Available at https://www.iasj.net/iasj
Iraqi Academic Scientific Journals
Journal homepage:
https://journals.uokerbala.edu.iq/index.php/UOKJ

Research Article

Towards Secure SDN: Survey of Machine Learning Approaches for Attack Detection and Mitigation

[1,]Wasan Mueti Hadi [2,] Manar Hamza [3,] Zahraa K. Al-Sendi
[1,3]Department of Computer Science, College of Computer Science and Information Technology, University of Kerbala, Iraq.
[2]Department of Information Technology, College of Computer Science and Information Technology, University of Kerbala, Kerbala, Iraq.

Article Info
Article history:
Received 6 -8-2025
Received in revised form 19-8-2025
Accepted 27-8-2025
Available online 30 -9 -2025
Keywords:
Software-defined networking (SDN) , Machine learning , Attack Detection, DDoS Mitigation, and Network Security.

Abstract:

Software-Defined Networking (SDN) has evolved as a revolutionary framework in contemporary network infrastructures, providing centralized control, programmability, scalability, and dynamic configuration. Nevertheless, its logically centralized architecture also presents vulnerabilities that adversaries may exploit, resulting in significant security dangers. Traditional security techniques frequently inadequately meet the intricate and dynamic threat landscape of SDN systems. This paper offers an extensive analysis of machine learning (ML) techniques for threat identification and mitigation in Software-Defined Networking (SDN). It connects theoretical advancements with practical applications, emphasizing how machine learning may function as a versatile and intelligent instrument to enhance software-defined networking security. The review commences by classifying principal attack vectors aimed at SDN components, encompassing the control plane, data plane, and communication channels. It subsequently analyzes supervised, unsupervised, and deep learning techniques utilized to identify and alleviate threats including Distributed Denial of Service (DDoS), spoofing, poisoning, and rule manipulation. The discussion also encompasses benchmark datasets and evaluation measures frequently employed in the literature.

Results indicate that machine learning substantially improves detection precision, flexibility, and scalability. Supervised learning is efficacious when labeled data are accessible, whereas unsupervised learning is beneficial for detecting novel or zero-day risks.Deep learning, specifically, attains exceptional efficacy in intricate assault situations. Nonetheless, significant hurdles persist, such as the scarcity of high-quality information, substantial computational demands, and the necessity for real-time adaptation. Future research must concentrate on hybrid models, collaborative detection, and the creation of realistic SDN-specific datasets to facilitate effective, scalable, and resilient security solutions.

Corresponding Author E-mail: wasan.m@uokerbala.edu.iq, manar.h@uokerbala.edu.iq, zahraa.k@uokerbala.edu.iq
Peer review under responsibility of Iraqi Academic Scientific Journal and University of Kerbala.

1-Introduction

Centralized management and programmability of network resources are provided under SDN operations by separating the control plane from the data plane along the service interface. This architecture also enables flexibility and scalability but introduces vulnerabilities, making attackers look for opportunities in the SDN environment with Distributed Denial of Service (DDoS), packet injection, and spoofing as some of the potential traditional attacks on the SDN establishment [1]. SDN transformed conventional networking by providing dynamic reconfiguration and scalability. However, the mitigation of DDoS attacks still remains a great challenge for conventional as well as SDN frameworks [2].

Various SDN controllers have been evolving, having their characteristics and identifiers. Some popular controllers are POX, NOX, OpenDaylight, Floodlight, ONOS, Ryu, and Hyperflow. These controllers play an important role in managing and coordinating the SDN environment [3].

The Research Nokia's Threat Intelligence Report of 2023 reveals that DDoS attacks from unprotected IoT devices have grown fivefold between 2022 and 2023 which causes network service interruptions. The number of IoT devices which contribute to DDoS attacks rose from 200,000 in the previous year to 1 million resulting in more than 40% of all DDoS traffic [4].

Machine learning (ML) methods applied to Software Defined Networking (SDN) systems have emerged as a practical solution to enhance security through detection and minimization of Distributed Denial of Service (DDoS) attacks. The SDN architecture which centralizes control functions makes it easier for attackers to launch DDoS attacks. The flexible approach of machine learning enables real-time detection and response to new threats which addresses these challenges. The paper evaluates various machine learning approaches for protecting Software-Defined Networking infrastructure against DDoS attacks.

The Identification Retrieval technique serves as the basis for a new DDoS detection system which detects attacks that cause resource depletion. This system utilizes network traffic features and the KSVD approach to learn a dictionary of network traffic parameters, with 89% detection accuracy [5].

