: 2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT), Kahului, HI, USA, mars 2019, pp. 180–185. https://doi.org/10.1109/INFOCT.2019.8711319
16. Yao, Z., Yan, Z.: Security in Software-Defined-Networking: A Survey. In: Security, Privacy, and Anonymity in Computation, Communication, and Storage, vol. 10066, G. Wang, I. Ray, J. M. Alcaraz Calero, et S. M. Thampi, Éd. Cham: Springer International Publishing, 2016, pp. 319–332 (2016). https://doi.org/10.1007/978-3-319-49148-6_27
17. Abhilash, G., Divyansh, G.: Intrusion detection and prevention in software defined networking. In: 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Indore, India, déc. 2018, pp. 1–4 (2018). https://doi.org/10.1109/ANTS.2018.8710141
18. Li, W., Meng, W., Kwok, L.F.: A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures. J. Network Comput. Appl. **68**, 126–139, juin 2016. https://doi.org/10.1016/j.jnca.2016.04.011
19. Shu, Z., Wan, J., Li, D., Lin, J., Vasilakos, A.V., Imran, M.: Security in software-defined networking: threats and countermeasures. Mobile Networks Appl. **21**(5), 764–776 (2016). https://doi.org/10.1007/s11036-016-0676-x

20. Mladenov, B.: Studying the DDoS attack effect over SDN controller southbound channel. In: 2019 X National Conference with International Participation (ELECTRONICA), Sofia, Bulgaria, mai 2019, pp. 1–4 (2019). https://doi.org/10.1109/ELECTRONICA.2019.8825601
21. Kuka, M., Vojanec, K., Kucera, J., Benacek, P.: Accelerated DDoS attacks mitigation using programmable data plane. In: 2019 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS), Cambridge, United Kingdom, pp. 1–3, September 2019. https://doi.org/10.1109/ANCS.2019.8901882
22. Dayal, N., Maity, P., Srivastava, S., Khondoker, R.: Research trends in security and DDoS in SDN. Secur. Commun. Networks **9**(18), 6386–6411 (2016). https://doi.org/10.1002/sec.1759
23. Bhaya, W., Manaa, M.E.: Review clustering mechanisms of distributed denial of service attacks. J. Comput. Sci. **10**(10), 2037 (2014)
24. Zargar, S.T., Joshi, J., Tipper, D.: A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Commun. Surv. Tutorials **15**(4), 2046–2069 (2013). https://doi.org/10.1109/SURV.2013.031413.00127
25. Dong, S., Abbas, K., Jain, R.: A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access **7**, 80813–80828 (2019). https://doi.org/10.1109/ACCESS.2019.2922196
26. Mishra, A., Gupta, B.B., Perakovic, D., Yamaguchi, S., Hsu, C.-H.: Entropy based Defensive Mechanism against DDoS Attack in SDN-Cloud enabled Online Social Networks. In: 2021 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, janv. 2021, pp. 1–6 (2021). https://doi.org/10.1109/ICCE50685.2021.9427772
27. Li, R., Wu, B.: Early detection of DDoS based on φ-entropy in SDN networks. In: 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, juin 2020, pp. 731–735 (2020). https://doi.org/10.1109/ITNEC48623.2020.9084885
28. Bawany, N.Z., Shamsi, J.A., Salah, K.: DDoS attack detection and mitigation using SDN: methods, practices, and solutions. Arab. J. Sci. Eng. **42**(2), 425–441 (2017). https://doi.org/10.1007/s13369-017-2414-5
29. Hung, S.-C., Iliev, N., Vamanan, B., Trivedi, A.R.: Self-organizing maps-based flexible and high-speed packet classification in software defined networking. In: 2019 32nd International Conference on VLSI Design and 2019 18th International Conference on Embedded Systems (VLSID), Delhi, NCR, India, janv. 2019, pp. 545–546 (2019). https://doi.org/10.1109/VLSID.2019.00128
30. Xu, Y., Muqing, W., Guohao, Y.: An effective routing mechanism based on fuzzy logic for software-defined data center networks. In: 2020 IEEE 6th International Conference on Computer and Communications (ICCC), Chengdu, China, déc. 2020, pp. 1793–1798 (2020). https://doi.org/10.1109/ICCC51575.2020.9344964
31. Novaes, M.P., Carvalho, L.F., Lloret, J., Proenca, M.L.: Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. IEEE Access **8**, 83765–83781 (2020). https://doi.org/10.1109/ACCESS.2020.2992044
32. Chen, M.-H., Ciou, J.-Y., Chung, I.-H., Chou, C.-F.: FlexProtect: a SDN-based DDoS attack protection architecture for multi-tenant data centers. In: Proceedings of the International Conference on High Performance Computing in Asia-Pacific Region - HPC Asia 2018, Chiyoda, Tokyo, Japan, 2018, pp. 202–209 (2018). https://doi.org/10.1145/3149457.3149476
33. Aizuddin, A.A., Atan, M., Norulazmi, M., Noor, M.M., Akimi, S., Abidin, Z.: DNS amplification attack detection and mitigation via sFlow with security-centric SDN. In: Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication - IMCOM '17, Beppu, Japan, 2017, pp. 1–7 (2017). https://doi.org/10.1145/3022227.3022230

