ENHANCED FEATURE SELECTION WITH STACKING METHOD FOR DDOS ATTACK DETECTION IN SOFTWARE DEFINED NETWORKING ENVIRONMENT

TAREQ I. A. ALASFOUR

UNIVERSITI SAINS MALAYSIA

2025

ENHANCED FEATURE SELECTION WITH STACKING METHOD FOR DDOS ATTACK DETECTION IN SOFTWARE DEFINED NETWORKING ENVIRONMENT

by

TAREQ I. A. ALASFOUR

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

May 2025

ACKNOWLEDGEMENT

First and foremost, I express my gratitude and thanks to Almighty Allah SWT for granting me patience, guidance, health, and the opportunity to work at such esteemed institutions as Universiti Sains Malaysia (USM) and the National Advanced IPv6 Center of Excellence (NAv6) and Cybersecurity Research Center (CYRES).

My sincere and utmost gratitude goes to my incredible supervisor, Dr. Chong Yung Wey, for her unwavering patience, guidance, encouragement, and advice throughout my studies. I have been extremely fortunate to have a supervisor who cares so deeply about my work and who always responded to my questions and queries. I hope that I'll never forget her kindness and may she receive multiple acts of kindness in return, insya-Allah.

I am also deeply grateful to NAv6 director, Assoc. Prof. Dr. Selvakumar Manickam, as well as to the lecturers, administrative staff, and technical staff for providing a supportive and conducive environment for my studies. Additionally, I am deeply grateful to TS. Dr. Mohd Najwadi bin Yusoff for his insightful guidance throughout the entire period of my research.

Finally, I would like to extend my heartfelt thanks to those closest to my heart: my beloved father and mother, for their continuous support, du'as, and encouragement; my dearest brothers and precious sisters, for helping make my dream come true and for their constant motivation; and last but not least, thank you to all my friends in Malaysia, Palestine, Iraq, and those who have supported me in any respect during my research. With gratitude, TARIQ EMAD ALI , USM, Penang, Malaysia, 2024.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

SDN	Software-defined networking
DDoS	Distributed Denial of Service
GAWFS	Genetic Algorithm Wrapper Feature Selection
Chi2	Chi-square
GA	Genetic Algorithm
MLP	Multi-Layer Perceptron
SVM	Support Vector Machine
RF	Random Forest
EnFS	Ensemble Feature Selection
ML	Machine Learning
DL	Deep Learning
CNN	Convolutional Neural Network
RNN	Recurrent Neural Network
LSTM	Long Short-Term Memory
PCA	Principal Component Analysis
RFE	Recursive Feature Elimination
ML/DL	Machine Learning/Deep Learning
OF	OpenFlow
AI	Artificial Intelligence

ANN	Artificial Neural Networks
GBM	Gradient Boosting Machine
DT	Decision Trees
RO	Research Objective
CSV	Comma Separated Value
PCAP	Packet Capture
TP	True Positive
TN	True Negative
FP	False Positive
FN	False Negative
DAR	Detection Accuracy Rate
QoS	Quality of Service
NIC	Network Interface Card
RFFI	Random Forest Feature Importance
SFFS	Sequential Forward Floating Selection
MI	Mutual Information
GB	Gradient Boosting
WVE	Weighted Voting Ensemble
LR	Logistic Regression

LIST OF APPENDICES

PENINGKATAN PEMILIHAN CIRI DENGAN KAEDAH PENYUSUNAN UNTUK MENGESAN SERANGAN DDOS DALAM PERSEKITARAN RANGKAIAN TAKRIFAN PERISIAN

ABSTRAK

Rangkaian yang ditakrifkan perisian (SDN) ialah pendekatan rangkaian komputer yang memisahkan sijil data dari sijil kawalan. Namun, sifat dinamik dan boleh diprogram SDN memperkenalkan cabaran keselamatan baru, terutamanya dalam mengesan serangan DDoS. Proliferasi serangan DDoS mengancam aksesibiliti dan prestasi rangkaian secara signifikan. Kaedah pemilihan ciri tradisional menghadapi kompleksiti data lalu lintas rangkaian, mengakibatkan prestasi pengesanan yang lemah. Bagi menangani ini, kami mencadangkan kaedah Pemilihan Ciri Pembungkus Algoritma Genetik (GAWFS). Pendekatan ini mengintegrasikan teknik Chi-squared dan Algoritma Genetik dengan kaedah korelasi pangkat Kendall untuk memilih ciri-ciri yang paling berkaitan. GAWFS secara berkesan mengurangkan dimensi ciri, menghapuskan kelebihan, dan mengenal pasti ciri-ciri yang berkaitan penting untuk klasifikasi. Untuk meningkatkan lagi ketepatan pengesanan, kami menggunakan model hibrid penyusunan. Model ini menggabungkan Perceptron Lapisan Pelbagai (MLP) dan Mesin Vektor Sokongan (SVM) sebagai pengklasifikasi asas, dengan Hutan Rawak (RF) sebagai meta-pengklasifikasi. Pengklasifikasi yang dicadangkan mencapai kadar ketepatan yang mengagumkan iaitu 99.86% untuk data yang dilihat dan 98.89% untuk data yang tidak dilihat, mewakili peningkatan kira-kira 5% dan 40% berbanding dengan kajian sebelumnya. Selain itu, masa latihan dikurangkan kepada 2,593 saat, penambahbaikan sekitar 29.92%.

