Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 238 (2024) 127–134

Procedia Computer Science

www.elsevier.com/locate/procedia

The 15th International Conference on Ambient Systems, Networks and Technologies (ANT)
April 23-25, 2024, Hasselt, Belgium

Exploring current solutions against DDoS attacks in SDN environment

Franco Jaraba[a], Gautam Mahajan[a], Jay Jani[a], Robert Ipu[a], and Sergey Butakov[b]*

[a] *Concordia University of Edmonton, Edmonton, AB, T5B 4E4, Canada*
[b] *Western New England University, Springfield, MA,01119, USA*

Abstract

Software Defined Networking (SDN) offers a novel approach to network management, with the potential to simplify administration and enhance security. However, as with any emerging technology, it comes with vulnerabilities that may impact its availability and functionality. A prevalent attack on SDN controllers is Distributed Denial of Service (DDoS), which, while not entirely preventable, can have its effects mitigated. This study explores the factors influencing the performance of industry solutions in defending SDN against DDoS attacks and evaluates their efficiency. It investigates various security challenges associated with DDoS attacks in both Information Technology (IT) and Operational Technology (OT) environments and contrasts the effects of distinct DDoS attack types on multiple levels of SDN communication, such as Northbound-Southbound and East-West. Lastly, the applicable solution's effectiveness was assessed based on the controller's hardware utilization and response time.

Keywords: DDoS; SDN; Software Defined Networking; IoT security; SCADA security

* Corresponding author. Tel.: +1-413-782-1250
E-mail address: sergey.butakov@wne.edu

10.1016/j.procs.2024.06.007

1. Introduction and related works

1.1. SDN Architecture and related security problems.

Contrary to a traditional network where the data, control, and application planes are vertically integrated, forming a complex structure, the Software Defined Networking (SDN) approach divides the entire Infrastructure into three planes: Data Plane, Controller Plane, and Application Plane. The main idea here is to divide the physical layer from the logical layer and control the entire network centrally from the control plane. SDN is the next-generation solution for solving complex IT infrastructure problems that can accumulate and integrate solutions from many vendors [1].

Generic topology of SDN technology is divided into application, control, and data planes.

Data/Infrastructure Plane: This is the bottommost layer consisting of all the hardware devices. This layer consists of devices such as routers, switches, access points, etc. [1]. The main function of this layer is to receive the rules/ policies and act on them by forwarding or blocking the packets.

Controller Plane: Controller Plane can be considered the brain of the SDN architecture. The main task of the Controller is to provide a high level of integration between the application and data plane to provide communication between network devices and applications SDN Controller is used to configure flow rules in the routers and switches in the data plane [2]. The controller uses the Northbound APIs for communication with the Application Layer and Southbound APIs for communication with the data plane. Another set of APIs called East-West APIs is used for the lateral communication between SDN controllers.

Application Plane: The application plane provides applications like Firewall, Load Balancer, QoS, Intrusion Detection System, Intrusion Prevention System, Network Virtualization, and Routing that are necessary for the infrastructure [1]. The Application Control Plane Interface (ACPI), which is also known as the Northbound interface, is responsible for communication between SDN controllers and the Application Plane.

1.2. Industrial Control Systems SDN Architecture

Industrial Control Systems (ICS) are used to run manufacturing and the critical infrastructure that powers the economies. These include power distribution, traffic management, water management, oil, and gas pipelines, etc. Industrial control systems include supervisory control and data acquisition systems (SCADA) used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to manage localized physical processes [3].

Due to security concerns in the recent past, ICS were once air-gapped with no connection to outside networks. However, modern control networks are seeing tighter integration with corporate networks. This integration significantly expands the attack surface for ICS networks. A clear example of this was the dragonfly attack [4] or the recent attack on Ukraine’s power infrastructure by state-sponsored actors using an exploit known as black energy [5].

To address some of these challenges, SDN has been proposed as an alternative to traditional architectural methods. SDN’s deny-by-default stance greatly compliments ICS networks' static nature. This allows control system engineers to define traffic flows at a circuit level, dictating the exact forwarding path for traffic. SDN controllers also allow the visualization of heterogeneous networks, thus providing control engineers the ability to monitor the entire network including components located in unmanned locations.

