Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

A Systematic Review on Software-Defined Networking Data-Plane Security

Achmad Mardiansyah[1,2,*], Naimah Yaakob[1,2], Mohd. Rashidi Che Beson[1,3], Ineke Kusumawati[4], Faisal Reza[5]

[1] Faculty of Electronic Engineering and Technology, Universiti Malaysia Perlis, Pauh Putra Campus, 02600 Arau, Perlis, Malaysia
[2] Centre of Excellence for Advanced Computing (AdvComp), Universiti Malaysia Perlis, Pauh Putra Campus, 02600 Arau, Perlis, Malaysia
[3] Centre of Excellence for Advanced Communication Engineering (ACE), Universiti Malaysia Perlis, Kangar Campus, 01000 Kangar, Perlis, Malaysia
[4] Payment Technology Lead, HSBC Singapore, 238839 Singapore
[5] Chief Technology Officer, PT Cloud Hosting, Kabupaten Sukabumi, Jawa Barat, 43353 Indonesia

ARTICLE INFO

Keywords:
Software-defined-networking; Security; Data-plane

ABSTRACT

As Software-Defined Networking (SDN) continues to redefine computer network, the security of its data plane has emerged as a critical concern. This systematic review delves into the area of Software-Defined Networking (SDN) data-plane security. We categorize and analyse existing research, covering threats, detection methods and mitigation strategies. By applying a comprehensive selection using advanced searching on Scopus and Mendeley database found (n=34), we analyse final primary data to provide insight on SDN data-plane security which consist of security attacks, detection and mitigation methods.

1. Introduction

The state of contemporary networking has experienced a significant shift as a result of the development of Software-Defined Networking (SDN). SDN has brought forth a ground breaking method in network design by separating the conventional function of control plane and data plane. This separation has enabled enhanced agility, flexibility, and programmability. Although SDN holds enormous potential in streamlining network administration and enhancement, it has simultaneously complemented in a set of challenges, especially concerning the security of the data plane.

In an SDN environment, the data plane is responsible to do forwarding and processing network traffic, serving as a vital element that significantly influences network operations. Its role in ensuring network functionality and securing the infrastructure, services, and data cannot be overstated. With the widespread adoption of SDN technology across various industries, it is crucial to thoroughly tackle data-plane security issues. This comprehensive approach is essential to preserve network integrity and confidentiality.

* *Corresponding author.*
E-mail address: amardiansyah@studentmail.unimap.edu.my

https://doi.org/10.37934/araset.60.2.134145

This systematic review has an objective to present a thorough and structured analysis of the current state of knowledge in the realm of SDN data-plane security. By systematically surveying and analysing existing literature, research findings, and developments, this study aims to provide a comprehensive perspective on the diverse aspects of data-plane security in Software-Defined Networking (SDN).

Throughout this review, we will explore various features of SDN data-plane security, encompassing foundational concepts, threat models, and countermeasures. By distilling insights from an extensive body of academic and industrial research, we aim to present a comprehensive perspective on the evolution of SDN data-plane security.

This paper analyses 34 papers, and summarise their contents into Table 1 to Table 6 below, grouped by attack types that are addressed by methodology.

Table 1
Summary of methods to detect/mitigate Denial-of-service attack

Citation number	Method/Remark
[1]	A Detection Method for Denial-of-Service Attacks Utilizing Entropy and Ensemble Learning-Based Scheme. This approach offers the advantage of leveraging computing nodes located at the edge for detection, thereby decreasing the workload on the controller.
[2]	This paper proposes a clustering technique named WOA-DD (Whale Optimization Algorithm-based Clustering) which employing a metaheuristic approach to reroute attack traffic. The key advantage of this method lies in its ability to maintain stable performance even under attack conditions.
[3]	This study introduces the Extreme Gradient Boosting (XGBoost) Algorithm for bandwidth detection and management across multiple profiles. Our proposed approach demonstrates remarkable effectiveness, achieving a detection accuracy of 99.9% for DDoS attacks while maintaining an impressively low false-positive rate.
[4]	This paper introduces a blockchain-based framework called BSD-Guard, positioned between the control plane and data plane, aimed at detecting attacks. The findings demonstrate the effective capability of BSD-Guard in efficiently detecting and blocking attacks, especially in multi-controller scenarios.
[5]	This paper uses neural network fed by flow table parameters to develop classifier.
[6]	This paper use machine learning Deep Factorization Machine (DeepFM) which extracting features from flow rules to build classifier to detect attack.
[7]	This paper proposes a framework named FMDADM that consist of 4 components on detecting and mitigating attack. The components are: ADR (average drop rate) for detection, DCMF (double-check mapping function) for detection in data-plane, a machine-learning module to do classification, and mitigation module.
[8]	This paper proposes FuzzyGuard, an extension to defend dos attack in the data-plane by utilising independent routing flow and fuzzy inference. Attack mitigation is done by probabilistic suppression modes. results show that the method can protect legitimate traffic during attack, with lower resource usage.
[9]	this paper proposes statistical metric known as the Interquartile Range (IQR) as detection. For mitigation handling, this paper uses existing features in SDN.
[10]	Method in this paper utilise statistical approach that is based on entropy data to detect and counter TCP SYN flood Distributed Denial of Service (DDoS) attacks. The algorithm has a three-step detection strategy to minimize incorrect warnings. The findings indicate that this method is both resource-efficient and low rate of false positives
[11]	This paper use algorithm called SDN Secure Control and Data Plane (SECOD) algorithm to mitigate DDoS. The experiment is conducted in IoT networks where the traffic is more predictable. The study reveals that DDoS attacks significantly affect random traffic, UDP, or TCP. Furthermore, the research findings show a 10% probability of controller unresponsiveness and a 40% likelihood of switch non-responsiveness

