JOIV : Int. J. Inform. Visualization, 6(4) - December 2022 809-814

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

Comparison of Feature Selection Methods for DDoS Attacks on Software Defined Networks using Filter-Based, Wrapper-Based and Embedded-Based

M.T. Kurniawan [a,b,*], Setiadi Yazid [a], Yudho Giri Sucahyo [a]

[a] *Computer Science Faculty, Indonesia University, Depok Jawa Barat, 16424, Indonesia*
[b] *Industrial Engineering Faculty, Jl. Telekomunikasi, Bandung Jawa Barat, 40257, Indonesia*
Corresponding author: [*]mochamd.teguh@ui.ac.id

***Abstract*—The development of internet technology is growing very rapidly. Moreover, keeping internet users protected from cyberattacks is part of the security challenges. Distributed Denial of Service (DDoS) is a real attack that continues to grow. DDoS attacks have become one of the most difficult attacks to detect and mitigate appropriately. Software Defined Network (SDN) architecture is a novel network management and a new concept of the infrastructure network. A controller is a single point of failure in SDN, which is the most dangerous of various attacks because the attacker can take control of the controller so that it can control all network traffic. Various detection and mitigation methods have been offered, but not many consider the capacity of the SDN controller. In this research, we propose a feature selection method for DDoS attacks. This research aims to select the most important features of DDoS attacks on SDN so that the detection of DDoS on SDN can be lightweight and early. This research uses a dataset [1] generated by a Mininet emulator. The simulation runs for benign TCP, UDP, and ICMP traffic and malicious traffic, which is the collection of TCP SYN attacks, UDP Flood attacks, and ICMP attacks. A total of 23 features are available in the dataset, some are extracted from the switches, and others are calculated. By using three methods, filter-based, wrapper-based, and embedded-based, we get consistent results where the pktcount feature is the highest feature importance of DDoS attacks on SDN.**

***Keywords*—Software-defined networking; detection system; feature selection; filter based; wrapper based; embedded based distributed denial-of-service.**

Manuscript received 15 Oct. 2022; revised 19 Nov. 2022; accepted 26 Dec. 2022. Date of publication 31 Dec. 2022.

I. INTRODUCTION

The development of the internet continues to increase every year. Not only the number of users but also the time users access the internet. The development of the internet also influences lifestyle and work style in society. Moreover, the effects of the COVID-19 pandemic have forced the public to interact with the internet. So, these demands that the network architecture and infrastructure must be able to adapt developments and needs of today's society. On the other hand, the government must get involved to solve the problem of cybercrime because this is a very serious threat to the internet [2].

In 2019 the Cisco cybersecurity report, about 30% of organizations experienced cyber-attacks [2]. The most common attack in a computer network is Distributed Denial of Service ((DDoS) [3]. The DDoS work by taking control of many hosts called botnets, and these botnets send many requests to victims to stop services. As a result, victims with limited resources are overloaded and cannot offer services to legitimate users.

A new paradigm in the Software Defined Network (SDN) architecture separates the control plane and the data plane. In SDN, the controller controls the network, and data planes work to forward the device [4]. So, the controller can easily manage the entire network from a single point [5]. With this separation, network management is even easier so that it can manage more and more complex. However, this separation results in various challenges, including security challenges. In addition to the general traditional attacks, SDN has its special attack [6]. The controller is a single point of failure in SDN, which is the most dangerous of various attacks because when the attacker controls the controller, the attacker will control all network traffic. One of the attacks that often occurs is

DDoS. The peak of a DDOS attack is when a legitimate user does not get service from the controller.

Various security solutions to reduce and prevent DDoS attacks on SDN are already discussed. The detection system is the first step in DDoS attack solutions. Moreover, it has been discussed comprehensively in [3],[7]. Various detection and mitigation system methods have been offered, including information theory, machine learning, and artificial intelligence. However, aspects that must be considered in SDN's detection and mitigation system are that detection and mitigation systems must be lightweight and early detection[8]–[13]. Due to the limited resources in SDN controllers, the memory capacity is very small [14] and performs multitasking. Furthermore,

Security aspects at SDN still receive special attention given the importance of these aspects [15], [16]. DDoS attacks can be divided into three categories, namely: volume-based attacks, protocol-based attacks, and application layer attacks. There are several types of known DDoS attacks [17] shown in Figure 1.

