Detection and mitigation of DDoS attacks in SDN based intrusion detection system

Meryem Chouikik[1], Mariyam Ouaissa[2], Mariya Ouaissa[3], Zakaria Boulouard[1], Mohamed Kissi[1]
[1]LIM, Hassan II University, Casablanca, Morocco
[2]Laboratory of Information Technologies, Chouaib Doukkali University, El Jadida, Morocco
[3]Computer Systems Engineering Laboratory, Cadi Ayyad University, Marrakech, Morocco

Article Info

Article history:

Received Sep 17, 2023
Revised Dec 21, 2023
Accepted Feb 24, 2024

Keywords:

Distributed denial of service
Intrusion detection systems
Mininet
OpenDaylight
OpenFlow
Software defined networks
Throughput

ABSTRACT

Software defined networks (SDN) have completely revolutionized the management and operation of networks. This novel technology entails a distinctive approach to management. Amidst the advancements, a notable security concern arises in the form of distributed denial of service (DDoS) attacks. To counteract this attack, the deployment of intrusion detection systems (IDS) assumes paramount importance. IDS plays a critical role in monitoring network traffic, promptly detecting irregularities that may signify a potential denial of service (DoS) assault. This study delves into a comprehensive exploration of a DDoS attack on an SDN network using the OpenDaylight controller and the Mininet emulator. Furthermore, the assessment extends to evaluating the DDoS attack's repercussions and the effectiveness of IDS in mitigating such risks. Various performance metrics, including throughput according to delay time, are monitored to gauge network performance under duress. The difference in throughput curves when comparing scenarios with and without IDS highlights the significant impact of intrusion detection. When the IDS was absent, there was a noticeable increase in oscillations, indicating greater network susceptibility. On the other hand, the presence of an IDS created a more regulated environment, reducing variances and promoting a more stable network.

Corresponding Author:

Mariya Ouaissa
Computer Systems Engineering Laboratory, Cadi Ayyad University
Marrakech, Morocco
Email: m.ouaissa@uca.ac.ma

1. INTRODUCTION

The concept of software defined networking (SDN) brings about a distinct separation between the control plane and the data plane within networks. This division introduces a heightened level of flexibility in network configuration and more efficient management capabilities [1]. SDN networks are governed by a centralized controller, which streamlines the implementation of security protocols and the identification of irregularities within network traffic. This aspect proves particularly beneficial in the mitigation of distributed denial of service (DDoS) attacks [2].

Contrarily, in traditional networks, control, and forwarding functions are tightly intertwined within individual network devices. Routing decisions and network policies are preconfigured on each device, necessitating manual interventions and device-specific updates for network changes [3]. This often leads to intricate and time-consuming network management processes, especially in large-scale setups. SDN disrupts this norm by uncoupling the control plane and data plane, introducing a centralized controller that takes charge of network management [4].

DDoS attacks exert specific impacts on SDN networks [5]. SDN networks might exhibit heightened vulnerability to attacks targeting the centralized controller that governs them. Moreover, the adaptable nature of SDN networks could potentially aid attackers in identifying and exploiting weaknesses [6]. Such DDoS attacks on SDN networks can occasionally extend their impact to affect other networks connected to the same controller, leading to widespread disruptions and outages [7]. Intrusion detection systems (IDS) serve as security tools or systems designed to monitor network and system activities, promptly identifying and responding to malicious or unauthorized actions. IDS scrutinizes network traffic, system logs, and relevant data sources to detect signs of intrusion or abnormal behavior [8].

