2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC) | 978-1-6654-1749-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/IMITEC52926.2021.9714581

A Review of Intrusion Detection Techniques in the SDN Environment

Rodney Sebopelo
Comp.Sc Dept & MaSIM
North-West University
Potchefstroom, South Africa
rodney.sebopelo@nwu.ac.za

Bassey Isong
Comp. Sc. Dept. & MaSIM
North-West University
Mafikeng, South Africa
isong.bassey@ieee.org

Naison Gasela
Comp. Sc. Dept. & MaSIM
North-West University
Mafikeng, South Africa
naison.gasela@nwu.ac.za

Adnan M. Abu-Mahfouz
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
a.abumahfouz@ieee.org

Abstract— **Despite the advantages of Software-defined networking (SDN) over the traditional networks, SDN is facing several challenges such as security threats and attacks, dominated by a distributed denial of service (DDoS) attacks that target the controller. In recent years, the SDN has witnessed several research attentions leading to proposals and the development of countermeasures such as intrusion detection systems (IDS). IDS plays a critical role in detecting and preventing malicious activities on the networks. Several detection techniques have been exploited for the effectiveness of the IDS such as pattern matching, anomaly-based and specification-based. With the nature of SDN architecture, flow-based anomaly detection has been effective and commendable. Therefore, this paper conducted a review of some of the IDS schemes in the SDN environment. It was aimed to identify the solution offers, techniques, challenges and provide research directions. The findings show that IDS in the SDN is an active research area and several techniques exist and are dominated by machine learning (ML) which exploits the network traffic flow to detect abnormal behaviours. Intrusion detection on the SDN is still at large and more ML techniques needs to be explored, considering the critically of the SDN controller.**

Keywords— SDN, DDoS attack, IDS, Machine learning, Flow-based Anomaly.

I. INTRODUCTION

With the rapid technological advancement and widespread internet usage, it has become more challenging to protect sensitive information on the networks due to the increase in the number of intruders or attackers targeting systems to steal critical information. To avoid integrity, confidentiality and availability compromises, various security countermeasures have been introduced such as firewalls, anti-viruses, etc. in the network environment but deemed inadequate to protect the entire system and others [1] as a result of dynamic network environment. Particularly, several organizations have implemented or deployed intrusion detection and prevention systems (IDPS) [1] to balance and strengthen the security of the network from malicious and unauthorized access. IDPS impacts stem from the immense role it plays against several attack types by protecting the system's information. Moreover, many of the historical events have proved that the intrusion prevention systems (IPS) approaches do not meet system requirements such as authentication and encryption as the first line of defence. The more the system becomes complex the higher the weaknesses that manifest which always pose security issues. Thus, intrusion detection systems (IDS) is deployed as a second defence layer to protect the network from attacks such as detecting and implementing appropriate measures that either prevent the attacks or reduce their impact. After such measures are taken the firewall, authentication, access control, etc can block certain actions and some users can be allowed to have access to other resources [2, 3]. An intrusion detection system (IDS) is a network defence software tool developed to monitor the network and other systems for malicious damages or activities that violate the policies, etc. It detects intrusions or malicious attacks and immediately send reports to the administrator or collected centrally with the security information and event management [1],[2].

Software-defined networking (SDN) is a network technology that emerges to address some of the critical challenges and complexities faced by traditional networks and accelerates innovation [67]. SDN has an architecture that is characterized by the separation of the control and the data plane which is logically centralized in control and is programable [67]. It offers several benefits and at the same time, faces several security threats and attacks due to its centralized and programmable controllers as well as vulnerabilities across its layers. The controller being the "intelligence" of the network serves as the primary target of attacks such as distributed denial of service (DDoS) attacks. With DDoS, attackers tend to fiddle with the resources of the controllers to degrade the network performance due to its criticality in the management of the network [4, 5]. To ensure network availability and quality of service (QoS), IDS is critical.

As a mitigation strategy, several security measures such as the IDS have been proposed and developed to guard networks which are classified into signature-based and flow-based anomaly detection techniques. However, several studies have shown that the signature-based techniques are not efficient for the SDN due to its architecture thus, attention has been shifted to the flow-based anomaly detection which effectively utilizes machine learning (ML), in particular, the deep learning (DL) algorithms to overcome the limitation of signature-based IDS [6]. ML algorithms' application in traffic classification has gained considerable attention in recent years and have been

employed to detect patterns based on the selected feature sets, encrypted traffic classification a lower cost of computation, improved QoS, routing prediction, resource management, security [7, 8] etc. Nguyen *et al.*[9] and Foremski *et al.* [10] highlighted the importance of ML-based traffic classification solutions while Tang *et al.* [11] also tested the capability of the DL model to address the challenges posed by network intrusions and DDoS attacks. Moreover, Abubakar *et al.* [6] employed ML to address network intrusions, indicating promising results while [12] showed the capabilities of ML in catching elephant flows in real-time. The ML techniques have significantly minimized the challenges posed by abnormal traffic and network intrusion and thus, have been applied or employed in the development of network intrusion systems to ensure accurate detection, minimize false alarm and effectiveness of guarding the network against attacks such as DDoS, DoS etc. [13, 14] taking advantage of the SDN architecture and OpenFlow protocol.

Several SDN-based IDS or IDPs have been proposed, developed, and deployed. However, the challenges posed by intrusions and attacks is yet to end. Therefore, this paper brings together some of the existing studies to identify the solution strategies, techniques and tools used, and research challenges faced in the context of SDNs to offer a practical countermeasure. We performed analysis on existing works to address the question: *What are the different security solutions offered by ML-based IDS in the SDN and how do they work?*

The rest of this paper is structured as follows: Section II presents related works; Section III presents the existing IDS approaches in the SDN and Section IV is the discussion of the paper while Section V and VI are the research opportunities and the paper conclusion respectively.