The drawbacks of the majority of existing DDoS detection methods, both statistical and machine learning-based, have been taken into account. Statistical methods rely on historical network flow statistics that may not reflect the current network traffic due to the dynamic nature of malicious network flows. These techniques have a strong dependence on user-defined thresholds that must be dynamic in order to adapt to network changes. Statistical methods like entropy and correlation are computer resource-intensive, rendering them impractical for real-time detection [3]. Machine learning algorithms work efficiently with limited data and identify the statistical characteristics of attacks prior to classification or analysis. Nevertheless, they need regular model updates to keep up with evolving attack patterns, and some methods take extremely long durations for testing [6]. Machine Learning (ML) is one of the areas of specialization in Artificial Intelligence (AI) with a specific definition.

A variety of robust machine learning methods have developed and are used on a daily basis in data mining. The system has the ability to infer useful models and structural patterns from the training set with these methods.

The two principal phases of a machine learning approach are the 1) training phase and 2) decision phase. During the machine learning training phase, employed methodologies utilize training data to get insights into the target system model. Utilizing a trained model, the system may produce an estimated output for each new input in the second step. Machine learning methodologies are generally classified based on

their learning paradigms, which include: supervised learning and unsupervised learning [7].

Machine learning and deep learning have proven to be superior alternatives to statistical or policy-based methods for detecting DDoS attacks [8].

Many machine learning-based security approaches for software-defined networking have been developed, including convolutional neural networks (CNN), support vector machines (SVM), and k-nearest neighbors (KNN). Among these machine learning techniques, convolutional neural networks (CNN) and support vector machines (SVM) were identified as more effective and cutting-edge in safeguarding software-defined networks (SDN) [9].

2.1- SDN Architecture

In a conventional network, the router functions as both the control and data plane. In the control plane, the router routinely refreshes the routing table and obtains the network status. In the data plane, the device directs incoming packets to their designated destination according to the routing table information. A conventional traditional network architecture is illustrated in Fig. 1 [10].

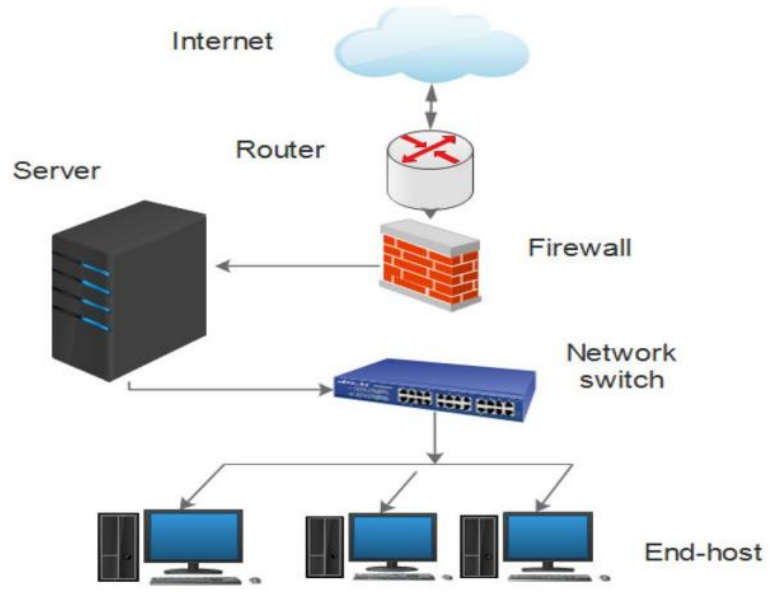

Fig 1: Traditional Network Architecture

Whereas, the figure 2 illustrates the three layers of an SDN: Data plane, Control plane and the Application programmable Interfaces (APIs)facilitating interaction among them [11,12].

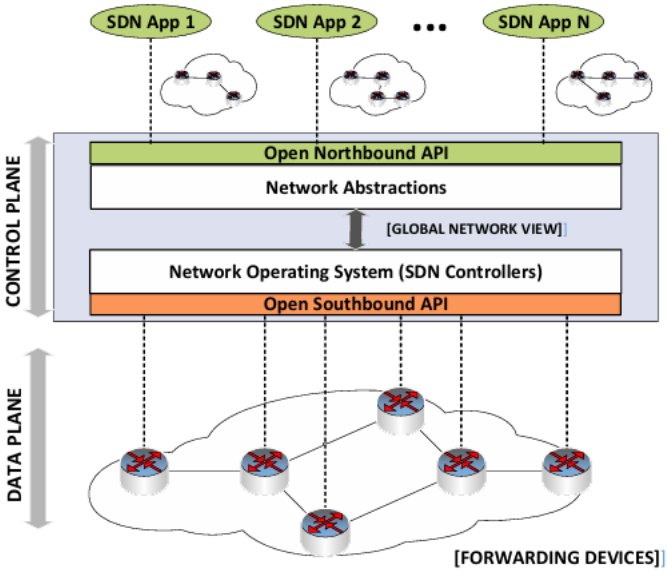

Fig 2: SDN Architecture

1-Data Plane: The data plane is the foundational layer of network devices such as routers, physical and virtual switches, and access points. These devices are accessible and controlled by SDN controller(s) [13].