Many studies have delved into the prominent security vulnerabilities presented by SDN networks and the pressing requirement to counteract the detrimental consequences of DDoS attacks that exploit these vulnerabilities. In one study [9], a software-defined intrusion detection system was developed which proactively neutralizes attacks at their source, ensuring the network functions as intended. This approach incorporates an IDS that can autonomously identify various DDoS threats, and upon detection, communicates with an SDN controller. Dridi and Zhani [10] introduced SDN guard, an innovative solution crafted to defend SDN networks from denial of service (DoS) attacks. This is achieved by intelligently rerouting potential harmful traffic, tweaking flow timeouts, and consolidating flow rules. Kandoi and Antikainen [11] highlights two unique DoS attacks tailored for OpenFlow SDN setups. The researchers simulated these attacks on Mininet and explored their impacts, noting that both the timeout duration of a flow rule and the bandwidth of the control plane significantly influence switch performance. Yet another paper [12] showcases DoS-Guard, a comprehensive and protocol-agnostic safeguard for SDN networks, designed to identify and alleviate such threats. Essentially, DoS-Guard is a streamlined add-on for SDN controllers, comprising three primary elements: a monitor, a detector, and a mitigator. Research by Tian *et al.* [13], the ramifications of DOS attacks on SDN controllers are examined. The researchers introduced two countermeasures, namely FlowSec and Blackbox. FlowSec's strategy limits the packet transmission rate to the controller, while Blackbox dynamically gauges threat levels, spotting and reacting to varying severe attacks in real-time.

This paper highlights the importance of effective IDS, as demonstrated by the SNORT IDS. The proficiency in reducing the effects of DDoS attacks and enhancing network stability is clear. Through a deep comprehension of the complex dynamics between cyber attacks and defensive mechanisms, this research empowers us to strengthen network defenses against the constantly changing landscape of cyber threats. The growing susceptibility to DDoS attacks, which may target the central SDN controller, stands out as a major concern [14]. In this scenario, IDS proves invaluable. IDS remains vigilant over system logs, network activities, and data sources to identify and react to suspicious or malicious actions. By analyzing network packets, IDS can recognize and issue alerts for potential security breaches or anomalies. Within SDN environments, IDS plays a crucial role in detecting and thwarting DDoS attacks by monitoring traffic patterns, spotting irregular behaviors, and initiating appropriate defenses. Integrating IDS into the SDN control plane enhances overall network security. IDS gains a comprehensive understanding of network traffic and dynamically enforces security protocols by leveraging SDN's programmability. By swiftly identifying potential threats, such as unusual traffic patterns or unexpected activities, IDS ensures the safeguarding of the SDN infrastructure. This integration bolsters network security by facilitating real-time monitoring and detection capabilities, augmenting the ability to identify and counter potential threats, including DDoS attacks [15].

The structure of this paper is organized as: section 2 provides an introduction to the background. Section 3 delves into the proposed design. Section 4 presents the results and discussions of the analysis. Conclusion are drawn in section 5.

2. BACKGROUND

2.1. Architecture for software defined network

The architecture of SDN was conceived to foster innovation in networking hardware. Constituting the crux of SDN are three layers and their corresponding communication interfaces. A depiction of these layers and communication interfaces follows [16], [17]. The forwarding layer, often referred to as the data plane, encompasses an array of devices, typically including switching, and routing components. Serving as the operational core, the data plane undertakes data transmission and collection duties. The control layer, commonly known as the control plane, is predominantly composed of one or more SDN controllers. Operating through a mechanism termed the south-bound API as illustrated in Figure 1, its principal role revolves around the management and orchestration of the underlying hardware infrastructure [18].

In an SDN-centric network, the core intelligence resides in the network controller, dictating the routes traffic flows will take across the network. Meanwhile, network devices like switches and routers simply relay packets according to the flow rules set by the controller. The control plane interacts with the data plane and the application plane via the southbound interface (SBI) and northbound interface (NBI), respectively. Such a setup enhances network management. To elaborate, it facilitates rapid, flexible, and automated network adjustments, optimizes the use of network assets, and eases the process of troubleshooting and debugging.