ENHANCED FEATURE SELECTION WITH STACKING METHOD FOR DDOS ATTACK DETECTION IN SOFTWARE DEFINED NETWORKING ENVIRONMENT

ABSTRACT

Software-defined networking (SDN) is a networking approach that separates the control plane from the data plane. However, the dynamic and programmable nature of SDNs introduces new security challenges, particularly in detecting Distributed Denial of Service (DDoS) attacks. The proliferation of DDoS attacks significantly threatens network accessibility and performance. Traditional feature selection methods struggle with the complexity of network traffic data, resulting in poor detection performance. To address this, we propose a Genetic Algorithm Wrapper Feature Selection (GAWFS) method. This approach integrates Chi-squared (Chi2) and Genetic Algorithm (GA) techniques with the Kendall rank correlation method to select the most relevant features. GAWFS effectively reduces feature dimensions, eliminates redundancy, and identifies crucial correlated features for classification. To further enhance detection accuracy, we employ a stacking ensemble model. This model combines Multi-Layer Perceptron (MLP) and Support Vector Machine (SVM) as base classifiers, with a Random Forest (RF) as the meta-classifier. Our proposed classifier achieves impressive accuracy rates of 99.86% for seen data and 98.89% for unseen data, representing improvements of approximately 5% and 40%, respectively, over previous studies. Additionally, the training time is reduced to 2,593 seconds, an improvement of approximately 29.92%. Validation on various publicly available benchmark datasets confirms the effectiveness of our approach, highlighting the significance of our enhanced feature selection method and stacking ensemble model in combating DDoS attacks.

CHAPTER 1

INTRODUCTION

SDN is a new network architecture that isolates the control and data planes to provide centralized administration of network resources. In traditional networks, routers and switches handle packet forwarding and network traffic control. However, SDNs decouple the control plane, allowing for greater flexibility and agility in network management. The control plane in SDNs is managed by a software controller, which communicates with network devices using protocols like OpenFlow. This controller has a global view of the network topology and can dynamically configure network policies such as routing and traffic engineering based on real-time traffic demands. This centralized approach improves adaptability to changing traffic patterns and optimizes network resources. SDNs offer numerous advantages over traditional networks, including faster deployment, reduced network downtime, improved scalability, and better network visibility and control. For example, SDN-based security solutions provide effective discovery and prevention of network assaults. (T. E. Ali, Morad, & Abdala, 2020). Despite these benefits, the adoption of SDN has been hampered by high implementation costs and the need for specialized expertise. Open-source SDN solutions such as OpenDaylight and ONOS are expected to facilitate increased adoption in the future (T. E. Ali, Morad, & Abdala, 2018). However, this architectural shift also introduces new security challenges, particularly regarding DDoS attacks. DDoS attacks are designed to make websites or network resources unavailable by flooding them with demand from multiple directions.

Detecting DDoS attacks presents a considerable challenge as a result of the use of legitimate network protocols, making it difficult to distinguish attackers from regular users within vast network traffic. This complexity is exacerbated when inappropriate feature selection and detection models are employed (Dahiya, Virmani, et al., 2023). Moreover, DDoS attacks can be swiftly executed using a variety of readily available tools such as Trinoo, Low Orbit Ion Cannon, Trinity, Stream, and Tribe Flood Network, each employing different flooding techniques (Aslam, Srivastava, & Gore, 2023). Therefore, effective detection of DDoS attacks depends heavily on feature selection methods and the implementation of high-performance classification algorithms (F. I. Ali, Ali, & Al-Dahan, 2023). Literature review reveals that feature selection techniques are often inadequate in many studies. Some utilize Ensemble Feature Selection (EnFS) methods (Danso et al., 2022; Elejla et al., 2022; Mansoor, Anbar, Bahashwan, Alabsi, & Rihan, 2023), while others employ deep learning (DL) for feature selection, such as in (Alabsi, Anbar, & Rihan, 2023). Alternatively, some studies manually select features (Ahuja, Singal, Mukhopadhyay, & Kumar, 2021; Dong & Sarem, 2019; Erhan & Anarim, 2020; Singh, Kaur, & Kaur, 2024), selecting varying numbers of features. Many studies prioritize improving classification models without adequately discussing feature selection methodologies (Altunay & Albayrak, 2023; Javeed, Gao, Khan, & Ahmad, 2021), which significantly impacts model performance.

In recent years, DDoS attacks have increased in frequency, severity, and complexity, posing challenges in detection and mitigation (Hnamte & Hussain, 2023). Various detection methods, including machine learning (ML), have been proposed to address the growing risk of DDoS attacks in SDN networks. ML algorithms can analyze network traffic in real-time, identifying abnormal patterns indicative of DDoS attacks

(Hamarshe, Ashqar, & Hamarsheh, 2023). Unlike signature-based methods, ML algorithms can detect previously unseen attacks by automatically learning from network traffic patterns. They are capable of handling massive amounts of information in immediate form, resulting in suitability for high-speed networks and improving entire network security(Kurakula, Akhila, Bhavya, & Sai, 2023).

In summary, integrating ML into DDoS attack detection in SDNs offers a more efficient and effective approach to identifying and mitigating attacks, reducing network downtime and associated costs. Our thesis contributes to network security by enhancing the detection capabilities in SDN environments, thereby improving overall network reliability and security.

1.1 Problem Statement

In recent years, Software-Defined Networking (SDN) has gained popularity due to its flexibility and centralized control. However, SDN is highly vulnerable to security threats, particularly Distributed Denial-of-Service (DDoS) attacks, which can overwhelm network resources and disrupt services. Machine learning (ML) and deep learning (DL) techniques have been widely explored for DDoS detection, but they face critical challenges in achieving high accuracy and generalizability. One major hurdle is the **dynamic nature of SDN**, where network traffic patterns can shift significantly, making it difficult for models to adapt and generalize across various network setups and attack types. Another challenge stems from the **centralized control of SDN networks**. While centralization offers benefits such as programmability and global visibility, it also introduces a **single point of failure**, making SDN controllers attractive targets for

malicious attackers. This complicates the detection of distributed attacks like DDoS, as the system must be capable of adjusting to new attack strategies while maintaining control over large-scale networks in real-time. Additionally, ensuring **low-latency decision-making** is critical in SDN environments, where rapid mitigation is required to prevent large-scale disruptions. These challenges, ranging from model adaptability and scalability to real-time threat detection, must be addressed to fully harness the power of ML/DL for secure SDN deployment.