2-Control Plane: The control plane is the most intelligent and critical component of an SDN system. It comprises one or many controllers that transmit various rules and policies to the data layer via the application plane [14].

3-Application Plane: This plane is the highest in SDN. The primary responsibility of this role is the management of software-related business and security applications [7].

2.2- SDN Security

The security concerns surrounding SDN encompass the open programmable API, wherein the API's open nature renders vulnerabilities more apparent to attackers. Unauthorized access to the central controller may result in significant harm to the information and the injection of malicious code into the system. SDN encounters several assaults, including application layer attacks, control layer attacks, and infrastructure layer attacks [15]. The fundamental attributes of a secure communications network include secrecy, integrity, information availability, authentication, and non-repudiation. To establish a network safeguarded from malicious attacks or inadvertent harm, security

professionals must protect the data [16]. The feature pertains to Dynamic Flow Control, which purportedly enhances security in two distinct manners: 1) by mandating the operation of security middleboxes as a synthesis of various flow control rules disseminated across the network infrastructure; and 2) through network applications either deployed atop the controller or linked to the controller via a northbound interface, thereby eliminating the necessity for supplementary hardware appliances that can be efficiently substituted by integrating security rules into standard network devices primarily designed for packet forwarding [17].

2.3- SDN Attacks

The advancement of networks generates novel attack vectors and both identifiable and obscure risks that can be exploited at any moment. Currently, identifying the vulnerabilities of SDN networks is challenging due to the absence of historical data regarding attack logs on this network. A classification of potential attacks can be established to serve as a reference and to provide a foundation for security. [18].

- **Spoofing attack**: Occurs when a nefarious entity falsifies or counterfeits data to deceive network devices or the SDN controller. For example, the assailant may gain access to the entire network merely by mimicking the controller's IP address [7].
- **Man-in-the-middle attack**: In the event of a Man-In-The-Middle (MITM) attack within Software-Defined Networking (SDN) environments, the potential for harm escalates the vulnerabilities of network components, as a nefarious actor can intercept all traffic between the data layer and the control layer through both northbound and southbound interfaces. Consequently, a malicious user can not only capture information but also alter such information originating from the system or context [19].
- **Distributed Denial of Service Attacks**: Software-Defined Networking (SDN) may itself be susceptible to Distributed Denial of Service (DDoS) attacks. Given that SDN is divided into three primary functional layers—infrastructure layer, control layer, and application layer—there exists the potential for malicious DDoS attacks to target these three layers of SDN's design. DDoS attacks on SDN can be categorized into three types based on potential targets: application layer DDoS attacks, control layer DDoS attacks, and infrastructure layer DDoS attacks [20].
- **Worm Infection/Scanning**: Scanning is a primary technique for preliminary intelligence collection employed by attackers to collect information about a specific target network, as well as by worms to identify susceptible targets for infection dissemination. An attacker can ascertain the quantity, kind, and address of hosts within a network through scanning, as well as the services provided on specific ports. This information is essential for executing more intricate attacks. Consequently, the ability to identify and counteract scanning is critically crucial for any network [21].
- **Fingerprint Attack**: An attacker can employ two modes while fingerprinting a remote host. One mode is the "Normal" mode, when the attacker interacts with the target host in a conventional manner. In "Normal" mode, the attacker can get restricted knowledge about the target host while remaining difficult for the defense to identify, as the attacker interacts with the target host as a legitimate user. Conversely, the other mode is the "Suspicious" model. In this scenario, the assailant transmits dubious probes to the target host, thereby acquiring extensive information regarding the target operating system. Nonetheless, the "Suspicious" mode is significantly more prone to detection by the defender, as it is one of the established attack patterns [22].

2.4-Machine learning (ML)

Machine learning constitutes a subset of artificial intelligence. It can autonomously identify data patterns. ML-based models learn autonomously and empirically, eliminating the necessity for explicit programming. The learning model acquires knowledge from samples, while explicit programming adheres to established rules or a constrained hypothesis. Machine learning is typically divided into three main categories: Supervised learning, Unsupervised Learning, and Semi - Supervised Learning. Machine learning enhances efficiency and reliability while decreasing costs in computational operations. Furthermore, it can swiftly and precisely produce models via data analysis. Machine learning offers technologies capable of processing vast quantities of data, exceeding human comprehension [23].