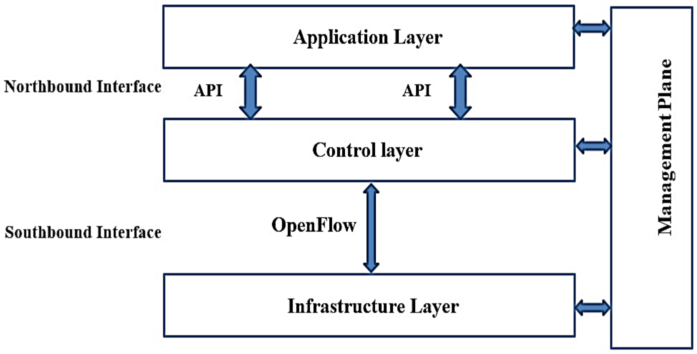

Figure 1. SDN architecture

2.2. Network security in software defined networking

Given the fluid and adaptable nature inherent to these networks, ensuring security for SDNs stands as a paramount concern. Below, you'll find pivotal insights into the security landscape of SDNs [19], [20].

- Targeted attacks on SDN controllers: the controllers in SDNs hold immense allure for potential attackers, serving as the neural hub of the network. Compromising a controller could yield catastrophic consequences, offering malefactors control over the entire network. They might reroute traffic, manipulate components maliciously, or even bring adversarial elements to a halt.
- Controller integrity and authenticity: guaranteeing the unadulterated authenticity of SDN controllers is of utmost importance. Robust mechanisms for authentication and integrity verification are imperative to ascertain that solely sanctioned and untainted controllers establish communication with the network.
- Data plane vulnerabilities: the partition between the control and data planes introduces novel vulnerabilities in the data plane. The security of switches and routers employed for data transfer becomes pivotal in combatting threats such as buffer overflows, injection of malicious traffic, and service disruptions.
- Isolation and multi-tenancy: in shared SDN environments, where disparate entities share a common network, meticulous isolation of locations is indispensable. This prevents cross-contamination and inadvertent data leaks, preserving each entity's integrity.
- Enforced access control: robust access control mechanisms must be enacted to ensure that exclusively authorized entities can interact with SDN resources and controllers, preventing unauthorized interventions.
- Confidentiality and encryption: upholding the confidentiality of data and safeguarding against interception mandates the implementation of encryption protocols for communications spanning various SDN network elements, encompassing controllers and data transmission components.
- The security landscape of SDN networks necessitates a comprehensive approach, combining technical safeguards, stringent security protocols, and heightened awareness to counter emerging threats in an environment characterized by extensive programmability [21].

3. PROPOSED DESIGN

This article centers its attention on cyber-attacks, with a specific focus on the impactful realm of DDoS attacks in the context of SDN. The primary objectives of these attacks involve undermining network performance, instigating disruptions, and enabling the centralized management and control of network resources. Achieving this is made possible through the segmentation of the control plane and data plane within a network's architectural framework. Amidst SDN's benefits, encompassing flexibility and scalability, emerges a parallel landscape of fresh security threats. Among the looming threats to SDN, DoS attacks prominently stand out. DDoS attacks [22], characterized by their overwhelming flood of traffic, serve to incapacitate network resources and disrupt services. The ramifications of DDoS attacks on an SDN network are profound, resulting in performance deterioration, downtime, and significant financial losses.

In this battle against such assaults, IDS emerge as pivotal guardians [23]. A cornerstone of network security, the IDS is exemplified by SNORT, a renowned open-source IDS. SNORT engages in the surveillance of network traffic, utilizing a blend of packet sniffing and signature-based detection to unearth potential threats and intrusions. Operating as an IDS, SNORT instantaneously scrutinizes network traffic, cross-referencing packet contents against a pre-established database of rules and signatures. These rules outline the behavioral patterns associated with well-known attacks or malicious activities.