One of the key issues in ML/DL-based DDoS detection is the presence of **redundant and irrelevant features** in modern SDN network datasets. These unnecessary features degrade model performance, introduce noise, and increase computational costs, leading to misclassification (Ahmed, Dahou, Chelloug, Al-qaness, & Elaziz, 2022). Existing feature selection techniques (filter, wrapper, and embedded) struggle to efficiently reduce dimensionality while preserving key features for attack detection (Hajisalem & Babaie, 2018). While wrapper methods use classification performance for selection, filter techniques rely on statistical measures, and embedded approaches integrate feature selection into the learning process (Yang, Wang, Fu, Kuo, et al., 2022). However, embedded techniques are computationally expensive and difficult to modify for improved classification (Abu Khurma et al., 2022). Recent studies have explored deep learning-based feature selection (Alabsi et al., 2023), but these methods face challenges such as overfitting, hyperparameter sensitivity, and high computational costs. Ensemble-based feature selection techniques (Elejla et al., 2022; Mansoor et al., 2023) improve feature stability but rely on fixed thresholds, which do not adapt to different datasets, leading to poor feature selection adaptivity (Dietterich, 2000).

Another significant challenge in existing approaches is the **low accuracy of models**, primarily due to ineffective feature selection and the inability to adapt to evolving attack patterns. Many studies rely on single-model classifiers such as Decision Trees (DT) (Cil, Yildiz, & Buldu, 2021), XGBoost (Le, Oktian, & Kim, 2022), and Convolutional Neural Networks (CNN) (Kim, Kim, Kim, Shim, & Choi, 2020), which, while effective for specific attacks, often struggle with generalization. To enhance accuracy, hybrid models (Akhtar & Feng, 2022; Altunay & Albayrak, 2023; Javeed et al., 2021; Wu, Guo, & Moustafa, 2020) combine multiple classifiers; however, they introduce several challenges. First, hybrid models demand substantial computational resources, increasing processing time and making real-time deployment difficult. Second, ensuring compatibility between different classifiers within a hybrid framework requires extensive hyperparameter tuning, significantly prolonging training time. Additionally, complex hybrid models often become highly specialized in detecting known attack patterns, limiting their ability to generalize to novel threats. Lastly, as more models are integrated into a hybrid approach, scaleability becomes increasingly difficult, posing challenges for large-scale SDN deployments. Ensemble models (Alotaibi & Ilyas, 2023; Gao, Shan, Hu, Niu, & Liu, 2019; Saharkhizan, Azmoodeh, Dehghantanha, Choo, & Parizi, 2020) improve detection rates but often rely on simplistic techniques such as majority voting, which can lead to poor classification performance, particularly in imbalanced datasets. Furthermore, many studies rely on simulated environments, which fail to capture real-world traffic complexities, making models less effective when deployed in live networks. Limited adaptability to dynamic attack strategies further reduces practical usability.

To address these issues, this study proposes an **enhanced feature selection approach**, Genetic Algorithm Wrapper Feature Selection (GAWFS), integrating Genetic Algorithm (GA), Chi-squared (Chi^2), and Kendall correlation methods to eliminate redundant features and improve classification accuracy. Additionally, we introduce a **stacking ensemble model** combining Support Vector Machine (SVM) and Multi-Layer Perceptron (MLP) as base classifiers, with Random Forest (RF) as the meta-classifier. This approach enhances feature integration, improves detection accuracy, and maintains computational efficiency for real-world SDN deployments.

1.2 Objectives

This thesis's primary objective is to provide a new methodology and improved feature selection technique for SDN DDoS assault detection. The following is a definition of specific aims.

1. To propose an enhanced feature selection method using a hybrid approach called Genetic Algorithm Wrapper Feature Selection (GAWFS) for dimensionality reduction. This method will utilize the Kendall rank correlation method to assess relationships between features and minimize errors. This objective aims to overcome the limitations of traditional feature selection methods and increase the accuracy of the machine learning model by choosing the subset of characteristics that are most significant for the target variable.

2. To propose a stacking method for DDoS attack detection in SDN using an enhanced ensemble learning approach. Unlike conventional ensemble models designed for traditional networks, this method is optimized for SDN's dynamic and

centralized nature. It introduces an improved stacking mechanism where SVM and MLP serve as base learners, and RF functions as a meta-model for adaptive decision-making. The novelty of this approach lies in its ability to leverage SDN-specific traffic characteristics, optimize feature selection, and enhance real-time adaptability for more effective DDoS detection. This is not a hybrid approach but a refined ensemble technique tailored to SDN environments. The model aims to achieve high accuracy, reduce false positives, and improve scalability, all while maintaining low computational overhead.

3. To benchmark the proposed model against existing ML/DL approaches for DDoS attack detection in SDN environment by evaluating its performance using various metrics, including accuracy, precision, recall, F1-score, false positives, and false negatives. This comparison aims to highlight the strengths, weaknesses, and overall impact of the proposed model on improving the effectiveness and efficiency of DDoS attack detection systems.