1-Supervised learning: Supervised machine learning techniques require external support. The input dataset is partitioned into training and testing datasets. The train dataset contains an output variable that requires prediction or classification. All algorithms identify patterns from the training dataset and utilize them for prediction or classification on the test dataset [24] Prominent supervised machine learning methodologies encompass Naive Bayes, Decision Trees, Nearest Neighbor, Support Vector Machines (SVM), Random Forest, Linear Regression, and Neural Networks [7].

2-Unsupervised Learning: The unsupervised learning algorithms extract limited features from the data. Upon the introduction of fresh data, it employs the previously acquired features to identify the class of the data. It is mostly utilized for clustering and dimensionality reduction [24]. Algorithms are employed to execute both clustering and association rule learning. Notable algorithms employed for implementing association rules include the a priori approach, the ECLAT algorithm, and the frequent pattern growth (FP) algorithm. Algorithms such as k-means clustering and principal component analysis (PCA) facilitate clustering [25].

3-Semi-Supervised Learning: Semi-supervised learning algorithms are techniques that integrate the strengths of both supervised and unsupervised learning. It can be advantageous in the domains of machine learning and data mining where unlabeled data is readily available, yet acquiring labeled data is a laborious endeavor. Some of Semi - Supervised Learning are: Generative Models, Self-Training and Transudative SVM [26].

3- Related Work

Sahoo et al. [27], suggested a machine learning approach, specifically the support vector machine (SVM), was presented for DDoS detection with a framework that detects OpenFlow (OF) changes at predefined time intervals.

During these periods, the controller transmits flow_stat_request to each switch within the network. The controller receives the flow statistics, which are subsequently transmitted to the statistics monitor module to extract the aforementioned features. Following feature selection, the proposed machine learning classifier categorizes traffic as either normal or malicious. A distinct module for DDoS mitigation is incorporated into the controller. Upon DDoS detection, the mitigation module promptly establishes a flow rule that discards any packets originating from the underlying switch. This rule restricts traffic to a designated IP destination address using a specific IP protocol. The remaining flows connect within the network conventionally. Aslam et al. [28] suggested their framework for the recognition of DDoS attacks, analyzing network traffic characteristics using machine learning methods in the adaptive multilayer feed-forward manner. These classifiers in the first layer of an adaptive multilayer feed-forward framework build an

SVM, Naive Bayes, Random Forest, K-nearest Neighbor Classifier, and Logistic Regression model for the detection of DDoS attacks using environment-specific training and testing datasets. The classifiers' results in the first layer are Angles by the Ensemble Voting algorithm. The adaptive framework performs the evaluation of real-time network traffic for DDoS detection in the third layer. The architecture uses a remote SDN controller to mitigate the identified DDoS attacks on OpenFlow switches and reallocate network resources to legitimate network hosts. The experimental results show that the performance of the novel framework dominates state-of-the-art methods in terms of accuracy in detecting DDoS attacks. Lai et al. [29] the authors proposed a comprehensive methodology based on machine learning to secure the Software-Defined Networks (SDNs) from DoS attacks. Different types of supervised learning techniques, including Random Forest, Logistic Regression, Decision Tree, XGBoost, and LightGBM, were considered. These forms of supervised learning were tested to perform an exhaustive comparison to realize the best strategies for the most rapid and accurate detection of DoS threats. The study pointed out that XGBoost and LightGBM performed extremely well, highlighting their potency for the enhancement of SDN security. The study also brought out the operational strength in combing through a few sets of machines learning algorithms, thereby indicating that the strategy can attain a better accuracy and efficiency when compared against using just one single algorithm in practice. Ashwin et al. [30] applied PSO and GNDO for feature selection, trained SVM and Decision Tree classifiers to detect DDoS, and implemented a focused mitigation framework for dealing with various types of floods attacks in SDN systems. Hussian et al. [31] The research used the Pycaret module as a minimalistic tool for the application of various machine learning algorithms. By incorporating the XGBoost model, Pycaret greatly improves DDoS detection performance and accuracy over legacy machine learning models such as Random Forest, Decision Tree, and Gradient Boosting. This method plays a pivotal role in protecting the availability, integrity, and confidentiality of cloud services and hence preventing financial loss and reputational damage, while security in general is improved. Rasheed et al. **[32]** The paper suggests employing a Support Vector Machine (SVM) as a machine learning classifier. The classifier is configured to identify Distributed Denial of Service (DDoS) attacks that target Software Defined Network (SDN) controllers specifically. Once the SVM classifier identifies a DDoS attack, a mitigation module is activated. The goal of this module is to block the identified attack streams, with the aim of mitigating the impact of the DDoS attack. Neethu et al. [33] The study compares 20 machine learning algorithms with a focus on feature engineering and class imbalance avoidance by using
the Synthetic Minority Oversampling Technique (SMOTE). The results show that ensemble techniques, including the LGBM Classifier, Random Forest Classifier, XGB Classifier, and Decision Tree Classifier, got almost perfect scores (approx. 100%) in all metrics, which demonstrates a possibility of overfitting. Models like AdaBoost Classifier, K-Neighbors Classifier, and SVC, on the other hand, performed somewhat worse at 99%, underscoring the difficulty of making accurate predictions in cybersecurity. The accuracy of simple models like Gaussian Naive Bayes, Linear Discriminant Analysis, and Logistic Regression was moderate to low, at about 70%. The results show that in order to achieve effective DDoS detection in SDN environments, a thorough approach to machine learning model selection and optimization is required.

