Machine Learning for Securing SDN based 5G Network

Article *in* International Journal of Computer Applications · January 2021

DOI: 10.5120/ijca2021921027

3 authors:

Hassan Alamri
Umm Al-Qura University
3 PUBLICATIONS **69** CITATIONS
SEE PROFILE

Vijey Thayananthan
King Abdulaziz University
84 PUBLICATIONS **509** CITATIONS
SEE PROFILE

Javad Yazdani
University of Central Lancashire
287 PUBLICATIONS **877** CITATIONS
SEE PROFILE

Machine Learning for Securing SDN based 5G Network

Hassan A. Alamri
Department of Computer Science
King Abdulaziz University
Jeddah, KSA

Vijey Thayananthan
Department of Computer Science
King Abdulaziz University
Jeddah, KSA

Javad Yazdani
School of Engineering
Faculty of Science and Technology
University of Central Lancashire

ABSTRACT

The fifth-generation (5G) network supports many systems such as reliable communication in potential applications that require maximum security. Advancement in Software-Defined Networking (SDN) is growing with the emerging network architectures targeted from many servers with the various types of Distributed Denial of Service (DDoS) attackers. When malicious users send DDoS attacks, the SDN based 5G networks face security problems and challenges. Despite the security solutions for preventing DDoS attacks in SDN, securing the SDN controller is one of the challenging problems. The purpose of this research is to analyze the suitable machine learning (ML) for securing the SDN controller targeted by DDoS attacks. This paper proposes a security scheme that includes the ML algorithm, adaptive bandwidth mechanism, and dynamic threshold technique. Therefore, the main focus is on the mitigation scheme of DDoS attacks considered in SDN controller through the ML trained model. In this scheme, the proposed approach uses the best ML as a method for finding security solutions that enhance the security of the SDN controller and network performance. In this method, the Extreme Gradient Boosting (XGBoost) and other ML algorithms were used, which not only enhance the accuracy of the security solutions but also improve the overall network performance.

General Terms

In this paper, the security of the SDN based 5G network is considered as a general term. Throughout this research, ML and detection technique of DDoS is considered to improve the security solutions of SDN based 5G networks.

Keywords

Machine learning; Distributed Denial-of-Service; SDN based 5G networks; Security solution; Extreme Gradient Boosting Algorithm (XGBoost)

1. INTRODUCTION

Advancing technology with SDN has introduced and created a new era of managing network and securing SDN based 5G network. Recent advances in security solutions have secured the existing network and have made a huge demand for securing the 5G communication network and beyond. Combining SDN technology and ML techniques not only provide the programmability but also enhances the accuracy of security solutions. With the recent DDoS attacks in the existing and SDN based 5G network, the demand for security solutions has become high. Although users expect the SDN based 5G network with low-cost security solutions, DDoS attacks and their mitigation process take more bandwidth. It means that bandwidth usage has increased exponentially when developing efficient security solutions. Regarding the network traffic classification, ML algorithms and SDN play an important role with a large number of network resources and features. Therefore, in this research, traffic classification based on ML is considered in the security solution, which supports securing SDN based 5G networks. Although many possible security solutions are available, ML-based security enhances the performance of SDN based 5G network affected by the DDoS attacks.

Studying and investigating the existing security issues and solutions for SDN based 5G networks are considered in much recent news through the industries' white papers. These demands motivate us to improve the security solutions in the potential systems related to all SDN based 5G networks. Thus, DDoS attacks are increasing from various resources because all systems connect with many resources and servers. So, a DDoS detection system is developed using ML and an adaptive bandwidth mechanism. Also, it is found that the SDN itself needed some security solutions for securing SDN controllers. In this research, multiple SDN controllers are employed for improving overall security solutions with the XGBoost algorithm. In the ML techniques, XGBoost enhances the accuracy of the adaptive bandwidth and DDoS detection.

Based on the study and investigation of security solutions, the ML classification for DDoS attacks and trained models for testing security solutions are established. Existing datasets helped us to analyze the model and improve security solutions. SDN has become a powerful paradigm due to the tremendous traffic growth and technology evolution, such as 5G, IoT, and big data. However, the main limitation of such a paradigm is the security aspect caused by the centralization point of SDN architecture. The primary threat to SDN is DDoS attacks, which occur in many security challenges of 5G. They are between the 5G access networks and edge clouds, links between the gateways and application servers, etc. Therefore, the scope of this research is to propose a robust security solution that protects the SDN based 5G network and emerging 5G network environment from the DDoS attacks created by DDoS attackers with minimum overhead.

Many network hosts and servers try to avoid DDoS attacks and abnormal network traffic. Identifying such traffic within the public web servers and individual 5G network hosts are not easy. In this situation, developing ML techniques within the SDN controllers will enhance the accuracy of finding abnormal traffic and the security level of the SDN-based security solutions. In this paper, a DDoS attack detection system has been presented using ML and SDN controllers.

In this research, the focus is on security issues of DDoS detection techniques through the following contributions. The main contribution of this paper is to develop a security solution influenced by adaptive bandwidth mechanism and dynamic threshold technique based on the ML technique, which supports the DDoS detection methods with SDN. Moreover, an SDN-based 5G network is prepared with the dataset to build and test the proposed ML model. In this contribution, the XGBoost algorithm is considered as an ML technique.

