



الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of Higher Education and Scientific Research
المدرسة الوطنية العليا للتكنولوجيات المتقدمة
National Higher School of Advanced Technologies



Department of Electrical Engineering And Industrial Computing

Final Year Project to Obtain the Diploma of

Master

-Field -

Communication

-Specialty-

Communications Systems and Networks

- Subject -

Study of Deep Learning-based methods for DDoS attack detection

Realized by

BELOUZ Yacine

BOUBAKEUR Dorsaf

Members of The Jury:

KHOUMERI El Hadi
LAKHDARI Kheira
BENDOUDA Djamila
REBAI Karima
BELAHCENE Abdelkader

President
Examiner
Examiner
Supervisor
Co-Supervisor

Algiers, the 25/06/2024

Academic year 2023–2024

Study of Deep Learning-based Methods for DDoS Attack Detection

Dorsaf BOUBAKEUR

*Electrical Engineering And Industrial Computing
National Higher School of Advanced Technologies
Algiers, Algeria
d_boubakeur@ensta.edu.dz*

Yacine BELOUZ

*Electrical Engineering And Industrial Computing
National Higher School of Advanced Technologies
Algiers, Algeria
y_belouz@ensta.edu.dz*

Abstract—This state-of-the-art provides a comprehensive examination of strategies to enhance the security of Software Defined Networking (SDN) environments, focusing on advanced anomaly detection methods to combat Distributed Denial of Service (DDoS) attacks. Emphasizing the utilization of different Deep Learning (DL) techniques, this paper presents a thorough exploration of frameworks aimed at identifying and mitigating DDoS threats within SDN infrastructures. We propose three different faceted taxonomies to delve into DDoS attack types, explore DL-based approaches for DDoS detection, and examine the available tools (software tools and datasets) that can be exploited for improving the detection of this type of attacks.

Index Terms—Software Defined Networking (SDN), Distributed Denial of Service (DDoS), Deep Learning (DL), Hybrid Model, Intrusion Detection System (IDS).

I. INTRODUCTION

SDN offers a novel network architecture by decoupling the control plane from the data plane, allowing centralized network management and programming [18]. Its architecture is divided into three layers as illustrated in figure 1.

Specifically, the Application Layer hosts various network applications and services. The Control Layer, featuring a centralized controller, manages the network, monitors devices through secure OpenFlow channels, configures flow tables, and serves as a mediator between the data plane and application plane using southbound and northbound APIs [26]. The Infrastructure Layer includes physical devices like switches and routers.

While SDN enhances agility, scalability, and flexibility, it also introduces security risks due to the centralization of the control function, making it vulnerable to attacks like DDoS [26]. DDoS attacks, executed using botnets, overwhelm the SDN controller with excessive traffic, straining its resources and preventing it from functioning properly [13, 14, 21]. Hence, detecting and preventing these attacks is crucial for network service providers.

The SDN controller currently lacks a robust integrated security defense system to distinguish between normal and malicious traffic. Various researchers have proposed machine learning solutions to detect and mitigate DDoS attacks, but these methods face challenges such as expensive feature en-

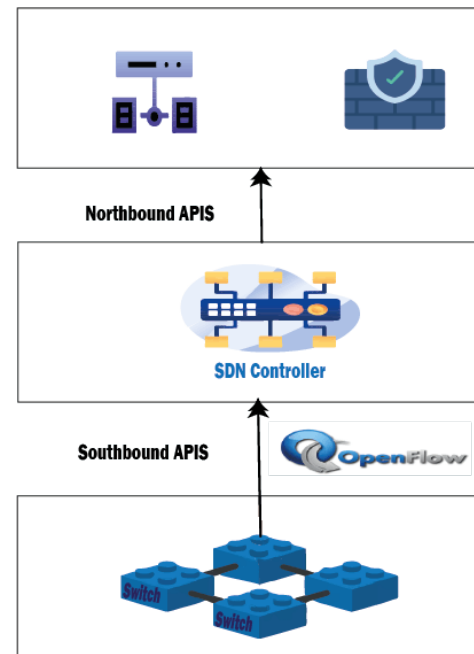


Fig. 1. SDN Layers

gineering and performance issues due to unqualified features, unrealistic datasets, or inappropriate algorithms [24].

DL-based Intrusion Detection Systems (IDSs) in SDN networks, utilizing methods like Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short Term Memory (LSTM), have been explored to address these threats [11]. This paper reviews and analyzes the literature on DDoS attacks detection, focusing on DL-based approaches.

The rest of this paper is organized as follows: Section 2 provides a background on DDoS attack types. Section 3 introduces DL-based approaches for DDoS attack detection. Section 4 highlights the tools used to develop IDSs. Section 5 compares the performance of various DL-based approaches. Finally, the study concludes in Section 6.