II. Related Works

IDS is an active research area and several research works have been done. This section discusses some of the surveys or review works performed in the perspective IDS in SDN. Nasrin Sultana *et al.* [15] comprehensively reviewed ML-based IDS and was evaluated using DL and developed an IDS framework in an SDN environment. Tiwari *et al.* [16] discussed some of the works that employed ML techniques that to achieve NIDS in the SDN environment. The authors presented the tools, techniques, and the IDS framework. They focused on increasing the detection accuracy against the abnormal detection using the two proposed algorithms. Also, Mesut *et al.* [17] comprehensively surveyed DL algorithms usage in cybersecurity applications. DL application was studied in many areas such as PC based malware, phishing, cyber intelligence detection, etc. Evaluation conducted shows more promising results compared to the traditional security applications and as well, presented the DL-based intrusion detection systems in the SDN networks while Tang *et al.* [18] conducted a survey on different IDS proposed or developed for SDN environment. In the same vein, Ibrahim *et al.* [19] presented an IDS which can locate and detect malicious behaviours through real-time traffic or flow analysis in the network.

Xie *et al.* [20] also conducted an in-depth survey on the application of ML techniques in the SDN in terms of intrusion from the perspective of the classification of traffic, routing and so on to improve the quality of experience and security. Nguyen *et al.* [21] also conducted such a comprehensive survey with a focus on the vulnerabilities that considers the common attack methods of ML. The study advocated for the development of a more secure ML-based SDN and other security applications as well as recommend taking threat models seriously while designing the ML-based IDS. In another work, Jafarian *et al.* [22] classified anomaly detection devices into entropy, DL, flow counting, information, and hybrid [22]. Research gaps and challenges such as SDN abnormal detection approaches were also discussed. Moreover, DoS was revealed as the most important external threat to the SDN and also discussed different methods for the collection of statistical data which are needed for the algorithms of anomaly detection. Share *et al.* [23] deeply surveyed intrusion detection in the SDN environment. Several different attacks were discussed, and the authors evaluated the possibilities of malicious attacks happening on the SDN network. Moreover, the authors also discussed various types of attacks and how the attacks work in the TCP IP and SDN networks as well as different data set for intrusion detection generated over the years. Also, Camilo *et al.* [24] presented a survey that discussed the security threats and a list of possible attacks malicious and can misconfigure the SDN. They presented the state-of-the-art categorised in a taxonomy that highlighted the main characteristics and the contributions.

III. Analysis of SDN-based IDS

This section presents a comprehensive analysis of the existing approaches to prevent or detect network intrusions in the SDN. The objective is to address the following sub research questions (RQs).

1. *What are the different security solutions offered by ML-based IDS?*
2. *How do the proposed ML-based work in the SDN landscape?*

These RQs were addressed by analysing the relevant papers that focused on ML-based IDS in the SDN. For RQ 1, the proposed solutions and the challenges addressed will be discussed while for RQ 2, a description of how these solutions work in general will be provided.

A. What are the different security solutions offered by ML-based IDS?

Awodele *et al.* [25] proposed a multiplayer framework for detection and prevention strategies that monitors the single host. The framework consists of three layers: file analyser, system resource analyser, and connection analyser [25]. The aim was to actualize the detection of malicious and unwanted activities to avoid the tampering of the important files, the connection of unauthorized access, etc. The authors proposed and employ the multi-layered framework where each layer can harness the existing capabilities of the signature and anomaly methodologies to thwart intrusions in the SDN. Rawat *et al.*

[26] presented an IDS for the detection and prevention of network attacks and threats in organizations. The challenges identified include network breaches, the detection and breach on time that is crucial, and the challenges observed while detecting unforeseen attacks. To achieve intrusion, the performance and the comparison of the classical ML approaches were performed involving a vast amount of feature extraction. Moreover, the unsupervised learning methods and DNN based on the NSL-KDD dataset were employed. With the DNN, 15 features were identified based on the principal analysis component. Also, Elsayed *et al.* [27] proposed an IDS technique in the SDN environment using ML techniques to address the challenges of security vulnerability and detect malicious traffic. Moreover, a systematic benchmark analysis of the existing ML approach was also proposed and limitations in the classical ML were identified.

Tang *et al.* [28] proposed a flow-based IDS using a DL approach to detect flow-based anomalies in the SDN landscape. In this approach, the controller maintains active monitoring of the OpenFlow switches and requests network statistics after a given time interval. The switches then respond with the network statistics in with the controller analyzes and correlates and send to the IDS module. The IDS module then analyses the network statistics to detect any malicious behaviour or activities using the deep learning approach Deep Neural Network (DNN) [28]. Once malicious behaviour is detected and identified, mitigation action is immediately taken by the OpenFlow protocol by way of flow table modification. To this end, new security policies are sent to the switches to the attacks. Experiments were performed NSL-KDD dataset for model training, 6 features selected, and 4 attack categories utilized. The results obtained show optimal hyper-parameter for DNN in terms of detection and FP rate. The performance shows an accuracy of 75.5%. Similarly, Jankowski *et al.* [29] also proposed a framework for the effective selection of ML algorithms for IDS in the SDNs. The authors discussed the solution for monitoring malicious network behaviours in the data plane and presented the statistics and features of the traffic analysed using the SDN functionalities. They achieved the detect intrusion using a virtual environment where traffic is produced for collection and analysis. Moreover, the efficiency of the selected ML models was examined as well as performed comparative analysis.