SDN provides comprehensive network management solutions in such use cases as Load Balancing [6], Network Monitoring and Management [6], and Unified Communication in Enterprises [7], [8]. All the advantages of SDN technology and its successful use cases promote its fast proliferation in the industry. Despite all the advances SDN brings along, the technology is susceptible to various cyberattacks including Distributed Denial of Service (DDoS). Given the fact that typically DDoS researchers look at the attacks on the data plane and assume proper isolation of the Noth- and West-East-bound communications, the impact of various DDoS on these links does not receive much attention in terms of practical evaluations. This paper provides insight into the effect of DDoS on the communication lines that are typically considered off the band in SDN architectures.

1.3. Security Problems and DDoS in SDN Ecosystem

There are a few weak spots in the SDN that exist at the three levels of SDN architecture. Two of these levels are the core or brain of the SDN known as the SDN controller and the other network forwarding devices. Vulnerabilities and weaknesses at various levels in the SDN architecture lead to attacks including DoS, DDoS, Spoofing, Tampering, Privileged Escalation, and IP address forgery to get trust from switches on the data plane [9] [10], configuration file injection, SQL injection attacks, etc. [11]. Although SQL injection is a web application-based attack but can affect the controller's database. The exploitation of these weak spots may lead to link failure, asynchronous updates of the forwarding devices, and SDN controller failure. This research is looking at the impact of DDoS attacks and the rest of the literature review will be focused on this problem.

A Distributed Denial of Service (DDoS) attack is a coordinated attack on a target system's services or network that is initiated indirectly through numerous computer devices controlled by an attacker. The "main victim" is the service under attack while the compromised systems used to launch the attack are sometimes referred to as "secondary victims." The use of secondary victims in a DDoS assault allows the attacker to scale up and launch a more disruptive attack while staying anonymous, as the secondary victims are the ones who actually produce the malicious traffic.

The logically centralized controller in an SDN architecture is the single point of failure, and if it fails, the entire network will be disrupted. For each Packet-In-Request received from a switch, the controller computes an action set. The controller's resources, such as CPU, memory, and I/O bandwidth, are used to calculate the action sets. Typically, an SDN controller can manage a very large number of requests at once, but there is always a limit to that amount. As a result, a DDoS attack that generates an excessive number of requests will exhaust the controller's resources leading to the situation where the genuine queries are eventually delayed or dropped. An attacker may also try to disrupt the controller's operation by using techniques such as buffer overflow, which can result in erroneous forwarding rules landing in the data plane [12].

Apart from the controller, the other targets for DDoS may include the links between the components of the SDN architecture: North-, South-, and West–East–bound communications. Even minor congestion in these channels can result in inexorable network delays. For example, delaying Packet-In messages on the South-bound line may significantly reduce network performance. A massive number of malicious flows created by a DDoS attack can saturate the secure channel, causing the entire network to go down. Failure of the controller or its communication lines can shut down the entire network and that is why it becomes the primary target for DDoS [13]. According to [14] the other potential threats that pose a high risk to the SDN controller include a lack of trust between components and software vulnerabilities in the controller itself.

1.4. Solutions against DDoS in SDN

Blocking all the attacker connections that are affecting the application's server from the internet access is one of the most effective ways to do instant protection against DDoS attacks, but it is not the most efficient due to the affection to the legitimate traffic. The main approach in protection is to separate legitimate and malicious traffic and block the latter. For example, in [15] researchers suggested using entropy to classify the traffic type based on the number of forwarded packets. They have achieved a relatively good detection ratio ranging from 96% to 100% for various combinations of [malicious]:[normal] traffic ratio. In another work, researchers used machine learning methods to achieve ~99% accuracy in malicious traffic classification and, subsequently, suppression [16]. As can be seen from these examples such classifiers may achieve high levels of accuracy, but they are yet to make it to the mainstream in industry solution as they are computationally extensive and require constant tuning.

Other research projects suggested relying on Network Function Virtualization (NFV) in a dispersed but reciprocal method to mitigate DDoS attacks [18]. Overall, they use one of the advantages of NFV which provides resilience in highly changeable demanding networks [19]. The technology lends to having a software and hardware area split, adjusting the network distribution services as required, and adapting to the progressive growth in the network as demand. This approach assumes that detecting the attacks far from the uplink can ease hardware usage; consequently, early detection of the attacks prevents overhead on the network devices and can release resources for legitimate traffic. For this, the technology relies on examining the packets throughout the whole network, gathering, and evaluating

them to identify inconsistencies, and having an aggressive response to changes in the environment to respond against different sorts of attacks, which can lead to an effective way to prevent outages in the network.