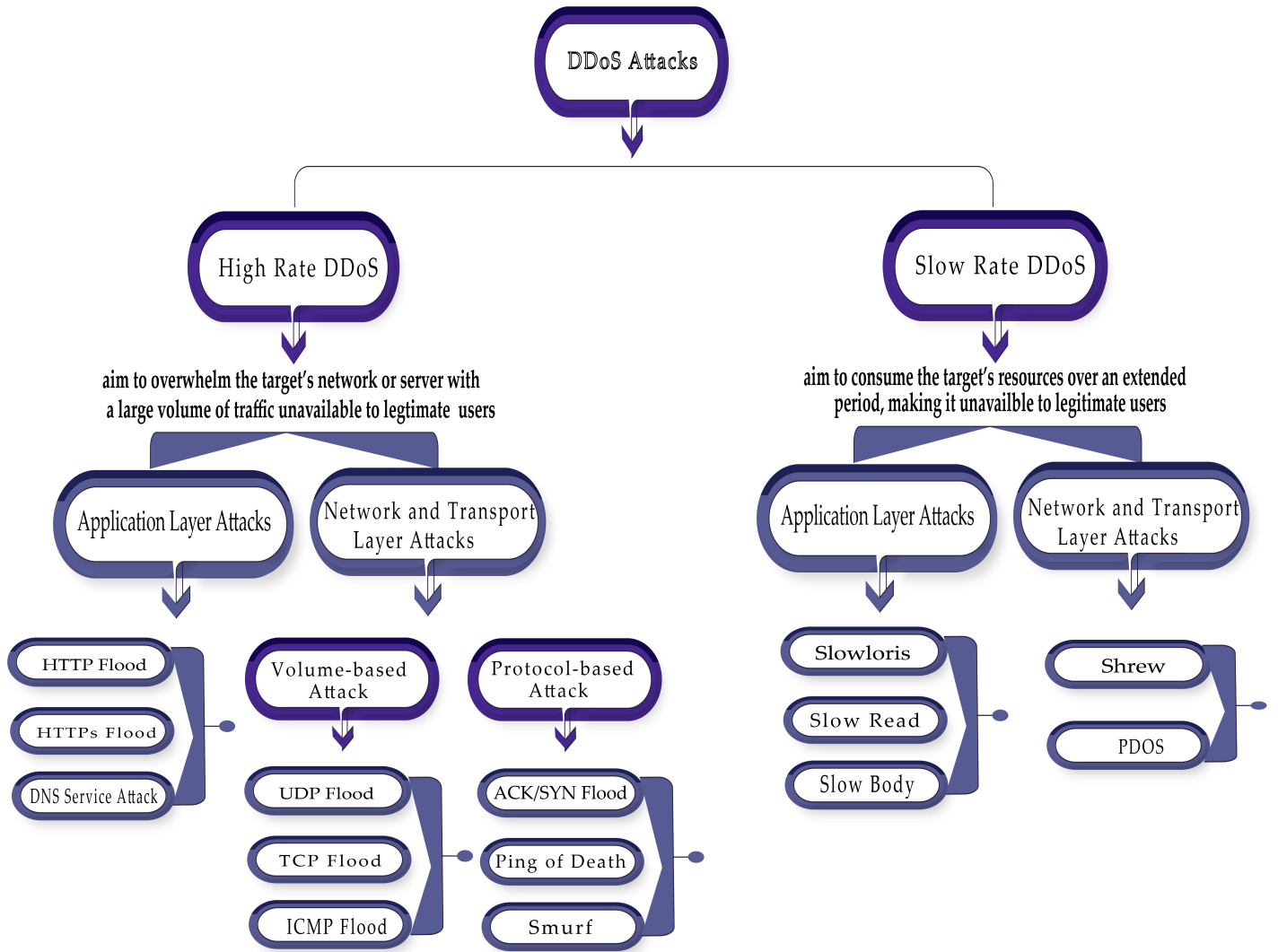


Fig. 2. DDoS Attack Types.

II. DDoS ATTACK TYPES

Each DDoS attack type targets a specific layer of the Internet's network stack. Taxonomy 2 illustrates several common DDoS attacks affecting different levels.

The high-rate DDoS attacks are aimed at flooding the victim server or machine with a large amount of traffic in a short period of time. The attack traffic is typically generated by the use of numerous compromised machines, known as botnets [5]. Over the past decade, numerous classification strategies for DDoS attacks have emerged in the literature. However, significant attention has been given to the study of DDoS flooding attacks, which have been categorized into two distinct groups based on the targeted protocol level: Application Layer Attacks and Network-Transport Layers Attacks.

Application Layer Attacks exploit the configurations and functionalities of protocols and services at the application

layer. These attacks aim to make applications unavailable to legitimate users, examples include DNS attacks, HTTP-GET, and HTTPs floods, among others [30]. These assaults typically target vulnerabilities specific to the software or services being used, aiming to disrupt their normal functioning. In the other hand, the Network-Transport Layers Attacks known as Infrastructure Layer Attacks, aim to disrupt data transmission and routing. On the network layer, these attacks consume bandwidth to suspend the service. While attacks on the transport layer disrupt data transfer and its integrity. These assaults exploit vulnerabilities in protocols like TCP and UDP, posing significant threats to network reliability and security in SDN environments [10, 35]. Volumetric DDoS attacks represent a big threat to network stability and security, several attackers coordinate the sending of high rate useless data across various protocols. Rather than exploiting specific protocol flaws, their goal is to saturate network bandwidth and exhaust the victim's computing resources or nearby

network links [25]. As shown in figure 2, the most relevant volumetric based attacks are TCP SYN, UDP flood, and ICMP attacks. There are also other attacks which use protocols from these layers [32, 33]. Specifically, protocol based attacks exploit weaknesses within various protocols, examples of such attacks include SYN/ACK flood and Smurf DDoS attacks, as well as notorious techniques like the Ping of Death.

Meanwhile, low-volume attacks also known as slow-rate DDoS attacks embrace the use of seemingly legitimate traffic at a slow pace. They unfold swiftly, often lasting few minutes and rarely exceeding an hour. Consequently, security teams are often unaware that their sites are under attack, as common tools fail to detect this type of threat [25]. Additionally, this type of attacks usually employs application layer protocols to overwhelm servers, with a particular focus on HTTP. The slow HTTP attack on the web server can occur in three distinct formats: Slowloris (Slow HTTP Header Attacks), Slow Post (RUDY), and Slow Read (Slow HTTP Read Attacks) [16]. Slowloris sends partial HTTP requests with incomplete HTTP header to the server and then periodically sends additional HTTP headers, keeping the connection open. RUDY operates by sending HTTP POST requests containing very small content sizes, often ranging from one to a few bytes, spaced out by slow intervals of time. As a result, the web server is forced to wait an extended period to receive the complete POST request. For Slow Read, the attacker sends a valid header and GET request to the web server but intentionally delays reading the response from the server. Another type of slow attacks that disrupts the functionality of the network is known as Shrew. It capitalizes on exposures within the TCP protocol. This attack involves sending small bursts of network traffic, which despite their size, are effective in incapacitating a host. PDOS (Permanent Denial of Service) entails denial of service through hardware sabotage. Such an approach exploits weaknesses by replacing a device's fundamental software with a corrupt firmware image. Unlike high-rate DDoS attacks, slow-rate DDoS attacks imitate genuine traffic and do not necessitate extensive resources to be executed, they can be initiated using only one machine. These differences make these attacks more complex and hard to detect [33].

III. DL-BASED APPROACHES FOR DDOS ATTACKS DETECTION

As emerging wireless networks like the Internet of Things (IoT) and 5G become increasingly prevalent, SDNs face heightened vulnerability to cyber threats. Among these threats, DDoS attacks stand out as particularly prevalent and influential.

After carefully analyzing the latest advancements in intrusion detection and SDN research, it is clear that using Machine Learning (ML) techniques offers strong potential for effectively detecting anomalies [8]. More importantly, DL

algorithms have been widely used recently to develop IDSs in SDN environments and shown high efficiency spotting DDoS attacks, various DL-based approaches were established to limit the threats of these attacks. Notably, the proposed approaches for DDoS attacks detection using DL techniques can be divided into several categories, including single, ensemble and hybrid models as illustrated in figure 3.

A. Single Model

Single model approaches use only one DL-based method for detection. Notably, some initiatives leverage SDN technology [22, 31, 34], which show considerable promise in effectively combating such threats. However, Yungaicela-Naula et al. [33] contend that integrating these solutions into real networks could be unfeasible or ineffective due to the use of unrealistic datasets, and the lack of experimental facilities or a physical network to test the proposed solutions in real scenarios. In [33], an automated security framework was defined, utilizing hardware components. This framework was employed to construct and assess an IDS built upon the SDN-SlowRate-DDoS dataset. This dataset, acquired from an SDN-based testbed, comprises contemporary DDoS attack instances. It was used for training and evaluating an LSTM based model. Various experiments were conducted to analyze different combinations of attackers and victims, an average accuracy of 87.535% and an average False Positive Rate (FPR) of 13.352% were revealed.