Satheesh *et al.* [30] presented an IDS technique based on flow-based anomaly using the ML techniques in an OpenFlow-based SDN. The approach was designed to address the challenges such as the flow of data packets over the network, which can assure bandwidth enforcement and so on. The intrusion detection was achieved by monitoring the network behaviour or traffic using the deployed ML model that classifies incoming packets as normal or abnormal packets. Guimaraes *et al.* [31] proposed an IPS framework for the SDN environment using SNORT and source fire. This was to address challenges of inflexibility, ease of configuration and modification. The SNORT strategy was used for the detection of anomaly attacks, though, multiple drawbacks were identified which emanates from the detection of intrusions using the signature-based technique since the technique is inept for anomaly behaviours detection. In the same vein, Shibli *et al.* [32] presented an IDPS framework based on mobile agents in the SDN. The authors aimed to address the challenges of the SDN being hacked as well as other malicious attacks. The security system employs secured mobile agents that constantly monitors the system, processing of the logs, detection of attacks, and host protection using automated response in real-time. Moreover, multiple drawbacks were also identified such as when the target of the malicious attacker is the mobile agent, the model can fail and become difficult to identify and protect the system from being hacked. Hence, some of the security structures can be adopted to protect the mobile agent.

Wagner *et al.* [33] proposed a model to address the challenges of how the IDS can be divided without using the matching technique of malicious insertion sequence, etc. to detect the mimicry attack. A theoretical framework was developed to evaluate IDS security performance in SDN against the mimicry attack and the results obtained shows the proposed approach outperformed other approaches. Tan *et al.* [34] presented a novel string matching technique that can be optimized to other matching algorithms to address malicious activities in the SDN. The model is designed such that the intruder's information is broadcasted to the other state machine to hold in the database by defining the rules and the comparison of the signatures of the intruder using the predefined detection signature. The algorithm was integrated into the framework to provide an efficient and effective security system. However, the drawback was on the practical implementation of the approach which requires the amount of memory. Thus, the algorithm failed to detect the behaviour which is anomaly intrusion. Mrdovic *et al.* [35] proposed a distributed IDS for the analysis of multiple placements of sensor nodes in the network segments selected to monitor the network traffic behaviour. The intrusion detection approach was based on SNORT which analyses the engine. MySQL database was used as a tool to record events with the assistance of the SNORT and the distributed IDS manage the console with the capabilities to monitor and configure the IDS alongside the capability to provide greater protection against attackers of the multiple computers that can be monitored continuously and prevent the malicious attack [36]. However, it requires much memory space and well-trained security staff to ensure continuity in management.

Bai *et al*. [37] proposed an IDS framework that involved two techniques which are misuse and anomaly detection methodologies. The approach addressed the challenge of the detection in different approaches such as data mining, data fusion, etc. used in the IDS. Both methods provide information on the existing detection technologies. The evaluation shows the methods detect intrusion and are sufficient and effective for the IDPS as well as able to respond to anomalies in real-time [34, 38]. The IDS framework proposed by Han *et al.* [39] was designed to combine multiple hosts and detect the detection of multiple intrusions to reduce the false-positive rate. The approach was to address the challenge of multiple malicious attacks detection in the network. Intrusion detection was achieved by employing the Hidden Markov model (HMM) as the speech recognition for the modelling of the call events in the system. Again, the

Decision Tree algorithm was also used as the classification model for future intrusions. Moreover, Janakiraman *et al.* [36] presented an IDS and rapid action (INDRA) framework to provide an IDPS which uses peer to peer techniques in a distributed environment to distribute the information of the intruder on the peer to peer network. The approach was to address the challenge faced during packets transmission in the network. To this end, IDPs is achieved via the INDRA which searches for the interruption of the security agent to cut off the packets that are affected. The IDPs is considered reliable and efficiently trustworthy. However, a large amount of data and memory space is required to store the collected malicious information [40, 41].

Laureano *et al.* [38] proposed a HIDS framework using the virtual machine to detect the behaviour of the system inside of the virtual machine. The technique was developed for the efficiency, duplication of the operating system for the intruders and was able to address the intrusion in the network. Moreover, the proposed approach can operate together on the same hardware and is cost-effective. Zhang *et al.* [42] proposed an adaptive IDS scheme that is based on flow count anomaly. It is an efficient detection technique and provides a better balance and monitoring overhead as well as accurate detection. Detection is achieved by changing the granularity and the measurement between the temporal and the spatial dimensions. The mechanism updates the flow counting rules and aggregates the traffic that detects the anomalies and at the same time, reducing the monitoring overhead. However, rules are delegated to control the load of an individual network device (switch) in the entire network. Also, greedy based rules were proposed to reduce the average number that is assigned to each device -switch. In a similar study, Garg *et al.* [43] like in [42] proposed the adaptive flow counting IDS approach for the detection of the anomaly in the SDN. It was designed to address the challenges of network overhead, controller overload policies, etc. In terms of anomaly detection, the IDS framework outperformed other schemes and provide the ability to reduce the complexity by the elimination of the overhead and the setting flags on the data that is aggregated. Moreover, the proposed technique can cover the entries of both small entries and the heavy network.

Ha *et al.* [44] proposed an IDS to detect and prevent malicious traffic in the SDN using a sampling strategy. It employs optimization to determine a suitable sampling rate for each switch to pay attention to suspicious traffics. Traffic flow is sampled based on the optimal sampling rate by quantifying each switch throughput, observed malicious traffic distribution and the information of the flow path by utilizing the functionalities provided by SDN. Traffic is inspected if its sample is less than or equal to the IDS processing capacity, otherwise, the desired sampling rate is applied. Once malicious traffic or behaviour is detected, an alert is sent, and appropriate action is taken to prevent such an attack. To evaluate the performance, simulations and experiments were conducted and results show the approach improves the analysis performance of malicious traffic in large-scale networks. The performance also indicates that the sampling scheme performed better than the naïve scheme. Granby *et al.* [45] developed a platform for detecting an anomaly in the SDN, a software that is a pluggable platform for the detection of an anomaly in the SDN data centre. The SDN-PANDA architecture is made up of the 3 centric controller application modules which are the network monitoring modules, detection module, and response module. Hommes *et al.* [46] presented the framework of the potential of the centralized network monitoring on SDN together with and OpenFlow. The authors stated the weakness of the flow tables, discussed, and showed the consequences for the DoS attacks using a testbed. To achieve intrusion, the authors proposed a framework that can detect and analyse topological variations based on the network service information running on the controller.