Hassan et al. [34] This study used a variety of machine learning techniques and data management techniques to improve classification accuracy, with a focus on early

threat identification in Software-Defined Network (SDN) environments. The study assessed eight distinct machine learning classification techniques for Software-Defined Network (SDN) attack detection. Several data treatment methods were used to address the dataset's class imbalance problem and raise the classification models' accuracy. Synthetic Minority with Random Oversampling SMOTE (Synthetic Minority Over-sampling Technique), Random Undersampling, Tomek linkage under-sampling, and Near-miss methodology under-sampling. Following the application of these techniques, the LDA classifier's accuracy rose to 98.79%. Support Vector Machine (SVM), AdaBoost (AB), Random Forest (RF), Naïve Bayes (NB), K-Nearest Neighbor (KNN), Classification and Regression Tree (CART), Logistic Regression (LR), and Linear Discriminant Analysis (LDA).The InSDN dataset, a novel attack-specific SDN dataset, was used to assess the tactics. At first, the LDA classifier's maximum accuracy was 98.6%.

Kavitha et al. [35] suggested improving DDoS attack detection in SDN by implementing and evaluating various machine learning algorithms, i.e., K Nearest Neighbor, Logistic Regression, and Decision Tree, using the KDD Cup 99 dataset for training. Liu et al. [36] introduced REAL-GUARD, a method for detecting and protecting Software-Defined Networks (SDN) from network security attacks. Machine learning-based approach with novel detection levels was the fundamental methodology. REAL-GUARD was defined as "effective, efficient, real-time, and machine learning-based mechanism." In threat detection, it especially employed decision tree methods.

4- Discussion and Comparative Analysis

According to the reviewed studies, machine learning (ML) techniques play a critical role in enhancing the detection and defense against Distributed Denial of Service (DDoS) attacks in Software-Defined Networking (SDN) environments. Each algorithm's effectiveness varies according to the dataset used, feature selection process, and detection framework architecture. Because of its ability to handle high-dimensional data and its efficacy with a limited number of training samples, the Support Vector Machine (SVM) is widely used. Rasheed et al. [32] and Sahoo et al. [27] showed that SVM-based systems achieved high detection accuracy when combined with SDN controllers. However, SVM's effectiveness is heavily impacted by kernel selection and parameter optimization, and it may have scalability problems with very large datasets. Due to their interpretability and ability to withstand noisy input, Random Forest (RF) and Decision Tree (DT) classifiers are frequently used. According to Aslam et al. [28] and Neethu et al. [33], ensemble methods like Random Forest achieved better results in terms of accuracy and false positive rates. However, these models might require a significant amount of memory and training time, particularly when applied to real-time SDN scenarios. Despite being simple and effective in some situations, K-Nearest Neighbor (KNN) has high processing costs during inference because distances from all training samples must be calculated. Using the KDD Cup 99 dataset, Kavitha et al. [35] showed good performance using KNN in combination with Logistic Regression and Decision Tree.