Mansoor et al. [26] proposed an approach called DLADSC with three stages: data preprocessing that prepares input data for further analysis by applying necessary transformations and normalization techniques, cross-feature selection where the most relevant and informative features to detect DDoS attacks on the SDN controller are identified, and detection using the Recurrent Neural Networks (RNNs) model. A benchmark dataset [7] was employed to train and evaluate the proposed approach using only five features, selected as the top-ranked ones through both Information Gain Ratio (IGR) and Chi-square cross-feature selection mechanisms. This dataset was specifically generated on a testbed comprising 10 mininet topologies, where switches are connected to a single Ryu controller, it was created through network simulations that included both benign traffic (TCP, UDP, and ICMP) and various types of malicious traffic, such as TCP Syn, ICMP, and UDP flood attacks. DLADSC detected effectively DDoS attacks with average detection accuracy, average precision, average FPR and average F1-measure of 94.186%, 92.146%, 8.114%, and 94.276%, respectively.

Liang et al. [24] utilized an LSTM-based approach for slow-rate DDoS attack detection, the proposed scheme only uses packet header information as input and does not require feature engineering, trained and tested using the CICIDS2017 dataset [28] that includes the slow body, slow header, and DoS Get attacks. The training process was accomplished using 15 flow parameters, the proposed model was compared with

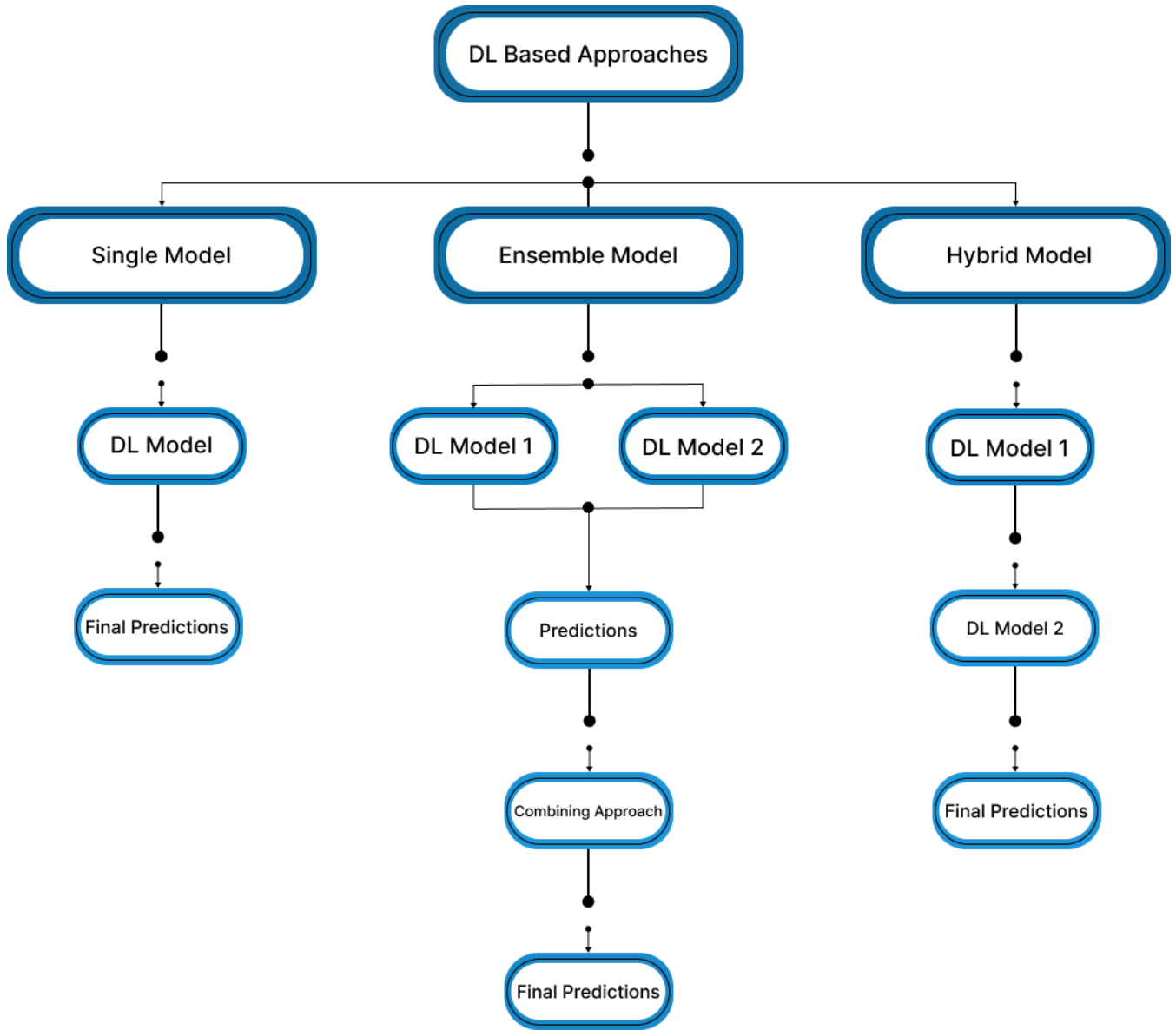


Fig. 3. Deep Learning Approaches.

the Decision Tree, ANN, and SVM methods. During training, the model exhibited performance metrics surpassing 99% for recall, precision, and F1 scores respectively. This approach took in consideration the real-world detection scenario where the attack is usually under-represented, if not un-represented at all in the available training data. Therefore, the model was tested on a different dataset which reduced the precision, recall, and F1 score to 70%, 80%, and 80%, respectively. This work [9] introduced the ONOS Flood Defender (OFD) application, that is designed to detect and mitigate DDoS attacks using five ML algorithms namely XGBoost, MLP, AdaBoost, Gradient Boost, and Random Forest. These models were trained and tested by the use of four benchmark datasets: CIC-DoS 2017, CIC-IDS 2018 [28], CIC-DDoS 2019 [29] and InSDN [17], each dataset contains approximately 84 features

generated by the CICFlowMeter tool in CSV format. Specifically, feature selection methods such as BORUTA, IRelief, Random Forest, Information Gain, and Chi-Square Test were utilized to identify the most relevant features encompassed in the datasets for DDoS detection, each technique selected the top 10 features from each dataset, and by taking in consideration the features chosen by each one of them, a final set of 10 common features was determined for each dataset. Additionally, six manually extracted statistical features were selected, resulting in a total of 16 features used to train and test the ML models with the ten-fold cross-validation technique. The application showed high effectiveness by detecting DDoS attack traffic using XGBoost and Multilayer Perceptron algorithms with accuracy of 99% and minimal testing times, the attacks were mitigated effectively by creating flow rules

to block assault packets in approximately 3.2 seconds.

B. Ensemble Model

An ensemble model approach combines predictions from multiple DL models to improve accuracy and robustness. Techniques like average voting aggregate the predictions of each model, taking the average of their outputs to produce a final prediction. This method leverages the strengths of each individual model, reducing the impact of any single model's weaknesses.

Shahzeb Haider et al. [20] proposed a deep CNN Ensemble mechanism for detecting DDoS attacks in SDNs. This approach, utilizing an Ensemble CNN, was compared with state-of-the-art DL based ensembles and hybrid methods, including Ensemble RNN, Ensemble LSTM, and Hybrid-Ensemble RL (RNN and LSTM). These methods combined similar or complementary DL models to create a new ensemble model for the detection task.