Shin *et al.* [47] proposed the security system called FRESCO, a model found between the OpenFlow layer of the application and the controller in the control plane that authorizes and secure the applications development for the network and traffic access. Intrusion is detected by simplifying security application development to spread the intermediate scripting API for secured access to network information. The security system also has a built-in module for the implementation of the security essential functions. In a similar study, Carvalho *et al.* [48] presented an IDS designed to constantly monitor network traffic and detect the anomalies which can impair the proper and function of the network. To achieve intrusion in this study the authors proposed the approach that provides the routine that follows the mitigation of the effect of the anomalies. Carvalho *et al.* [49] also presented an SDN based IDS to monitor network traffic and detects abnormal behaviours that can harm the network. During anomaly detection, the approach performs in-depth analysis by inspecting loopholes at the network traffic level and implement appropriate countermeasures to ensure availability. The centralized monitoring is based on OpenFlow-based SDN and normal profiles are employed to detect traffic patterns as well as invoke mitigation policy. The approach was assessed using a testbed to simulate DDoS and port scan attacks. The results obtained from the experiment show the proposed approach achieved higher detection rates than other approaches and can effectively add to the resiliency of the network. Also, Lee *et al.* [50] presented an IDS technique known as Athena having an interface for development and functions for anomaly detection synthesis. It is a distributed application and is scalable. To achieve intrusion, the authors evaluated the system performance concerning usability, scalability and so in real-world environments.

Peng *et al.* [51] proposed a flow-based IDS for the detection and prevention of malicious traffic flows in the OpenFlow-based SDN. The scheme was designed to address the challenges posed by DDoS attacks in the network using two separate modules called pre-processing, a normalised vector flow feature and anomaly detection. It uses the ML algorithm to compute abnormality and independence of the

TABLE I. SUMMARY OF IDS APPROACHES IN THE SDN BASED ON MACHINE LEARNING

Ref	Challenge	Proposed Solutions	Approach	Implementation Tool	Network	Algorithm
[25]	Malicious, tampering of the important files, and connection of unauthorized	Multiplayer IDPS framework	Signature and anomaly methods	Mininet, Scikit-learn with Python	SDN	SVM, Neural network etc.
[26]	Intrusion attacks on organization networks	IDPS	ML	Python sklearn	SDN controller	Neural networks
[27]	Security vulnerability	Systematic benchmark traffic analysis	ML	Mininet and Python Sklearn	SDN Network	Classical ML algorithms
[28]	Security, potential threats, and flow-based.	A flow-based anomaly detection system	ML	Mininet	SDN controller	Deep Neural Network (DNN)
[29]	Malicious activities in the SDN data plane	Statistics and features of the traffic network	ML	Java library of WEKA	Virtual environment	Naive Bayes, KNN, etc.
[30]	Intrusions, Flow of packets over the network	IDS framework based on Flow-based anomaly	ML	Tensorflow	SDN scenario	K-means clustering algorithm
[31]	Network intrusions	IPS framework	SNORT and Sourcefire	N/A	SDN	N/A
[32]	Intrusions and security of the deployed mobile agent	IDPS Framework	Processing of the logs, detection of attacks etc.	N/A	SDN	N/A
[33]	Intrusions and malicious insertion sequence	IDS Framework	Application and the operating system	N/A	SDN controller or switch	N/A
[34]	Broadcast of the intruder's information	String matching technique	ML	MATLAB 2016a	SDN Application	Deep learning algorithms for feature reduction
[35]	Intrusions and malicious activities	Distributed IDS Framework	SNORT	MySQL	SDN	N/A
[37]	Security of the IDS	Misuse and anomaly detection	Data mining, data fusion etc.	N/A	SDN	N/A
[38]	Intrusions	HIDS framework	Flow based approach	N/A	SDN	N/A
[42]	Balance and monitoring overheads	Adaptive flow counting scheme	Temporal and spatial dimensions	N/A	Developed Testbed	N/A
[52]	Inefficient anomaly detections	Adaptive aggregation of the flow framework	Merging algorithms into a single procedure	BoNeSi (DDoS attack tool)	SDN Topology	Random Forests, Stochastic Gradient Boosting
[44]	Intrusions and malicious traffic	Sampling technique of the traffic	Intrusion Inspection capability	N/A	SDN	N/A
[45]	Detection of anomaly in the SDN data centre	platform for anomaly detection applications (PANDA)	3 centric controller application modules	N/A	SDN	N/A
[46]	Intrusions, DDoS attack	Framework for detection and analysis	Theory of information	N/A	Testbed local topology	l2_learning.py
[47]	The security system	Detection and mitigation framework	FRESCO	Python and runs as an OpenFlow application and C++	SDN environment	TRW-CB
[48]	Security, intrusions, DoS attack attacks	6 flows attribute for real-time detection and mitigation	Ant Colony Optimization for Digital Signature	Scapy	SDN environment	Multi-dimensional flow aggregation
[49]	Security and availability	IDS framework	SDN-based ecosystem	Scapy	SDN with OpenFlow	Round-Robin
[50]	Security monitoring and projects analysis	Integration of anomaly detection development framework	ML Athena	Spiffy	SDN infrastructures	LFA
[51]	Intrusions, malicious packets	IDS based Traffic Classification framework	ML	Mininet	SDN environment	DPTCM-KNN

detection point to classify traffic flow as either normal or anomaly. It operates by exploiting the network statistics available to the controller from the OpenFlow-enable switches at regular intervals. Once the controller gets the important features using the flow table information, it then sends them to IDS for deep inspection by classification using the DPTCM-KNN algorithm. It then generates a report which is sent to the controller for modification of the flow table forwarding rules-based based on the report and send to the OpenFlow switches for appropriate action. Performance evaluation was performed using the RYU controller on Mininet with 11 features. Results showed the approach achieves a higher precision rate and lower FP rate.