However, these conventional models may have difficulties in generalizing to contemporary SDN traffic patterns. **XGBoost and LightGBM**, as shown by Lai et al. [29], surpassed numerous classical models by utilizing gradient boosting and sophisticated optimization methods. Their capacity to manage feature interactions and absent values renders them appropriate for intricate SDN systems. Nonetheless, these models are frequently regarded as "black boxes," which constrains their explainability in essential network protection applications. Furthermore,

REAL-GUARD, introduced by Liu et al. [36], integrated **Decision Tree techniques** into a real-time detection system. The framework's focus on both packet and flow-level characteristics enhanced its efficacy in managing dynamic SDN traffic. The real-time aspect is essential for practical applications, although scalability and responsiveness to emerging threats continue to pose difficulties. A notable trend in the literature is the increasing prevalence **of hybrid and ensemble models**, as seen in the studies by Aslam et al. [28] and Neethu et al. [33]. By amalgamating the strengths of many classifiers and incorporating feature engineering methods such as SMOTE, these systems attained near-optimal performance, but with heightened system complexity. A persistent difficulty is the **class imbalance** evident in the majority of SDN-related datasets. To increase the effectiveness of classifiers, several studies, such as Hassan et al. [34], used balancing techniques like SMOTE and under-sampling. While these techniques improve accuracy, there is a chance that they will overfit or overlook important patterns in minority classes.

Table 1: Comparative Analysis of ML Algorithms for DDoS Detection in SDN

Algorithm	Accuracy	Real-Time Suitability	Interpretability	Scalability	Remarks	Reference
SVM	High	Moderate	Low	Moderate	Effective in high-dimensional data; performance sensitive to parameters	[27], [28], [32]
Random Forest (RF)	Very High	Moderate	Moderate	Low to Moderate	High detection rate but computationally expensive	[28], [33]
Decision Tree (DT)	Moderate to High	High	High	Moderate	Fast, interpretable; used in REAL-GUARD and other frameworks	[30], [36]
K-Nearest Neighbor	Moderate	Low	High	Low	High complexity in large datasets; not ideal for real-time detection	[35], [33]
Logistic Regression	Moderate	High	High	High	Simple, fast; but less effective with nonlinear or complex patterns	[35], [33]
XGBoost	Very High	Moderate	Low	High	Gradient boosting with strong performance; limited explainability	[29]
LightGBM	Very High	Moderate	Low	Very High	Efficient on large datasets; best accuracy in some comparative studies	[29], [33]

5- Conclusion

Notwithstanding considerable advancements in using machine learning methodologies to bolster Software-Defined Network (SDN) security, some issues persist. Subsequent research should concentrate on creating real-time, lightweight detection models tailored to the resource-limited and dynamic characteristics of SDN systems. Moreover, sustaining robust security necessitates adaptive learning systems capable of evolving in response to emerging threats. The integration of deep learning and reinforcement learning methodologies demonstrates potential for enhancing detection precision and reaction efficiency. Furthermore, hybrid models integrating several machine learning approaches are essential, as is the development and utilization of genuine, SDN-specific datasets. Collaborative and cross-layer detection methodologies can enhance the robustness of SDN architectures. Addressing these concerns will facilitate the development of more pragmatic and effective security solutions for the future of SDN.

6- Future Research Direction

Many challenges remain even after significant progress in applying machine learning to software-defined networking security. Future research should focus on developing real-time, lightweight models suitable for SDN environments and adaptive systems that can learn from new threats. Combining deep learning and reinforcement learning techniques can improve the accuracy of detection. Authentic SDN-specific datasets, cross-layer collaborative detection processes, and hybrid models are also required. A promising strategy for proactive threat mitigation is the incorporation of machine learning-based security into software-defined networking architecture.

Refrences

[1] E. Fenil and P. M. Kumar, “Towards a secure software defined network with adaptive mitigation of DDoS attacks by machine learning approaches,” in 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), IEEE, 2022, pp. 1–13. Accessed: Aug. 01, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/97526

[2] A. A. Alashhab et al., “Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model,” IEEE Access, vol. 12, pp. 51630–51649, 2024, Accessed: Aug. 01, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10489935/

[3] A. Kaur, C. R. Krishna, and N. V. Patil, “A comprehensive review on Software-Defined Networking (SDN) and DDoS attacks: Ecosystem, taxonomy, traffic engineering, challenges and research directions,” Comput. Sci. Rev., vol. 55, p. 100692, 2025, Accessed: Aug. 01, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013724000753.

[4] B. Bala and S. Behal, “AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges,” Comput. Sci. Rev., vol. 52, p. 100631, 2024, Accessed: Aug. 01, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013724000157.

[5] Zhang and W, “Machine Learning-Driven Security Solutions for SDN: A

Comprehensive Survey," IEEE, vol. 10, 2023.

[6] Ali, T.E., Chong, Y.W. and Manickam, S., 2023. Machine learning techniques to detect a DDoS attack in SDN: A systematic review. Applied Sciences, 13(5), p.3183.