Upon discovering a match, SNORT generates alarms or logs, delivering a comprehensive breakdown of the suspected intrusion. Among its capabilities, SNORT employs deep packet inspection, a technique that delves into network protocols and payloads to identify various attack forms. These functionalities collectively safeguard SDN networks against potential threats targeting switches, controllers, and links. In the scope of this study, throughput and latency were gauged using the widely used Iperf tool, both before and after the incorporation of SNORT, as well as before and after a DDoS attack. This section delves into the intricacies of the design and deployment of SNORT within an SDN framework, with the objective of detecting and mitigating DDoS assaults. Illustrated in Figure 2 is a model outlining the topology of a DDoS attack within an SDN network, alongside the application of SNORT IDS. This model encompasses two critical phases: the initiation of the DDoS attack and its subsequent detection via SNORT IDS.

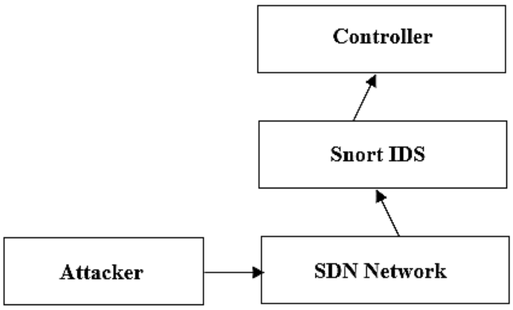

Figure 2. DDoS attack in SDN

The measurement of throughput and latency is facilitated through the utilization of the popular open-source tool, Iperf. This tool effectively assesses the speed and quality of network connections by generating network traffic between a client and server. Among the myriad metrics that Iperf can monitor, throughput, latency, and packet loss are prominent factors that contribute to the evaluation.

4. RESULTS AND DISCUSSION

In this simulation scenario, our focus shifts to executing a DDoS attack within an SDN network [24], alongside the incorporation of the SNORT intrusion detection system. After these actions, we proceed to capture data both pre and post DDoS attack, as well as prior to and after implementing the SNORT IDS.

4.1. Experimental setup

Our experimental setup was hosted on a server equipped with Ubuntu 20.04, powered by an Intel(R) Core (TM) i7-1165G7 CPU @ 2.80 GHz and bolstered by 16 GB RAM. For network topology emulation, we leveraged Mininet 2.3.0, a platform that facilitates the creation of a virtual ecosystem comprising hosts, switches, controllers, and links. The OpenFlow switch implementation was done using OpenvSwitch (OVS). The entire virtual network was orchestrated by OpenDaylight, with the interaction between the switches and the OpenDaylight controller facilitated by the OpenFlow protocol, version 1.3. To mimic the DDoS attack dynamics, we employed the hping3 utility, renowned for dispatching tailored TCP/IP packets. Additionally, for generating throughput and delay essential for attack initiation, we utilized Iperf, a robust packet manipulation tool [25].

4.2. Scenario before DDoS attack

Examining the graph depicted in Figure 3, it becomes apparent that with the progression of time, there exists a fluctuation in the flow rate within the range of 9.3 to 10.5 Mbps. This variation persists until the 12th time unit, at which point the flow rate stabilizes at 9.6 Mbps. Upon further scrutiny, a declining trend in flow rate emerges, evident as the measurement drops to 9.38 Mbps by the 15th time unit. After this point, alterations in throughput become more pronounced, coinciding with the DoS attack.

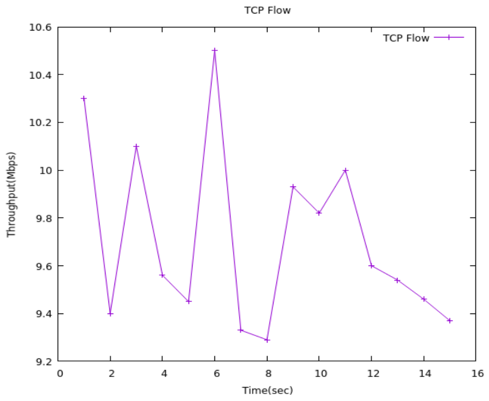

Figure 3. Throughput before the scenario of DDoS attack

4.3. Scenario after the DDoS attack

Referring to the graph displayed in Figure 4, an initial surge is notable, with the flow reaching its pinnacle value of 630 Mbps at time 1. Subsequently, a noticeable reduction follows, accompanied by fluctuations within the range of 8 to 12 Mbps. This pattern leads us to the inference that a decline in throughput becomes evident post the DDoS attack.