B. How do the proposed ML-based work in the SDN landscape?

In this paper, several IDS and IDPs have been reviewed and discussed. Most of the approaches focused on the ML and DL techniques to offer security solutions to the SDN, taking advantage of the SDN functionality such as the OpenFlow, the controller, and the abstract view of the network. The intrusion detection is based on flow-based anomalies.

In this approach, the SDN controller maintains active monitoring of the OpenFlow switches and request for network statistics after a given time interval. This involved send an ofp_flow_stats_reguest [28],[51] message from the controller requesting the network statistics. The OpenFlow enabled switches will then respond to the message by sending an ofp_flow_stats_reply message with the network statistics to the controller. Once received, the controller analyses and correlates the report from the network. All the statistics will then be sent IDS module which is found either in or outside the control plane. The IDS module then analyses the network statistics to detect any real-time malicious behaviour or intrusions using the ML or DL model integrated into it. Once detection and identification of an anomaly have occurred, the OpenFlow protocol will effectively take mitigating action by modifying or updating the flow table. Moreover, new policies are then disseminated to the switches to guard against further attacks in the network.

This operation is common to all the studies or approaches that are based on network flow anomaly detection.

IV. Discussions

Security is one of the greatest challenges confronting the SDN, a new network model introduced to address the challenges of network complexities and inflexibility experienced in the traditional networks. Despite the benefits the network paradigm brought to the network world, it is also being affected by some of the issues it was introduced to address. Though several security measures have been proposed and developed such as the IDS and IPS or IDPS to guard against incessant intrusions and attacks such as the DoS, DDoS attacks, etc., the intrusions and attacks on the SDN, particularly, the controller is yet from being over. Security issues flourish in the SDN because since it was not part of the initial architectural design of the technology. This paper has reviewed and presented the analysis of existing literature on IDS and IPS in the SDN environment. discussed some of the related challenges, issues, proposed solutions and so on that the SDNs experienced. The study identified the different solution strategies, challenges addressed in each case and some research directions. The summary of the analysis is shown in Table I.

The analysis performed revealed that SDN is still faced with different issues such as security, malicious traffic, controller failure, etc. Though security wasn't considered in the initial architectural design of the SDN, the network has excellent functionalities that pave the automation of security measures such as the IDS. Also, the security of the SDN is an active research area and several works have been done in both academia and the industry. Moreover, many security measures have been designed and developed such as the IDS, IPS and the hybrid approach, which is the IDPS using several technics such SNORT, statistical, traffic classification, ML, etc. each having its good sides and drawbacks. In this paper, we focused on the ML-based approaches where models such as DL, SVM, Naïve Bayes, KNN, K-means and so on have been incorporated into various security frameworks individually or hybrid. Moreover, each algorithm was trained and tested on different objectives and parameters to evaluate their performance. Also, several tools were utilized in addition to SDN functionality such as the OpenFlow to achieve intrusion detection and traffic classification via network flow analysis.

In all the techniques adopted for IDS or IDPS, it was revealed that the ML techniques were more effective in the detection of flow-based anomalies and attacks in the SDN environment. Moreover, it makes the routing process more intelligent and independent for traffic classification, prediction, etc. unlike techniques like the SNORT which uses the signature-based failed to detect the anomaly behaviours in the network [33]. This is due to ML/DL algorithms effective performance and detection accuracy but also come with multiple challenges. ML techniques can improve network communication to sustain the network when multiple challenges are encountered and others. Findings prove that ML techniques can be applied to SDNs to improve security, privacy, prediction, etc. ML algorithms should be chosen based on the performance accuracy it brings and the consistency to handle the network management challenges.

V. Opportunities for Research

This section discusses some of the identified research opportunities or directions. Rawat *et al.* [26] recommend continuous real-time model training to be implemented that has better performance rather than training them on static data. Elsayed *et al.* [27] also suggested implementing a DL-based technique with better performance compared to the state-of-the-art ML methods used in their work. For the framework proposed by Jankowski *et al.* [29], further research on traffic monitoring in the SDN control plane is recommended. This involved extending the MADMAS functionality to detect the attacks against the controller. Similarly, the research idea in Satheesh *et al.* [30] can be extended with other ML techniques to assess the quality of the network traffic in the real-world SDN environment. Niyaz *et al.* [53] emphasize the importance of exploring ML techniques for IDS using features extracted

from raw bytes of packet headers rather than feature reduction from the derived features. Tan *et al.* [28] also suggested improved performance of both traffic classification and IDS as well as implementing the number of hidden layers and hidden neurons model on a real-world SDN traffic. Similarly, Tiwari *et al.* [54] reiterated that despite the existence of several ML and DL algorithms, the intrusions challenge in the SDN is far from over. Thus, future work should consider more algorithms to increase the effectiveness, detection efficiency and accuracy against several intrusion attacks. In the same vein, Hande *et al.* [55] stated that to identify, overcome security challenges and achieve distinctive solutions, ML should be explored further to provide programming functionality that allows the organization and management of SDN according to the needs.