The other approach used in the industry for DDoS protection is to provide better shielding of the management traffic from public traffic in the SDN infrastructure. Various forms of VPN protocols such as IPSec, SSL, PPTP, L2TP, and MTLS are widely used [20] [21] to achieve this isolation but they are also susceptible to DDoS [22].

1.5. Contribution

The paper aims to evaluate the performance of currently available industry solutions against DDoS attacks, with three subprojects focusing on various specific aspects of the SDN architecture:

- The first aims to identify the effectiveness of Ubuntu Kernel Parameter security mechanisms against the distributed denial of service attacks in layer 3 of the TCP/IP model. Attacks will be focused on disrupting the North-South communication between an application located behind an edge node and a virtual machine located in the public network.
- The second proposed research contribution is focused on identifying the existing DDoS prevention mechanisms to secure East–West (lateral) communication and conducting a comparative analysis of the performance of SDN against DDoS attacks in various scenarios. To check the effectiveness of the VPN against DDoS attacks, a VPN will be implemented in the SDN infrastructure between two sites having SDN controllers in high availability.
- The third proposed research aims to analyze the impact of DDoS attacks on SDN controllers when implemented in ICS architectures.

2. Experimental Setup

The goal of this experimental research is to provide insights into the performance of an SDN Controller while under a DDoS attack. This project aimed at testing SDN controllers under three scenarios:

- *Subproject 1*: This project aims to identify the effectiveness of OS kernel parameters used in a virtual machine that will be deployed in a public network to countermeasure the effect of the DDoS in a public web server.
- *Subproject 2*: This subproject aims to analyze the impact of DDoS attacks targeting the East-West communication between SDN controllers at two sites before and after the mitigation mechanism is applied.
- *Subproject 3*: Examine how SDN controllers in ICS networks perform when subjected to a DDoS attack.

2.1. Subproject 1: OS hardening

The first project intends to test the Ubuntu OS kernel parameter's performance in a controlled environment with 1 Apache web application located behind the edge node and 33 attackers' virtual machines located in the outside network. The SDN environment will be implemented in a simulated environment with 3 servers and 3 workstations each playing different roles on the network: Servers play the following roles: Attacker (malicious traffic generator); Victim (managing application host); Edge (separation of public and private network segments and SDN controller hosting). Workstations have been used to host virtual machines to generate legitimate traffic and manage the architecture.

The attack was scheduled to instruct the attacker node to deploy Ubuntu Linux-based virtual machines with pre-configured flood scripts every 5 min. This means, the number of attacking actors and volume of DDoS packets will be increasing every 5 min and will be measured by NetFlow flows in the edge node.

2.2. Subproject 2: VPN

The second subproject aims to evaluate the performance of an SDN infrastructure when subjected to DDoS attacks in a redundant SDN environment. More specifically, the attack is aimed at East–West communication – communication between redundant controllers. POX SDN controller was used for the experiment. The performance will be measured in two scenarios: without and with VPN protection for the E-W line. The performance of the SDN

infrastructure will be evaluated using the *cbench* tool - an SDN controller benchmarking tool. The tool measures the number of flows/milliseconds in consecutive iterations of the test to determine the SDN infrastructure's performance prior to and during the DDoS attacks and the effectiveness of the VPN in mitigating the DDoS attacks.

For this subproject, a fully virtualized SDN environment was implemented using an OpenStack server. All the instances were created using Ubuntu Linux and StrongSwan VPN was used for establishing site-to-site VPN. Details of the setup are provided in Fig. 1. Three DDoS attack scenarios were performed on the setup:

- The first attack scenario aimed to test the performance of the Pox controller during an internal DDoS attack from multiple hosts toward the server located on the data plane. During a TCP SYN flood attack from h2, h3, h4, h5, and h6 to h1, the performance was measured using *cbench*, 16 switches, 10 iterations, and 1M packets per test.
- The second attack scenario aimed to test the performance of the Pox controller during an attack on the management interface targeting East-West communication between two Pox controllers in high availability. The attack was carried out on the central router without VPN, and the performance was measured using *cbench*, 16 switches, 10 iterations, 1,000,000 packets per test, and latency mode.
- The third attack scenario aimed to test the performance of the Pox controller while the security mechanism (VPN) was in place during a DDoS attack on the management interface targeting East-West communication between two Pox controllers in high availability. The attack was carried out on the central router with VPN, and the performance was measured using *cbench*, 16 switches, 10 iterations, and 1,000,000 packets per test.