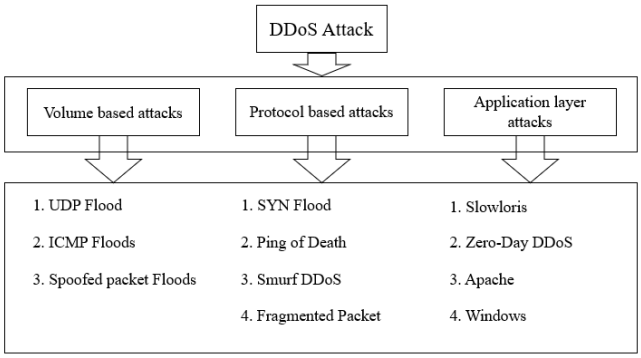

Fig. 1 Classification of DDoS Attacks [17]

- The first is volume-based attacks, all the available bandwidth between the target and the internet consumed by the attacker, allowing for congestion. The way is to send a number of requests to the victim in large numbers requests [2]. ICMP Flood attack is one example of this categorization[3].
- Second is Protocol-based attacks, also known as state-exhaustion attacks, where the strategy is to use up the available table capacity on the server or other resources such as firewalls. This attack takes advantage of the weaknesses in layers 3 and 4 to be inaccessible to the target[2]. TCP-SYN Flood attack is one example of this categorization [3].
- The third is an application attack; the goal of this attack is exhaustion the resources. The attacker dominates network traffic by consuming server resources from the connections made to the victim. The attacker exploits the weaknesses of layer 7 [2].

Application layer attacks are more difficult to detect than volume-based attacks and protocol-based attacks because a larger amount of traffic is sent, making them quite similar. There are many types of DDoS attacks, but this research only discusses TCP SYN attacks, UDP Flood attacks, and ICMP attacks, which refer to the dataset of DDOS attack SDN Dataset [1], [18], [19]. Many features are taken into the calculation in the dataset to detect DDoS, which causes the detection process to take a long time and waste resources, even though the detection system on SDN requires lightweight and early detection because limitation of SDN resources. Therefore, in this research, the author makes use feature selection method to reduce the calculations performed.

There have been many studies on detection systems of DDoS attacks, but there are still some limitations that can be investigated further, namely:

- Detection system: most of the research focuses on high accuracy without considering the resource limitation of the controller. Differences in characteristics and traffic patterns between normal traffic and attack traffic are still the approach method for detection systems.
- Mitigation system: few of the research work focuses on a mitigation system. Because once a DDoS attack is detected, DDoS attacks are much more difficult to detect because it is very difficult to distinguish between large amounts of normal traffic and DDoS traffic or DDoS traffic at a low rate and normal traffic.
- The complexity of the detection system: several approaches based on deep learning and machine learning have been carried out, but they have complex operations and require a long time in the detection process; moreover, SDN requires early detection.

According to previous research [1],[18] for problem-solving, we improve the feature selection scheme in DDoS attack detection in this research. The following contribution of this research:

- Categorize between attack and normal traffic in the dataset [19]: In order to differentiate between attack traffic and normal traffic, an investigation of traffic traces is carried out to find the features that have the most influence;
- Proposing a novel feature selection method: based on these features, using three different methods to see the consistency of the results. The three methods used are the filtering method, wrapper method, and embedded method.

The organization of this paper is as follows. Section 2 discusses the materials and methods that contain analysis of current detection system research. Section 3 result and discusses how to distinguish normal and attack traffic with a model and analysis of important features. This section also discusses details of our proposed approach, including feature selection methods. And section 4 conclusion and the work present a challenge and future work.

II. Materials and Method

Numerous research works on DDoS attack detection on SDN are presented here. This part summarizes SDN, DDoS attack, and DDoS attack detection methods. Detection methods used for Intrusion detection systems (IDS) can be classified into three, namely [20]: anomaly-based, signature-based, and hybrid-based detection techniques.

A. Signature-Based Detection Techniques

The characteristic of this method is that it has a repository of attack signatures, and this repository is used as a comparison with network traffic against [21]. A detection alert is raised when the match is found. The advantages of this method are that if the attack pattern already exists in the

repository, it will be easy to detect, but if the attack pattern is not in the repository, then the attack cannot be detected. It is the weakness of this method [22].

B. Anomaly-Based Detection Techniques

The characteristic of this method is to see anomaly traffic compared to the traffic baseline in general, which is monitored continuously [23]. This method compares the actions of the system with the baseline is then utilized. This method's weakness is that every deviation from the authorized threshold is recorded using an alarm, but no classification for the detected attack is provided [21]. This method is very effective for a new attack pattern compared with signature-based detection techniques.

