Detection Methods for Software Defined Networking Intrusions (SDN)

Dr. Soma Prathibha[1], Bino J[2], Md. Tabil Ahammed[3], Chinmoy Das[3], Shariar Rahman Oion[4], Sudipto Ghosh[4]and Maharin Afroj[4]

[1]Department of Information Technology, Sri Sai Ram Engineering College, Chennai, Tamilnadu, India
[2]Department of ECE, St. Joseph's Institute of Technology Chennai, Tamilnadu, India
[3]Department of EEE,Bangladesh University of Business and Technology Dhaka, Bangladesh
[4]Department of CSE, Bangladesh University of Business and Technology Dhaka, Bangladesh
E-mail :somaprathi25@gmail.com, stephenbino@gmail.com, ahtabil53@gmail.com, chinmoyd299@gmail.com, shariaroion05@gmail.com, sudiptoghosh555@gmail.com, maharinshova@gmail.com

2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) | 978-1-6654-9529-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/ACCAI53970.2022.9752574

Abstract **It is possible to govern and manage traffic robustly while guaranteeing as a result of which is secured from any threats in line with client requirements in a Software Defined Network (SDN). By separating the data and control layers, SDN is an emerging technology that aims to simplify the complexity of network operations. There are several security concerns with SDN, and the divide adds to one of them. Due to the split, some attack types, such as DDoS assaults, may confuse SDN performance. SDN-based Network Intrusion Detection Systems (NIDS) have created a variety of methods to secure computer systems and address SDN security issues. Also examined and studied in this research are several intrusion detections approaches that affect SDN networks. SDN network security issues may be overcome with the aid of these intrusion detection methods.**

Keywords — Data Layer, Network Intrusion Detection Systems, Distributed Denial-of-Service Software Defined Network, Control Layer.

I.INTRODUCTION

To keep up with the exponential growth of conventional networks, it has become more difficult to deal with hostile activity on the network [1]. Known sectors and businesses are at peril from these cyberattacks. Malicious assaults destroy, steal, damage, change, and obtain access to critical sensitive data. Because of its dynamic, controllable, easy-to-implement economics and adaptable character, SDN is an increasingly popular new technology for today's dynamic systems [2]. SDN is based on the principle of separating the data layer from the control layer. There are three levels to SDN's architecture: an application layer, a control layer and a data layer that are separated from each other. Contrast this with a typical network system, which merges the data and control layers into one. There are various benefits of using SDN over conventional network architectures. In the application layer, you'll find a wide range of programs needed to do a wide range of tasks in the workplace.

The SDN control layer on the centralized controller implements these software programs. When an SDN application makes a network request, the controller uses a northbound interface in order to connect with the application. When it comes to SDN, a single or a few controllers operate as the "brain" of the system, which controls the network switches and maintains all the network's functions through extensive monitoring and administration. [3] Devices such as switch and router are responsible for delivering all the data on the network. [4], [5]. A wired or wireless connection is used to link these gadgets together. Figure 1 depicts the SDN architecture in its entirety, with each layer clearly labelled.

Although the SDN design has many advantages, it also has a number of disadvantages, including an attack, vulnerabilities, and threat vectors [6]. In the present period, SDN security is an extraordinary topic for academic study, and SDN has been supported to reduce cyberspace infiltration assaults. SDN networks may also be targeted by attackers, and this can be done efficiently [7]. Therefore, the introduction of a Network Intrusion Detection System (NIDS) is necessary to combat security threats. It is the goal of this article to describe and evaluate the many studies on intrusion detection systems that are based on SDN-based networks. In addition, an SDN network's attack classes and intrusion detection method will be predicted.