Gupta *et al* [56] discussed that with a dynamic change of the network, the IDS can be extended to detect other network attackers such as spoofing, U2R, R2L and others. Also, ML methods can be implemented for extracting features in addition to a good classifier to handle more network data features for large-scale networks. Muhammad *et al.* [57] and Dey *et al.* [58] also suggested for some of the proposed mitigation techniques to be realized and deployed in a real-world network as well as assess their performance on a large-scale network while Polat *et al.* [59] added that application of ML techniques and feature selection methods showed the effectiveness of DDoS attacks detection in the SDN environment and can be a promising reduction in processing load. Chinmay *et al.* [60] stressed that future work should concentrate more on other algorithms and more metrics to increase the efficiency of detection and mitigation of attacks, and the proposed framework should be compared and evaluate for performance. Moreover, Zhu *et al.* [61] expressed that, reducing time consumption when using prediction techniques in the detection of attacks is still an open area to be considered in future work while Latah *et al.* [62] advised that results obtained from the proposed model should be compared with other ML models to enhance the detection rate and other flow-based features.

In [63], Barki *et al.* recommended that due to the dynamic changes in SDNs, the hidden Markov model could be used as an alternative approach to detect DDoS attacks in the SDN settings in future while Le *et al.* [64] expressed the need for testbeds to be expanded and improve further experiments on real-world traffic and other kinds of attack to improve the system should be considered for performance. Similarly, Amara *et al.* [65] recommended that deployment of an unsupervised or semi-supervised method for traffic classification should be accompanied with the right information from a data collection point of views such as user and network use profiles or either traffic predictions to ensure better performance of the SDN. In the same vein, Phan *et al.* [66] suggested the design of some new functional modules to further improve packet processing in their proposed mechanism to detect malicious packets in messages from the data plane and optimize the bandwidth allocation to secure communication channel. In addition, the comparison of their proposed IDS scheme to other ML techniques using more evaluation criteria is still an open challenge.

VI. Conclusion

SDNs is still faced with several challenges such as a collection of information, detection precision, and the inability of the controller to completely defend against the DDoS attacks when the control messages are shared in the network. Thus, SDN has to be protected and monitored for security, privacy etc. at all times. This paper has reviewed and presented several ML-based IDS and IPS security strategies in the SDN. This paper presented some solution approaches, strategies used, tools and research challenges offered in the literature. The findings revealed several IDS strategies in the SDN, the adaptability of SDN functionality for IDS automation, and several attacks that target SDN daily, dominated by DDoS attacks. Moreover, critical analysis shows that the application of the ML techniques for intrusion detection is very effective and each algorithm has advantages and disadvantages due to the nature of the SDN environment. However, intrusion in the SDN is far from over and more techniques need to be explored. In future, the application of ML in SDN for intrusion detection should be considered other algorithms like the DL techniques to improve the performance and detection accuracy. Moreover, in other problems such as controller placements, security should also be considered to achieve a practical solution since most problems in the SDN can't be solved in isolation. Thus, the future work is the incorporation of security in solving a practical controller placement in a large-scale SDN environment.

Acknowledgment

This research was supported by the FRC, MaSIM and the Department of Computer Science at the North-West University Mafikeng Campus, South Africa.

References

[1] K. Scarfone and P. J. N. s. p. Mell, "Guide to intrusion detection and prevention systems (idps)," vol. 800, no. 2007, p. 94, 2007.

[2] Y. F. Jou *et al.*, "Design and implementation of a scalable intrusion detection system for the protection of network infrastructure," in *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00*, 2000, vol. 2: IEEE, pp. 69-83.

[3] E. Y. Chan *et al.*, "IDR: an intrusion detection router for defending against distributed denial-of-service (DDoS) attacks," in *7th International Symposium on Parallel Architectures, Algorithms and Networks, 2004. Proceedings.*, 2004: IEEE, pp. 581-586.

[4] N. Williams, S. Zander, and G. Armitage, "A preliminary performance comparison of five machine learning algorithms for practical IP traffic flow classification," *ACM SIGCOMM Computer Communication Review,* vol. 36, no. 5, pp. 5-16, 2006.

[5] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "Fragmentation-based distributed control system for software-defined wireless sensor networks," *IEEE transactions on industrial informatics,* vol. 15, no. 2, pp. 901-910, 2018.

[6] A. Abubakar and B. Pranggono, "Machine learning-based intrusion detection system for software-defined networks," in *2017 Seventh International Conference on Emerging Security Technologies (EST)*, 2017: IEEE, pp. 138-143.

[7] J. Xie *et al.*, "A survey of machine learning techniques applied to software-defined networking (SDN): Research issues and challenges," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 1, pp. 393-430, 2018.

[8] J. Yan and J. Yuan, "A survey of traffic classification in software-defined networks," in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, 2018: IEEE, pp. 200-206.

[9] T. T. Nguyen and G. Armitage, "A survey of techniques for internet traffic classification using machine learning," *IEEE communications surveys & tutorials,* vol. 10, no. 4, pp. 56-76, 2008.

[10] M. Shafiq, X. Yu, A. A. Laghari, L. Yao, N. K. Karn, and F. Abdessamia, "Network traffic classification techniques and comparative analysis using machine learning algorithms," in *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, 2016: IEEE, pp. 2451-2455.

[11] T. A. Tang, D. McLernon, L. Mhamdi, S. A. R. Zaidi, and M. Ghogho, "Intrusion Detection in SDN-Based Networks: Deep Recurrent Neural Network Approach," in *Deep Learning Applications for Cyber Security*: Springer, 2019, pp. 175-195.

[12] P. Wang, F. Ye, X. Chen, and Y. Qian, "Datanet: Deep learning-based encrypted network traffic classification in sdn home gateway," *IEEE Access,* vol. 6, pp. 55380-55391, 2018.

[13] A. Dawoud, S. Shahristani, and C. Raun, "A deep learning framework to enhance software-defined networks security," in *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 2018: IEEE, pp. 709-714.