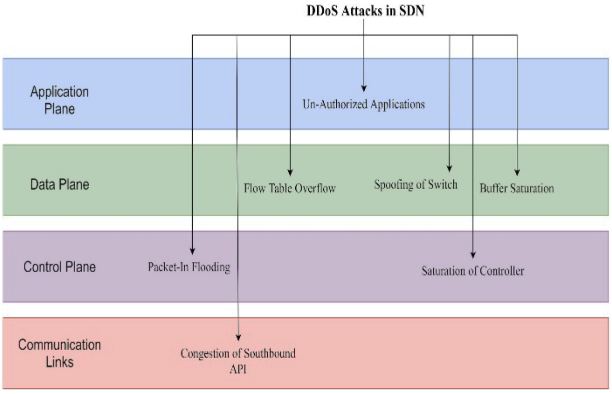

Fig 1: Types of DDoS attacks at different layers of SDN

As shown in Figure 1, SDN has to face many types of DDoS attacks targeted in all three planes of SDN [1]. Although four layers are considered for DDoS attacks, the communication between the controller and switches allows the DDoS attacks to attack three planes of SDN through the communication links.

The rest of the paper focuses on the detection technique of DDoS attacks for securing SDN based 5G networks with the following sections. Some literature reviews and approaches of ML are discussed in section 2. After that, section 3 provides the proposed solution, which is the ML for securing SDN. Section 4 introduces the idea of managing traffic classification models for ML algorithms through the datasets influenced by ML. Also, the selected ML algorithms are elaborated in this section. Analysis of the proposed solution with ML in section 5. In this analysis, the performance of security solutions is covered. Section 6 summarizes the points as conclusions and includes future work of securing the SDN controller.

2. LITERATURE REVIEW

This section discusses the four different approaches used for analyzing the ML, securing the SDN controller, and some attacks involved in this research. According to [1], the DDoS attacks in SDN and cloud computing environments allow us to learn the evolving DDoS attacks and SDN based technologies during the heavy traffic and massive data in modern network architecture and applications. Regarding the SDN based on architecture, issues, and challenges of securing SDN controllers, it is very important to analyze the limitations of traditional and SDN-based networks [2]. Here, SDN plays an important role in improving security and controllability, limiting the level of security through SDN properties such as programmability, logically centralized control, and simplified management. An evolutionary Support Vector Machine (SVM) model for DDoS attack detection in SDN is introduced in [3] to secure and analyze the emerging network architecture influenced by SDN control and data planes. According to [4, 5], deep learning, and other ML approaches for intrusion detection in software-defined networking allow us to understand SDN controllers' detection techniques where DDoS attacks are increasing in the emerging networks. Although many detections and mitigation techniques are available, paper [6] provides early detection of low rate DDoS attack to SDN based data center networks using information distance metrics. This technique improves and controls the traffic securely with efficient SDN based traffic management, which not only secures the data center but also prevents DDoS attacks. These days SDN supports improving the emerging network and novel dynamic framework [7 – 10] where many detection approaches are focused on detecting DDoS. They are SDN using metaheuristic clustering, joint entropy-based DDoS defense scheme, an attacks detection system for OpenStack-based private cloud, etc. In addition, SDN based cloud computing environment is secured by DDoS attacks and detected by one of these detection techniques.

Distributed Denial of Service (DDoS) attack is an attempt to cripple the targeted service or network by flooding the target with massive internet traffic. Such an attack uses a set of compromised network sources such as computers (bots) to simultaneously send the malicious traffic to the target to prevent access for the legitimate traffic to the network resources [10, 11]. DDoS attacks can be classified into three main categories [12], namely: volume-based attacks, protocol-based attacks, and application-layer attacks. Machine learning is a subfield of Artificial Intelligence (AI) that enables system algorithms to learn and improve through the experience without human intervention [13]. Security threats in SDN are categorized into three categories based on the SDN architecture, which are threats to the application layer, threats to the control layer, and threats to the data layer [14, 15]. In the SDN environment, the communication between the controller and the switches is vulnerable to the man in the middle attack due to the indirect connection between the controller and switches. Thus, the attacker can place an agent node between the controller and switches to perform several attacks such as session hijacking, DNS spoofing, eavesdropping, and black hole attack [16]. In the SDN data layer, the DoS attack overflows the buffer flow and the flow table by sending a large number of packets to the switches. The buffer flow and the flow table of the switches have limited space; thus, the attacker exploits this weakness to perform such an attack. As a result, the flow table of the switches as well as the buffer flow will be overloaded, and the coming legitimate packets get dropped [17]. Solutions [18] that have been proposed under this approach are based on some predefined rules on the traffic flow.

According to [19, 20], the ML techniques are focused to improve the security solutions in the SDN based emerging networks. Here, the detection system of HTTP DDoS attacks in a cloud environment based on information-theoretic entropy and random forest (RF) is introduced. In addition, an adaptive DDoS attack detection method based on multiple kernel learning is considered for analyzing security solutions. Papers [21, 22] focus on threshold approaches to improve the security solutions which detect and minimize the DDoS attacks. Here, Dynamic Controller Scheduling (DCS) Strategy can be considered to enhance controller robustness against DDoS attacks. Initially, switches and controllers are assigned to each other by performing bidirectional selection mapping through preference lists that are based on some metrics of both controllers and switches. Then, DCS applies an optimal mapping algorithm to finalize the controller-switches mapping since the bidirectional selection mapping forms an initial mapping only. DCS works along with the defense scheme to reduce the controller's overhead and optimize the controller response time.

Although many ML approaches for analyzing SDN controllers were investigated, some ML examples through these papers [23- 27] are considered. They are ML-based DDoS attacks detection, ML-based modern type DDoS detection, advanced support vector machine- (ASVM-) based detection, applied computing, and informatics HTTP flood attack detection in application layer using ML metrics and bio-inspired bat algorithm.

Paper [28] focuses on the defense method for securing the SDN-based cloud with 3 ML approaches. They are ML-based on SOM and SVM, enhanced history-based IP filtering scheme (eHIPF), and hybrid scheme, which is the combination of ML-based and eHIPF. A Safe-guard scheme (SGS) for protecting the control plane against DDoS attacks in software-defined networking not only improves the security solutions but also enhances the overall protections [29]. Here, the controller dynamic defense module plays an important role in detecting the anomaly traffic in the multiple controllers located in the control plane of SDN. In this module, SGS uses the controller's clustering method for minimizing the effects of DDoS attacks.