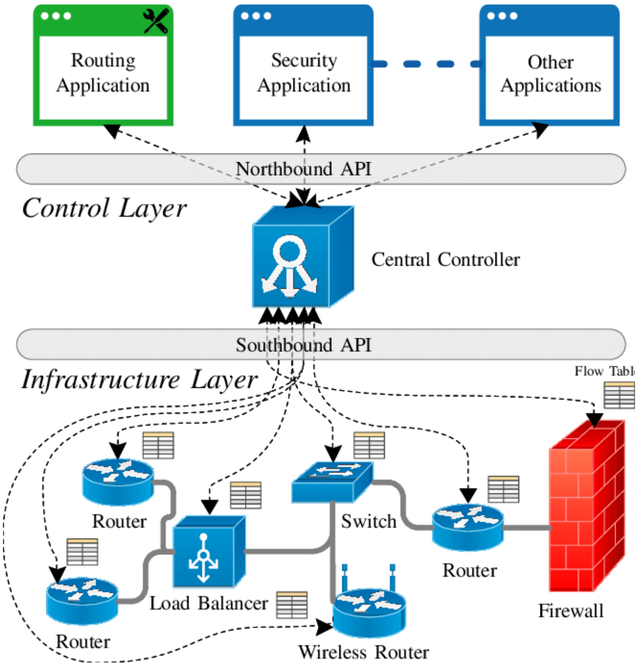

Fig 1. Architecture for Software Defined Networking (SDN).

II. Overview Of Intrucsion Detection Systems

Intrusion Detection System

Globally, the number of intrusions is increasing as the amount of cyberspace grows. As a result, in order to prohibit unlawful operations and safeguard sensitive information, cyber-attacks must be appropriately regulated. Cyberspace must be guarded against intrusion by considering and enforcing three key ideas in information security. Integrity, secrecy, and availability [5] are three principles. SDN network architecture's forwarding (infrastructure) and control layers have been divided up and centralized, creating new opportunities for hackers to carry out a variety of assaults. Attackers are using tactics distinct from those used against a more conventional network [8]. To follow up on an initial assault that has already been conducted, compromise operators might be used. There are several vulnerabilities that may be exploited in SDN applications, allowing attackers to gain control of the controller without having to use traditional authentication techniques [2]. DoS and flow rule mishandling are two examples of new attacks that have emerged, might be launched by the attacker as a result. All kinds of assaults that abuse the target computer systems or infrastructures, networks or personal computers in order to damage or steal the data or information systems are known as cyber-attacks. DDoS assaults, probe attacks, injection attacks of SQL, man-in-the-middle attacks and other types of attacks are all frequent in cyberspace.

Network traffic and system activity are observed and inspected in order to discover malicious or unauthorized occurrences. The term "Intrusion Detection System" refers to any software or hardware that is specifically designed to detect intrusions (IDS). IDS are mostly used to prevent a network from being hacked. Anomaly-based detection and signature-based detection are the two most common types of intrusion detection schemes [9]. An attack's signature database is equivalent to a new dataset in signature-based detection. Anomaly-based models may successfully identify new and previously detected assaults.

Systems in the cyberspace are protected by a variety of various types of security technologies and systems. The security functionality of these technologies differs from one another. packet headers are examined by firewalls to filter incoming and outgoing traffic flow according to pre-determined rules and conditions. Port number, IP address, and protocol are just a few examples of information included in packet headers. For cyber-attack prevention, firewalls typically act on the outside of a network to prevent them from entering the network [10]. They are unable to block suspicious activity on their own, and as a result, an administrator is required. In contrast to IPSs, it functions as an IDS but is able to terminate an identified threat proactively. A general overview of intrusion detection systems and the defense mechanisms that go along with them may be shown in Figure 2.