1.3 Research Contribution

Based on research, traditional feature selection methods and single algorithms, whether used independently or with hybrid learning methods, often have limited effectiveness in detecting DDoS attacks, as discussed in the problem statement section. The main contributions of this thesis are summarized as follows:

1. **Enhanced Feature Selection Method:** A novel enhanced feature selection method using a hybrid feature selection method called GAWFS integrated with the Kendall rank correlation method. This approach assesses relationships between features

to minimize errors and contributes to dimensionality reduction, improving the accuracy and performance of DDoS attack detection by selecting informative, highly correlated, and representative features. This method identifies the most effective features from a dataset without redundancy, enhancing the detection accuracy and efficiency of DDoS attacks. The novel technique consistently decreases dataset dimensionality by picking just those characteristics that are important and most correlated and removing redundant and extraneous ones. GAWFS achieves this by:

- Selecting features that are not correlated with each other, reducing the risk of overfitting the model.
- Selecting features relevant to the target variable, even if not directly correlated with it, thanks to the genetic algorithm's effective exploration of the feature space.
- Being less computationally expensive than wrapper methods, as it doesn't require building and evaluating a model for each feature subset.
- Utilizing the correlation method to select only the most relevant features.

2. **Novel Detection Model Using Ensemble Learning in SDN:** In this work, we propose a novel ensemble learning-based detection model for DDoS attacks, specifically designed for SDN environments. Unlike traditional ensemble methods used in conventional networks, which rely on fixed traffic patterns and limited adaptability, our model is optimized to handle the unique dynamic nature of SDN traffic. The key novelty of this approach lies in its ability to leverage SDN-specific traffic characteristics. SDN networks are highly dynamic, with traffic

patterns changing rapidly due to the centralized nature of the SDN controller. Our model addresses this challenge by integrating enhanced feature selection techniques from Research Objective (RO1) that are tailored to SDN environments, ensuring more relevant data is used for attack detection with an improved stacking mechanism where SVM and MLP are used as base learners and Random Forest (RF) is employed as the meta-model. This setup allows the model to adapt better to evolving attack strategies. While traditional ensemble methods rely on predefined rules and static configurations, our stacking approach dynamically adjusts to detect new and emerging DDoS attack patterns in real-time, making it particularly effective for SDN networks that are subject to frequent changes in traffic flow. Moreover, this model is designed to be computationally efficient with low overhead, which is critical for real-time DDoS detection in SDN environments. The RF meta-model, in particular, helps handle noisy data often generated by DDoS attacks, ensuring the system remains robust even under high traffic loads. So, the novelty of this model comes from its customization to SDN's unique characteristics, its dynamic adaptation to changing attack patterns, and its efficiency in real-time detection. These improvements set our model apart from conventional ensemble techniques, offering a more effective and scalable solution for DDoS attack detection in SDN networks.

3. **Comparative Evaluation:** A comparative evaluation is conducted, comparing and evaluating the proposed model with existing ML/DL models for the detection of DDoS attacks. This comprehensive study employs a variety of performance indicators, including accuracy, precision, recall, and false positive rate. The comparison gives a fair evaluation of the suggested model's performance

and emphasizes its advantages over other current techniques.

This research could lead to the development of a new DDoS attack detection method that enhances the security of networks and systems against modern DDoS attacks with varying scenarios. This advancement could help protect businesses and individuals from the damage caused by diverse modern DDoS attacks.

1.4 Structure of the Thesis

This thesis's subsequent chapters are categorized as follows:

- **Chapter 2 :-** SDN, ML, and DL frameworks are thoroughly explained from a security standpoint. A summary of the literature will be given next to discuss earlier research on identification strategies for DDoS assaults.
- **Chapter 3 :-** Provides a detailed explanation of the initiative's investigative processes. The purpose of this section is to provide a detailed explanation of the strategies that will be employed to accomplish the primary research objective.
- **Chapter 4 :-** Shows how the suggested approach is designed and put into practice, including how the studies are set up.
- **Chapter 5 :-** Examines how well the suggested strategy performs using the cases from Section 4.
- **Chapter 6 :-** Comprises the research contributions, conclusion, and possible future work for this research.

CHAPTER 2

RELATED WORK

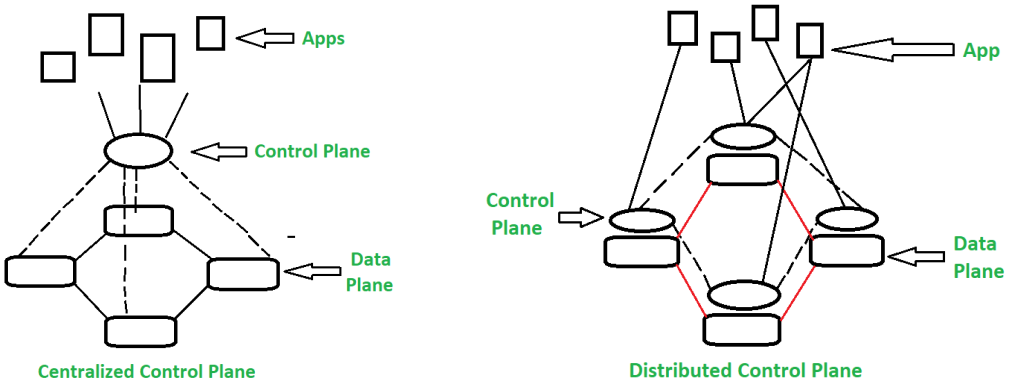
This chapter offers an overview of the fundamental concepts behind detection techniques in SDN. It includes a literature review that explores previous research efforts, highlighting challenges faced and how they've been addressed. The review also builds a foundational understanding essential for the development and direction of this project. Section 2.1 presents a background to SDN networking layers. Section 2.2 defined and discussed the modern ML algorithms. The DL is defined and discussed in section 2.3. Section 2.4 defined the DDoS attack and its types. In section 2.5 explain the meaning of the dataset and its importance to building a detection model, and then define the advantages and disadvantages of the four data representation techniques, as well as, in this section, the feature's identification. Explain the advantages and disadvantages of the three common feature selection methods. In section 2.6 the related work in detection approaches is discussed. At the end, Section 2.8 provides a brief discussion and a summary of the key points covered in the chapter.