[12]	This paper uses statistical analysis and entropy from traffic header parameters. The effectiveness of this approach is validated through a comparison with several Machine Learning algorithms.
[13]	This paper shows that a denial-of-service attack can be launched using Slow TCAM (Ternary content-addressable memory) Exhaustion attack (Slow-TCAM), and Slow Saturation attack. Therefore, by monitoring and TCAM, SDN network could setup rules to allow particular host to send a number of packets per second
[14]	Method used in this study is sFlow and a sampling that is based on adjustable polling with Snort as Intrusion Detection System (IDS) and a deep learning model to identify attacks. The findings demonstrated a significantly enhanced detection accuracy.

Table 2
Summary of methods to detect/mitigate Fingerprint/reconnaissance (recon) attack

Citation number	Method/Remark
[15]	This paper uses dynamic scheduling and probabilistic scrambling to obfuscate target. This approach offers significant advantages, notably minimizing adverse effects on performance during attacks. Moreover, it enables the alteration of SDN fingerprint information, preventing attackers from gaining insights into the target.
[16]	This paper uses a detailed access control approach, termed Fine-Grained Access Control Method based on Blockchain Smart Contracts (FACSC), designed specifically for SDN hosts. The method utilizes the programming protocol-independent packet processor (P4) to filter and forward packets. The results demonstrate the effectiveness of this approach in ensuring authentication for SDN network terminals while maintaining minimal authentication processing overhead.
[17]	This paper is a new enhancement to the Moving Target Defense (MTD) technique. The improvement utilizes IP addresses for alignment among nodes in the network path by creating synchronization signatures based on hash chains. One notable advantage of this approach is that it does not introduce extra networking overhead, apart from the initial seed distribution, which can be done offline. The results demonstrate that the cost for attackers to acquire information significantly rises when compared to the previous method.
[18]	This paper use method called SMCDS (SDN-based Moving Target Defense for Control and Data Plane Security), a system capable of concealing the target (controller) during an attack.

Table 3
Summary of methods to detect/mitigate Man-in-the-middle (mitm) attack

Citation number	Method/Remark
[19]	This paper used a combination between classical key distribution and quantum key distribution to ensure confidentiality and authenticity in SDN traffic. The findings demonstrate the efficacy of this hybrid key in strengthening the transport layer security.
[20]	In this paper, Blockchain technology will be implemented in every SDN controller, enabling them to relay condensed topological information to the blockchain via smart contracts. The findings demonstrate the efficacy of this approach in establishing trust among various controllers and ensuring secure routing across diverse domains.

Table 4
Summary of methods to detect/mitigate spoofing/poisoning attack

Citation number	Method/Remark
[21]	This paper uses a platform that is based on pattern analytics to detect and block attacker. Benefit of the platform is customizable pattern analytics.
[22]	In this study, entropy properties of Software-Defined Networking (SDN) links are leveraged to identify link-fabrication attacks. The findings demonstrate the effectiveness of the proposed approach in detecting prevalent topological attacks, offering thorough and holistic security protection for network topology.

[23]	This paper introduces a method to counter ARP spoofing by implementing a validation process within the controller. The findings demonstrate the effectiveness of this approach in thwarting ARP spoofing attacks.
[24]	This paper proposed Security-Aware Programmable (SECAP) Switch, to detect attack.

Table 5
Summary of methods to detect/mitigate routing attack

Citation number	Method/Remark
[25]	This paper use blockchain technology to address routing attacks, by adding previously withheld routing data from the controller to a multichain blockchain. Results demonstrate the performance surpasses the conventional single-controller SDN topology in terms of throughput, bandwidth stability, and jitter.