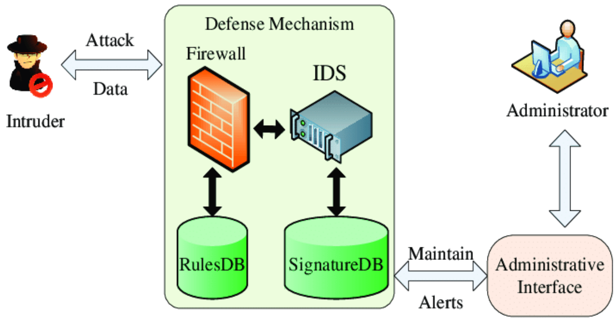

Fig 2. Intrusion Detection System Categories

IDSs Types

It is possible to categorize IDSs based on the sorts of activity they analyze and the detection methods they use. Intrusion detection systems (IDSs) may be divided into two categories in accordance with the nature of the work they analyze: Host-based IDSs and Network-based IDSs (NIDS). Both Signature-Based intrusion detection systems and Anomaly Based intrusion detection systems may be classed as IDS types.

IDS Types by Analyzed Activities

a) IDS depending on the host

This kind of intrusion detection system is called a host-based intrusion detection system (HIDS). They're set in place on computers so that you may look into things like processes, system logs, files, and other things like that. For example, HIDSs might be placed to keep tabs on a single target by monitoring their actions and simultaneously comparing the data to verify whether there is unwanted or suspicious behaviour. But even if monitoring each system is analytic, only a single host may access the IDS process, which uses resources and may impair performance on the individual system, and intrusions aren't detected the particular system is the only way for them to progress.

b) Network-based IDS

Intrusion detection systems of this kind are known as host-based systems (HIDS). They're installed on computers so that you may access things like processes, system logs, files, and more. For example, HIDSs might be used to spy on individual hosts by monitoring their behaviours and concurrently analyzing the data to check whether there is undesired or suspicious activity. Only one host may access IDS, which consumes resources and slows down the individual system's performance, even if the monitoring is analytic. Intrusions are only identified after they've already reached the particular system, which is a drawback.

IDS Types by Detection Method

a) IDS based on signatures

Attack signatures are stored in the database of this form of IDS and identify known malicious threats. It uses a signature database to monitor traffic and verify the input stream for intrusions. Attack signatures must be updated often for this sort of IDS to be successful. Even with the most recent improvements, this sort of IDS can only detect threats that have already been recognized.

b) Anomaly Based IDS

Identification of commonly utilized bandwidth, protocols, and ports is the goal of anomaly detection, which is an investigation of a system's "normal or anticipated" activities. In the event of a deviation from this standard behavior, the alarm will sound. Unlike other types of IDS, this one does not need regular database maintenance or upgrades. There are many false positives that are difficult to go through, and it may identify unidentified threats. It is also more difficult to acquire proof of the breach since there is no clear signature to identify it.

Defense Mechanisms for SDN

Researchers throughout the world have been captivated by SDN's ability to solve problems and provide innovative security methods [11]. For legacy networks, SDN's present growth has provided a beneficial stage for the security perspective. Cyber-attacks can only be regulated if they have a universal viewpoint and are programmable. Statistical and machine-learning (ML) based defenses are two main categories. Statistical analysis is the process of acquiring and analyzing data to identify suspicious activity. Traffic packets' behavior and features are the basis for this investigation. " Network traffic is analyzed using statistical models, and if the records cannot be trimmed using these models, they are classed as harmful data. Machine Learning is a technology that has gotten a lot of interest recently and is made up of a number of different components. A variety of security-related algorithms have been developed. SDN network intrusions are also being developed to identify and ameliorate them. In order to separate legitimate from malicious communications, these methods are used as a classifier. Table 1 summarizes many articles on Machine Learning based detection techniques. Based on how they are learned, supervised, unsupervised, and semi-supervised learning algorithms are all examples of machine learning algorithms.

A neural network model may be learned in both supervised and unsupervised environments. An engaged dataset that includes both the correct inputs and the correct results is required for most models. A mathematical function is attempted to be modelled by the algorithm in order to predict these results and their inputs. Regression and Classification are two of the main duties of supervised training. When it comes to unsupervised training, the goal is not to utilize any output but rather to understand the relevant data entry in the training dataset itself. An unsupervised learning technique known as reconstruction is an exception. In other words, intolerant whether the model was used in the assessment already had an understanding of the dataset. The proper outcome is seen as a kind of supervision.