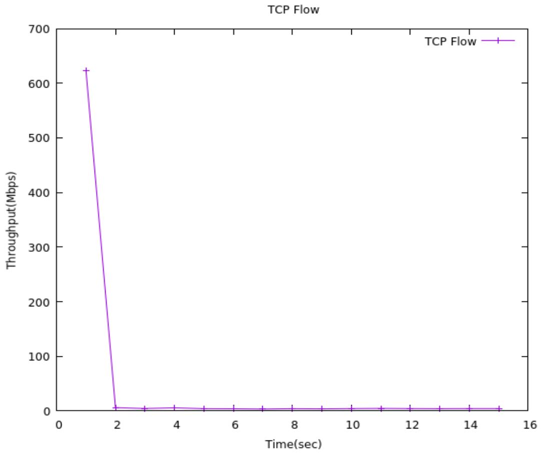

Figure 4. Throughput after the scenario of DDoS attack

4.4. Scenario without integrated intrusion detection systems

Upon scrutinizing the graph illustrated in Figure 5, a tripartite division becomes evident in the absence of an IDS. In the initial segment, a peak value is observed, subsequently undergoing a gradual decline until it reaches zero. The subsequent part maintains a steady value, while the concluding phase showcases an incremental ascent, transforming the curve into an upward trajectory. This discernment leads us to the conclusion that prior to the incorporation of SNORT, the flow rate oscillates between decline, stability, and augmentation.

4.5. Scenario with integrated intrusion detection systems

Based on the data presented in Figure 6, it becomes evident that the utilization of an IDS imparts distinct characteristics to the curve depicted in the Figure 6. Notably, there are segments within the curve that exhibit clear increments, while other portions display marginal decreases. The pinnacle value within this context is recorded during the 9th time unit. In essence, this study thoroughly examined throughput dynamics by simulating DDoS attacks and implementing SNORT IDS. Operating within a strategically structured Mininet-OpenDaylight setup, diverse scenarios were analyzed to illuminate nuanced throughput shifts. Analysis revealed a marked pre-attack throughput curve fluctuation, showcasing the disruptive influence of

DDoS assaults on network performance. However, with the introduction of DDoS attacks countered by SNORT IDS, a distinct transformation emerged. Post-attack, the throughput curve displayed heightened stability, implying the efficacy of defense mechanisms in mitigating detrimental impacts.