Each DL architecture was evaluated using the CICIDS2017 benchmark dataset, with the top features selected via RandomForestRegressor. Four features were specifically chosen for DDoS attack detection. All approaches demonstrated high efficiency, achieving accuracy, precision, recall, and F1 score above 98% and exhibiting a low FPR below 0.05%. However, the proposed CNN Ensemble method outperformed the others, achieving a detection accuracy of 99.45% and minimal computational complexity.

Fatmah Alanazi et al. [8] constructed an ensemble model that can be integrated with any commercial SDN controller. Thus, there were four models proposed by the authors as shown in table I. Model A and B built by using three base learners, and three methods were used to combine their predictions: average voting, majority voting, and optimal weights. On the other hand, Model C and D built by using two base learners and applied average voting and optimal weights to predict the final output.

TABLE I
THE PROPOSED ENSEMBLE MODELS.

Model	Construction
A	1D CNN, 2D CNN, LSTM
B	1D CNN, 2D CNN, GRU
C	1D CNN, 2D CNN
D	LSTM, GRU

These models were evaluated using CICIDS2017 dataset [28] by only four features which resulted in a very high accuracy above 98% for all the models. Also, the method of average voting revealed better results compared to the majority voting and optimal weights methods. The proposed models were compared to the single models: 1D CNN, 2D CNN, LSTM and GRU. As the results have shown, the ensemble models are more effective than the single ones. Plus, the model C gave the best results among all the other three proposed DL approaches and single models.

The approach C was compared with other competing ensemble approaches and it achieved better accuracy than all of the previous methods that used the same dataset for evaluation. The proposed ensemble CNN achieved better accuracy than the ensemble CNN in [19] and [20], that used two similar CNN models. Compared to them the accuracy was increased to 99.77% and the FPR was reduced to 0.0009% using the same dataset and number of features.

C. Hybrid Model

Hybrid models combine two DL classifiers within a single architecture, with one classifier layered on top of the other. This setup allows the first classifier to process input data and pass its output to the second classifier for further refinement, enhancing the overall predictive performance by leveraging the strengths of both models.

Yungaicela-Naula et al. [27] implemented a DL-based slow DDoS attack detection approach that operates in SDN environments, using a hybrid CNN-LSTM model. The proposed method aimed to enhance the performance compared to each separate DL model in the ensemble DL models [8].

The proposed architecture consists of three modules: flow collector, feature extractor and calculator, and DL-based detector. The utilized dataset was created by generating benign traffic using hping3 and attack traffic flows using several open-source slow DDoS attack tools for an emulated SDN-based network. 12 features were considered for training and evaluating this model. After testing and evaluating the performance of the hybrid approach, the authors compared it with MLP and 1-Class SVM models. The hybrid CNN-LSTM model surpassed both of them in term of performance by achieving over 99% of accuracy, precision, recall, and F1 score.

Yungaicela-Naula et al. [34] worked on creating a solution to detect two types of DDoS attacks: Transport Layer DDoS Attacks and Application Layer DoS/DDoS Attacks by using different Artificial Intelligence (AI) methods. The ML detection techniques used in this study are Support Vector Machine (SVM), Random Forest (RF) and K-Nearest Neighbors (KNN). Four DL mechanisms were employed as well, namely, MLP, CNN, Gated Recurrent Units (GRUs), and LSTM. For training these models in a real testbed, the authors proposed two up to date datasets: the CICIDS2017 [28] and CICDDoS2019 [29].

The SVM and CNN models are excluded from the testbed-based models assessment since these methods presented the worst FPRs after comparing different performance metrics for each method using both datasets. Finally, to test this approach, different online free tools were used to generate traffic. The generated traffic was composed of various attack rates: low, medium and high to evaluate the intelligent classification mechanisms at different rates.

TABLE II
MODELS RANKING FOR TESTBED-BASED EVALUATION [34].

Rank	SYN	UDP	DrDNS	Slow Body	Slow read	Slow Header
1	GRU	RF	GRU	GRU	LSTM	GRU
2	KNN	GRU	KNN	KNN	GRU	MLP
3	LSTM	LSTM	RF	LSTM	KNN	LSTM

The table II presents the top three models ranked according to their detection rates and FPRs across various attacks assessed in the testbed. Both of the GRU and LSTM models demonstrated effectiveness in handling both high volume and low-volume attacks under different conditions. These models achieved high detection rates, up to 95% for slow rate attacks and above 98% for high volume attacks, indicating their robustness and reliability compared to other methods.

IV. USED TOOLS

The figure 4 provides an overview of different tools that can be used for the development of DDoS attack detection methods. It encompasses software tools for SDN emulation and control, DDoS attack generation tools to test IDSs and create datasets, and available datasets that can be exploited for training and evaluating the proposed solutions.

A. Software Tools

In the architecture of SDN-based approaches, the utilization of network emulators plays a crucial role in testing and validating the IDSs functionality. Two popular choices for network emulation are Mininet and GNS3. Specifically, Mininet is a powerful tool known for its simplicity and ease of use. It allows users to create virtual networks quickly, replicating complex network topologies on a single machine [4]. On the other hand, GNS3 tends to be more resource-intensive and complex to set up. Once the network topology is established using Mininet or GNS3, the next step involves connecting the emulator to an SDN controller. These controllers serve as the brain of the network, various types of SDN controllers exist, each possessing distinct characteristics and capabilities. Open Network Operating System (ONOS) is renowned for its scalability and robustness, rendering it suitable for expansive SDN deployments [35]. OpenDayLight (ODL) is another widely adopted controller, boasts a modular architecture and comprehensive support for diverse protocols and southbound APIs [1]. Additionally, Ryu is a lightweight controller with a focus on simplicity and ease of development, making it ideal for small-scale SDN applications and research projects [2]. By connecting a network emulator to one of these SDN controllers, it would be possible to effectively simulate and evaluate the performance of SDN-based approaches in a controlled environment.

B. DDoS Generation Tools

DDoS generation tools are software applications designed to simulate DDoS attacks against systems or servers. These tools are specifically tailored to test the resilience and effectiveness

of trained models under high-stress conditions, replicating real-world DDoS attack scenarios. By generating controlled and scalable traffic patterns, they enable cybersecurity professionals to evaluate their models performance in detecting and mitigating DDoS threats in real-time. Numerous tools are available that can produce both legitimate-looking traffic and attack traffic, capable of bypassing existing DDoS defense solutions [12].

- **hping3** :It is a Multi-purpose network tool, that is used for generating and analyzing TCP/IP packets. It can handle random packet sizes and fragmentation, making it ideal for stress testing and security audits. hping3 is capable of firewall rule testing, and protocol-based network performance testing. Through a command-line interface, it can simulate high-rate DDoS attacks, providing a powerful tool for cybersecurity professionals to simulate network traffic under various conditions.
- **Iperf** :This multi-threaded generator allows client-server configurations to have multiple connections, making it ideal for active measurements of maximum achievable bandwidth on IP networks. It is a Java-based traffic generator that can produce both legitimate and attack traffic at the network and application layers to assess the maximum achievable bandwidth [12].
- **SlowHTTPTest** :It is a highly configurable tool designed to simulate Slow Application Layer DDoS attacks by prolonging HTTP connections in various ways. This allows cybersecurity professionals to test and evaluate the resilience of web servers and applications against these types of slow attacks [3].