[14] S. Vissicchio, L. Vanbever, and O. J. A. S. C. C. R. Bonaventure, "Opportunities and research challenges of hybrid software-defined networks," vol. 44, no. 2, pp. 70-75, 2014.

[15] N. Sultana, N. Chilamkurti, W. Peng, R. J. P.-t.-P. N. Alhadad, and Applications, "Survey on SDN based network intrusion detection system using machine learning approaches," vol. 12, no. 2, pp. 493-501, 2019.

[16] S. Tiwari, V. Pandita, S. Sharma, V. Dhande, and S. Bendale, "Survey On SDN Based Network Intrusion Detection System Using Machine Learning Framework," ed: IRJET, 2019.

[17] M. Uğurlu and İ. A. Doğru, "A Survey on Deep Learning-Based Intrusion Detection System," in *2019 4th International Conference on Computer Science and Engineering (UBMK)*, 2019: IEEE, pp. 223-228.

[18] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, M. Ghogho, and F. J. E. El Moussa, "DeepIDS: deep learning approach for intrusion detection in software-defined networking," vol. 9, no. 9, p. 1533, 2020.

[19] [19] J. Ibrahim and S. J. I. J. Gajin, "SDN-based intrusion detection system," vol. 16, pp. 621-624, 2017.

[20] J. Xie *et al.*, "A survey of machine learning techniques applied to software-defined networking (SDN): Research issues and challenges," vol. 21, no. 1, pp. 393-430, 2018.

[21] T. N. J. a. p. a. Nguyen, "The challenges in SDN/ML-based network security: A survey," 2018.

[22] T. Jafarian, M. Masdari, A. Ghaffari, and K. J. C. C. Majidzadeh, "A survey and classification of the security anomaly detection mechanisms in software-defined networks," vol. 24, no. 2, pp. 1235-1253, 2021.

[23] K. Shingare, R. Nandurkar, P. Shrivastav, and S. Bendale, "A Comprehensive Survey of Intrusion Datasets for SDN and Conventional Networks."

[24] J. C. C. Chica, J. C. Imbachi, J. F. B. J. J. o. N. Vega, and C. Applications, "Security in SDN: A comprehensive survey," vol. 159, p. 102595, 2020.

[25] O. Awodele, S. Idowu, O. Anjorin, V. J. J. I. i. I. S. Joshua, and I. Technology, "A Multi-Layered Approach to the Design of Intelligent Intrusion Detection and Prevention System (IIDPS)," vol. 6, 2009.

[26] S. Rawat and A. J. a. p. a. Srinivasan, "Intrusion detection systems using classical machine learning techniques versus integrated unsupervised feature learning and deep neural network," 2019.

[27] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. J. a. p. a. Jurcut, "Machine-learning techniques for detecting attacks in SDN," 2019.

[28] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software-defined networking," in *2016 international conference on wireless networks and mobile communications (WINCOM)*, 2016: IEEE, pp. 258-263.

[29] D. Jankowski, M. J. I. J. o. E. Amanowicz, and Telecommunications, "On efficiency of selected machine learning algorithms for intrusion detection in software-defined networks," vol. 62, no. 3, pp. 247-252, 2016.

[30] N. Satheesh *et al.*, "Flow-based anomaly intrusion detection using machine learning model with software-defined networking for OpenFlow network," vol. 79, p. 103285, 2020.

[31] M. Guimaraes and M. Murray, "Overview of intrusion detection and intrusion prevention," in *Proceedings of the 5th annual conference on Information security curriculum development*, 2008, pp. 44-46.

[32] A. Shibli and S. Muftic, "Intrusion Detection and Prevention System using Secure Mobile Agents," in *SECRYPT*, 2008, pp. 107-113.

[33] [33] D. Wagner and P. Soto, "Mimicry attacks on host-based intrusion detection systems," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 255-264.

[34] L. Tan and T. Sherwood, "A high throughput string matching architecture for intrusion detection and prevention," in *32nd International Symposium on Computer Architecture (ISCA'05)*, 2005: IEEE, pp. 112-122.

[35] S. Mrdović and E. Zajko, "Secured intrusion detection system infrastructure," 2005.

[36] [36] R. Janakiraman, M. Waldvogel, and Q. Zhang, "Indra: A peer-to-peer approach to network intrusion detection and prevention," in *WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003.*, 2003: IEEE, pp. 226-231.

[37] Y. Bai and H. Kobayashi, "Intrusion detection systems: technology and development," in *17th International Conference on Advanced Information Networking and Applications, 2003. AINA 2003.*, 2003: IEEE, pp. 710-715.

[38] M. Laureano, C. Maziero, and E. J. C. N. Jamhour, "Protecting host-based intrusion detectors through virtual machines," vol. 51, no. 5, pp. 1275-1283, 2007.

[39] S.-J. Han and S.-B. Cho, "Combining multiple host-based detectors using a decision tree," in *Australasian Joint Conference on Artificial Intelligence*, 2003: Springer, pp. 208-220.

[40] M. Mittal, A. Khan, C. J. I. J. o. S. Agrawal, and E. Research, "A Study of Different Intrusion Detection and Prevention System," vol. 4, no. 8, pp. 1526-1531, 2013.

[41] [41] H. El-Taj, F. Najjar, H. Alsenawi, M. J. I. J. o. C. S. Najjar, and I. Security, "Intrusion detection and prevention response based on signature-based and anomaly-based: Investigation study," vol. 10, no. 6, p. 50, 2012.

[42] [42] Y. Zhang, "An adaptive flow counting method for anomaly detection in SDN," in *Proceedings of the ninth ACM conference on Emerging networking experiments and technologies*, 2013, pp. 25-30.