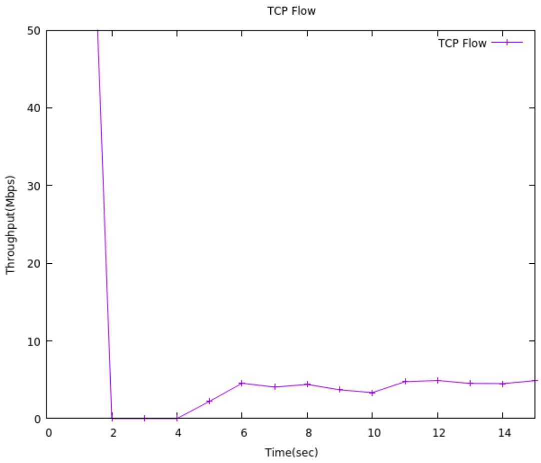

Figure 5. Throughput without IDS

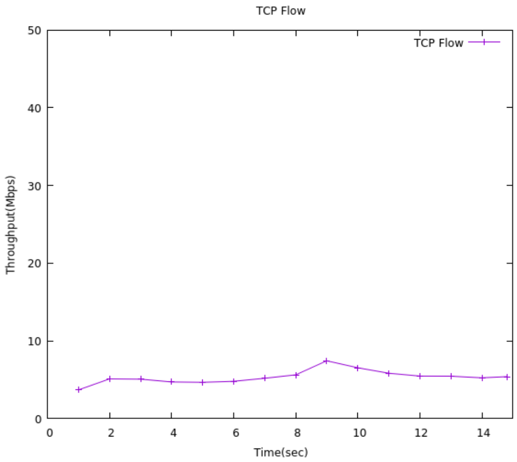

Figure 6. Throughput with IDS

Moreover, the interplay between IDS deployment and throughput variations unveiled a noteworthy insight. The contrast between throughput curves with and without IDS emphasized intrusion detection's discernible influence. Absence of IDS correlated with amplified oscillations, signaling heightened vulnerability. Conversely, IDS deployment fostered controlled conditions, curtailing fluctuations, and enhancing network stability.

5. CONCLUSION

To sum up, this study delved into network throughput dynamics using DDoS attacks and SNORT IDS in a controlled Mininet-OpenDaylight setup. Observations unveiled meaningful insights. Before DDoS attacks, we witnessed disruptive throughput fluctuations. After implementing DDoS attacks and SNORT IDS, curves stabilized, highlighting successful defense mechanisms. Notably, SNORT IDS further minimized variations, emphasizing its efficacy in enhancing network stability. This research underscores the critical role of robust IDS, exemplified by SNORT IDS. Its ability to mitigate DDoS impacts and refine network stability is evident. By understanding the intricate interplay between attacks and defenses, we equip ourselves to fortify networks in the face of evolving cyber threats. These findings offer practical implications for real-world network resilience strategies. Recognizing the attack-defense dynamics, we gain insights into constructing more robust networks. This study provides a valuable lens through which to navigate the complexities of network security, fostering a proactive approach to cybersecurity in an ever-changing digital landscape.

REFERENCES

[1] Y. Li and M. Chen, “Software-defined network function virtualization: A survey,” *IEEE Access*, vol. 3, pp. 2542–2553, 2015, doi: 10.1109/ACCESS.2015.2499271.

[2] M. Chouikik, M. Ouaissa, M. Ouaissa, Z. Boulouard, and M. Kissi, “Impact of DoS attacks in software defined networks,” in *AIP Conference Proceedings*, 2023, vol. 2814, no. 1, doi: 10.1063/5.0148496.

[3] M. Yang, Y. Li, D. Jin, L. Zeng, X. Wu, and A. V. Vasilakos, “Software-defined and virtualized future mobile and wireless networks: A survey,” *Mobile Networks and Applications*, vol. 20, no. 1, pp. 4–18, 2015, doi: 10.1007/s11036-014-0533-8.

[4] D. S. Rana, S. A. Dhondiyal, and S. K. Chamoli, “Software defined networking (SDN) challenges, issues and solution,” *International Journal of Computer Sciences and Engineering*, vol. 7, no. 1, pp. 884–889, 2019, doi: 10.26438/ijcse/v7i1.884889.

[5] Q. Waseem, W. Isni Sofiah Wan Din, A. Aminuddin, M. Hussain Mohammed, and R. F. Alfa Aziza, “Software-defined networking (SDN): A review,” in *ICOIACT 2022 - 5th International Conference on Information and Communications Technology: A New Way to Make AI Useful for Everyone in the New Normal Era, Proceeding*, 2022, pp. 30–35, doi: 10.1109/ICOIACT55506.2022.9972067.