C. Datasets

The DL models are trained on diverse datasets to comprehend patterns and relationships within the data. Subsequently, it undergoes testing on distinct datasets to assess their performance. Multiple publicly accessible datasets are employed to gauge the DL models efficacy [21] such as the ones cited in the table III. The CIC-DDoS2019 dataset contains benign traffic and the most up-to-date common attacks, it is separated into two days, one for training and other for testing. The training day contains 12 different types of DDoS attacks, including DNS, MSSQL, and Syn. Besides, the testing day encompasses six distinct types of DDoS attacks: Syn, UDP, NetBIOS, LDAP, UDP-Lag, and MSSQL [9]. The CICIDS2017, in the other hand, is widely used to train and evaluate different SDN testbeds [24, 28, 34]. It contains realistic background network traffic and a variety of attack traffic. This dataset covers five days of network traffic, two of which encompass DoS and DDoS attacks [24]. Specifically, it includes six application-layer DoS/DDoS attacks: slow-send body, slow-send header, slow read, DoS HTTP Get flooding, improved DoS HTTP Get flooding, and DDoS HTTP Get flooding. SDN Slow-Rate DDoS is a realistic dataset presented in [26], not available online. Given the availability of real data for training, alternative resources opt for simulated datasets that encompass all needed

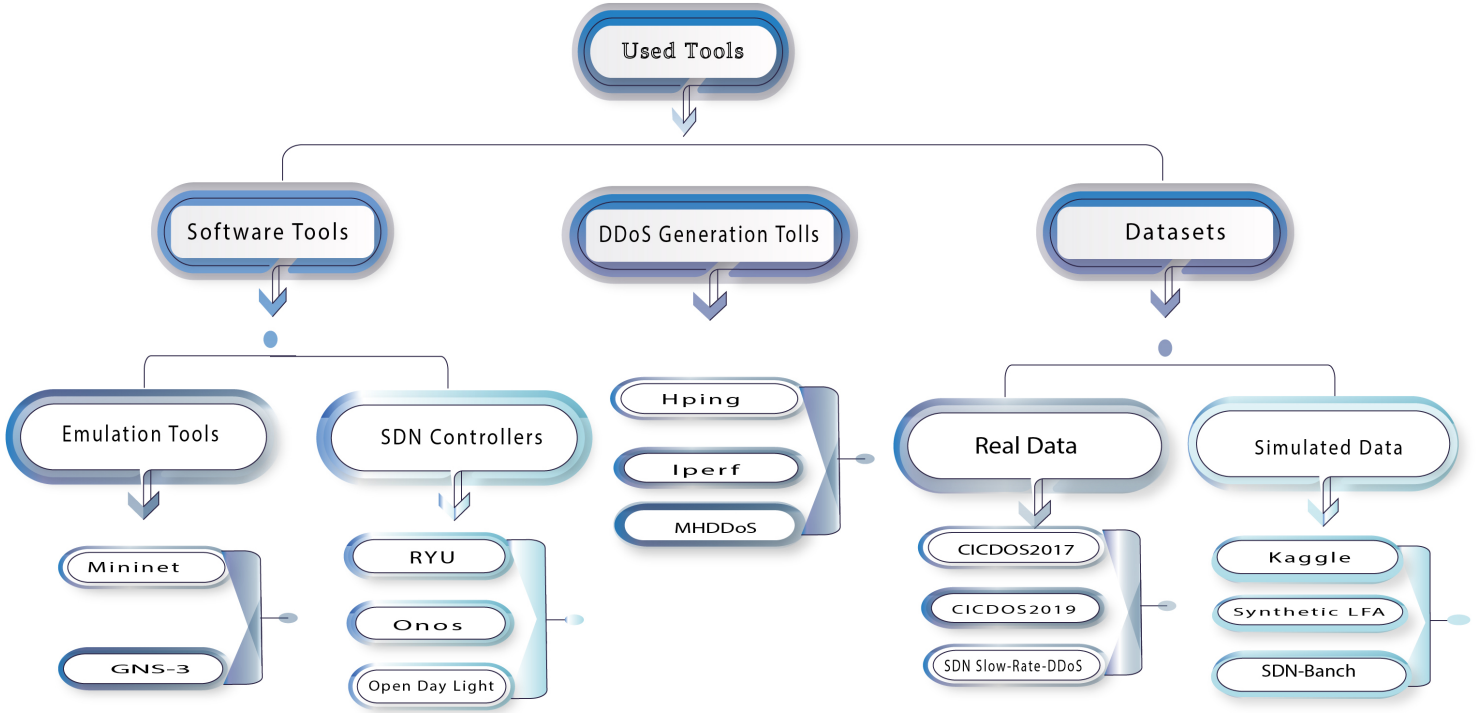


Fig. 4. Used Tools.

features. These include platforms like Synthetic LFA [22], and SDN-ben [7].

TABLE III
THE DATASETS USED IN THE PROPOSED MODELS.

Dataset	Type	SDN	Real/Simulated
CICDDoS2019	HR DDoS		Real
CIC-IDS 2018 [28]	DDoS		Real
CICDDoS2017	SR DDoS		Real
SDN-SlowRate-DDoS	SR DDoS	✓	Real
Benchmark Dataset	HR DDoS	✓	Simulated
Generated Dataset	SR DDoS	✓	Simulated
N-Balot	HR DDoS		Real
InSDN [17]	DDoS	✓	Simulated

V. PERFORMANCE ANALYSIS

A. Evaluation Metrics

Evaluation metrics serve as tools to assess the effectiveness and efficiency of a model's performance. Specifically, in the context of the suggested DDoS attacks detection model, these metrics play a crucial role in determining the model's accuracy, reliability, and ability to detect and mitigate DDoS attacks [21]. A confusion matrix illustrates the number of correct and incorrect predictions generated by the model in comparison to the actual outcomes (or true labels) within the test data [15]. Typically presented as a square matrix, it features rows depicting the actual class labels and columns representing the predicted class labels. In a binary classification scenario, there are four potential outcomes: True Positives (TP), False

Positives (FP), True Negatives (TN), and False Negatives (FN) as illustrated in IV.

TABLE IV
CONFUSION MATRIX METRICS. [21].