[7] M. H. Bashaa, W. S. Bhaya, and N. H. K. Al-aaraji, "Integration of Zero Trust Architecture and Machine Learning for Improving the Security of Software Defined Networking: A Review," J. Intell. Inform. Netw. Cybersecurity, vol. 1, no. 1, p. 1, 2025, Accessed: Aug. 01, 2025. [Online]. Available: https://jiinc.uobabylon.edu.iq/journal/vol1/iss1/1.

[8] N. Aslam, S. Srivastava, and M. M. Gore, "A Comprehensive Analysis of Machine Learning- and Deep Learning-Based Solutions for DDoS Attack Detection in SDN," Arab. J. Sci. Eng., vol. 49, no. 3, pp. 3533–3573, Mar. 2024, doi: 10.1007/s13369-023-08075-2.

[9] M. Shahzad, S. Rizvi, T. A. Khan, S. Ahmad, and A. A. Ateya, "An Exhaustive Parametric Analysis for Securing SDN Through Traditional, AI/ML, and Blockchain Approaches: A Systematic Review," Int. J. Networked Distrib. Comput., vol. 13, no. 1, p. 12, June 2025, doi: 10.1007/s44227-024-00055-8.

[10] S. Rout, K. S. Sahoo, S. S. Patra, B. Sahoo, and D. Puthal, "Energy Efficiency in Software Defined Networking: A Survey," SN Comput. Sci., vol. 2, no. 4, p. 308, July 2021, doi: 10.1007/s42979-021-00659-9.

[11] M. S. Bonfim, K. L. Dias, and S. F. L. Fernandes, "Integrated NFV/SDN Architectures: A Systematic Literature Review," ACM Comput. Surv., vol. 51, no. 6, pp. 1–39, Nov. 2019, doi: 10.1145/3172866.

[12] Z. Latif, K. Sharif, F. Li, M. M. Karim, S. Biswas, and Y. Wang, "A comprehensive survey of interface protocols for software defined networks," J. Netw. Comput. Appl., vol. 156, p. 102563, 2020, Accessed: Aug. 01, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804520300370.

[13] M. Karakus and A. Durresi, "A survey: Control plane scalability issues and approaches in software-defined networking (SDN)," Comput. Netw., vol. 112, pp. 279–293, 2017, Accessed: Aug. 01, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S138912861630411X.

[14] H. Farhady, H. Lee, and A. Nakao, "Software-Defined Networking: A survey," Comput. Netw., vol. 81, pp. 79–95, Apr. 2015, doi: 10.1016/j.comnet.2015.02.014.

[15] Y. Liu, B. Zhao, P. Zhao, P. Fan, and H. Liu, "A survey: Typical security issues of software-defined networking," China Commun., vol. 16, no. 7, pp. 13–31, 2019, Accessed: Aug. 01, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8766905/.

[16] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "Sdn Security: A Survey," in 2013 IEEE SDN for Future Networks and Services (SDN4FNS), Nov. 2013, pp. 1–7. doi: 10.1109/SDN4FNS.2013.6702553.

[17] J. C. Correa Chica, J. C. Imbachi, and J. F. Botero Vega, "Security in SDN: A comprehensive survey," J. Netw. Comput. Appl., vol. 159, p. 102595, June 2020, doi: 10.1016/j.jnca.2020.102595.

[18] A. N. Alhaj and N. Dutta, "Analysis of Security Attacks in SDN Network: A Comprehensive Survey," in Contemporary Issues in Communication, Cloud and Big Data Analytics, vol. 281, H. K. D. Sarma, V. E. Balas, B. Bhuyan, and N. Dutta, Eds., in Lecture Notes in Networks and

Systems, vol. 281. , Singapore: Springer Singapore, 2022, pp. 27–37. doi: 10.1007/978-981-16-4244-9_3.

[19] R. Gonzaga and P. N. M. Sampaio, "Mitigating man in the middle attacks within context-based sdns," in 8th international workshop on ADVANCEs in ICT infrastructures and services (ADVANCE 2020), 2020, pp. 1–8. Accessed: Aug. 05, 2025. [Online]. Available: https://hal.science/hal-02495155/.

[20] Q. Yan and F. R. Yu, "Distributed denial of service attacks in software-defined networking with cloud computing," IEEE Commun. Mag., vol. 53, no. 4, pp. 52–59, 2015, Accessed: Aug. 05, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7081075/.

[21] M. Conti, F. De Gaspari, and L. V. Mancini, "A novel stealthy attack to gather SDN configuration-information," IEEE Trans. Emerg. Top. Comput., vol. 8, no. 2, pp. 328–340, 2018, Accessed: Aug. 05, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8293865/.