34. Zheng, J., Li, Q., Gu, G., Cao, J., Yau, D.K.Y., Wu, J.: Realtime DDoS defense using COTS SDN switches via adaptive correlation analysis. IEEE Trans. Inform. Forensic Secur. **13**(7), 1838–1853 (2018). https://doi.org/10.1109/TIFS.2018.2805600
35. Buragohain, C., Medhi, N.: FlowTrApp: an SDN based architecture for DDoS attack detection and mitigation in data centers. In: 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), Noida, Delhi NCR, India, févr. 2016, pp. 519–524 (2016). https://doi.org/10.1109/SPIN.2016.7566750
36. Alsaeedi, M., Mohamad, M.M., Al-Roubaiey, A.A.: Toward adaptive and scalable OpenFlow-SDN flow control: a survey. IEEE Access **7**, 107346–107379 (2019). https://doi.org/10.1109/ACCESS.2019.2932422
37. Panchen, S., Phaal, P., McKee, N.: InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks. https://tools.ietf.org/html/rfc3176 (consulté le 25 juin 2019)
38. Wang, L., Li, Q., Jiang, Y., Jia, X., Wu, J.: Woodpecker: detecting and mitigating link-flooding attacks via SDN. Comput. Networks **147**, 1–13 (2018). https://doi.org/10.1016/j.comnet.2018.09.021
39. Liu, J., Lai, Y., Zhang, S.: FL-GUARD: a detection and defense system for DDoS attack in SDN. In: Proceedings of the 2017 International Conference on Cryptography, Security and Privacy - ICCSP '17, Wuhan, China, 2017, pp. 107–111 (2017). https://doi.org/10.1145/3058060.3058074
40. Niyaz, Q., Sun, W., Javaid, A.Y.: A deep learning based DDoS detection system in software-defined networking (SDN). EAI Endorsed Trans. Secur. Saf. **4**(12) (2017), Consulté le: 29 octobre 2020. [En ligne]. Disponible sur: https://eudl.eu/doi/10.4108/eai.28-12-2017.153515
41. Lim, S., Ha, J., Kim, H., Kim, Y., Yang, S.: A SDN-oriented DDoS blocking scheme for botnet-based attacks. In: 2014 Sixth International Conference on Ubiquitous and Future Networks (ICUFN), Shanghai, China, pp. 63–68, juill. 2014. https://doi.org/10.1109/ICUFN.2014.6876752
42. Dridi, L., Zhani, M.F.: SDN-guard: DoS attacks mitigation in SDN networks. In: 2016 5th IEEE International Conference on Cloud Networking (Cloudnet), pp. 212–217, October 2016. https://doi.org/10.1109/CloudNet.2016.9
43. Shin, S., Yegneswaran, V., Porras, P., Gu, G.: AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS '13, Berlin, Germany, 2013, pp. 413–424 (2013). https://doi.org/10.1145/2508859.2516684
44. Shang, G., Zhe, P., Bin, X., Aiqun, H., Kui, R.: FloodDefender: protecting data and control plane resources under SDN-aimed DoS attacks. In: IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, Atlanta, GA, USA, mai 2017, pp. 1–9. https://doi.org/10.1109/INFOCOM.2017.8057009
45. Birkinshaw, C., Rouka, E., Vassilakis, V.G.: Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks. J. Network Comput. Appl. **136**, 71–85 (2019). https://doi.org/10.1016/j.jnca.2019.03.005
46. Wang, H., Xu, L., Gu, G.: FloodGuard: a dos attack prevention extension in software-defined networks. In: 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, juin 2015, pp. 239–250. https://doi.org/10.1109/DSN.2015.27
47. Wu, P., Yao, L., Lin, C., Wu, G., Obaidat, M.S.: FMD: a DoS mitigation scheme based on flow migration in software-defined networking: FMD: A DoS mitigation scheme based on flow migration in software-defined networking. Int. J. Commun. Syst. **31**(9), e3543 (2018). https://doi.org/10.1002/dac.3543

48. Son, S., Shin, S., Yegneswaran, V., Porras, P., Gu, G.: Model checking invariant security properties in OpenFlow. In: 2013 IEEE International Conference on Communications (ICC), Budapest, Hungary, juin 2013, pp. 1974–1979. https://doi.org/10.1109/ICC.2013.6654813
49. Ball, T., et al.: VeriCon: towards verifying controller programs in software-defined networks. In: Proceedings of the 35th ACM SIGPLAN Conference on Programming Language Design and Implementation, New York, NY, USA, pp. 282–293 (2014). https://doi.org/10.1145/2594291.2594317
50. Zaalouk, A., Khondoker, R., Marx, R., Bayarou, K.: OrchSec Demo: Demonstrating the Capability of an Orchtestrator-based Architecture for Network Security, p. 3
51. Shirali-Shahreza, S., Ganjali, Y.: Traffic statistics collection with FleXam. .In: Proceedings of the 2014 ACM conference on SIGCOMM - SIGCOMM '14, Chicago, Illinois, USA, pp. 117–118 (2014). https://doi.org/10.1145/2619239.2631441