Table 6
Summary of methods to detect/mitigate combined attack

Citation number	Addressed security issue	Method/Remark
[26]	Main-in-the-middle attack, spoofing attack	This paper adds extra cryptographic authentication on data-plane that is called synchronize secret, to distinguish attack traffic from legitimate traffic. Benefit of this method is low disconnect rate of 0.01%.
[27]	Denial-of-service attack, flooding	This paper employs an enhanced whitelist/blacklist filtering approach to identify attacks. In the experimental phase, the outcomes are compared with those obtained using the Bloom filter. This method enhances accuracy by 2% while utilizing only half of the memory.
[28]	Denial-of-service attack, poisoning attack	This paper presented a novel multi-controller architecture, wherein the controllers operate independently without any east-west connection. One controller function as a typical SDN controller, while the second controller, referred to as the observer node, monitors the network. The detection process comprises two distinct phases: a learning phase and a running phase. The findings indicate the absence of errors in the detection algorithm. Nevertheless, there is an observed increase in reaction time, which subsequently affects the overall system performance.
[29]	Denial-of-service attack, port-scanning attack	Here author used Intrusion Detection and Prevention System (IDPS) as new node in SDN network. The system incorporates two connection-based mechanisms: the Credit-Based Threshold Random Walk (CB-TRW) and Rate Limiting (RL). Furthermore, it employs the Port Bingo (PB) algorithm and Quality of Service (QoS) to proactively thwart potential attacks. The study's findings indicate that it effectively identifies and mitigates port-scanning and Denial of Service (DoS) attacks in real-time, with a minimal occurrence of false positives.
[30]	Denial-of-service, reconnaissance attack	This paper introduces a methodology comprising two fundamental strategies: Self Cleansing Intrusion Tolerance (SCIT) integrated with a Recovery-Based model to guarantee controller availability, and Moving Target Defense (MTD) to proactively counter adaptive adversaries. The findings demonstrate a reduced probability of attacker success in SCIT when compared to static scenarios.
[31]	Denial-of-service attack, port-scan attack	This paper use method that is called LSTM-FUZZY. The method operates through three key phases: profiling, unusual pattern detection, and mitigation. The outcomes demonstrate the system's effectiveness in both detecting and mitigating attacks.

[32]	Denial-of-service attack, port-scan attack	This paper optimises Programming Protocol-Independent Packet Processors (P4) to facilitate a multi-layer edge scenario, exploring three distinct use cases: dynamic traffic engineering (such as traffic offload and optical bypass) and cybersecurity (including distributed denial of service and port scan attacks). the findings showcase the successful deployment of dynamic traffic engineering and cybersecurity protocols on P4 switches, all without the need for controller intervention. Furthermore, our system demonstrates remarkable scalability and latency performance, aligning closely with those observed in contemporary commercial OpenFlow switches.
[33]	Spoofing attack, Denial-of-service attack	This study employs forward flooding rules for attack detection and mitigation. The findings demonstrate that this approach enhances network performance, specifically in terms of packet delivery rates. e
[34]	Denial-of-service attack, mitm attack	This paper uses orchestrated Deep Learning (DL) to detect attack. Result shows the it can achieve accuracy of 99.57% using CICIDS-2028 dataset.

2. Methodology

The systematic review methodology comprises four fundamental phases that were employed to select numerous pertinent papers for this research.

2.1 Identification

In the initial phase, we identified keywords and their associated terms by consulting thesauruses, dictionaries, encyclopaedias, and existing research. Once the relevant keywords were chosen, we created search strings for the Scopus and Mendeley databases, as indicated in Table 7. During this systematic review process, a total of 936 papers were obtained from both databases in this stage of the study.

Table 7
The search string

Database	Keywords
Scopus	TITLE-ABS-KEY ((software AND defined AND networking) OR sdn) AND security AND attack AND (data-plane OR "data plane")
Mendeley	((software AND defined AND networking) OR sdn) AND security AND attack AND (data-plane OR "data plane")

2.2 Screening

During the screening stage, the collection of potentially pertinent research items is checked for content that corresponds to the established research question(s). The selection of research items is based on SDN security in data-plane aspect. Criterion for inclusion on Table 8 are applied on search result which left 108 articles in total.

Table 8
The selection criteria

Criterion	Inclusion	Exclusion
Timeline/years	2019 – 2023	< 2019
Document type	Journal/Article	Non-journal/non-article
Publication stage	Final	In press
Keyword	- Network security - Denial-of-service attack - Data-plane - attack detection	Besides inclusion keywords
Source type	Journal	Non-journal
Language	English	Non-English
Open access	All open access	Non-open access

Keywords are updated automatically as well after applying criterion. After applying filters using provided graphical user interface, database provider updated the keyword accordingly. New updated keyword can be seen on Table 9. After combining both databases, there are 30 articles duplicated which remains 78 articles in total.