2.1 Background

2.1.1 Software-Defined Networking (SDN)

The fundamental concept of SDN is to permit community designers to broaden new offerings, which include QoS, bandwidth control, and traffic engineering. The separation of control and data planes enables innovation and evolution in networking concepts. The controller is the brain of SDN. The data plane has switches and devices

(Xu, Qin, & Song, 2022). The controller of an SDN infrastructure is in charge of creating routing tables, also known as flow tables, and figuring out the routes for packet forwarding over the network, as illustrated in Figure 2.1.



(a) Software-Defined Networking

(b) Traditional networking

Figure 2.1: Software-Defined Networking vs. Traditional Networking

2.1.2 SDN Controller

The SDN controller serves as the central point that connects and manages the network, often referred to as the network's "brain". Southbound application APIs, such as OpenFlow, facilitate communication with switches, while northbound APIs enable interaction with SDN applications. The controller performs diverse duties, together with accumulating network facts and figuring out network devices. Additional modules may be incorporated into the controller to enhance functionalities, including community tracking and traffic detection (Chaudhary, Aujla, Kumar, & Chouhan, 2022). Numerous SDN controllers supporting various programming languages (e.g., C++, Python, Java) have been developed. Given SDN's emphasis on fostering innovation, many of these platforms are open-source. The capabilities of each controller are shaped by the respective community supporting its development. There are a lot of controllers, such as POX, NOX, MUL, FloodLight, and ODL.

2.1.3 OpenFlow Protocol and Switch

OpenFlow (OF) is widely used as a South-bound API in SDN networks. As depicted in Figure 2.2, an OF switch contains a minimum of a single flow table and a layer of abstraction. The flow table comprises flow entries, which specify how packets are handled and sent. When a packet arrives at an OF transfer, the header record is retrieved and compared against entries inside the drift desk. If a healthy float is detected, the switch executes the instructions or moves related to the matched float access (Sossalla, Rischke, & Fitzek, 2022). If no match is detected, the switch responds in accordance with the controller's instructions, which may include forwarding the packet to the controller, discarding the packet, and so on.

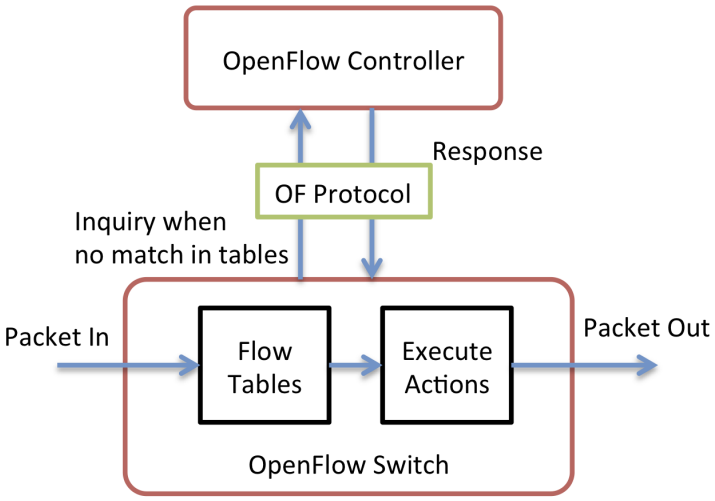


Figure 2.2: Communications via OpenFlow protocol

2.2 Machine Learning

Machine Learning (ML) is a subfield of Artificial Intelligence (AI) that focuses on creating algorithms and statistical models that are capable of learning from data to make predictions or decisions without explicit programming. In essence, ML allows

machines to learn and grow via experience rather than being expressly programmed to perform certain tasks. ML algorithms examine complicated information, find patterns and correlations, and then make predictions or judgments based on those patterns and relationships (Greener, Kandathil, Moffat, & Jones, 2022).There are several types of machine learning algorithms (supervised learning, unsupervised learning, and reinforcement learning). Supervised learning (Figure 2.3) uses labeled data to train algorithms with known output. The algorithm develops a relationship between the input data and the desired output. Common supervised learning algorithms are linear regression, logistic regression, decision trees (DT), random forests (RF), support vector machines (SVM), naive Bayes classifiers (NB), artificial neural networks (ANN), and gradient boosting machines (GBM) (Kreuzberger, Kühl, & Hirschl, 2023).

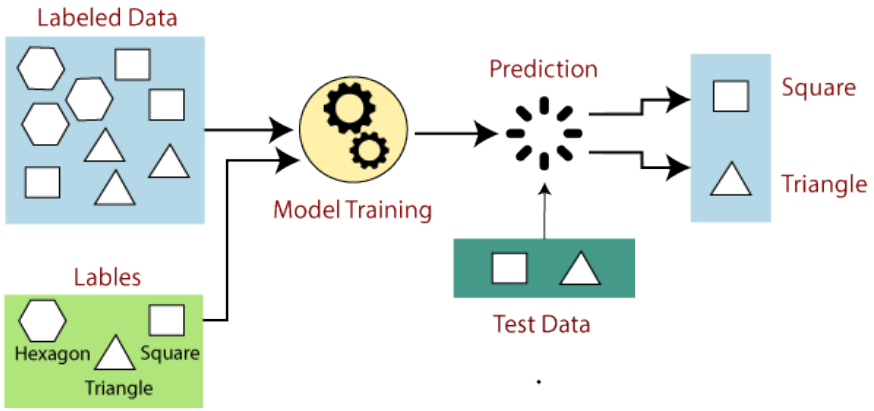


Figure 2.3: Supervised Learning

2.2.1 Linear Regression and Logistic Regression

Linear regression is a supervised learning approach that predicts an ongoing output parameter using one or more input variables (predictors or independent variables). The algorithm models the relationship between the input variables and the output variable by fitting a linear equation to the data, aiming to minimize the difference between pre-