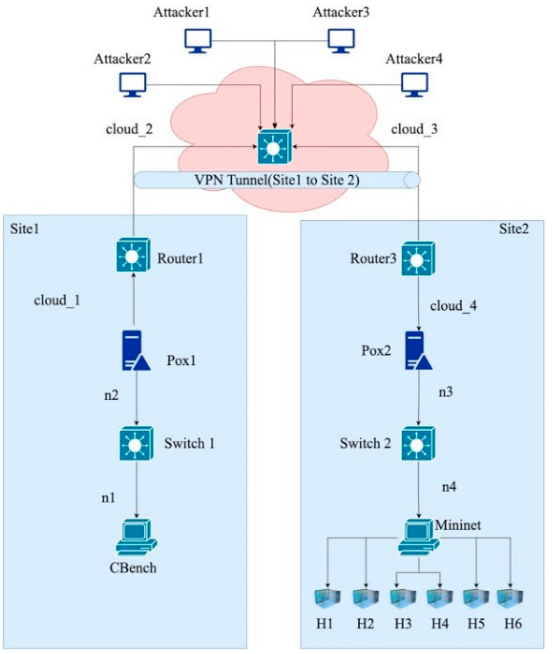

Fig. 1: Experimental setup for subproject 2

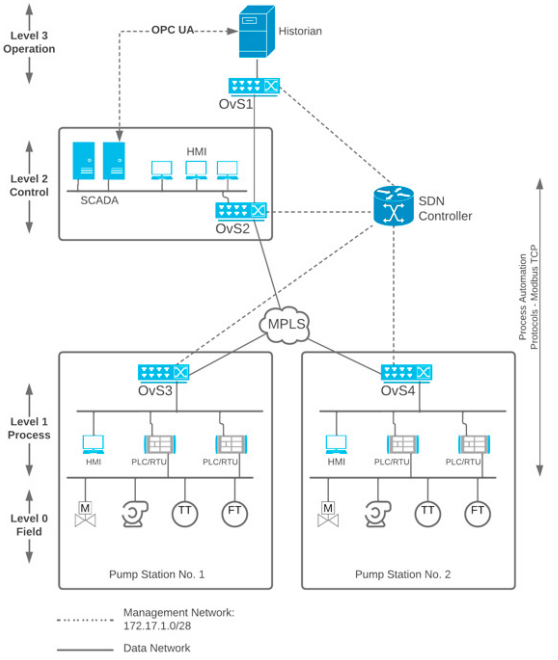

Fig. 2: Experimental setup for subproject 3

2.3. Subproject 3: Industrial Control Systems

In the experiment, the performance of a single Software-Defined Networking (SDN) controller will be assessed when it is integrated into an Industrial Control System (ICS) environment. Two SDN controllers, Floodlight and Faucet, have been selected for evaluation in this project. These controllers were selected due to their significant differences in implementation and supported OpenFlow protocols. The ICS environment shown in Figure 2 will be simulated with the aid of emulators, complete with the most popular ICS protocols such as OPC-UA for the historian and Modbus. A DDoS attack will be carried out using the Low Orbit Ion Cannon (LOIC) tool targeted at the SDN controller on TCP port 6653, which is typically used for OpenFlow communications.

3. EXPERIMENTAL RESULTS

3.1. Subproject 1: OS hardening results.

Initially, a baseline measurement of the time response from the legitimate clients was required to identify the SDN functioning under the attack without any protective measures applied. The same measurements were taken after the protective measurements such as OS hardening were applied. Figure 3 compares the results of the SDN infrastructure before and after the OS hardening was applied. It is noticed that the average response time increased by 19% which could indicate continued communication from the legitimate traffic and the Apache server, as indicated in Figure 3.