According to [30 – 34], ML techniques minimize the effect of DDoS attacks and increase the accuracy of security solutions. Here, the authors used four supervised ML algorithms and training models with the dataset; they are DT, SVM, Logistic Regression (LR), and KNN. Further, ML supports to develop a flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks. Hybrid ML techniques enhance the security solution and allow us to analyze the detection of DDoS attacks on the SDN control plane. The authors used the CICDoS 2019 data set to analyze the performance of some ML algorithms; they are Random Tree (RT), REP Tree, RF, SVM, etc. In the ML, XGBoost Classifier and an interpretable learning algorithm based on XGBoost support to analyze the DDoS attacks and fault predictions in the optical network, respectively. Also, the XGBoost algorithm improves the security performance of security solutions with maximum accuracy, high speed, low false rate, etc.

In order to effectively learn the measurements of the DDoS attacks, ML algorithms will require a considerable amount of data. In the ML, evaluation metrics with the dataset and data representation obtained from the DDoS attacks will allow us to analyze the performance of the SDN based 5G network with the different ML algorithms. Regarding the measurements, the ML algorithms (LR, RF XGBoost) and the entire dataset to analyze the precision, recall, and F1 measure is considered [35]. According to [36], the NSL-KDD dataset is evolved from the KDDCup'99 dataset, and it supports to solve various types of DDoS attacks during the traffic classification. Regarding the cross-validation, these datasets are copied and used for testing the DDoS problems. Also, some copies are used in the ML approaches as a training set of ML trained models.

An intelligent trust model for hybrid DDoS detection in SDN enhances the trust management and security solutions of SDN based 5G networks [37]. Without an efficient protection mechanism, the SDN controller is flooded with unsecured traffic, which damages the function of the SDN controller and degrades the performance of the SDN based 5G networks. The depletion of bandwidth and other SDN based 5G network resources depend on the secured traffic damaged by the adversary who attacks using massive forged packets and traffic.

Although many techniques of DDoS detection are available, ML is becoming a popular technique for detecting DDoS attacks in 5G, SDN-based 5G networks, 5G+, etc. Table 1 shows some examples of ML-based DDoS detection used for SDN based 5G networks. The SDN based 5G technology supports to develop secure emerging networks that enhance the secure communication services within the 5G and 5G+ systems and applications. Features of 5G and beyond, such as user-centricity, flexibility, scalability, etc., depending on the SDN controllability and other properties. When DDoS attackers target the SDN controllers, traffic involved with 5G features and services will be affected.

From the security perspective, the SDN controller handles the rules securely and keeps all security policies set by the network manager. Although security policies are changeable, the SDN controller handles dynamically according to the security problems considered in the adversary model of the underlying network or requirements of the business applications.

Table 1. DDoS detection in SDN based 5G using ML

DDoS attacks in SDN based 5G network	**ML methods**
SDN based traffic affected by DDoS attackers. To detect DDoS attacks	Neural network model, SOM
Collected flow entries with fixed time intervals at the SDN controllers	Periodic flow-based detection
Bloom filter used in switch memory to manage the DDoS traffic	Load balancing, Bloom filter
Lower down the burden between control-plane and data-plane.	Interface mitigation.
Semi-supervised to detect anomalies in SDN.	SVM anomaly detection

The detector of the security solution depends on the supervised classifier. In the ML techniques, the classifier must be trained before starting to detect the DDoS attacks. In order to train the classifier, labeled samples of the dataset obtained from the DDoS related traffic can be used. Normal and abnormal network traffic can be guessed from the previous behaviors of a fixed period of network data. Collecting these previous data allow us to build the training database and ML trained model for identifying and analyzing the network traffic.

Some DDoS attacks spoil the SDN based on 5G networks dynamically when using the 5G based autonomous systems. In the 5G network systems, some examples of the 5G security challenges are as follows:

- The link between the access network and users or IoT when flash network traffic occurs.
- During the radio interfacing, DDoS attacks are networked through connected devices.
- DDoS prevention is essential for managing virtual services user plane integrity.
- Mandated cybersecurity, cyberattacks, DDoS protection in the network involved with SDN and IoT core functions
- DoS attacks on the infrastructure and end-user devices.
- Application services of SDN based 5G+ network targeted by the signaling attacks.

When employing the ML to detect DDoS attacks during these challenges, ML with suitable algorithms improves the accuracy of security solutions through the trained model and dataset.

3. PROPOSED APPROACH WITH ML

This section discusses the detail of the proposed system design, including the detection method of system design, the threshold technique, and the theoretical model. In the detection method, the adaptive bandwidth control mechanism and the traffic classification model are used. Here, the workflow of the proposed solution is illustrated to show the integration between the proposed system components in detecting and mitigating attacks in SDN. Finally, the detection method with ML in the theoretical model is integrated.

3.1 Detection Method

As shown in figure 2, SDN organizes all types of traffics into three categories. The default threshold is set, which allows the detection modules to detect the behavior of the traffic. Based on the rate of traffic, these three modules detect the DDoS attacks using adaptive bandwidth. Heavy, medium, and light traffic allows the model to detect the DDoS attacks.