[22] Z. Zhao, F. Liu, and D. Gong, "An SDN-Based Fingerprint Hopping Method to Prevent Fingerprinting Attacks," Secur. Commun. Netw., vol. 2017, pp. 1–12, 2017, doi: 10.1155/2017/1560594.

[23] A. M. Rahmani et al., "Machine Learning (ML) in Medicine: Review, Applications, and Challenges," Mathematics, vol. 9, no. 22, Art. no. 22, Jan. 2021, doi: 10.3390/math9222970.

[24] L. Sindayigaya and A. Dey, "Machine Learning Algorithms: A Review," Int. J. Sci. Res. IJSR, vol. 11, no. 8, pp. 1127–1133, Aug. 2022, doi: 10.21275/SR22815163219.

[25] S. Naeem, A. Ali, S. Anam, and M. M. Ahmed, "An unsupervised machine learning algorithms: Comprehensive review," Int. J. Comput. Digit. Syst., 2023, Accessed: Aug. 05, 2025. [Online]. Available: https://www.researchgate.net/profile/Aqib-Ali-6/publication/368983958_An_Unsupervised_Machine_Learning_Algorithms_Comprehensive_Review/links/643c783f1b8d044c632ba4ab/An-Unsupervised-Machine-Learning-Algorithms-Comprehensive-Review.pdf.

[26] K. S. Sahoo et al., "An evolutionary SVM model for DDOS attack detection in software defined networks," IEEE Access, vol. 8, pp. 132502–132513, 2020, Accessed: Aug. 05, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9142183/.

[27] M. Aslam et al., "Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT," Sensors, vol. 22, no. 7, Art. no. 7, Jan. 2022, doi: 10.3390/s22072697.

[28] J. Lai, "Machine Learning-Based Network Detection Research for SDNs," in ITM Web of Conferences, EDP Sciences, 2025, p. 01015. Accessed: Aug. 05, 2025. [Online]. Available: https://www.itm-conferences.org/articles/itmconf/abs/2025/01/itmconf_dai2024_01015/itmconf_dai2024_01015.html.

[29] A. Ashwin, V. Santhosh, R. T. Venkatesh, N. Gowthami, and S. Tamilselvi, "Detection and Mitigation of DDoS Attack in SDN Using Feature Based SVM and Decision Tree Approach," in 2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS), IEEE, 2024, pp. 325–330. Accessed: Aug. 05, 2025. [Online].

Available: https://ieeexplore.ieee.org/abstract/document/10823201/.

[30] M. A. Hussian, S. Vasantha, S. Ala, K. Pendam, and S. Rame, "Mitigating Denial of Service Attacks through Machine Learning-based Intrusion Detection," in 2024 International Conference on Intelligent Systems and Advanced Applications (ICISAA), IEEE, 2024, pp. 1–5. Accessed: Aug. 05, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10829262/.

[31] S. Rasheed and M. S. Rathore, "Support Vector Machine Based DDoS Detection and Mitigation in Software Defined Networks," J. Innov. Comput. Emerg. Technol., vol. 4, no. 2, 2024, Accessed: Aug. 05, 2025. [Online]. Available: https://www.jicet.org/index.php/JICET/article/view/161.

[32]Neethu and S, "Comprehensive Performance Evaluation of Machine Learning Algorithms for detecting DDoS attacks in SDN," IAES, vol. 13, 2024.

[33] H. A. Hassan, E. E. Hemdan, W. El-Shafai, M. Shokair, and F. E. Abd El-Samie, "Detection of attacks on software defined networks using machine learning techniques and imbalanced data handling methods," Secur. Priv., vol. 7, no. 2, p. e350, Mar. 2024, doi: 10.1002/spy2.350.

[34] O. Blial, M. Ben Mamoun, and R. Benaini, "An Overview on SDN Architectures with Multiple Controllers," J. Comput. Netw. Commun., vol. 2016, pp. 1–8, 2016, doi: 10.1155/2016/9396525.

[35] M. Kavitha, M. Suganthy, A. Biswas, R. Srinivsan, R. Kavitha, and A. Rathesh, "Machine learning techniques for detecting ddos attacks in sdn," in 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), IEEE, 2022, pp. 634–638. Accessed: Aug. 05, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10029110/.

[36] Q. Liu, H. Ruan, H. Li, X. Li, and X. Wang, "REAL-GUARD: A Machine Learning based Real-time Mechanism for Combining Packet and Flow Features to Mitigating Network Attacks in SDN," in Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies, in CIAT 2020. New York, NY, USA: Association for Computing Machinery, Jan. 2021, pp. 451–458. doi: 10.1145/3444370.3444612.