Further studies of traffic patterns indicated that even though the hardening created additional delays in the legitimate traffic VM – Apache server traffic, there are no HTTP packets lost in the channel. It seems the mitigation appliance controls the bandwidth for TCP connections and SYN packets going through the appliance. On the other hand, additional delays on the kernel level can be a communication bottleneck due to the required bandwidth for the overlay network. To summarize it was concluded that Ubuntu kernel parameters can serve as a reasonable protection mechanism for SDN controller hosts, but vertical scaling of the hardware may be required due to increased workloads on the resources allocated to the appliance.

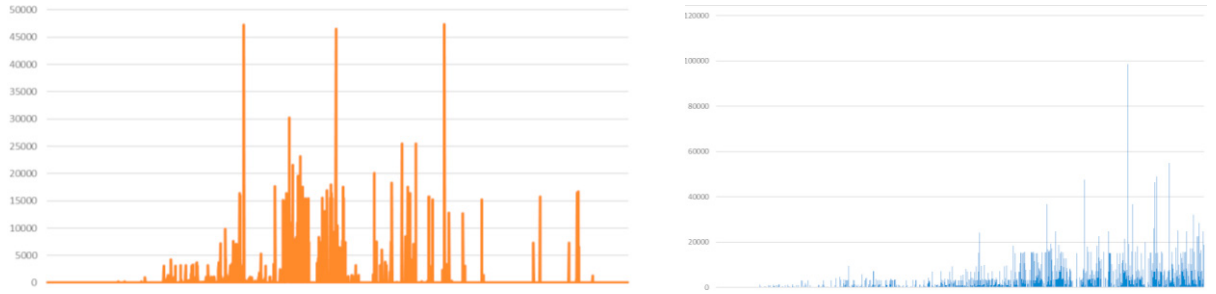

Fig. 3: Experimental setup for subproject 1: Apache response time during the attack. Left: without OS hardening; Right: with OS hardening.

3.2. Subproject 2: VPN application results.

The DDoS attack on the SDN management interfaces was performed with an increasing number of bots generating attacking traffic: 1, 2, and 4 bots. Figure 4 shows the results when a DDoS attack was performed on the management interface with 2 bots. The number of epochs in Figure 4 represents the number of cycles to observe traffic generated by *cbench*. Without VPN, the min/max/avg/stdev was 525.04/2832.97/859.21/699.62 responses/s. During the attack, the number of flows/ms dropped to around 0.5257. However after the VPN was established between Site 1 and Site 2, the number of flows/ms increased to 1.586.

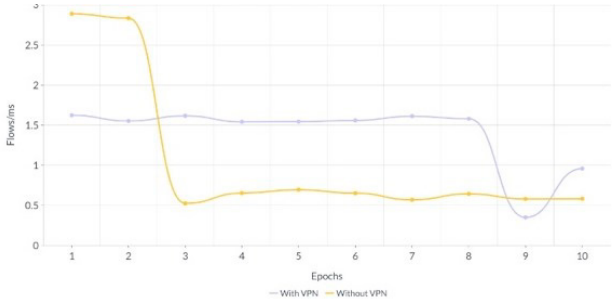

Fig. 4: Experimental setup for subproject 2: without VPN and with VPN between redundant controllers.

The analysis of test results indicated that the number of flows per second increased for a few iterations when a Virtual Private Network (VPN) was used to securely transmit data from Router 2 during an ongoing Distributed Denial of Service (DDoS) attack. Prior to the attack and the VPN connection, the average number of flows per second was

2956.57. However, during the DDoS attack aimed at disrupting East-West communication between the POX controllers located at Site 1 and Site 2 without VPN, the average number of flows decreased to 814.99. Such a decrease may represent a significant performance issue on loaded systems with high availability requirements. As figures 39 and 40 show, DDoS without VPN enabled resulted in the disruption of communication between the controllers. After enabling the VPN connection between Site 1 and Site 2, it was observed that the controller was not disconnected during the attack, as it happened without VPN, and the test was completed with an average of 1593.40 flows per second. From the above observations, it can be concluded that while VPN protects East-West communication from a comparatively smaller DDoS attack, it is still prone to DDoS attacks and additional isolation must accompany VPN implementation for East-West communication protection against larger scale DDoS attacks.