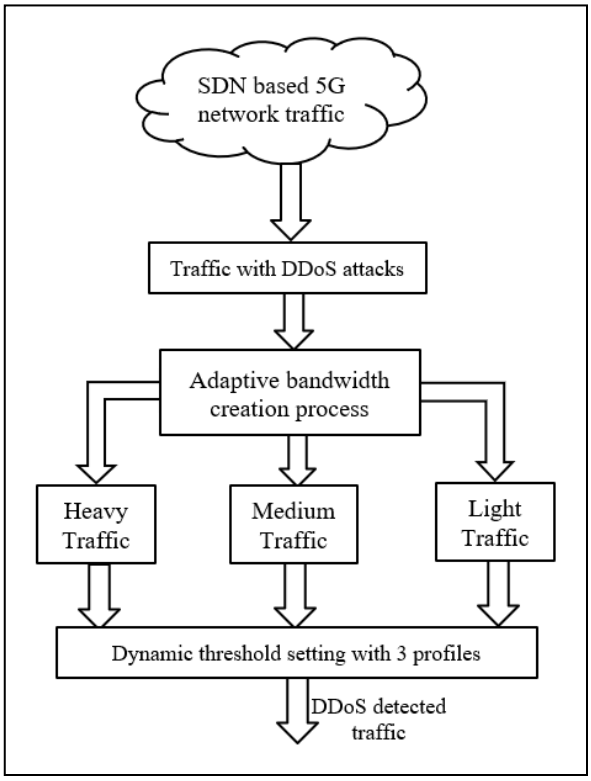
SDN based 5G network traffic
Traffic with DDoS attacks
Adaptive bandwidth creation process
Heavy Traffic
Medium Traffic
Light Traffic
Dynamic threshold setting with 3 profiles
DDoS detected traffic

Fig 2: Process of setting the adaptive bandwidth

The proposed model identifies the DDoS attacks through the bandwidth measurements depended on the characteristic of the traffic. Although bandwidth is proportional to throughput, heavy, moderate, and light traffic use large, medium, and small bandwidths, respectively. Dynamic threshold setting can be used for improving the DDoS detection ratios, and it allows the attacked or abnormal traffic to distinguish the levels of the DDoS attacks. Although three profiles are set for the threshold limits, the dynamic threshold enhances the number of the profiles.

3.2 Threshold Setting

According to the nature of the traffic and 5G network service, the threshold can be set manually or dynamically. From the traffic analysis and theory, the default threshold was used, but SDN can reset the threshold according to the nature of the traffics dynamically. The success rate of DDoS attack detection depends on the selection of the threshold, ML algorithms, trained model, and techniques. Mitigation of DDoS attacks also may rely on the same detection procedures known as the workflow of the proposed solution. Workflow depends on the following 3 phases.

- Monitoring: In this phase, traffic flow with the set threshold, SDN rules with the threshold violation counter, and bandwidth
- Bandwidth controlling: This phase works with the minimum bandwidth limits, which filter the DDoS attacks and count the threshold violations.
- Detection: In the bandwidth controlling phase, if threshold violation is above the set threshold limit, this phase will detect the DDoS attacks.

The traffic classification supports tracing and mitigate the attacked traffic, which includes the DDoS attacks detected through these 3 phases with selected dataset and ML trained model. In the DDoS mitigation, the quantitative ability of the ML trained model supports to ease of the mitigation. In this detection and mitigation, trained SVM algorithms and models enhance the success rate of a security solution, which supports to improve the accuracy of DDoS detection. The SVM models are responsible for extracting the particular characteristics values of the received network traffic.

3.3 Proposed Theoretical Model

As shown in figure 3, this paper has proposed the theoretical model. In this proposed system, securing the SDN controller depends on the DDoS attack mitigation scheme and SDN that is composed of an adaptive bandwidth mechanism and a trigger-based learning model based on the XGBoost algorithm. As shown in figure 3, the 5G system can be built with a DDoS security solution, which uses the ML with the XGBoost algorithm. Here, the ML-based security solution converts weaker classifiers of signals into a high-performance stronger classifier.

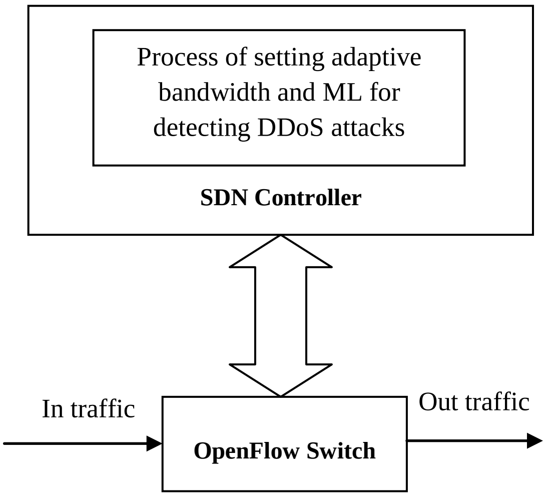
Process of setting adaptive bandwidth and ML for detecting DDoS attacks
SDN Controller
In traffic
OpenFlow Switch
Out traffic

Fig 3: The proposed model with ML and SDN

Advancements of autonomous systems based on SDN and 5G networks depend on efficient security solutions. The proposed model provides many benefits, including protection for securing SDN based 5G networks. In this model, SDN and ML play excellent roles, such as programmable traffic monitoring. It means efficiency in detecting DDoS attack patterns increases through the programmable SDN controller and specific ML algorithm.

During the DDoS detection, the ML algorithm monitors the interactions of flow dynamically. These interactions are representing the abnormal behavior of flow between the starting and endpoints. When more interactions occur, the time of the flow within these points will increase sharply. In each flow, ML not only monitors the interactions but also calculates the time for identifying DDoS attacks. In the SDN-based 5G networks, the DDoS detection and mitigation by utilizing SDN controller, which includes the ML techniques allow the proposed solution to provide reliable network security solution.

Regarding the DDoS attacks and attacked 5G networks or infrastructure, the SVMs algorithms are firstly trained on the dataset. Once the ML model is trained based on the selected SVM algorithm, the proposed model should be able to identify the normal and abnormal traffic influenced by the DDoS attacks. Here, differentiation of the normal and attacked traffic depends on the efficiency of the SVM algorithm. Also, the use of an SDN controller monitors the packets of OpenFlow protocol obtained through the link layer between the north and south bounds. These monitored packets are sent to SVM algorithms for identifying the legitimate network traffic and DDoS attacks. The security solution based on the XGBoost algorithm enhances the ability of the solution against DDoS and service disruption attacks.