Actual Annotation	Predicted Annotation	
	Positive	Negative
Positive	TP	FN
Negative	FP	TN

The two fundamental metrics used for measuring the performance of a retrieval system are precision and Recall. Precision measures the number of correct instances retrieved divided by all retrieved instances.

$$Precision : P = \frac{TP}{TP + FP}$$

Recall measures the number of correct instances retrieved divided by all correct instances. It evaluates the model's accuracy in identifying the fraction of positive cases that are actually positive.

$$Recall : R = \frac{TP}{TP + FN}$$

Another important metric is F1-score which represents the harmonic mean of precision and recall.

$$F1 - score : F = 2 * \frac{P * R}{P + R}$$

Accuracy is another measurement defined as the proportion of true instances retrieved, both positive and negative, among

all instances retrieved. It evaluates the model's performance in terms of effectively detecting instances.

$$Accuracy : A = \frac{TP + TN}{TP + TN + FP + FN}$$

B. Performance Evaluation

In the preceding section, various IDSs were developed by employing optimal DL methodologies, subsequently evaluated in term of performance by choosing a real updated dataset that provides all the training requirements for crafting an effective IDS. Consequently, the careful selection of the most suitable model is paramount prior to initiate the construction of any system.

The performance evaluation of each approach, including single models, ensemble models, and hybrid models, is highlighted in tables V, VI, and VII, respectively. Specifically, performance metrics such as accuracy, precision, recall, F1-score, and FPR were employed to measure the performance. Interestingly, each table is categorized based on the datasets used in the proposed approaches.

Table V delves into the performance evaluation of the proposed single models, where the CICDoS 2017 dataset [28] was employed to train and test five models including two LSTM, CNN, MLP and GRU based frameworks. The LSTM approaches stand out for achieving the highest performance metrics and the lowest FPR. On the other hand, MLP, CNN, and GRU based approaches have also attained high performance. However, MLP approach got the lowest accuracy among the remaining two algorithms, even though it had a lower FPR compared to the CNN model. Also, CICDDoS 2019 dataset [29] was used in four DL based solutions namely CNN, MLP, GRU and LSTM. All the proposed approaches showed high performance exceeding 99% of accuracy, precision, recall, and F1-score. But, they achieved a high FPR above 1%. Notably, the MLP based framework showed the lowest FPR relatively with 1.503%.

Moreover, an LSTM based approach was proposed using SDN-Slow Rate-DDoS dataset [33]. Even though the employed dataset is based on various experiments of slow-rate DDoS attacks conducted on a real testbed, the proposed solution showed poor performance with an accuracy of 87.535% and FPR of 13.352%. Moreover, an RNN based framework was introduced with the use of Benchmark dataset [7] that is produced on a testbed based on Mininet tool, this approach achieved relatively low performance and high FPR of 8.114%. In the case of the ONOS Flood Defender (OFD) application, the MLP based approach exhibits the shortest testing time for the CIC-DDoS 2019 and InSDN datasets. Conversely, XGBoost demonstrates the minimum testing time for the CIC-DoS 2017 and CIC-IDS 2018 datasets. This illustrates that MLP and XGBoost outperform other classifiers in speed of testing unknown data for DDoS attacks detection. Additionally, the XGBoost classifier achieved the highest accuracy across all four datasets.

In the context of ensemble models, table VI provides a summary of the outcomes resulting from merging predictions generated by different DL Models: 1D-CNN, 2D-CNN, LSTM, and GRU [8]. This study devised four distinct combinations of these models, as detailed in I. To combine the individual predictions of these classifiers into a unified model, two conditions were established. If the ensemble comprised only two models, two methods were employed for combining their predictions namely average voting and optimal weights. For ensembles consisting of three models, majority voting was introduced in addition to the previous two methods. The four ensemble models perform well for all the evaluation metrics. The accuracy was very high, and for all the models, it exceeded 98%, meaning they correctly classified almost 98% of all the observations in the test data. Also, the precision score for models A and C hovered around 98%, indicating that out of all the normal occurrences predicted by the model, 98% were accurately classified. However, 2% of the predictions were incorrectly identified as attack events. Finally, the model C that combines two classifiers based on 1D CNN and 2D CNN, exhibited the highest performance metrics with an accuracy of 99.77 %, along with an impressively low FPR of 0.0009. Compared with other single and ensemble models. It succeeded to attend the lowest FPR, which is a very sensitive metric in evaluating the performance of classification models. Additionally, the CICDoS2017 dataset in [8] played a crucial role in enabling this model to accurately detect slow DDoS attacks, and the results showed that this ensemble improved generalization performance, by aggregating predictions from 1D CNN and 2D CNN models that are trained on different subsets of the data. It helped to capture a broader range of patterns and features, resulting in enhanced overall performance on unseen data which reduced the FPR.

Regarding hybrid models, table VII highlights the performance results of the hybrid approaches. The CNN-LSTM model [27] that utilized Generated Dataset [27] for training and testing achieved remarkable high performance metrics exceeding 99%. Also, N-BaIoT dataset [6] that encompasses IIoT (Industrial Internet of Things) supportive features, gathered from IoT devices infected by the most perilous malwares namely Mirai and BASHLITE, was employed to train and test three hybrid DL models namely Cu-LSTMGRU+Cu-BLSTM, Cu-DNN-GRU, and Cu-DNN-LSTM [23]. The three approaches have proven their effectiveness with high performance metrics, although, Cu-LSTMGRU+Cu-BLSTM framework outperformed the other ones with an accuracy, precision, F1-score, recall, and FPR of 99.45%, 99.34%, 99.47%, 98.49%, and 0.003%, respectively.

After extensive analysis and study of the previous research, we have arrived at a conclusion that the top three DL models which form the foundation of a robust IDS are: LSTM as a standalone model, 1D CNN and 2D CNN as an ensemble model, and CNN-LSTM as a hybrid model. These approaches have demonstrated the ability to achieve the highest metric performance results, including accuracy, precision, recall, F1 score, and FPR, surpassing other models utilized in the study.

TABLE V
EVALUATION METRICS FOR EACH DATASET USED IN DL SINGLE ALGORITHMS.

Dataset	Method	Accuracy	Precision	F1-Score	Recall	FPR
CICDos 2017 [28]	LSTM [24]	-	99.9%	99.9%	99.9%	-
	CNN [34]	98.881%	98.886%	98.883%	98.881%	0.974%
	MLP [34]	98.133%	98.127%	98.124%	98.133%	0.772%
	GRU [34]	99.427%	99.432%	99.428%	99.427%	0.594%
	LSTM [34]	99.473%	99.474%	99.473%	99.473%	0.389%
	MLP [9]	98.3%	97.8%	89.5%	96.0%	-
	XGBoost [9]	99.8%	99.2%	99.7%	98.5%	-
	AdaBoost [9]	97.3%	98.1%	99.0%	99.5%	-
	Random forest [9]	98.1%	97.8%	96.3%	97.4%	-
	Gradient boost [9]	98.2%	97.1%	97.5%	96.2%	-
CIC-IDS 2018 [28]	MLP [9]	98.5%	97.4%	98.5%	96.3%	-
	XGBoost [9]	99.7%	99.2%	98.5%	98.9%	-
	AdaBoost [9]	99.2%	98.7%	98.5%	98.3%	-
	Random forest [9]	99.0%	98.2%	98.4%	98.5%	-
	Gradient boost [9]	98.7%	98.6%	98.1%	98.4%	-
InSDN [17]	MLP [9]	99.1%	98.9%	98.7%	97.6%	-
	XGBoost [9]	99.9%	99.0%	99.7%	99.4%	-
	AdaBoost [9]	99.6%	98.6%	97.1%	98.4%	-
	Random forest [9]	98.5%	98.4%	98.6%	97.2%	-
	Gradient boost [9]	98.6%	97.2%	97.0%	97.5%	-
CICDDoS 2019 [29]	CNN [34]	99.130%	99.335%	99.194%	99.130%	4.392%
	MLP [34]	99.897%	99.899%	99.898%	99.897%	1.503%
	GRU [34]	99.808%	99.873%	99.872%	99.8873%	4.454%
	LSTM [34]	99.877%	99.879%	99.878%	99.877%	1.571%
	MLP [9]	97.2%	96.3%	95.3%	97.0%	-
	XGBoost [9]	99.5%	99.6%	98.2%	98.7%	-
	AdaBoost [9]	98.8%	98.4%	98.3%	98.6%	-
	Random forest [9]	99.1%	98.5%	98.7%	98.4%	-
	Gradient boost [9]	99.2%	98.7%	98.0%	98.2%	-
SDN-SlowRate-DDos [33]	LSTM [33]	87.535%	-	-	-	13.352%
Benchmark Dataset [7]	RNN [26]	94.186%	92.146%	94.276%	-	8.114%