3.3. Subproject 3: Hardening SDN in ICS environment

The DDoS attack has significantly impacted the controller's performance, causing the average responses per second to fall to a minimum of 65,000. A decrease in packet count from 2800 to 1900 reveals that the controller is overloaded to process some of the legitimate traffic. During the attack, there was a significant increase in resource utilization, with CPU usage jumping to over 75% and remaining at that level until the controller failed.

The mitigation strategy against this attack involves utilizing the rate limit feature in iptables embedded firewall. It uses the *recent module* to track and control the rate at which new connections are allowed. The default rate limit rule in UFW is configured to allow up to 6 new connections per IP address within a 30-second time frame. As shown in Figure 7, after implementing the remediation, the average response rate per second has significantly improved, to a minimum of 100,000 and a maximum of 135,000 responses/sec during the test period that ran the full 30 minutes and with four attacking bots.

The experiment demonstrates that an SDN controller can become a single point of failure in a network if appropriate protective measures are not implemented. Although built-in firewall options within the controller can help reduce the impact of an attack, they should serve as a secondary defense measure due to the resource-intensive nature of the mitigation process. Relying solely on these inbuilt firewalls could lead to the controller performance being compromised by a large-scale attack. To effectively protect the controller, it is recommended to use a dedicated device, specifically designed to withstand such attacks, such as a proxy firewall positioned between the controller and switches.

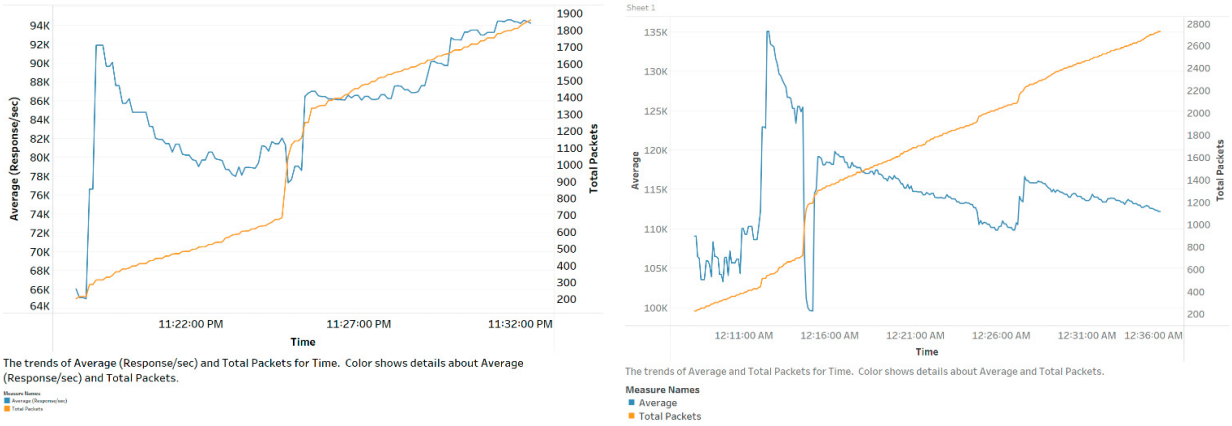

Fig. 5: Experimental setup for subproject 3: left without OS hardening; right – with OS hardening.

4. CONCLUSION

In this study, three distinct DDoS attack mitigation mechanisms were examined in separate SDN environments. The first subproject employed the kernel parameter in an operating system as a DDoS countermeasure for a web server application. In the second subproject, VPN was utilized to analyze and mitigate the impact of DDoS on east-west communication between two SDN controllers. The third subproject implemented host system firewall rules to defend against DDoS attacks in an Industrial Control System SDN ecosystem. After conducting experiments and analyzing the outcomes for all three subprojects, it was determined that none of the mitigation techniques provided complete

protection against DDoS attacks in SDN environments. One noticeable limitation of the conducted experiments was the time limit of the attacks. They lasted no more than 60 minutes while some known DDoS attacks were carried out for days. The extension of the attack timeframe will be carried out as future projects. The experimental findings confirmed the necessity for multi-layered security solutions. Potential measures to add to the ones explored in the project include reverse proxies, dedicated firewall appliances, Intrusion Detection/Prevention Systems, and high-availability setups with controller load balancing. Future research is required to evaluate cross impact of multi-layered setups in ICS protection.

References

[1] D. B. Rawat and S. R. Reddy, "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 325-346, 2017.