4. CLASSIFICATION AND RESULTS

Although employing a real-time traffic classification method for SDN based 5G network, the proposed method will allow researchers to enhance the security solution when DDoS attacks affect emerging networks such as 5G and beyond. This research focuses on investigating the network traffic classify DDoS attacks in the SDN based 5G networks for analyzing the classification accuracy. The ML strategies support classification problems with different models, such as SVM, which allow researchers to handle multi-stage training. Here, the proposed approach improves the performance of classification accuracy, which reaches 100% when using the selected classification model, which requires a dataset and correct trained ML model. Investigating DDoS attacks in short and long sliding windows is one of the strategies considered through the traffic classification of the trained ML model.

4.1 Classification with XGBoost Algorithm

Studies of algorithms for detecting DDoS attacks based on classification techniques allow us to explore the best ML algorithms such as XGBoost. To address the behavior of the traffic, whether they are normal or abnormal, there is a need for an efficient classification algorithm. In this paper, the XGBoost algorithm is selected to be used because it classifies the traffic flow efficiently when the SDN controller sets the dynamic threshold according to the situation of the traffic flow. Classifying DDoS attack detection based on an adaptive bandwidth mechanism is one of this algorithm's roles because it distinguishes the DDoS attack and normal traffic accurately with low processing overhead. Classification model based on the XGBoost algorithm allows us to develop trigger-based detection, which supports to detect the DDoS attacks when traffic flow exceeds the limit of the set threshold. In order to evaluate the DDoS detections with the SDN environment, the XGBoost algorithm enhances not only the security solution of the 5G networks but also reduces energy consumption and latency. In addition, it provides many benefits SDN based 5G networks; they are such as high speed, high classification accuracy, algorithmic simplicity, etc. It supports real-time classification techniques, as well.

4.2 Results with Selected Datasets

In this paper, the recent datasets were used, which consist of the various DDoS attacks that happened in 5G network applications. According to the proposed DDoS detection solution, figure 4 confirms that CPU utilization of the proposed approach is better than other ML approaches. The first approach is without any defense. The second approach is the machine learning approach based on a sliding window manner with a time interval of 5 seconds. The third approach is machine learning based on a sliding window manner with a time interval of 1 second. The last approach is the proposed approach. To conduct the above evaluation, all the abovementioned approaches ran for 60 seconds. In the first 25 seconds, no attack is launched to monitor the overhead of each approach in the normal status of the network (no attack). Then, both normal and attack traffic are generated afterward to measure the CPU utilization of each approach during the attack mitigation.

It can be observed from the figure that when there is no attack launched during the first 25 seconds, the CPU consumption of the proposed approach is a little higher than that of the no defense approach due to the design of the proposed mechanism. Therefore, the overhead of the proposed approach is reasonable and tolerated as opposed to both machine learning approaches based on the sliding window method. After launching the attack, the overhead of the no defense approach exponentially increased and peaked CPU utilization because the DDoS attack aims to overwhelm the network resources. Therefore, with the absence of a protection mechanism, the maximum capacity of the CPU is consumed. On the other hand, other approaches produced little overhead due to the protection mechanism. However, the proposed approach achieved the lowest overhead among all approaches during the attack owing to the algorithms and techniques used as well as the trigger-based approach. Both machine learning approaches based on sliding window manner with different time intervals produced higher CPU consumption than the proposed approach due to the detection loop approach and the continuous statistics collection from the data plane devices.

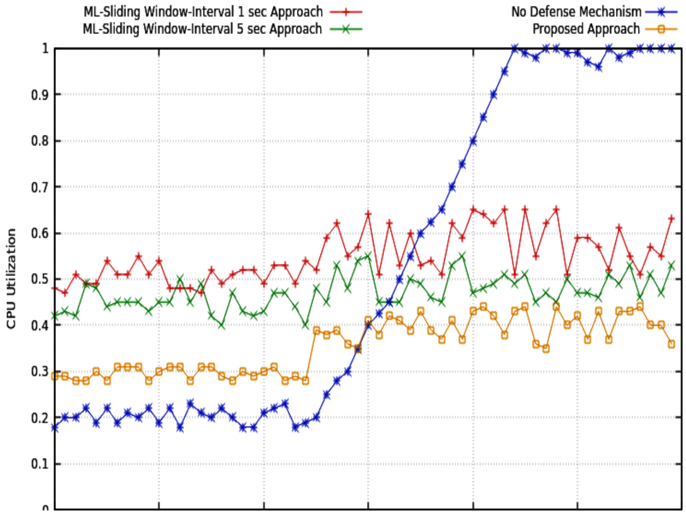

Fig 4: CPU Utilization of the SDN Controller

It can be observed that XGBoost achieved superior results in all performance metrics in terms of binary and multiclass classification with both datasets. In binary classification, XGBoost gained a rate of 99.7%-100% for all metrics with the CICDDoS2019 dataset, while it attained 99.2%-100% with the NSL-KDD dataset. RF and LR achieved lower performance metrics values than XGBoost with a rate of 98.5%-99% and 80%-85%, respectively, with the

CICDDoS2019 dataset, while they recorded a rate of 99.5%-99.7% and 93.5%-94%, respectively, with the NSL-KDD dataset. In multiclass classification, XGBoost achieved higher performance metrics with both datasets with a rate of 91.3%-93% and 96%-99.9%, respectively. In contrast, LR recorded the lowest performance metrics among all algorithms being evaluated with a rate of 31%-40% with the CICDDoS2019 dataset and 31%-58% with the NSL-KDD dataset.