C. Hybrid-Based Detection Techniques

This method combines the two previous methods to get a better one. Ahuja et al. [1] classified normal traffic and attack traffic based on the features in the data set with deep learning algorithms. The first stage is pre-processing, where traffic is classified into one of the classes. And applying Stacked Auto-Encoder Multi-Layer Perceptron (SAE-MLP) resulted in an accuracy score of 99.75% explained in the paper. But in this research, the selection process has not been carried out so that all features are still taken into the detection process.

Balkanli et al. [24] discuss the effects of the usage of distinct feature selection algorithms on robust backscatter DDoS detection. By employing two well-known feature selection algorithms, namely Chi-Square and Symmetrical Uncertainty, four different training sets with four different feature sets are analyzed, together with the Decision Tree classifier. The research results show that it is feasible to expand a robust detection system that can generalize well to the converting backscatter DDoS behaviors over time using a small number of selected features. However, in this research, the dataset DDoS attack is still for traditional networks, not for SDN.

Another research by Matsa et al. [25] revealed that the Canadian Institute of cybersecurity intrusion detection systems implemented the Forward Feature Selection (FFS) method for selecting the best features for distributed denial of service attacks. By used Deep Learning, an advanced machine learning approach, convolutional neural network, and deep neural network was used to enforce a hybrid method of combining two deep learning algorithms. Using the FFS method, this research used feature selection to detect distributed denial of service on the SDN. This algorithm still has a high computational cost because evaluating capabilities do one by one after the other till the quality-acting functions are determined.

Abbas et al. [26] address attack-specific feature selection to identify the features that impact anomaly detection most. DoS, DDoS, brute force, probe, web, and botnet attacks classify by SDN intrusion dataset. And then, pre-processing is carried out using feature selection to select the most influential features in the different attacks. The selected features will be used to train the model, lowering the computational cost of modeling while preserving the model's overall performance. Distinct evaluation and simulation consequences are then supplied to expose the major functions and their impact on the different attacks, such as brute force, web, DoS, probe, DDoS, and botnet attacks.

Polat et al. [27] studied SDN, specifically security SDN; the experiment shows DDoS attacks in SDN have been detected using machine learning-based models. Early-stage specific features were received from SDN for the dataset in normal traffic and under DDoS attack traffic. And then, feature selection methods were to simplify the models, facilitate their interpretation, and provide a shorter training time. And those datasets, both with and without feature selection methods, were trained and tested with Naive Bayes (NB), Artificial Neural Network (ANN), K-Nearest Neighbors (KNN), and Support Vector Machine (SVM) classification models. However, the computational cost is still high because the number of selected features became determined either through the algorithm itself or by the threshold value given to the algorithm.

Data or dataset is a collection of data objects that represent an entity or attribute. Attributes represent the characteristics of a data object. The data object is also known as a record, point, sample, or instance. Examples of attributes in the data are source IP, destination IP, and destination port. Attributes are also known as variables or features. One public dataset is obtained from Mendeley [19] in this study.

The wrapper, filter, and embedded methods were used as feature selection methods. To achieve its goal, each feature selection method has its own algorithm. In the initial stage, data exploration was carried out. It aims to understand the data. The understanding of this data helps in determining the technique to be used and assists in the process of analyzing the data. From the dataset obtained, such as the amount of data and the type of data, the total data in the dataset is 104,345, with 23 features. The following are the features and data types of the features.

TABLE I
FEATURE AND TYPE OF DATA

NO	Feature	Type of data
1	dt	int64
2	*switch*	int64
3	src	object
4	dst	object
5	pktcount	int64
6	bytecount	int64
7	dur	int64
8	dur_nsec	int64
9	tot_dur	float64
10	*flow*s	int64
11	packetins	int64
12	pktper*flow*	int64
13	byteper*flow*	int64
14	pktrate	int64
15	Pair*flow*	int64
16	Protocol	object
17	port_no	int64
18	tx_bytes	int64
19	rx_bytes	int64
20	tx_kbps	int64
21	rx_kbps	int64
22	tot_kbps	float64
23	label	float64

Table 1 shows that there are three different types of data from 23 features, namely int64, object, and float64. Programming languages recognize several types of data, such as integers. An integer data type is a data type that consists of whole numbers (does not contain fractional values or decimal values) in the form of positive or negative numbers. One type of integer data is int64, and another type of data is a float, consisting of decimal numbers in the form of fractional numbers. The last is the object data type, which is a data type that not only stores data but also contains information on how to process the data.