dicted and actual outputs (Manoj, Yugesh, Girish, & Reddy, n.d.). Logistic regression, also a supervised learning algorithm, predicts a categorical output variable based on input variables. Models the probability that the output variable belongs to a particular category using a logistic function, adjusting the parameters to maximize the likelihood of correct predictions. It is commonly used for binary classification tasks (Stojanov, Lazarova, Veljkova, Rubartelli, & Giacomini, 2023).

2.2.2 Decision Trees (DT)

Decision trees are supervised learning algorithms that perform regression and classification problems. They recursively partition the data into subsets based on input features until the subsets are sufficiently homogeneous with respect to the output variable. Each internal node tests an input feature, and each leaf node represents a class label or regression value. Decision trees are interpretable but can overfit with deep trees or noisy data. Variants include random forests and gradient boosting (Coatrini-Soares et al., 2023).

2.2.3 Random Forests (RF)

Random forests are ensemble learning methods that combine multiple decision trees to improve accuracy and reduce overfitting. They train decision trees on different subsets of data and use a majority vote for final predictions. Random forests handle high-dimensional datasets and interactions between features, making them popular for classification problems (Bao, Huang, & Wu, 2023).

2.2.4 Support Vector Machines (SVM)

SVM in (Figure 2.4) are a supervised learning algorithm for classification and regression analysis. SVMs create hyperplanes in high-dimensional space to classify new data based on trained features. They increase the margin between the hyperplane and the closest data points, which improves generalization. SVMs use kernel functions to transform nonlinear data into higher-dimensional space (Ndungi, 2023).

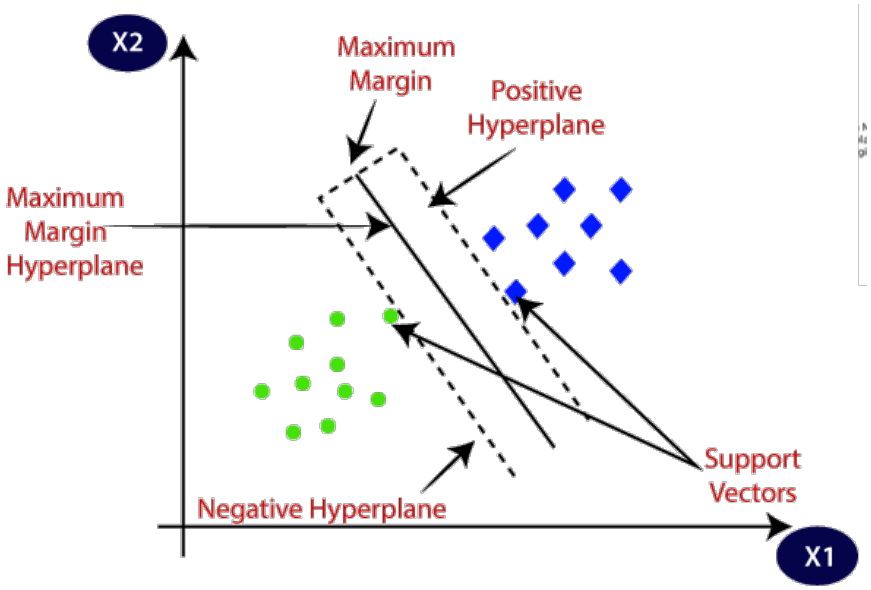


Figure 2.4: Support Vector Machine (SVM) Algorithm

2.2.5 Naive Bayes Classifiers

Naive Bayes classifiers use Bayes' theorem, assuming that the features are independent for probabilistic classification. They are effective for tasks such as text classification and spam filtering. Types include Gaussian Naive Bayes, Multinomial Naive Bayes, and Bernoulli Naive Bayes (Zhao & Xia, 2023).

2.2.6 Artificial Neural Networks (ANN)

Artificial Neural Networks (ANN), in Figure 2.5 imitate the structure and function of the human brain, consisting of layers of linked nodes. ANNs process information through neurons, applying activation functions to produce outputs. They excel in tasks such as image and speech recognition, natural language processing, and predictive modeling (John & Deshpande, 2023).

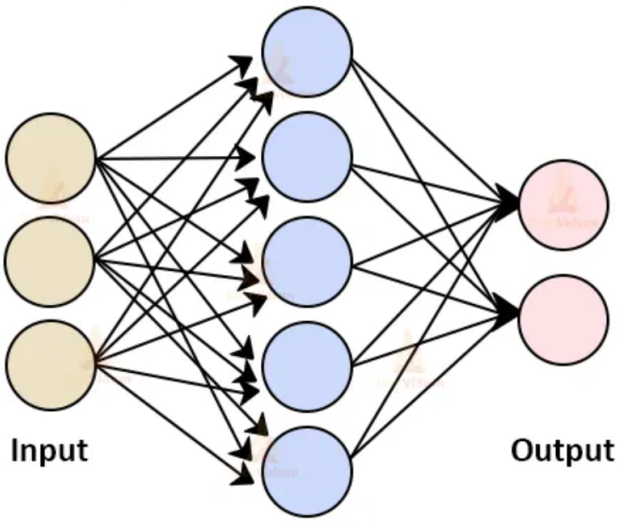


Figure 2.5: Artificial Neural Networks (ANN) Algorithm

2.3 Deep Learning

Deep learning is a subfield of ML that focuses on building artificial neural networks with multiple layers. Deep learning has revolutionized artificial intelligence by enabling machines to perform complex tasks such as image recognition, natural language processing, and decision-making with high accuracy (Menghani, 2023). One of its key advantages is the automatic discovery and extraction of features from raw data, making it ideal for processing large, unstructured datasets such as images, audio, and text. Deep learning algorithms excel in identifying subtle patterns and relation-