[6] M. Chouikik, M. Ouaissa, M. Ouaissa, Z. Boulouard, and M. Kissi, “Software-defined networking security: A comprehensive review,” *Big Data Analytics and Computational Intelligence for Cybersecurity*, vol. 111, pp. 91–108, 2022, doi: 10.1007/978-3-031-05752-6_6.

[7] R. Ruslan, N. B. Othman, M. F. M. Fuzi, and N. Ghazali, “Scalability analysis in mininet on software defined network using ONOS,” in *ETCCE 2020 - International Conference on Emerging Technology in Computing, Communication and Electronics*, 2020, pp. 1–6, doi: 10.1109/ETCCE51779.2020.9350892.

[8] J. E. Varghese and B. Muniyal, “An efficient IDS framework for DDoS attacks in SDN environment,” *IEEE Access*, vol. 9, pp. 69680–69699, 2021, doi: 10.1109/ACCESS.2021.3078065.

[9] P. Manso, J. Moura, and C. Serrão, “SDN-based intrusion detection system for early detection and mitigation of DDoS attacks,” *Information (Switzerland)*, vol. 10, no. 3, 2019, doi: 10.3390/info10030106.

[10] L. Dridi and M. F. Zhani, “SDN-guard: DoS attacks mitigation in SDN networks,” in *Proceedings - 2016 5th IEEE International Conference on Cloud Networking, CloudNet 2016*, 2016, pp. 212–217, doi: 10.1109/CloudNet.2016.9.

[11] R. Kandoi and M. Antikainen, “Denial-of-service attacks in OpenFlow SDN networks,” in *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, 2015, pp. 1322–1326, doi: 10.1109/INM.2015.7140489.

[12] J. Li, T. Tu, Y. Li, S. Qin, Y. Shi, and Q. Wen, “DoSGuard: Mitigating denial-of-service attacks in software-defined networks,” *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22031061.

[13] Y. Tian, V. Tran, and M. Kuerban, “DoS attack mitigation strategies on SDN controller,” in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*, 2019, pp. 701–707, doi: 10.1109/CCWC.2019.8666456.

[14] M. Rahouti, K. Xiong, Y. Xin, S. K. Jagatheesaperumal, M. Ayyash, and M. Shaheed, “SDN security review: Threat txonomy, implications, and open challenges,” *IEEE Access*, vol. 10, pp. 45820–45854, 2022, doi: 10.1109/ACCESS.2022.3168972.

[15] M. S. Farooq, S. Riaz, and A. Alvi, “Security and privacy issues in software-defined networking (SDN): A systematic literature review,” *Electronics (Switzerland)*, vol. 12, no. 14, 2023, doi: 10.3390/electronics12143077.

[16] 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, 2016.

[17] O. Blial, M. Ben Mamoun, and R. Benaini, “An overview on SDN architectures with multiple controllers,” *Journal of Computer Networks and Communications*, vol. 2016, 2016, doi: 10.1155/2016/9396525.

[18] E. Kaljic, A. Maric, P. Njemcevic, and M. Hadzialic, “A survey on data plane flexibility and programmability in software-defined networking,” *IEEE Access*, vol. 7, pp. 47804–47840, 2019, doi: 10.1109/ACCESS.2019.2910140.

[19] V. Varadharajan, K. Karmakar, U. Tupakula, and M. Hitchens, “A policy-based security architecture for software-defined networks,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 897–912, 2019, doi: 10.1109/TIFS.2018.2868220.

[20] M. B. Jimenez, D. Fernandez, J. E. Rivadeneira, L. Bellido, and A. Cardenas, “A survey of the main security issues and solutions for the SDN architecture,” *IEEE Access*, vol. 9, pp. 122016–122038, 2021, doi: 10.1109/ACCESS.2021.3109564.

[21] H. Wang, L. Xu, and G. Gu, “FloodGuard: A DoS attack prevention extension in software-defined networks,” in *Proceedings of the International Conference on Dependable Systems and Networks*, 2015, vol. 2015-Septe, pp. 239–250, doi: 10.1109/DSN.2015.27.