The performance of LR, RF, and XGBoost is attributed to their operational procedure and the ability to select the best parameters, as well as the correlation of the features used from the dataset. Thus, the LR algorithm has the lowest values in all performance metrics compared to other algorithms. LR is a linear algorithm that results in poor performance in multiclass classification, and it is not flexible to adapt to complex data. XGBoost attained a superior performance compared to other algorithms due to the use of additive learning techniques, which keeps improving weak learners' prediction. Also, XGBoost overcomes the overfitting problem and attains full utilization of computational resources.

In Table 2, binary and multiclass classification is compared with the following matrices given in percentage (%); they are accuracy (Acc), precision (Pre), Recall (Rec), and F1 measure (F1). With two datasets (CICDDoS2019 and NSL-KDD), three ML algorithms are compared; they are LR, RF, and XGBoost (XG), respectively [38].

Table 2. Performance of Classifiers

		Binary Classification			**Multiclass Classification**		
		LR	**RF**	**XG**	**LR**	**RF**	**XG**
CICDDoS 2019	**Acc**	80	98.5	99.7	35	83	91.3
	Pre	85	99	100	38	88	93
	Rec	80	99	100	40	88	93
	F1	80	99	100	31	88	92
NSL-KDD	**Acc**	93.5	99.5	99.2	52	93	99.9
	Pre	94	99.6	100	56	88	99
	Rec	94	99.6	100	58	89	96
	F1	94	99.7	100	32	88	97

Using ML algorithms (LR, RF, and XG), performance is compared for evaluating normal and DDoS attack classes. Thus, labeled classes such as binary and multi-class classification are considered. Further, the approach of evaluating the overhead of the proposed system in SDN is illustrated. The DDoS attacks are serious threats to many autonomous systems involved with SDN based 5G networks. The DDoS attacks block the availability of smart infrastructure services considered in the autonomous system. Here, a combination of ML and SDN approaches the detection rate of a DDoS attack in a smart service.

Table 3. The False-Positive Rate of Each Classifier

	CICDDoS2019	**NSL-KDD**
LR	0.0176	0.015
RF	0.0015	0.0008
XG	0.0005	0.0003

Table 3 shows the results of false-positive rate, which allows us to validate the DDoS detection. In this comparison, the results of the proposed model are obtained using 2 different datasets. The lowest rate indicates that the XG model enhances DDoS attack detection and mitigation with high accuracy [38].

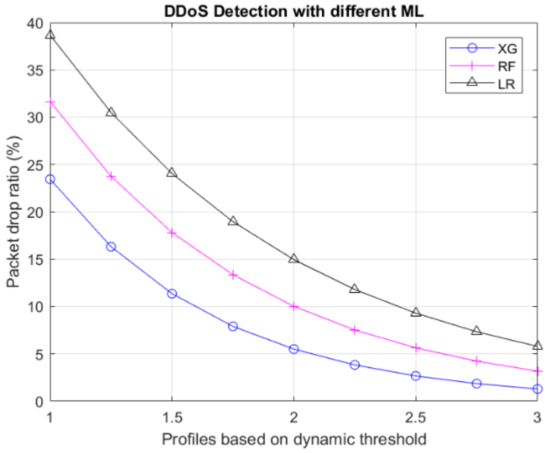

Fig 5: Packet drop ratio vs. dynamic threshold with ML

As shown in figure 5, DDoS detection depends on the packet dropping ratio, which influences the dynamic threshold. When packet drops decrease, the 5G network will improve from the DDoS attacks. In this result, the XG algorithm plays an important role in enhancing the ability of the DDoS detection rate because the algorithmic simplicity of XG is one of the benefits considered in the ML technique. When XG is used for training the ML model, the building and testing time of the model is very quick.

5. ANALYSIS OF SECURITY WITH ML

This section discusses the detail of the proposed solution with the necessary security analysis, which includes the ratio of the DDoS detection and performance of the SDN-based 5G network involved with the SDN controller. Also, it provides an analysis of the proposed solution with ML, SDN, and a comparison of other approaches when employing different ML techniques.

5.1 Analysis of security issues

The performance evaluation was conducted using two different datasets allowed for analyzing the various types of DDoS attacks. The evaluation of all algorithms was performed based on the classification report metrics to measure each classifier's performance. Table 4 shows the ML-based security issues for analyzing the SDN based 5G infrastructure. The proposed DDoS mitigation system showed an outstanding performance in detecting high volume-based DDoS attacks. However, further researches are needed to tackle the low-rate DDoS attack, which is very difficult to detect. One possible solution to this limitation is enhancing the proposed adaptive bandwidth threshold technique to have upper and lower thresholds. Hence, the upper bandwidth threshold detects the high volume-based DDoS, while the lower one deals with low rate DDoS attacks. Another solution to the low-rate DDoS attack can be achieved by developing another module to the proposed design to monitor the outgoing connections. The major aim of low rate attack is to leave connections open on the targeted victim for a long time.

In the analysis of the proposed model, SDN may use more separate modules inside the SDN controller. These modules enhanced the efficacy of DDoS detection and mitigation when SDN based 5G networks face varied traffic with DDoS attacks. In the DDoS detection analysis, mitigation modules work immediately according to the policy and rules set in the SDN controller. In the security analysis, the flow table of

DDoS attacks is increasing with heavy traffic of SDN based 5G network and SDN-enabled cloud environment.