TABLE VI
EVALUATION METRICS FOR EACH DATASET USED IN DL ENSEMBLE MODELS.

Dataset	Ensemble models	Accuracy	Precision	F1-Score	Recall	FPR
CICDos 2017 [28]	1D CNN, 2D CNN, LSTM [8]	99.7%	98%	98%	97%	0.0012%
	1D CNN, 2D CNN, GRU [8]	99.69%	97%	97%	96%	0.0016%
	1D CNN, 2D CNN [8]	99.77%	98%	98%	97%	0.0009%
	LSTM, GRU [8]	98.73%	94%	89%	82%	0.0027%
	Hybrid-Ensemble RL [20]	98.75%	98.98%	99.11%	99.25%	0.025%
	Ensemble LSTM [20]	98.17%	98.09%	98.7%	99.32%	0.045%
	Ensemble RNN [20]	98.69%	98.61%	99.05%	99.5%	0.03%
	Ensemble CNN [20]	99.45%	99.57%	99.61%	99.64%	0.01%

TABLE VII
EVALUATION METRICS FOR EACH DATASET USED IN DL HYBRID MODELS.

Dataset	Hybrid models	Accuracy	Precision	F1-Score	Recall	FPR
Generated Dataset [27]	CNN-LSTM [27]	+99%	+99%	+99%	+99%	-
N-BaIoT [6]	Cu-LSTMGRU+Cu-BLSTM [23]	99.45%	99.34%	99.47%	98.49%	0.003%
	Cu-DNN-GRU [23]	98.31%	96.8%	98.81%	98.64%	0.043%
	Cu-DNN-LSTM [23]	97.82%	97.47%	99.28%	99.28%	0.049%

In the provided context, the diagram 5 illustrates the selection of three DL-based methodologies recognized for their high performance in detecting slow DDoS attacks. They have showcased the most effective performance when deployed using real slow DDoS datasets. It's essential to highlight that detecting slow DDoS attacks presents greater challenges compared to high-rate DDoS attacks due to their subtle and intermittent nature. However, selecting the appropriate dataset plays a crucial role in training these robust models, enabling them to identify all the necessary features accurately.

The utilization of the CICDos 2017 dataset, which is

continuously updated to reflect the latest developments in slow DDoS attacks, underscores its invaluable contribution to keep the IDSs up to date. By leveraging this updated dataset, IDSs remain equipped to effectively detect and mitigate evolving threats posed by slow DDoS attacks, ensuring the security and resilience of the network infrastructure in real-world scenarios.

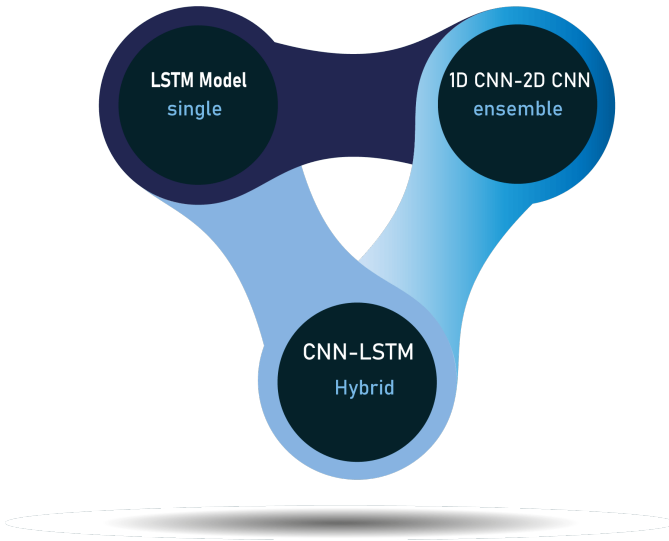


Fig. 5. The Chosen DL Models.

VI. CONCLUSION

In conclusion, this survey has shed light on the significant threats that DDoS attacks pose to SDN networks, emphasizing the urgent need for robust Intrusion Detection Systems (IDSs). Researchers have responded to this challenge by exploring various solutions and methodologies, with deep learning-based approaches emerging as particularly promising avenues. Among the plethora of techniques and models used and tested to create the ideal IDS, three distinct deep learning models have demonstrated remarkable effectiveness in identifying malicious traffic of DDoS attacks within SDN environments. These models are the closest to be ready and applicable in real-world scenarios. The chosen DL approaches, namely LSTM as single model, Model C (1D CNN and 2D CNN combination) as ensemble model, and the CNN-LSTM as hybrid model, have showcased superior performance in detecting and mitigating DDoS attacks.

It is crucial to note that the evaluation of these methods was performed using datasets featuring slow-rate DDoS attacks, which are considered particularly hazardous due to their challenging detection. These datasets are the Generated Dataset and CICDos 2017 which are available online and updated with the latest slow DDoS attacks variations. This deliberate choice of datasets has equipped these models with the capability to detect and address the subtle and stealthy nature of such attacks.

Looking ahead, given the robustness of the three DL-based models highlighted previously, integrating these approaches within a comprehensive SDN-based architecture and evaluating their performance using real-world data is crucial to prove their resilience in actual scenarios. Such an approach aims to prepare the models for real-world implementation by enhancing their performance, especially considering that the

DDoS attacks encountered may differ from those present in the training datasets. Relying solely on outdated data may provide a misleading assessment of the models effectiveness in detecting DDoS attacks, potentially leading to virtual rather than real-world performance.