III. Discussion of Several Intrusion Detection Methods

More than a few studies have been done on SDN technology, and some of these articles are reviewed in this section. There are studies that analyze and SDN controller and intrusion detection system performance may be evaluated using several performance metrics. Through traffic analysis, several sections of the description discuss how to identify and prevent intrusive assaults in the OpenFlow network. It's like a black hole when it comes to dealing with these kinds of assaults. When there are no unknown hazards in the experiment, supervised learning approaches outperform unsupervised ones. Because the user must choose the number of clusters, k-means suffers from the fact that it can only deal with numerical data. For large datasets, it takes a long time to train SVM since it is difficult to grasp and interpret the final model and variable. When using the SOM approach to develop meaningful clusters, it is necessary to have crucial and enough data available. In contrast, it has a drawback in that it cannot learn on its own. Flow-based intrusion detection for SDN was suggested by Ajaeiya et al who found that the supervised classifier is better at detecting encrypted flows. Researchers found that their flow-based IDS had a low false alarm rate and could detect malicious traffic flow with a high degree of accuracy (measured by the classification model's F_1 score). DDoS attacks against SDN controllers were detected using SADDCS, a statistical-based technique for identifying malicious activity in networks. SDN controllers are less likely to be targeted since the suggested design increases detection accuracy while reducing false positive/negative flow rates, according to the authors. The most critical concern in SDN networks is the security of controllers from threats and attacks. On the basis of these characteristics, the detection rate and the window size may be determined, the authors developed an optimization method to monitor and analyze network traffic. Furthermore, classification approaches may be used to reduce DDoS attacks and enhance sequential ratio tests by providing accurate results and random distribution of the classification techniques. To better understand DDoS assaults [12] presented anomaly detection as one of the well-known methods for detecting network anomalies. As a result, focusing just on DoS assaults is an issue. Qualitative datasets are needed to investigate a variety of assaults so that the limitations of low accuracy and large false alerts may be avoided and overcome. DDoS assaults are the only kind of attack that may use this type of attack. As a means of detecting anomaly, the SDN controller should employ a confidence interval and mean throughput. This research increases accuracy and decreases costs. Due to its focus on throughput, it is not compatible with large-scale networks since it mainly focuses on the infrastructure layer for detection of attacks. SDN has a single point of failure because of packet overflow at the controller [16]. It was thus recommended to avoid DDoS attacks by using methods based on statistics. Controlling network overloading at the controller resulted in a reduction in detection time. The dataset generated using a Python application is insufficient to cover all possible assault scenarios. Public datasets are very large and include numerous redundant entries that seem to be useless for any IDS training. To properly train any machine learning method, a large and high-quality dataset is required. An excellent dataset may certainly lead to better algorithms, but it is also expensive and time-consuming to create. As a result of these issues, the dataset that is currently accessible does not meet all of our needs. This is due to the fact that there are no publicly available datasets prepared specifically for training and assessment of anomaly detection algorithms for SDN networks. We must generate an SDN dataset with a high degree of quality and completeness, and suggest customizing it for testing intrusion detection systems' performance, according to [35]. The problem was solved by using feature selection techniques to provide datasets free of duplication and reduced in irrelevance for the identification of anomalies in SDN environments. Unsolved problem: reducing the false warnings frequency in the identification of previously unknown attacks. Due to low accuracy and excessive false alerts, this technique of intrusion detection is unreliable. As a result, the system has low performance and is inefficient and ineffective. Entropy-based rule and Correlation-based [14] rule to identify DDoS assaults in opposition to SDN controllers.