[2] F. Hu, Q. Hao and K. Bao, "A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation," IEEE Communication Surveys & Tutorials, vol. 16, no. 4, pp. 2181-2206, 2014.

[3] Joint Task Force Transformation Initiative, "NIST SP 800-30 Rev.1," 17 September 2012. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final. [Accessed 14 October 2022].

[4] J. T. Langill, "Defending Against the Dragonfly Cyber Security Attacks," 22 October 2014. [Online]. Available: https://www.belden.com/hubfs/resources/knowledge/white-papers/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks-AB_Original_68751.pdf?hsLang=en. [Accessed 25 November 2022].

[5] U.S. Department of Homeland Security, "ICS Alert (IR-ALERT-H-16-056-01)," Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 25 February 2016. [Online]. Available: https://us-cert.cisa.gov/ics/alerts/ir-alert-h-16-056-01. [Accessed 14 October 2022].

[6] T. Zinner, M. Jarschel, T. Hobfeld, T. G. Phuoc and W. Kellerer, "Interfaces, attributes, and use cases: A compass for SDN," IEEE Communications Magazine, vol. 52, no. 6, pp. 210-217, 2014.

[7] J. Tourrilhes, P. Sharma, S. Banerjee and J. H. L. Pettit, "The Evolution of SDN and OpenFlow: A Standards Perspective," HP Labs, 2014.

[8] R. Bobba, D. R. Borries, R. Hilburn, J. Sanders, M. Hadley and R. Smith. Software-Defined Networking Addresses Control System Requirements: A Collection of Technical Papers Representing Modern Solutions, 2018, pp. 6-7, 2014.

[9] M. Iqbal, F. Iqbal, F. Mohsin, D. M. Rizwan and D. F. Ahmad, "Security Issues in Software Defined Networking (SDN): Risks, Challenges and Potential Solutions," International Journal of Advanced Computer Science and Applications, vol. 10, no. 10, pp. 298-303, 2019.

[10] A. Sebbar, K. Zkik, Y. Baddi, M. Boulmalf and M. D. Ech-Cherif El Kettani, "Secure Data Sharing Framework Based on Supervised Machine Learning Detection System for Future SDN-Based Networks.," in Machine Intelligence and Big Data Analytics for Cybersecurity Applications, Springer, 2020, pp. 355-371.

[11] Q. Ilyas and R. Khondoker, "Security Analysis of FloodLight, ZeroSDN, Beacon and POX SDN Controllers," in SDN and NFV Security, Springer, 2018, pp. 85-98.

[12] M. Dabbagh, B. Hamdaoui, M. Guizani and A. Rayes, "Software-defined networking security: pros and cons," IEEE Communications Magazine, vol. 53, no. 6, pp. 73-79, 2015.

[13] F. M. V. Ramos, D. Kreutz and P. Verissimo, "Towards secure and dependable software-defined networks," Proceedings of the second ACM SIGCOMM workshop on Hot topics in software-defined networking, p. 55–60, 2013.

[14] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76, 2015.

[15] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in 2015 International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, USA, 2015.

[16] K. K. Karmakar, V. Varadharajan and U. Tupakula, "Mitigating attacks in Software Defined Network (SDN)," in 2017 Fourth International Conference on Software Defined Systems (SDS), Valencia, Spain, 2017.

[17] B. Nugraha and R. N. Murthy, "Deep Learning-based Slow DDoS Attack Detection in SDN-based Networks," in 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Leganes, Spain, 2020.

[18] L. Zhou and H. Guo, "Applying NFV/SDN in mitigating DDoS attacks," in IEEE Region 10 International Conference TENCON, Penang, Malaysia, 2017.

[19] 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 , vol. 18, no. 1, pp. 236-262, 2015.

[20] J. Jones, H. Wimmer and R. J. Haddad, "Pptp VPN: An analysis of the effects of a DDoS attack," 2019 SoutheastCon, pp. 1-6, 2019.

[21] Y. Zhou and K. Zhang, "DoS vulnerability verification of IPSec VPN," 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)}, pp. 698-702, 2020.

[22] D. A. Zaripova and M. A. A. Ugli, "Network security issues and effective protection against network attacks," International Journal on Integrated Education, vol. 4, no. 2, pp. 79-85, 2021.