REFERENCES

- [1] Installing opendaylight - opendaylight documentation scandium documentation. https://docs.opendaylight.org/en/latest/getting-started-guide/installing_opendaylight.html.
- [2] Ryu sdn framework. <https://ryu-sdn.org/>.
- [3] shekyan/slowhttpstest: Application layer dos attack simulator. <https://github.com/shekyan/slowhttpstest>.
- [4] Mininet. <https://mininet.org/>, 2024.
- [5] Hasan A. Understanding distributed denial of service (ddos) attacks and its analysis. *Insights2Techinfo*, pp.1, 2023.
- [6] Abebe Abeshu and Naveen Chilamkurti. Deep learning: The frontier for distributed attack detection in fog-to-things computing. *IEEE Communications Magazine*, 56(2):169–175, 2018.
- [7] Nisha Ahuja, Gaurav Singal, and Debajyoti Mukhopadhyay. Ddos attack sdn dataset. *Mendeley Data*, 1:17632, 2020.
- [8] Fatmah Alanazi, Kamal Jambi, Fathy Eassa, Maher Khe-makhem, Abdullah Basuhail, and Khalid Alsubhi. Ensemble deep learning models for mitigating ddos attack in software-defined network. *Intelligent Automation & Soft Computing*, 33(2), 2022.
- [9] Naziya Aslam, Shashank Srivastava, and MM Gore. Onos ddos defender: A comparative analysis of existing ddos attack datasets using ensemble approach. *Wireless Personal Communications*, 133(3):1805–1827, 2023.
- [10] Bindu Bala and Sunny Behal. Ai techniques for iot-based ddos attack detection: Taxonomies, comprehensive review and research challenges. *Computer science review*, 52:100631, 2024.
- [11] Afsaneh Banitalebi Dehkordi, MohammadReza Soltanaghahi, and Farsad Zamani Boroujeni. The ddos attacks detection through machine learning and statistical methods in sdn. *The Journal of Supercomputing*, 77(3):2383–2415, 2021.
- [12] Sunny Behal and Krishan Kumar. Characterization and comparison of ddos attack tools and traffic generators: A review. *Int. J. Netw. Secur.*, 19(3):383–393, 2017.
- [13] Ammarah Cheema, Moeenuddin Tariq, Adnan Hafiz, Muhammad Murad Khan, Fahad Ahmad, and Muhammad Anwar. Prevention techniques against distributed denial of service attacks in heterogeneous networks: A systematic review. *Security and Communication Networks*, 2022:1–15, 2022.
- [14] Cloudflare. What is a distributed denial-of-service (ddos) attack? <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>.

- [15] Hercules Dalianis. *Evaluation Metrics and Evaluation*, pages 45–53. Springer International Publishing, Cham, 2018.
- [16] A Dhanapal and P Nithyanandam. The slow http distributed denial of service attack detection in cloud. *Scalable Computing: Practice and Experience*, 20(2):285–298, 2019.
- [17] Mahmoud Said Elsayed, Nhien-An Le-Khac, and Anca D Jurcut. Insdn: A novel sdn intrusion dataset. *IEEE access*, 8:165263–165284, 2020.
- [18] Open Networking Foundation. Software-defined networking: The new norm for networks. <https://opennetworking.org/wp-content/uploads/2011/09/wp-sdn-newnorm.pdf>, April 13, 2012.
- [19] Shahzeb Haider, Adnan Akhunzada, Ghufraan Ahmed, and Mohsin Raza. Deep learning based ensemble convolutional neural network solution for distributed denial of service detection in sdns. In *2019 UK/China Emerging Technologies (UCET)*, pages 1–4. IEEE, 2019.
- [20] Shahzeb Haider, Adnan Akhunzada, Iqra Mustafa, Tanil Bharat Patel, Amanda Fernandez, Kim-Kwang Raymond Choo, and Javed Iqbal. A deep cnn ensemble framework for efficient ddos attack detection in software defined networks. *Ieee Access*, 8:53972–53983, 2020.
- [21] Md Alamgir Hossain and Md Saiful Islam. Enhancing ddos attack detection with hybrid feature selection and ensemble-based classifier: A promising solution for robust cybersecurity. *Measurement: Sensors*, page 101037, 2024.
- [22] Chih-Hsiang Hsieh, Wei-Kuan Wang, Cheng-Xun Wang, Shi-Chun Tsai, and Yi-Bing Lin. Efficient detection of link-flooding attacks with deep learning. *Sustainability*, 13(22):12514, 2021.
- [23] Danish Javeed, Tianhan Gao, Muhammad Taimoor Khan, and Duaa Shoukat. A hybrid intelligent framework to combat sophisticated threats in secure industries. *Sensors*, 22(4):1582, 2022.
- [24] Xiaoyu Liang and Taieb Znati. A long short-term memory enabled framework for ddos detection. In *2019 IEEE global communications conference (GLOBECOM)*, pages 1–6. IEEE, 2019.
- [25] Francisco Sales de Lima Filho, Frederico AF Silveira, Agostinho de Medeiros Brito Junior, Genoveva Vargas-Solar, and Luiz F Silveira. Smart detection: an online approach for dos/ddos attack detection using machine learning. *Security and Communication Networks*, 2019:1–15, 2019.
- [26] Amran Mansoor, Mohammed Anbar, Abdullah Ahmed Bahashwan, Basim Ahmad Alabsi, and Shaza Dawood Ahmed Rihan. Deep learning-based approach for detecting ddos attack on software-defined networking controller. *Systems*, 11(6):296, 2023.
- [27] Beny Nugraha and Rathan Narasimha Murthy. Deep learning-based slow ddos attack detection in sdn-based networks. In *2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pages 51–56. IEEE, 2020.
- [28] Iman Sharafaldin, Arash Habibi Lashkari, Ali A Ghorbani, et al. Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp*, 1:108–116, 2018.
- [29] Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak, and Ali A Ghorbani. Developing realistic distributed denial of service (ddos) attack dataset and taxonomy. In *2019 international carnaham conference on security technology (ICCST)*, pages 1–8. IEEE, 2019.
- [30] Karanpreet Singh, Paramvir Singh, and Krishan Kumar. Application layer http-get flood ddos attacks: Research landscape and challenges. *Computers & security*, 65:344–372, 2017.
- [31] Dan Tang, Yudong Yan, Siqi Zhang, Jingwen Chen, and Zheng Qin. Performance and features: Mitigating the low-rate tcp-targeted dos attack via sdn. *IEEE Journal on Selected Areas in Communications*, 40(1):428–444, 2021.
- [32] Vishal Verma and Vasudha Kumar. Dos/ddos attack detection using machine learning: A review. In *Proceedings of the International Conference on Innovative Computing & Communication (ICICC)*, 2021.
- [33] Noe M Yungaicela-Naula, Cesar Vargas-Rosales, Jesus Arturo Perez-Diaz, Eduardo Jacob, and Carlos Martinez-Cagnazzo. Physical assessment of an sdn-based security framework for ddos attack mitigation: Introducing the sdn-slowrate-ddos dataset. *IEEE Access*, 2023.
- [34] Noe Marcelo Yungaicela-Naula, Cesar Vargas-Rosales, and Jesus Arturo Perez-Diaz. Sdn-based architecture for transport and application layer ddos attack detection by using machine and deep learning. *IEEE Access*, 9:108495–108512, 2021.
- [35] Z Zhigang. What is a ddos attack? ddos attack types and defense. huawei. <https://info.support.huawei.com/info-finder/encyclopedia/en/DDoS+Attack.html>, July 26, 2023.