Table 9
The search string after applying inclusion

Database	Keywords
Scopus	TITLE-ABS-KEY (((software AND defined AND networking) OR sdn) AND security AND attack AND (data-plane OR "data plane")) AND PUBYEAR > 2018 AND PUBYEAR < 2024 AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (PUBSTAGE , "final")) AND (LIMIT-TO (EXACTKEYWORD , "Network Security") OR LIMIT-TO (EXACTKEYWORD , "Denial-of-service Attack") OR LIMIT-TO (EXACTKEYWORD , "Attack Detection")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (SRCTYPE , "j")) AND (LIMIT-TO (OA , "all"))
Mendeley	((software AND defined AND networking) OR sdn) AND security AND attack AND (data-plane OR "data plane")

2.3 Eligibility

In the eligibility phase, a set of 78 papers was prepared. During this stage, thorough checking was applied to all article titles and abstracts to ensure they aligned with the required criteria for inclusion and supported the current study's objectives. Consequently, 43 papers were disqualified due to their titles lacking significant relevance to the study's goals or their abstracts not corresponding (1 paper). As of the current writing, 34 articles remain eligible for review.

Figure 1 shows stages of systematic literature review, started from identification stage to collect articles based on our intention where we apply basic keywords on databases, followed by screening phase where we apply inclusion filter based on Table 8 criterion on both query result. We then combine results from both database into single list to identify and remove duplicated records. In eligibility stage, we check title and abstract of each article and exclude them if they are not relevant to our scope. Finally, we have a refined list articles to review.

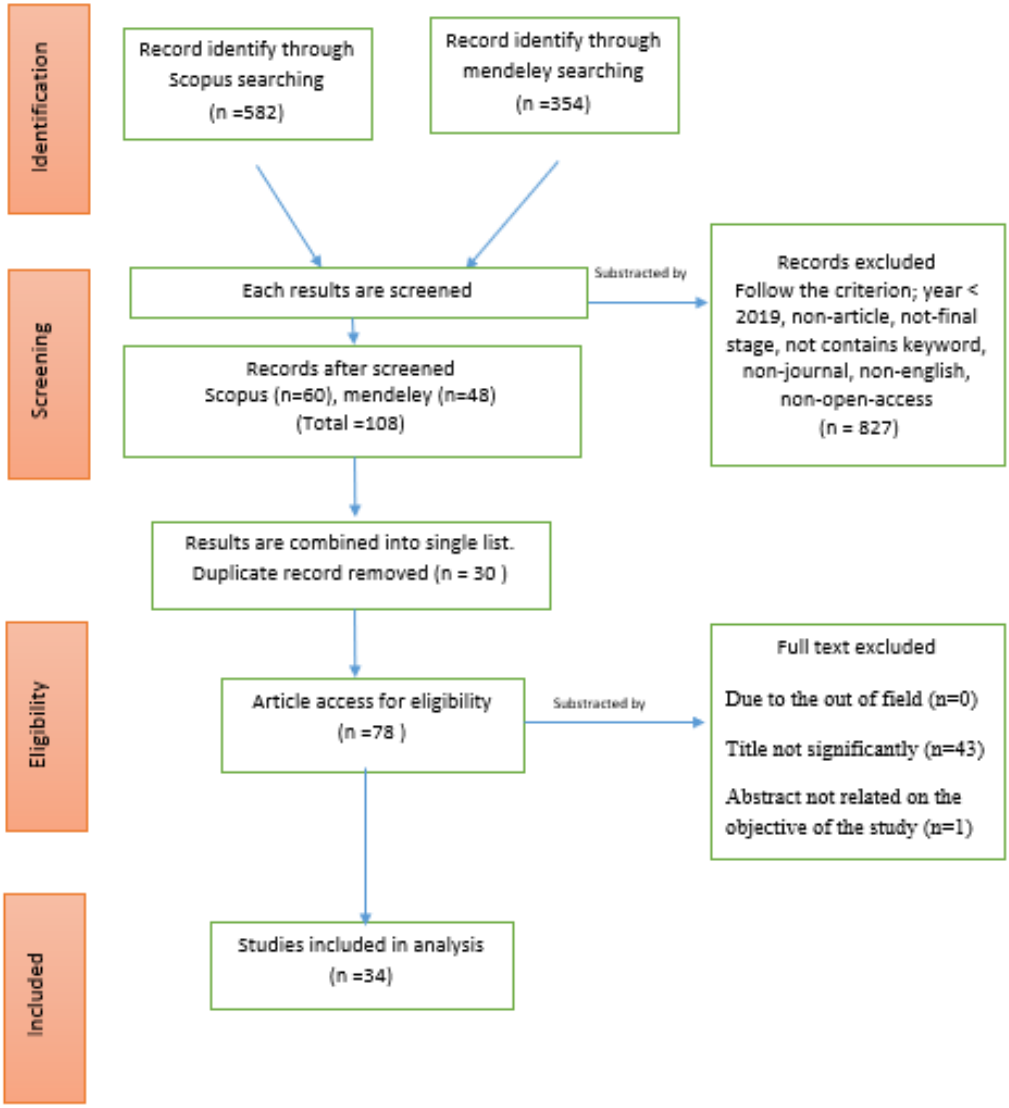

Fig. 1. Flow diagram of the proposed searching study

3. Results and Finding

Thirty-four (34) articles were extracted and analysed after search technique. In this review, we classify method in each article into categories based on which attack type the method can mitigate. All papers were classified into 6 categories based on attack type:

i. Denial-of-service (DOS) attack
ii. Fingerprint/reconnaissance (recon) attack
iii. Man-in-the-middle (mitm) attack
iv. Spoofing/poisoning attack
v. Routing attack
vi. Combined attack

Method in this category is designed to address multiple attack type. Taxonomy diagram of methodology can be seen in Figure 2.

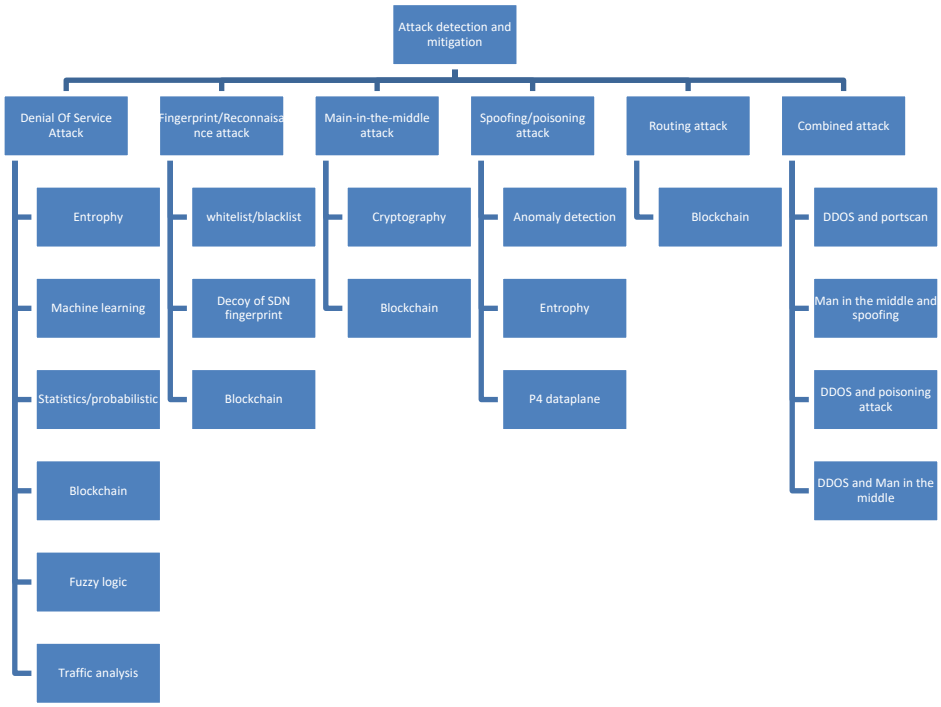

Fig. 2. Taxonomy diagram of methodology

3.1 Denial-of-Service Attack

Denial-of-service issue is a popular topic in this review by 14 papers out of 34. Denial-of-service is a major issue in SDN due to natural design of SDN where controller is the central node/decision of the whole network which consequently can bring a single-point-of-failure of the system.

Here we classify some methods that are commonly used for detect/mitigate:

i. Machine learning or AI: This method applies machine learning algorithm such as decision tree, KNN, VSN, XGboost. Training phase is needed to generate model, where the data is split into 20-80 to generate model. The model then will be applied on running controller to classify traffic whether its legitimate traffic or DOS [2,3,5-7,14].
ii. Statistics/probabilistic: These methods collect data from flow, and then develop statistical grouping such as inter-quartile-range to classify traffic [9,10].
iii. Entropy: This method uses entropy concept in information theory combined with traffic parameter such as source/destination IP address, transport protocol (TCP or UDP), transport layer source/destination port, or other layer 3 protocol such as ICMP, which result in an entropy value. The entropy value is monitored to determine if an attack happen or not [1,5,10,12].
iv. Blockchain: This approach introduces an extra blockchain layer positioned between the data plane and the control plane. This blockchain layer is employed for traffic analysis purposes [4].
v. Fuzzy logic: This approach uses fuzzy logic to dynamically adjust security parameters based on network conditions and threat severity, which give flexibility and adaptive mechanism [8].
vi. Traffic analysis: This approach uses monitoring on traffic, SDN flow table, and resources (such as bandwidth usage) to detect and mitigate attack [11,13,14].

Methods for detecting denial-of-service attack are summarized in Table 1.