The null value is checked and handled in the next stage by dropping the record. That is applied because the technique used is supervised. After checking, 1012 data are null, and the data are dropped. After that, the duplication of data is checked. This data duplication has two possibilities: identical data or, indeed, duplicates. There were 5091 duplicate data dropped on the data because it was duplicated. The following process is to recheck the data and get a total of 94,797 data with 23 features.

After that, the protocol feature changes the value where previously it was an object whose contents contained TCP, UDP and ICMP were changed to integer form where ICMP was changed to 1, TCP became 2, and UDP became 3. To be able to perform further calculations. Then the next step is to check each feature's mean, standard deviation, min, and max. After that, we examine the data distribution for each feature to see whether there is an anomaly, then check outliers for each feature.

III. Result and Discuss

A. *Filtering Based*

The first method is the filtering method, where the filtering process is conducted using a heatmap. Statistical method used to achieve of the features calculated by filter-based feature selection method which provide very good contributions. In Figure 2, the process given to the reduced feature set is made by selecting the best feature set of the assessed features. In this research, the heatmap algorithm is used to describe the distribution of places and frequencies of statistics in coloring. Heatmap is a graphical illustration of record data where the individual values contained in a matrix are represented as colors. The values taken by variables in the hierarchy are represented by a color-coding system similar to that used by both fractal maps and tree maps. This calculation's results create a model, and the feature selection process is carried out [28], [29].

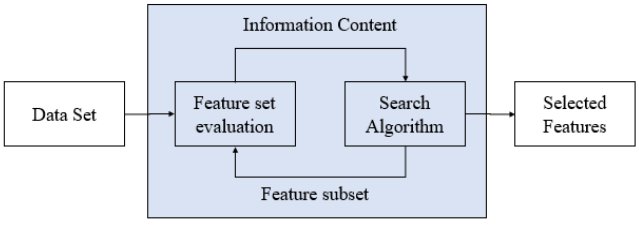

Fig. 2 Algorithm of A filter-based feature selection

The following is the result of feature selection using the filter-based method in Figure 3. Colors on a heatmap have different meanings. The dark green color shows a strong relationship between features and labels. The label feature here is an attack determinant, not the yellow indicates less correlation, and the red indicates no correlation between features and labels. From the heatmap, several features that influence DDoS attacks, in this case, labels, are found. Here are 10 features with the highest correlation value to labels.

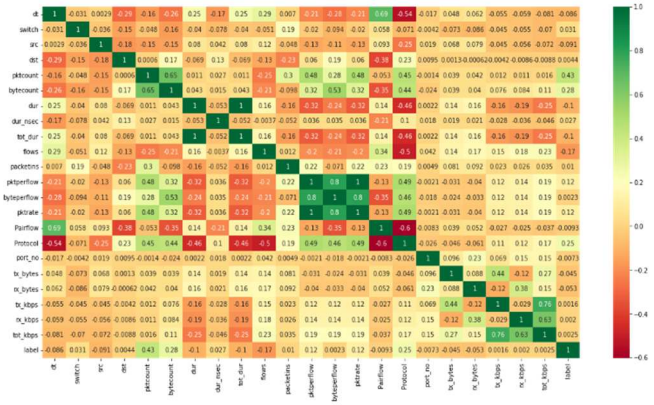

Fig. 3 Heatmap of Dataset

From Table 2, it can be seen below that of the 23 features, the ten features above are the most influential on DDoS attacks, and the pktcount feature is the highest. The pktcount feature counts the number of packages in a given time. That is closely related to DDoS attacks because this attack requires the process of transmitting a large number of packets in a given time (flooding attack) [30].