Table 4. Security issues of SDN based 5G network

	Approaches of ML		
	SVM	**SVM with SDN**	**XGBoost**
Security parameter	All basic DDoS attacks are detected	Some types of DDoS are noted with SDN rules and detected by SVM	Various types of DDoS attacks are detected dynamically
5G Network	Genetic Algorithm (GA) can be used 5G feature selection	Multiple detections with multi-layer SVM and SDN	Enhance the ability of the solution against DDoS attacks
SDN based 5G network	Block all ports of the SDN based 5G channels	Single SDN controller causes massive DDoS attacks to the network infrastructure	Ensuring secure access and authorizing in SDN based autonomous services
Limitations	Traditional and 5G+ features can be used for attack traffic detection	The best dataset may be used for optimizing security parameters	Best dataset and GA may be used for securing real-time security

When attackers send a large number of violated packets on random occasions, the correlation of data traffic becomes abnormal attacked by the DDoS attacks. When they send the small-sized packets, identifying correlation is not easy, but its standard deviation is much lower than the legitimate packets. During the DDoS attacks, not only this standard deviation will be lower, but also packet drops will increase.

5.2 Security Issues and Challenges

Identifying normal and abnormal burst-data behaviors of SDN based 5G network is very challenging when developing the trained model of the dataset for ML techniques. Both classes of network traffic have similar intrinsic characteristics. In this section, some research limitations and challenges that need further researches in the future are discussed. These limitations and challenges can be summarized as follows:

Implementing the proposed solution in a single controller SDN environment yielded good performance in DDoS attack mitigation. However, with large-scale networks, the single controller SDN architecture becomes a bottleneck problem in which can be addressed by distributed multiple controllers. Nevertheless, the distributed controller demands a method of sharing information between controllers, which might result in computational and communication overhead in the control plane. Researchers can look forward to finding lightweight information coordination between controllers.

Another limitation of implementing the proposed defense in the distributed controllers' environment is the controller's placement and the assignment of devices in the data plane to each controller. If a set of data plane devices is assigned with the closest controller, then controller failure would cripple this subnet due to a single point of failure. Such limitations can be resolved by master-slave controllers' assignment. Each set of data plane devices is assigned with a master controller and backup (slave) controller in case of failure. Researchers can also investigate and develop a master-slave controllers' assignment mechanism to assign the switches in the data plane with the best controller.

The trade-off between the performance of defense techniques and resource consumption is a significant challenge since the DDoS attacks put massive pressure on the target resources. Therefore, it is essential to ensure that the defense mechanism consumes as low as possible of the targeted system resources while mitigating DDoS attacks.

Zero-day attack detection is always the most challenging of any security solution. DDoS attackers utilize an advanced method for launching attacks with high power and complexity. Thence, zero-day attacks detection is considered a promising research area to enhance the DDoS defense in SDN based applications.

6. CONCLUSION AND FUTURE WORK

In this paper, a security solution is proposed which detects DDoS attacks for securing SDN controller using suitable ML algorithms. In this research, SDN based on an adaptive bandwidth mechanism played an important role in securing the SDN controller, where the XGBoost algorithm was used for mitigating DDoS attacks. In this analysis, a dataset influenced by ML algorithms was used which supports enhancing the security solutions with the adaptive bandwidth mechanism. Although three profiles are set to compare the results, the adaptive bandwidth and dynamic threshold setting control the DDoS attacks; the XGBoost algorithm enhances the accuracy of the security performance. Also, XGBoost overcomes the full utilization of CPU and other resources with minimum energy cost and complexity. In future works, essential improvements will be conducted on the performance of the SDN based security solutions and prevent DDoS attacks using dynamic threshold set by ML. This approach will enhance the ability of security solutions with the different dynamic thresholds for securing the emerging 5G+ networks. The use of this approach with adaptive bandwidth algorithm and ML technique will enhance the accuracy of security solution and reduce the packets drop ratio.

7. ACKNOWLEDGMENTS

I am glad that I completed this work successfully. This work would be impossible without the help of Dr. Vijey Thayananthan. I would like to thank him for his expert advice and usual support.

8. REFERENCES

[1] S. Dong, K. Abbas, and R. Jain, "A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments," IEEE Access, vol. 7, pp. 80813–80828, 2019.

[2] S. Singh and S. Prakash, "A survey on the software-defined network based on architecture, issues, and challenges," 2019 3rd Int. Conf. Comput. Methodol. Commun., no. Iccmc, pp. 568–573, 2019.

[3] K. S. Sahoo et al., "An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks," IEEE Access, vol. 8, pp. 132502–132513, 2020.

[4] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, M. Ghogho, and F. El Moussa, "DeepIDS: Deep learning approach for intrusion detection in software-defined networking," Electron., vol. 9, no. 9, pp. 1–18, 2020.

[5] S. Kumar and Md. Mahbubur, "Effects of Machine Learning Approach in Flow-Based," 2019.

[6] 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.

[7] M. Shakil, A. Fuad Yousif Mohammed, R. Arul, A. K. Bashir, and J. K. Choi, “A novel dynamic framework to detect DDoS in SDN using metaheuristic clustering,” Trans. Emerg. Telecommun. Technol., no. February pp. 1–18, 2019.

[8] 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.

[9] K. B. Virupakshar, M. Asundi, K. Channal, P. Shettar, S. Patil, and D. G. Narayan, “Distributed Denial of Service (DDoS) Attacks Detection System for OpenStack-based Private Cloud,” Procedia Comput. Sci., vol. 167, no. 2019, pp., 2297–2307, 2020.

[10] K. Bhushan and B. B. Gupta, “Distributed denial of service (DDoS) attack mitigation in a software-defined network (SDN)-based cloud computing environment,” J. Ambient Intell. Humaniz. Comput., vol. 10, no. 5, pp. 1985–1997, 2019.

[11] K. Huang, L. Yang, X. Yang, Y. Xiang, and Y. Y. Tang, "A Low-Cost Distributed Denial-of-Service Attack Architecture," in IEEE Access, vol. 8, pp. 42111-42119, 2020, doi: 10.1109/ACCESS.2020.2977112.

[12] S. Dong, K. Abbas, and R. Jain, “A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments,” IEEE Access, vol. 7, pp. 80813–80828, 2019.