3.2 Fingerprint/Reconnaissance (Recon) Attack

A reconnaissance attacker will gather information about their target as much as possible. Information such as IP address, mac address, used DNS server, gateway, DHCP server, protocol used, are some examples. Some methods used to mitigate this are:

i. Whitelist/blacklist: This approach only allows legitimate user to access the network [16].
ii. Decoy of SDN fingerprint: This approach uses dynamic update of SDN fingerprint information to avoid attack, such as IP address, network type, controller type [15,17,18].
iii. Blockchain: This approach uses blockchain access list mechanism to allows only legitimate user [16].

Methods for detecting Fingerprint/reconnaissance attack are summarized in Table 2.

3.3 Man-in-the-Middle (MITM) Attack

Man-in-the-middle attacker sits between communicating nodes and able to collect the traffic which can lead to confidentiality issue. Some methods for mitigation:

i. Cryptography: This approach apply encryption during communication, so that only authenticated user with key can understand the content [19].
ii. Blockchain: This approach applies blockchain method in SDN environment, using smart-contract to build trust among network elements [20].

Methods for detecting Man-in-the-middle attack are summarized in Table 3.

3.4 Spoofing/Poisoning Attack

In Poisoning/Spoofing attack, attacker actively hijack a communication or sent malicious packet to the target. For example, in ARP poisoning, attacker intercepts ARP process and as a result, traffic will go to the attacker. some methods to mitigate:

i. Anomaly detection: This approach deploys anomaly detection to detect malicious activity from attacker [21,23].
ii. Entrophy: This approach uses entropy parameter to enhance detection capability [22].
iii. P4 dataplane: This approach needs P4 supported SDN switch which is capable to be programmed to detect attack [22,24].

Methods for detecting Spoofing/poisoning attack are summarized in Table 4.

3.5 Routing Attack

Routing is a layer 3 (network layer) process where a packet needs to be forwarded to different subnet. Attack on routing can change how packets are routed on the SDN by manipulating routing control information. Some methods for mitigation:

i. Blockchain: This approach uses blockchain in SDN communication. To enhance network security against routing attacks, the SDN network's critical data, encompassing routing details like IP and MAC addresses, is securely stored on a blockchain platform, employing a technology known as multichain [25].

Methods for detecting routing attack are summarized in Table 5.

3.6 Combined Attack

Some articles offer methods to detect and mitigate multiple type of attacks, such as ability to detect Denial-of-service attack and port-scan (reconnaissance) attack. These methods require more tools to do detection, hence bring more complexity to the system. For example, using statistical analytics to detect DOS attack and IDPS (intrusion detection and prevention system) to detect attack like port-scanning.

Methods for detecting combined attack are summarized in Table 6.

4. Conclusions

Security issues on data-plane aspect is still dominated by detection/mitigation of denial-of-service attack where machine learning, AI, and statistical methods are popular choice for detection due to its capability to adapt and learn new pattern. The use of additional node such as Intrusion detection system (IDS) integration can bring more capability to detect/mitigate multiple attacks. The use of cryptographic methods such as blockchains and asymmetric encryption can enhance security in terms of confidentiality.

Acknowledgement

This research is supported by the Ministry of Higher Education through Fundamental Research Grant Scheme (FRGS/1/ 2020/ICT11/UNIMAP/02/1).

References

[1] Yu, Shanshan, Jicheng Zhang, Ju Liu, Xiaoqing Zhang, Yafeng Li, and Tianfeng Xu. "A cooperative DDoS attack detection scheme based on entropy and ensemble learning in SDN." *EURASIP Journal on Wireless Communications and Networking* 2021, no. 1 (2021): 90. https://doi.org/10.1186/s13638-021-01957-9

[2] Shakil, Muhammad, Alaelddin Fuad Yousif Mohammed, Rajakumar Arul, Ali Kashif Bashir, and Jun Kyun Choi. "A novel dynamic framework to detect DDoS in SDN using metaheuristic clustering." *Transactions on Emerging Telecommunications Technologies* 33, no. 3 (2022): e3622. https://doi.org/10.1002/ett.3622

[3] Alamri, Hassan A., and Vijey Thayananthan. "Bandwidth control mechanism and extreme gradient boosting algorithm for protecting software-defined networks against DDoS attacks." *IEEE Access* 8 (2020): 194269-194288. https://doi.org/10.1109/ACCESS.2020.3033942

[4] Jiang, Shanqing, Lin Yang, Xianming Gao, Yuyang Zhou, Tao Feng, Yanbo Song, Kexian Liu, and Guang Cheng. "BSD-Guard: A Collaborative Blockchain-Based Approach for Detection and Mitigation of SDN-Targeted DDoS Attacks." *Security and communication networks* 2022, no. 1 (2022): 1608689. https://doi.org/10.1155/2022/1608689