TABLE II
HEATMAP RESULTS 10 FEATURES THAT AFFECT DDOS ATTACKS

NO	Feature	value
1	pktcount	0.43
2	bytecount	0.28
3	Protocol	0.25
4	pktper*flow*	0.12
5	pktrate	0.12
6	*switch*	0.031
7	dur_nsec	0.027
8	packetins	0.01
9	Dst	0.0044
10	byteper*flow*	0.0023

B. *Wrapper Based*

This method uses a classification algorithm; all features are tried to find the ideal attribute. From figure 4, it can see the process is finished when the ideal subset of features is reached then a reduced data set is created. One of the wrapper-based feature selection algorithms is the feature importance selection algorithm used in this research. Feature importance shows how often an attribute is used in constructing a tree by calculating the information gained. The higher the value, the higher the importance of the attribute. The algorithm used is a decision tree. The decision tree is a method that uses two approaches, namely averaging and boosting. The averaging approach builds several basic models, and the average of each model is used as the final prediction. Boosting approach builds several base models sequentially, where the error function is used to train a particular model depending on the previous model's performance model. The following are the results of calculating feature importance on the DDoS attack dataset on SDN.

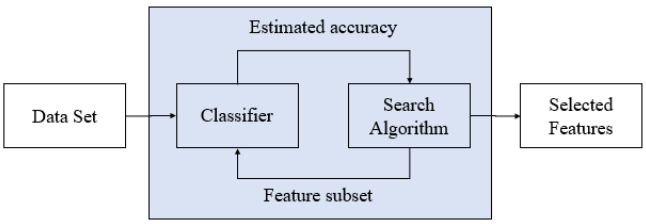

Fig. 4 Algorithm of A wrapper-based feature selection

The following is the result of features selection using the wrapper-based method:

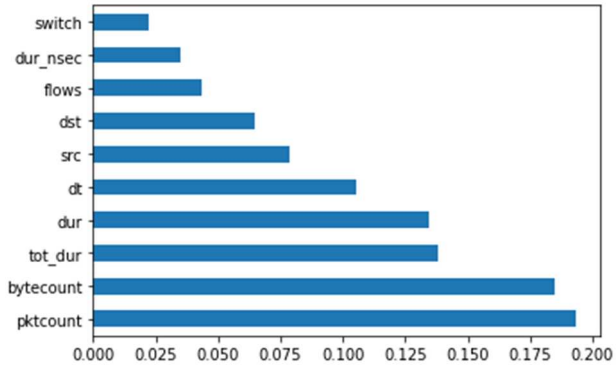

Fig. 5 The results of the calculation of the Importance Feature taken are the 10 highest

Figure 5 shows that the features that have the most influence on DDoS attacks are pktcount, then bytecount, tot_dur, dt, scr, dst, flows, dur_nsec, and switch. Pktcount remains the most important because it is closely related to DDoS attacks. After all, this attack involves sending a large number of packets in a certain amount of time (flooding attack) [30].

C. Embedded Based

This method used a classification algorithm to choose the feature with the most impact. In figure 6, in this algorithm, the features that contribute the most to the accuracy of the model are identified by feature selection. The purpose of feature selection is to reduce irrelevant features in the detection process. In this research, one of the embedded-based feature selection algorithms used is the Chi-Square algorithm. This algorithm used statistical theory to test the independence of a term with its category. Eliminating confounding features in classification is one of the feature selection purposes. In Chi-Square feature selection based on statistical theory, two events, namely the appearance of features and the appearance of categories, are then sorted for each term value from the highest. The Chi-Square test in statistics is applied to test the independence of the two events. From the calculation of the feature importance, 10 data with the highest score among other features can be seen in table 12 below:

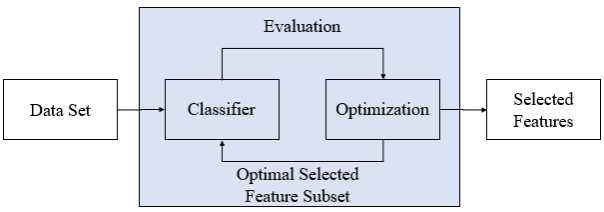

Fig. 6 Calculation Results Using Univariate Selection

Table 3 shows that the features that have the most influence on DDoS attacks are pktcount, switch, dt, bytecount, dst, flows, scr, dur, tot_dur, and dur_nsec. Pktcount remains the most important about DDoS because it is closely related to DDoS, which the name of this attack is the process of sending large packets in a certain amount of time (flooding attack) [30]. From the three methods, 3 features are taken as input for calculating the detection system. The three features are as follows: pktcount, scr, and so on