[22] Z. A. El Houda, L. Khoukhi, and A. S. Hafid, “Bringing intelligence to software defined networks: Mitigating DDoS attacks,” *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2523–2535, 2020, doi: 10.1109/TNSM.2020.3014870.

[23] P. Manso, J. Moura, and C. Serrão, “SDN-based intrusion detection system for early detection and mitigation of DDoS attacks,” *Information (Switzerland)*, vol. 10, no. 3, 2019, doi: 10.3390/info10030106.

[24] S. Scott-Hayward, S. Natarajan, and S. Sezer, “A survey of security in software-defined networks,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 623–654, 2015.

[25] A. Dugar and M. Madiajagan, “Study of SDN using mininet,” *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 7, no. 5, pp. 181–188, 2016.

BIOGRAPHIES OF AUTHORS

Meryem Chouikik received her engineer’s degree in Network and Telecommunications in 2021. She is currently a Ph.D. student at FST Mohammedia, Morocco. Her research interests include network, telecommunications, internet of things, SDN, and communication vehiculaire. She can be contacted at email: meryem.chouikik-etu@etu.univh2c.ma.

Mariyam Ouaissa is currently an Assistant Professor in Networks and Systems at ENSA, Chouaib Doukkali University El Jadida, Morocco. She is a Ph.D. in Computer Science and Networks graduated in 2019, at the Laboratory of Modelisation of Mathematics and Computer Science, from Moulay Ismail University, ENSAM, Meknes, Morocco. Her main research topics are IoT, M2M, WSN, vehicular networks, and cellular networks. She is mainly working on M2M congestion overload problem, security and the resource allocation management. She has published more than 40 research papers. She is an Editor in several books (Springer, De Gruyter, and RGN Publications) and guest editor in several special issues of journals (IGI Global, River Publishers, EAI Publisher, and RGN Publications). She can be contacted at email: mariyam.ouaissa@edu.umi.ac.ma.

Mariya Ouaissa is currently a Professor in Cybersecurity and Networks at Cadi Ayyad University, Marrakech, Morocco, and practitioner with industry and academic experience. She is a Ph.D. graduated in 2019 in Computer Science and Networks, at the Laboratory of Modelisation of Mathematics and Computer Science from ENSAM-Moulay Ismail University, Meknes, Morocco. She has made contributions in the fields of information security and privacy, internet of things security, and wireless and constrained networks security. Her main research topics are IoT, M2M, D2D, WSN, cellular networks, and vehicular networks. She has published over 20 papers (book chapters, international journals, and conferences/workshops), 8 edited books, and 5 special issue as guest editor. She can be contacted at email: m.ouaissa@uca.ac.ma.

Zakaria Boulouard is currently a Professor at Department of Computer Sciences at the "Faculty of Sciences and Techniques Mohammedia, Hassan II University, Casablanca, Morocco". In 2018, he joined the "Advanced Smart Systems" Research Team at the "Computer Sciences Laboratory of Mohammedia". He received his Ph.D. degree in 2018 from "Ibn Zohr University, Morocco" and his Engineering Degree in 2013 from the "National School of Applied Sciences, Khouribga, Morocco". His research interests include artificial intelligence, big data visualization and analytics, optimization, and competitive intelligence. He can be contacted at email: zakaria.boulouard@fstm.ac.ma.

Mohamed Kissi received his Ph.D. degree from the UPMC, France in 2004 in Computer Science. He is currently a Professor in Department of Computer Science, University Hassan II Casablanca, Faculty of Sciences and Technology, Mohammedia, Morocco. His current research interests include machine learning; data and text mining (Arabic). He is the author of many research papers published at conference proceedings and international journals in Arabic text mining, bioinformatics, genetic algorithms, and fuzzy sets and systems. He can be contacted at email: mohamed.kissi@fstm.ac.ma.