Table 1 Comparative Study of Different SDN-Based Research work

S/N	Reference	Training Dataset	Technique	Attack Type	Evaluation Metrics	Problem	Solution
1	[16]	For producing data flow, Scapy is the best choice.	Window widths and the mean entropy are two statistical approaches to consider.	DDoS	Packet loss and Detection Rate.	A single point of failure due to packet overflow at the controller.	DoS attacks might be prevented by using mean entropy, which is the pace at which the percentage drops.
2	[17]	NSL-KDD dataset	Naive Bayes and Random Forests are examples of classical ML methods.	The nature of the attack is unknown.	F- score, Recall, Accuracy and Precision	Machine learning performance is affected by a variety of factors, including the selection of features and the dataset utilized.	Advocate the use of Deep learning techniques for identifying and classifying attacks.
3	[18]	Traffic Flow, Real Time, Time Series Data	Clustered Optimization on Technique for machine learning approaches	DDOS	Threshold Values Window size and Detection Rate.	Threats and attacks aimed at overloading the controller in the center.	Promote the implementation of an optimal approach for classifying and detecting malicious traffic flow based on the statistics of packet flow.
4	[19]	Self-Made generated traffic Dataset	Statistical Approach: Confidence interval and mean Throughput	TCP SYN Flood, TCP ACK Flood and DDoS.	Throughput	Problem of DDoS flooding Attack in SDN.	Confidence intervals and mean throughput may be used to discover anomalies in the SDN controller.

SDN Technology has recently been a hot topic in the academic community because of security concerns and the fast growth of network operability. When it comes to the identification of harmful traffic behaviors in experiments on the publicly available systems that detect intrusions (IDSs), showed that conventional machine-learning based approaches failed to outperform classical based on machine learning techniques in terms of accuracy and precision. A system for detecting and responding to threats was provided by the authors (e.g., DDoS attack). When compared to the current IDS system, our suggested framework provides a better quality of service. Malicious actions discovered by the IDS are alerted by sending an alert to the control panel. The control panel may then take action to prevent such attacks from happening again. An intrusion detection system based on machine learning was presented by Muthamil and Deepalakshmi (2019) to address the security concerns of SDN networks. K-Means and C4.5 Algorithms are included into this hybrid machine learning approach. The trial results showed that the suggested approach can accurately distinguish normal and harmful events with 97.66 percent accuracy, according to the authors. In an SDN context, a system for preventing and detecting intrusions (IDPS) was developed and implemented by Birkinshaw et al. [15] to monitor network traffic flow and identify and fight against malicious actions such as DDoS, security policy destruction, and port scanning assaults. In order to protect the IDPS from assaults by lowering the thresholds in the detection algorithm, the suggested architecture has the ability to identify and halt real-time assaults and reduce the number of false positives. In addition, a number of testing tools were used to create and simulate an SDN network. The authors examined and analyzed how a denial-of-service (DoS) attack on an SDN network might be affected by the network's capacity and latency (jitter). Furthermore, a denial-of-service assault (DoS attack) overwhelms the controller with a deluge of packets. The majority of the previous research has focused on identifying attacks in SDN-based Open Flow networks deep learning, streaming data, data mining and machine. Improved system performance and better intrusion detection may be achieved via the use of machine learning (ML) methods. The accuracy of deep learning techniques has yet to reach a high level whereas that of machine learning has already reached around 99 percent. In order to detect intrusive assaults, employing a single controller in an SDN environment was an unreliable strategy. It was suggested that numerous controllers may be utilized in SDN to handle new packets, and feature selection techniques could be employed for anomaly detection in SDN systems to eliminate redundancy and unnecessary data. Last but not least, the model's creator claims that it will boost efficiency and safety thanks to its accurate and minimal false alarms.

IV. CONCLUTION

An overview of several kinds of intrusion detection systems and the new technology of Software-Defined Networking (SDN) was presented in this article (SDN). It also reviewed and summarized several studies on intrusion detection methods, highlighting their strengths and weaknesses. Machine learning may be used to discover vulnerabilities and monitor network traffic flow in SDN, based on this comparative study of diverse research efforts, according to the authors of this paper.