IV. Conclusion

In this research, DDoS attacks are serious attacks on software define networks. That leads us to try to find feature importance in DDoS attacks. The discovery of the most important feature is needed to get a lightweight and early detection solution for DDoS attacks. This research has used the DDoS attack on SDN dataset, which is the complete dataset accessible by the Mendeley dataset. It also examined three diverse machine learning methods: filter-based, wrapper-based, and embedded-based. The result of the experiment shows that the three methods show different results. The filter-based method discovers the top three most influential features: pktcount, bytecount, and protocol. Compared to that, the wrapper-based method discovered that pktcount, bytecount, and tot_dur are the most influential feature. Lastly, the top three most influential features using the embedded-based method are pktcount, switch, and dt. However, the result shows there are similarities between the three methods; pktcount gets the highest score for the three methods. Our research proposes to contribute to the research conducted on the detection of DDoS systems in SDN. This paper contributes that, as shown in experiments, feature selection methods are important for the detection of DDoS system, which requires lightweight and early detection because of the limited resources owned by SDN. Finally, the limitations and future possibilities of the result of this study as input for the calculation of the detection system are explored.

Limited resources and computing complexity in a controller characterize the software-defined network. These variables significantly add to the difficulty in security issues at SDN difficulties in security system issues, including the detection of DDoS systems. Despite the many studies on DDoS detection systems in SDN, many challenges still need to be studied in more depth. For instance, create public SDN traffic datasets because assessing and validating DDoS prevention strategies on real networks will be difficult, so efforts to create datasets are very important. And this will make the evaluation and validation of DDoS detection techniques on SDN much easier. It is possible to use deep learning methods to identify and check packets in real-time against datasets because deep learning methods can split the data and compare it with the performance of the classifier's utilization. The results of this study are used as input for the DDoS detection system in SDN, which requires lightweight and early.

References

[1] N. Ahuja, G. Singal, and D. Mukhopadhyay, "DLSDN: Deep learning for DDOS attack detection in software defined networking," *Proc. Conflu. 2021 11th Int. Conf. Cloud Comput. Data Sci. Eng.*, pp. 683–