[43] G. Garg and R. Garg, "Security of networks using efficient adaptive flow counting for anomaly detection in SDN," in *Artificial Intelligence and Evolutionary Computations in Engineering Systems*: Springer, 2016, pp. 667-674.

[44] T. Ha *et al.*, "Suspicious traffic sampling for intrusion detection in software-defined networks," vol. 109, pp. 172-182, 2016.

[45] B. R. Granby, B. Askwith, and A. K. Marnerides, "SDN-PANDA: software-defined network platform for anomaly detection applications," in *2015 IEEE 23rd International Conference on Network Protocols (ICNP)*, 2015: IEEE, pp. 463-466.

[46] S. Hommes, R. State, and T. Engel, "Implications and detection of dos attacks in OpenFlow-based networks," in *2014 IEEE Global Communications Conference*, 2014: IEEE, pp. 537-543.

[47] S. W. Shin, P. Porras, V. Yegneswara, M. Fong, G. Gu, and M. Tyson, "Fresco: Modular composable security services for software-defined networks," in *20th Annual Network & Distributed System Security Symposium*, 2013: Ndss.

[48] L. F. Carvalho, G. Fernandes, J. J. Rodrigues, L. S. Mendes, and M. L. Proença, "A novel anomaly detection system to assist network management in SDN environment," in *2017 IEEE International Conference on Communications (ICC)*, 2017: IEEE, pp. 1-6.

[49] L. F. Carvalho, T. Abrão, L. de Souza Mendes, and M. L. J. E. S. w. A. Proença Jr, "An ecosystem for anomaly detection and mitigation in software-defined networking," vol. 104, pp. 121-133, 2018.

[50] S. Lee, J. Kim, S. Shin, P. Porras, and V. Yegneswaran, "Athena: A framework for scalable anomaly detection in software-defined networks," in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2017: IEEE, pp. 249-260.

[51] H. Peng, Z. Sun, X. Zhao, S. Tan, and Z. J. I. A. Sun, "A detection method for anomaly flow in a software-defined network," vol. 6, pp. 27809-27817, 2018.
[52] G. Garg and R. Garg, "Detecting anomalies efficiently in SDN using adaptive mechanism," in *2015 Fifth International Conference on Advanced Computing & Communication Technologies*, 2015: IEEE, pp. 367-370.
[53] Q. Niyaz, W. Sun, and A. Y. Javaid, "A deep learning-based DDoS detection system in software-defined networking (SDN)," *arXiv preprint arXiv:1611.07400,* 2016.
[54] S. Tiwari, V. Pandita, S. Sharma, V. Dhande, and S. Bendale, "Survey on SDN based network intrusion detection system using machine learning framework," 2019.
[55] Y. Hande and A. Muddana, "A Survey on Intrusion Detection System for Software Defined Networks (SDN)," *International Journal of Business Data Communications and Networking (IJBDCN),* vol. 16, no. 1, pp. 28-47, 2020.
[56] S. Sen, K. D. Gupta, and M. M. Ahsan, "Leveraging Machine Learning Approach to Setup Software-Defined Network (SDN) Controller Rules During DDoS Attack," in *Proceedings of International Joint Conference on Computational Intelligence*, 2020: Springer, pp. 49-60.
[57] M. E. Ahmed, H. Kim, and M. Park, "Mitigating DNS query-based DDoS attacks with machine learning on software-defined networking," in *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*, 2017: IEEE, pp. 11-16.
[58] S. K. Dey and M. Rahman, "Effects of Machine Learning Approach in Flow-Based Anomaly Detection on Software-Defined Networking," *Symmetry,* vol. 12, no. 1, p. 7, 2020.
[59] H. Polat, O. Polat, and A. Cetin, "Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models," *Sustainability,* vol. 12, no. 3, p. 1035, 2020.
[60] C. Dharmadhikari, S. Kulkarni, S. Temkar, and S. Bendale, "Comparative Analysis of DDoS Mitigation Algorithms in SDN," *CLIO An Annual Interdisciplinary Journal of History,* vol. 6, no. 4, pp. 169-178, 2020.
[61] L. Zhu, X. Tang, M. Shen, X. Du, and M. Guizani, "Privacy-preserving DDoS attack detection using cross-domain traffic in software-defined networks," *IEEE Journal on Selected Areas in Communications,* vol. 36, no. 3, pp. 628-643, 2018.
[62] M. Latah and L. Toker, "Towards an efficient anomaly-based intrusion detection for software-defined networks," *IET Networks,* vol. 7, no. 6, pp. 453-459, 2018.
[63] L. Barki, A. Shidling, N. Meti, D. Narayan, and M. M. Mulla, "Detection of distributed denial of service attacks in software-defined networks," in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2016: IEEE, pp. 2576-2581.
[64] A. Le, P. Dinh, H. Le, and N. C. Tran, "Flexible network-based intrusion detection and prevention system on software-defined networks," in *2015 International Conference on Advanced Computing and Applications (ACOMP)*, 2015: IEEE, pp. 106-111.
[65] P. Amaral, J. Dinis, P. Pinto, L. Bernardo, J. Tavares, and H. S. Mamede, "Machine learning in software-defined networks: Data collection and traffic classification," in *2016 IEEE 24th International conference on network protocols (ICNP)*, 2016: IEEE, pp. 1-5.
[66] T. V. Phan and M. Park, "Efficient distributed denial-of-service attack defense in SDN-based cloud," *IEEE Access,* vol. 7, pp. 18701-18714, 2019.
[67] B. Isong, R. R. S. Molose, A. M. Abu-Mahfouz and N. Dladlu, "Comprehensive Review of SDN Controller Placement Strategies," in IEEE Access, vol. 8, pp. 170070-170092, 2020, DOI: 10.1109/ACCESS.2020.3023974