[5] Yue, Meng, Huaiyuan Wang, Liang Liu, and Zhijun Wu. "Detecting DoS attacks based on multi-features in SDN." *IEEE Access* 8 (2020): 104688-104700. https://doi.org/10.1109/ACCESS.2020.2999668

[6] Wang, Jing, Xiangyu Lei, Qisheng Jiang, Osama Alfarraj, Amr Tolba, and Gwang-jun Kim. "DoS Attack Detection Based on Deep Factorization Machine in SDN." *Comput. Syst. Sci. Eng.* 45, no. 2 (2023): 1727-1742. https://doi.org/10.32604/csse.2023.030183

[7] Khedr, Walid I., Ameer E. Gouda, and Ehab R. Mohamed. "FMDADM: A multi-layer DDoS attack detection and mitigation framework using machine learning for stateful SDN-based IoT networks." *IEEE Access* 11 (2023): 28934-28954. https://doi.org/10.1109/ACCESS.2023.3260256

[8] Huang, Meigen, and Bin Yu. "FuzzyGuard: A DDoS attack prevention extension in software-defined wireless sensor networks." *KSII Transactions on Internet and Information Systems (TIIS)* 13, no. 7 (2019): 3671-3689. https://doi.org/10.3837/tiis.2019.07.019
[9] Swami, Rochak, Mayank Dave, and Virender Ranga. "IQR-based approach for DDoS detection and mitigation in SDN." *Defence Technology* 25 (2023): 76-87. https://doi.org/10.1016/j.dt.2022.10.006
[10] Batool, Sehrish, Farrukh Zeeshan Khan, Syed Qaiser Ali Shah, Muneer Ahmed, Roobaea Alroobaea, Abdullah M. Baqasah, Ihsan Ali, and Muhammad Ahsan Raza. "[Retracted] Lightweight Statistical Approach towards TCP SYN Flood DDoS Attack Detection and Mitigation in SDN Environment." *Security and Communication Networks* 2022, no. 1 (2022): 2593672. https://doi.org/10.1155/2022/2593672
[11] Wang, Song, Karina Gomez, Kandeepan Sithamparanathan, Muhammad Rizwan Asghar, Giovanni Russello, and Paul Zanna. "Mitigating ddos attacks in sdn-based iot networks leveraging secure control and data plane algorithm." *Applied Sciences* 11, no. 3 (2021): 929. https://doi.org/10.3390/app11030929
[12] Linhares, Tiago, Ahmed Patel, Ana Luiza Barros, and Marcial Fernandez. "SDNTruth: innovative DDoS detection scheme for software-defined networks (SDN)." *Journal of Network and Systems Management* 31, no. 3 (2023): 55. https://doi.org/10.1007/s10922-023-09741-4
[13] Pascoal, Tulio A., Iguatemi E. Fonseca, and Vivek Nigam. "Slow denial-of-service attacks on software defined networks." *Computer Networks* 173 (2020): 107223. https://doi.org/10.1016/j.comnet.2020.107223
[14] Ujjan, Raja Majid Ali, Zeeshan Pervez, Keshav Dahal, Ali Kashif Bashir, Rao Mumtaz, and Jonathan González. "Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN." *Future Generation Computer Systems* 111 (2020): 763-779. https://doi.org/10.1016/j.future.2019.10.015
[15] Wang, Tao, and Hongchang Chen. "A lightweight SDN fingerprint attack defense mechanism based on probabilistic scrambling and controller dynamic scheduling strategies." *Security and Communication Networks* 2021, no. 1 (2021): 6688489. https://doi.org/10.1155/2021/6688489
[16] Jiang, Bingcheng, Qian He, Mingliu He, Zhongyi Zhai, and Baokang Zhao. "FACSC: Fine-Grained Access Control Based on Smart Contract for Terminals in Software-Defined Network." *Security and Communication Networks* 2023, no. 1 (2023): 6013270. https://doi.org/10.1155/2023/6013270
[17] Chang, Sang-Yoon, Younghee Park, and Bhavana Babu Ashok Babu. "Fast IP hopping randomization to secure hop-by-hop access in SDN." *IEEE Transactions on Network and Service Management* 16, no. 1 (2018): 308-320. https://doi.org/10.1109/TNSM.2018.2889842
[18] Hyder, Muhammad Faraz, and Muhammad Ali Ismail. "Securing control and data planes from reconnaissance attacks using distributed shadow controllers, reactive and proactive approaches." *IEEE Access* 9 (2021): 21881-21894. https://doi.org/10.1109/ACCESS.2021.3055577
[19] Mahdi, Suadad S., and Alharith A. Abdullah. "Enhanced security of software-defined network and network slice through hybrid quantum key distribution protocol." *Infocommunications journal* 14, no. 3 (2022): 9-15. https://doi.org/10.36244/ICJ.2022.3.2
[20] Zeng, Zhihao, Xiaoning Zhang, and Zixiang Xia. "Intelligent blockchain-based secure routing for multidomain SDN-enabled IoT networks." *Wireless Communications and Mobile Computing* 2022, no. 1 (2022): 5693962. https://doi.org/10.1155/2022/5693962
[21] Buzura, Sorin, Mihaiela Lehene, Bogdan Iancu, and Vasile Dadarlat. "An extendable software architecture for mitigating ARP spoofing-based attacks in SDN data plane layer." *Electronics* 11, no. 13 (2022): 1965. https://doi.org/10.3390/electronics11131965
[22] Gao, Yang, and Mingdi Xu. "Defense against software-defined network topology poisoning attacks." *Tsinghua Science and Technology* 28, no. 1 (2022): 39-46. https://doi.org/10.26599/TST.2021.9010077
[23] Khalid, Harman Yi, Parishan M. Ismael, And Ahmad Baheej Al-Khalil. "Efficient mechanism for securing software defined network against ARP spoofing attack." *Journal of Duhok University* 22, no. 1 (2019): 124-131. https://doi.org/10.26682/sjuod.2019.22.1.14
[24] Smyth, Dylan, Sandra Scott-Hayward, Victor Cionca, Sean McSweeney, and Donna O'Shea. "SECAP switch—Defeating topology poisoning attacks using P4 data planes." *Journal of Network and Systems Management* 31, no. 1 (2023): 28. https://doi.org/10.1007/s10922-022-09714-z
[25] Singh, Surjit, Vivek Mehla, and Srete Nikolovski. "LSSDNF: a lightweight secure software defined network framework for future internet in 5G–6G." *Future Internet* 14, no. 12 (2022): 369. https://doi.org/10.3390/fi14120369
[26] Yao, Jiaying, Zhigeng Han, Muhammad Sohail, and Liangmin Wang. "A robust security architecture for SDN-based 5G networks." *Future Internet* 11, no. 4 (2019): 85. https://doi.org/10.3390/fi11040085
[27] Yang, Chun-Hao, Jhen-Ping Wu, Fang-Yi Lee, Ting-Yu Lin, and Meng-Hsun Tsai. "Detection and Mitigation of SYN Flooding Attacks through SYN/ACK Packets and Black/White Lists." *Sensors* 23, no. 8 (2023): 3817. https://doi.org/10.3390/s23083817