REFERENCES

[1] Khorasi, Nooruddin. "Software Defined Networking (SDN) Based Solution for Data Center Construct." (2021).

[2] Susilo, Bambang, and Riri Fitri Sari. "Intrusion Detection in Software Defined Network Using Deep Learning Approach." 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2021.

[3] Siddiqui, Gufran, and Sandeep K. Shukla. "Supervised Machine Learning-Based DDoS Defense System for Software-Defined Network." Machine Vision and Augmented Intelligence—Theory and Applications. Springer, Singapore, 2021. 667-681.

[4] Nugraha, Beny, Naina Kulkarni, and Akash Gopikrishnan. "Detecting Adversarial DDoS Attacks in Software-Defined Networking Using Deep Learning Techniques and Adversarial Training." 2021 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, 2021.

[5] Björnerud, Philip. "Anomaly Detection in Log Files Using Machine Learning." (2021).

[6] Padhi, Adarsh, Gyanaranjan Sahoo, and Satyabrata Maity. " Feature Selection and Deep Learning Technique for Intrusion Detection System in IoT." Intelligent and Cloud Computing. Springer, Singapore, 2021. 653-662.

[7] Corsini, Andrea, Shanchieh Jay Yang, and Giovanni Apruzzese. "On the Evaluation of Sequential Machine Learning for Network Intrusion Detection." arXiv preprint arXiv:2106.07961 (2021).

[8] Dang, Quang-Vinh. "Intrusion Detection in Software-Defined Networks." 2021 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, 2021.

[9] K. Vijayakumar and M. Anathi "An Intelligent approach for Dynamic Network Traffic Restriction using MAC Address Verification" Computer Communications, ISSN: 0140-3664, February 2020.

[10] UMARNANI, VIPIN, and DR JITENDRA SINGH CHOUHAN. "Security in Software Defined Networks (SDN): Challenges and Research Opportunities."

[11] Hasegawa, Hirokazu, and Hiroki Takakura. "A Dynamic Access Control System based on Situations of Users." ICISSP. 2021.

[12] Ramprasath, J., et al. "Distributed Denial of Service (DDoS) and Denial of Service (DoS) anomaly detection and mitigation in Software-Defined Network (SDN)."

[13] Banitalebi Dehkordi, A., M. R. Soltanaghaie, and F. Zamani Boroujeni. "Distributed Denial of Service Attacks Detection in Software Defined Networks." Electronic and Cyber Defense 9.1 (2021): 43-59.

[14] Sudar, K. Muthamil, and P. Deepalakshmi. "Flow-Based Detection and Mitigation of Low-Rate DDOS Attack in SDN Environment Using Machine Learning Techniques." IoT and Analytics for Sensor Networks. Springer, Singapore, 2022. 193-205.

[15] Sasikumar, Seethal. "Network Intrusion Detection and Deduce System." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.9 (2021): 404-410.

[16] Chaganti, Rajasekhar. "Review of Distributed Denial of Service Attack Detection Techniques in Software Defined Networking and Cloud Computing."

[17] Musumeci, Francesco, et al. "Machine-Learning-Enabled DDoS Attacks Detection in P4 Programmable Networks." Journal of Network and Systems Management 30.1 (2022): 1-27.

[18] K. Vijayakumar, C. Arun, "Integrated cloud based risk assessment model for continuous integration", International Journal of Reasoning-based Intelligent Systems, ISSN: 1755-0556 (Print),1755-0564(Online), Novmber 2018,.

[19] Revathi, M., V. V. Ramalingam, and B. Amutha. "A Machine Learning Based Detection and Mitigation of the DDOS Attack by Using SDN Controller Framework." Wireless Personal Communications (2021): 1-25.