688, 2021, doi: 10.1109/Confluence51648.2021.9376879.
[2] N. N. Tuan, P. H. Hung, N. D. Nghia, N. Van Tho, T. Van Phan, and N. H. Thanh, "A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN," *Electron.*, vol. 9, no. 3, pp. 1–19, 2020, doi: 10.3390/electronics9030413.
[3] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *Int. J. Distrib. Sens. Networks*, vol. 13, no. 12, 2017, doi: 10.1177/1550147717741463.
[4] Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, "Security in Software-Defined Networking: Threats and Countermeasures," *Mob. Networks Appl.*, vol. 21, no. 5, pp. 764–776, 2016, doi: 10.1007/s11036-016-0676-x.
[5] Ö. Tonkal, H. Polat, E. Başaran, Z. Cömert, and R. Kocaoğlu, "Machine learning approach equipped with neighbourhood component analysis for ddos attack detection in software-defined networking," *Electron.*, vol. 10, no. 11, 2021, doi: 10.3390/electronics10111227.
[6] J. C. Correa Chica, J. C. Imbachi, and J. F. Botero Vega, "Security in SDN: A comprehensive survey," *J. Netw. Comput. Appl.*, vol. 159, no. December 2018, p. 102595, 2020, doi: 10.1016/j.jnca.2020.102595.
[7] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Comput. Electr. Eng.*, vol. 15, no. 4, pp. 2046–2069, 2013, doi: 10.1016/j.compeleceng.2018.09.001.
[8] S. Oshima, T. Nakashima, and T. Sueyoshi, "Early DoS/DDoS detection method using short-term statistics," *CISIS 2010 - 4th Int. Conf. Complex, Intell. Softw. Intensive Syst.*, pp. 168–173, 2010, doi: 10.1109/CISIS.2010.53.
[9] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in *2015 International Conference on Computing, Networking and Communications, ICNC 2015*, 2015, pp. 77–81, doi: 10.1109/ICCNC.2015.7069319.
[10] R. Li and B. Wu, "Early detection of DDoS based on phi-entropy in SDN networks," *Proceedings of 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2020*. pp. 731–735, 2020, doi: 10.1109/ITNEC48623.2020.9084885.
[11] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in *Proceedings - Conference on Local Computer Networks, LCN*, 2010, pp. 408–415, doi: 10.1109/LCN.2010.5735752.
[12] K. S. Sahoo, D. Puthal, M. Tiwary, J. J. P. C. Rodrigues, B. Sahoo, and R. Dash, "An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics," *Futur. Gener. Comput. Syst.*, vol. 89, pp. 685–697, 2018, doi: 10.1016/j.future.2018.07.017.
[13] K. Kalkan, L. Altay, G. Gür, and F. Alagöz, "JESS: Joint Entropy-Based DDoS Defense Scheme in SDN," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 10, pp. 2358–2372, 2018, doi: 10.1109/JSAC.2018.2869997.
[14] M. Yue, H. Wang, L. Liu, and Z. Wu, "Detecting DoS Attacks Based on Multi-Features in SDN," *IEEE Access*, vol. 8, pp. 104688–104700, 2020, doi: 10.1109/ACCESS.2020.2999668.
[15] D. B. Rawat and S. R. Reddy, "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 1, pp. 325–346, 2017, doi: 10.1109/COMST.2016.2618874.
[16] L. F. Eliyan and R. Di Pietro, "DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges," *Futur. Gener. Comput. Syst.*, vol. 122, pp. 149–171, 2021, doi: 10.1016/j.future.2021.03.011.
[17] M. Malik and Y. Singh, "A Review: DoS and DDoS Attacks," *Int. J. Comput. Sci. Mob. Comput.*, vol. 4, no. 6, pp. 260–265, 2015.
[18] N. Ahuja and G. Singal, "DDOS Attack Detection Prevention in SDN using OpenFlow Statistics," *Proc. 2019 IEEE 9th Int. Conf. Adv. Comput. IACC 2019*, pp. 147–152, 2019, doi: 10.1109/IACC48062.2019.8971596.
[19] N. Ahuja, G. Singal, and D. Mukhopadhyay, "DDOS attack SDN Dataset," vol. 1, no. September, p. 17632, 2020, doi: 10.17632/jxpfjc64kr.1.
[20] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, 2017, doi: 10.1016/j.jnca.2017.02.009.
[21] R. J. Alzahrani and A. Alzahrani, "Security analysis of ddos attacks using machine learning algorithms in networks traffic," *Electron.*, vol. 10, no. 23, 2021, doi: 10.3390/electronics10232919.
[22] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, N. Kumar, and M. M. Hassan, "A Privacy-Preserving-Based Secure Framework," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 1–12, 2022.
[23] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan, and K. K. R. Choo, "A Privacy-Preserving-Framework-Based Blockchain and Deep Learning for Protecting Smart Power Networks," *IEEE Trans. Ind. Informatics*, vol. 16, no. 8, pp. 5110–5118, 2020, doi: 10.1109/TII.2019.2957140.
[24] E. Balkanli, A. Nur Zincir-Heywood, and M. I. Heywood, "Feature selection for robust backscatter DDoS detection," *Proc. - Conf. Local Comput. Networks, LCN*, vol. 2015-Decem, pp. 611–618, 2015, doi: 10.1109/LCNW.2015.7365905.
[25] L. S. Matsa, G. A. Zodi-Lusilao, and F. Bhunu-Shava, "Forward Feature Selection for DDoS Detection on Cross-Plane of Software Defined Network Using Hybrid Deep Learning.," *2021 3rd Int. Multidiscip. Inf. Technol. Eng. Conf. IMITEC 2021*, 2021, doi: 10.1109/IMITEC52926.2021.9714561.
[26] N. Abbas, Y. Nasser, M. Shehab, and S. Sharafeddine, "Attack-Specific Feature Selection for Anomaly Detection in Software-Defined Networks," in *2021 3rd IEEE Middle East and North Africa COMMunications Conference, MENACOMM 2021*, 2021, pp. 142–146, doi: 10.1109/MENACOMM50742.2021.9678279.
[27] 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, p. 1035, 2020, doi: 10.3390/su12031035.
[28] Z. M. Hira and D. F. Gillies, "A Review of Feature Selection and Feature Extraction Methods Applied on Microarray Data," *Adv. Bioinformatics*, vol. 2015, no. 1, pp. 2–4, 2015.
[29] B. Venkatesh and J. Anuradha, "A review of Feature Selection and its methods," *Cybern. Inf. Technol.*, vol. 19, no. 1, pp. 3–26, 2019, doi: 10.2478/CAIT-2019-0001.
[30] M. De Donno, A. Giaretta, N. Dragoni, and A. Spognardi, "A taxonomy of distributed denial of service attacks," *Int. Conf. Inf. Soc. i-Society 2017*, vol. 2018-Janua, pp. 100–107, 2018, doi: 10.23919/i-Society.2017.8354681.