[13] V. Duddu, “A survey of adversarial machine learning in cyber warfare,” Def. Sci. J., vol. 68, no. 4, pp. 356–366, 2018.

[14] K. Nisar, I. Welch, R. Hassan, A. H. Sodhro, and S. Pirbhulal, “A Survey on the Architecture, Application, and Security of Software Defined Networking,” Internet of Things, vol. 12, p. 100289, 2020.

[15] M. Iqbal, F. Iqbal, F. Mohsin, M. Rizwan, and F. Ahmad, “Security issues in software-defined networking (SDN): Risks, challenges, and potential solutions,” Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 10, pp. 298–303, 2019.

[16] A. Pradhan and R. Mathew, “Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN),” Procedia Comput. Sci., vol. 171, no. 2019, pp., 2581–2589, 2020.

[17] H. S. Abdulkarem and A. Dawod, "DDoS Attack Detection and Mitigation at SDN Data Plane Layer," 2020 2nd Global Power, Energy, and Communication Conference (GPECOM), Izmir, Turkey, 2020, pp. 322-326, doi: 10.1109/GPECOM49333.2020.9247850.

[18] K. K. Karmakar, V. Varadharajan, and U. Tupakula, “Mitigating Attacks in Software Defined Network (SDN),” Cluster Comput., 2019.

[19] M. Idhammad, K. Afdel, and M. Belouch, “Detection system of HTTP DDoS attacks in a cloud environment based on information-theoretic entropy and random forest,” Secur. Commun. Networks, vol. 2018, 2018.

[20] J. Cheng, C. Zhang, X. Tang, V. S. Sheng, Z. Dong, and J. Li, “Adaptive DDoS attack detection method based on multiple-kernel learning,” Secur. Commun. Networks, vol. 2018, pp. 1–19, 2018.

[21] A. Raj, A. S. Bhat, L. V. Namboothiri, “Effective threshold defence against DOS attack on SDN controller,” Int. J. Pure Appl. Math., vol. 119, no. 10, pp. 691–698, 2018.

[22] J. David and C. Thomas, “Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic,” Comput. Secur., vol. 82, pp. 284–295, 2019.

[23] Z. He and R. B. Lee, “Machine Learning-Based DDoS Attack Detection From Source Side in Cloud,” 2017 IEEE 4th Int. Conf. Cyber Secur. Cloud Comput., pp. 114–120, 2017.

[24] I. Sreeram, V. Praveen, and K. Vuppala, “Applied Computing and Informatics HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm,” Appl. Comput. Informatics, vol. 15, no. 1, pp. 59–66, 2019.

[25] I. Sofi, A. Mahajan, and V. Mansotra, “Machine Learning Techniques used for the Detection and Analysis of Modern Types of DDoS Attacks,” pp. 1085–1092, 2017.

[26] R. Santos and E. Moreno, “Machine learning algorithms to detect DDoS attacks in SDN,” Concurr. Comput. Pr. Exper., pp. 1–14, 2019.

[27] M. M. Oo, S. Kamolphiwong, T. Kamolphiwong, and S. Vasupongayya, “Advanced support vector machine-(ASVM-) based detection for distributed denial of service (DDoS) attack on software-defined networking (SDN),” Comput. Networks Commun., vol. 2019, pp. 12, 2019.

[28] T. V. Phan and M. Park, “Efficient distributed denial-of-service attack defense in sdn-based cloud,” IEEE Access, vol. 7, pp. 18701–18714, 2019.

[29] Y. Wang, T. Hu, G. Tang, J. Xie, and J. Lu, “SGS: safe-guard scheme for protecting control plane against DDoS attacks in software-defined networking,” IEEE Access, vol. 7, pp. 34699–34710, 2019.

[30] K. S. Arpitha, “Ddos Attacks Using Machine Learning,” J. Xi’an Univ. Archit. Technol., vol. XII, no. IV, pp. 3380–3384, 2020.

[31] D. Zhu and S. Member, “A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning,” pp. 155859–155872, 2020.

[32] V. Deepa, K. M. Sudar, and P. Deepalakshmi, “Detection of DDoS attack on SDN control plane using hybrid machine learning techniques,” 2018 Int. Conf. Smart Syst. Inven. Technol., Icssit, pp. 299–303, 2019.

[33] Z. Chen, F. Jiang, Y. Cheng, X. Gu, W. Liu, and J. Peng, "XGBoost Classifier for DDoS Attack Detection and Analysis in SDN-Based Cloud," 2018 IEEE International Conference on Big Data and Smart Computing (BigComp), Shanghai, 2018, pp. 251-256, doi: 10.1109/BigComp.2018.00044.

[34] Zhang, Chunyu, Danshi Wang, Chuang Song, Lingling Wang, Jianan Song, Luyao Guan, and Min Zhang. "Interpretable learning algorithm based on XGboost for fault prediction in an optical network." In Optical Fiber Communication Conference, pp. Th1F-3. Optical Society of America, 2020.

[35] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, “Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy,” Proc. - Int. Carnahan Conf. Secur. Technol., vol. 2019-Octob, no. Cic, 2019.

[36] S. Das, D. Venugopal, S. Shiva, and F. T. Sheldon, “Empirical Evaluation of the Ensemble Framework for Feature Selection in DDoS Attack,” no. Ml, pp. 56–61, 2020.

[37] Gong, Changqing, Delong Yu, Liang Zhao, Xiguang Li, and Xianwei Li. "An intelligent trust model for hybrid DDoS detection in software-defined networks." Concurrency and Computation: Practice and Experience 32, no. 16 (2020): e5264.

[38] Alamri, Hassan A., and Vijey Thayananthan. "Bandwidth Control Mechanism and Extreme Gradient Boosting Algorithm for Protecting Software-Defined Networks Against DDoS Attacks." IEEE Access 8 (2020): 194269-194288.