ships that are difficult for humans to discern (Shlezinger, Whang, Eldar, & Dimakis, 2023). Popular architectures include CNNs, RNNs, GANs), and Multi-Layer Perceptrons (MLPs), applied in various domains including computer vision, NLP, and autonomous driving (Hu, Jin, Zheng, Weng, & Ding, 2023).

2.3.1 Convolutional Neural Networks (CNNs)

CNNs are deep neural networks that are mainly used for image and video recognition. They employ convolutional operations to extract features from input images. CNNs are typically made up of convolutional, pooling, and fully connected layers and excel at tasks including object identification and facial recognition. They have also found applications in NLP and speech recognition (MacEachern, Esau, Schumann, Hennessy, & Zaman, 2023).

2.3.2 Recurrent Neural Networks (RNNs)

RNNs are designed for sequential data processing, such as time series or text data. They maintain memory of previous inputs through feedback loops, enabling predictions based on historical context. RNNs are crucial in NLP and speech recognition, though they face challenges with long-term dependency due to vanishing gradients. Advanced RNN architectures such as LSTM and GRU address these issues effectively (Habib, Karmakar, & Yearwood, 2023).

2.3.3 Multi-Layer Perceptron (MLP)

MLP (Figure 2.6) is a versatile feedforward neural network with multiple layers of interconnected neurons. It handles complex non-linear relationships and is widely used

for both classification and regression tasks. Trained via backpropagation, MLPs have applications in image and speech recognition, NLP, and financial prediction (Chaiprasittikul et al., 2023).

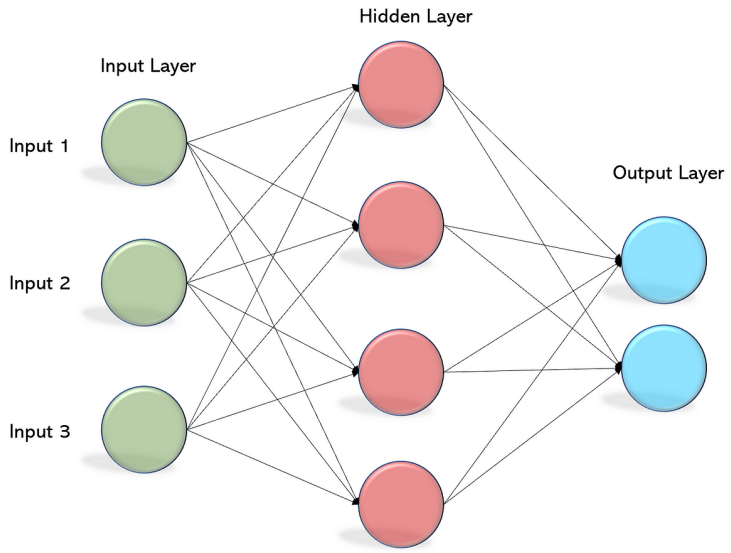


Figure 2.6: Multi-Layer Perceptron (MLP)

2.4 Distributed Denial of Service (DDoS) Attacks in SDN

DDoS attacks are among the most severe cybersecurity threats, overwhelming network infrastructures with excessive traffic and causing significant service disruption. In a typical DDoS attack (Figure 2.7), malicious actors flood networks with large volumes of requests, often using botnets of compromised devices to exhaust system resources and deny legitimate user access (SENKI, 2021). The first major DDoS attacks were reported in 1999, and their scale and sophistication have increased over the years, particularly during events like the COVID-19 pandemic, where the reliance on digital services surged (Khweiled, Jazzar, & Eleyan, 2021).