[28] Desgeorges, Loïc, Jean-Philippe Georges, and Thierry Divoux. "Implementation of a SDN Architecture Observer: Detection of Failure, Distributed Denial-of-Service and Unauthorized Intrusion." *Security and Communication Networks* 2023, no. 1 (2023): 7244541. https://doi.org/10.1155/2023/7244541

[29] Birkinshaw, Celyn, Elpida Rouka, and Vassilios G. Vassilakis. "Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks." *Journal of Network and Computer Applications* 136 (2019): 71-85. https://doi.org/10.1016/j.jnca.2019.03.005

[30] Sanoussi, Nouhad, Kaouthar Chetioui, Ghizlane Orhanou, and Said El Hajji. "ITC: Intrusion tolerant controller for multicontroller SDN architecture." *Computers & Security* 132 (2023): 103351. https://doi.org/10.1016/j.cose.2023.103351

[31] Novaes, Matheus P., Luiz F. Carvalho, Jaime Lloret, and Mario Lemes Proença. "Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment." *IEEE Access* 8 (2020): 83765-83781. https://doi.org/10.1109/ACCESS.2020.2992044

[32] Paolucci, Francesco, Federico Civerchia, Andrea Sgambelluri, Alessio Giorgetti, Filippo Cugini, and Piero Castoldi. "P4 edge node enabling stateful traffic engineering and cyber security." *Journal of Optical Communications and Networking* 11, no. 1 (2019): A84-A95. https://doi.org/10.1364/JOCN.11.000A84

[33] Jamil, Faisal, Harun Jamil, and Abid Ali. "Spoofing attack mitigation in address resolution protocol (ARP) and DDoS in software-defined networking." (2022). https://doi.org/10.26735/VBVS3993

[34] Javeed, Danish, Muhammad Shahid Saeed, Ijaz Ahmad, Prabhat Kumar, Alireza Jolfaei, and Muhammad Tahir. "An intelligent intrusion detection system for smart consumer electronics network." *IEEE Transactions on Consumer Electronics* 69, no. 4 (2023): 906-913. https://doi.org/10.1109/TCE.2023.3277856

Name of Author	Email
Achmad Mardiansyah	amardiansyah@studentmail.unimap.edu.my
Naimah Yaakob	naimahyaakob@unimap.edu.my
Mohd. Rashidi Che Beson	rashidibeson@unimap.edu.my
Ineke Kusumawati	ineke.kusumawati@gmail.com
Faisal Reza	reza@idcloudhost.com