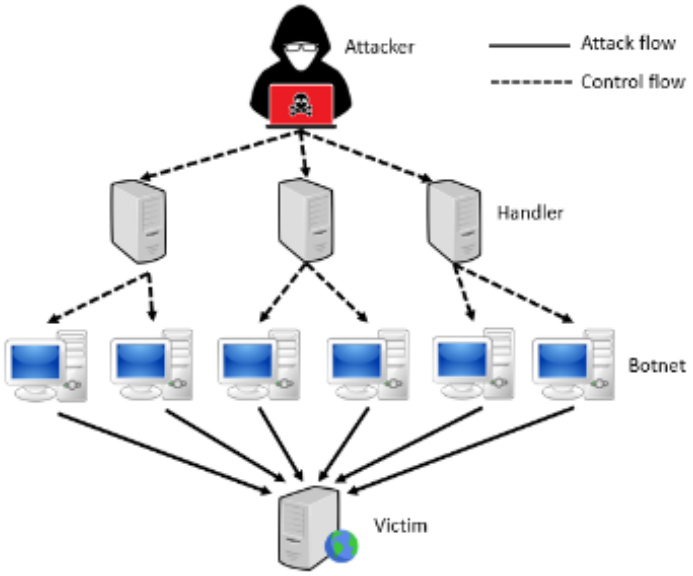


Figure 2.7: Illustration of a DDoS Attack Architecture

One of the largest recorded DDoS attacks occurred in June 2020, when Amazon Cloud faced an unprecedented 2.3 Tbps attack, highlighting the growing intensity of such threats (Amazon, 2020). Forecasts suggest that DDoS attacks will continue to increase in both frequency and complexity, necessitating advanced mitigation strategies (Cisco, 2020). Researchers have explored artificial intelligence (AI) driven approaches, particularly machine learning (ML) and deep neural networks (DNNs), to enhance DDoS detection and response mechanisms. These models leverage datasets to classify different attack patterns and improve detection accuracy (Hadi, Hayat, Musthaq, Hussain, & Cao, 2022; Wei et al., 2021). However, while AI-based solutions are promising, the dynamic nature of modern DDoS attacks requires continuous adaptation and refinement of defensive mechanisms (Chartuni & Márquez, 2021; A. Maheshwari, Mehraj, Khan, & Idrisi, 2022; Shieh et al., 2021). SDN has revolutionized traditional network architectures by shifting from traditional decentralized models to a more flexible, programmable structure. SDN's separation of the control plane (which makes routing decisions) from the data plane (which forwards packets) introduces several

advantages, such as centralized traffic management and dynamic resource allocation. However, this architectural shift also exposes SDN to new security risks, making it particularly vulnerable to DDoS attacks. Unlike conventional networks, which distribute routing decisions across multiple devices, SDN relies on a centralized controller, which becomes a single point of failure. If an attacker successfully floods the network with malicious requests, the SDN controller may become overwhelmed, leading to significant network-wide failures. The following vulnerabilities make SDN an attractive target for DDoS attacks:

- **Controller Overload:** SDN controllers handle flow rule installations for each new traffic request. Attackers exploit this by generating massive numbers of new flows, forcing the controller to process excessive requests, which can degrade performance or cause service outages.
- **Flow Table Exhaustion:** SDN switches maintain limited flow table capacities. Attackers inject an overwhelming number of unique flows, consuming all available memory and preventing the switch from processing legitimate traffic.
- **Northbound/Southbound API Exploits:** SDN communication relies on APIs that connect applications to controllers (Northbound) and controllers to switches (Southbound). Attackers exploit API vulnerabilities to manipulate flow rules or inject malicious traffic.
- **Protocol Specific Attacks:** SDN commonly uses OF for switch-controller communication. Attackers can manipulate OpenFlow messages to bypass security policies or disrupt the network.

Several real-world SDN-based attack scenarios illustrate how DDoS can cripple an entire network:

- **Control Plane Saturation:** Attackers generate a flood of new, unique flow requests, forcing SDN switches to forward them to the controller for processing. This results in excessive CPU and memory consumption, potentially causing the controller to crash.
- **Data Plane Flooding:** By targeting SDN switches, attackers overwhelm flow tables with excessive entries, leading to legitimate traffic being dropped or delayed.
- **IoT Botnet-Based Attacks:** Large-scale botnets, such as Mirai, leverage thousands of compromised IoT devices to generate high-volume traffic directed at SDN controllers, disrupting network operations (Hadi et al., 2022).

Therefore, DDoS attacks pose a significant challenge to SDN environments due to the centralized nature of SDN controllers, making them prime targets for attack. The vulnerabilities of SDN such as controller overload, flow table exhaustion, and OpenFlow protocol exploitation—highlight the urgent need for robust detection and mitigation mechanisms. Future advancements in intelligent traffic filtering, blockchain authentication, and decentralized SDN architectures will be crucial in strengthening SDN networks against DDoS attacks and ensuring a secure, resilient infrastructure.

2.5 Datasets Issues and Representations

Datasets are fundamental for training, evaluating, and improving machine learning models used in DDoS attack detection. They ensure that models are accurate, fair, and reliable by providing the necessary data to develop algorithms. The representation of data significantly influences the performance and generalization capabilities of these models. Here's why datasets are vital for detecting DDoS attacks:

- **Training machine learning models:** Datasets provide the data necessary for ML models to learn and detect DDoS attacks.
- **Evaluating machine learning models:** Datasets are used to assess the performance of machine learning models in detecting DDoS attacks, ensuring their effectiveness.
- **Improving machine learning models:** Datasets boost the performance of machine learning models by detecting and fixing faults.

Without datasets, training and evaluating ML models for DDoS attack detection would be challenging, hindering effective network protection. Therefore, selecting good datasets is critical, meeting specific requirements to ensure efficacy (Gupta, Das, & Panda, 2020; S. M. A. Rahman, Hossain, Islam, & Choo, 2022b; Rodrigues, Paula, & Barbosa, 2021):

- **Relevance:** Datasets must contain relevant data related to DDoS attacks to address the specific problem.

- **Completeness:** They should include all necessary data for training and evaluating models, often requiring labeled data for effective evaluation metrics.
- **Accuracy:** Data accuracy is crucial for effective model learning and performance.
- **Representativeness:** Datasets must mirror real-world data to ensure models can handle diverse scenarios.
- **Scalability:** They should be scalable to accommodate complex models that require larger datasets as they grow.

Effective datasets are essential for developing accurate and stable ML models that satisfy particular requirements in DDoS attack detection. Subsequently, this research evaluates existing DDoS datasets against these criteria in Section 2.5.2. The following subsection discusses various representations used in existing datasets.

2.5.1 Dataset Representations

Dataset representations refer to the way data are structured within datasets, which affects the performance of machine learning models. Different representations cater to varying needs and complexities:

- **Flow-based representations:** Utilize flow-based data, aggregating packets with identical IP addresses, ports, and protocols (S. M. A. Rahman, Hossain, Islam, & Choo, 2022a; W. Wang, Sun, Zhang, Liu, & Zhang, 2022; Zhang, Wang, Liu, Zhang, & Liu, 2023). These are straightforward to collect and process, making them suitable for real-time detection, but they may lose individual packet details.