International Journal of Future Generation Communication and Networking
Vol. 13, No.2s, (2020), pp. 1700–1707

Comparative Analysis of DDoS Mitigation Algorithms in SDN

Chinmay Dharmadhikari[1], Salil Kulkarni[2], Swarali Temkar[3], Shailesh Bendale[4]

[1,2,3]B.E. Student, Dept. of Computer Engineering, NBN Sinhgad School of Engineering, Ambegoan, Pune- 411041, Maharashtra, India
[4]Professor, Dept. of Computer. Engineering, NBN Sinhgad School of Engineering, Ambegaon, Pune – 411041, Maharashtra, India

Abstract

Today, Software Defined Network (SDN) is the most popular network architecture. It is one of the famous applications of virtualization. It has completely changed the perspective of the network industry. SDN basically separates the data plane from the control plane providing a centralized control over the network with the help of a controller. Although SDN provides a simplified way to control the network, it is prone to various security attacks such as DoS attacks, Man in the middle attacks etc. One of the most common attack SDN faces is Distributed Denial of Service Attack (DDoS). It attacks the server and disrupts the whole network. Thus, it is very important to detect and mitigate these attacks. There are several approaches in the market to detect and mitigate these attacks. However, there is no significant comparison among these approaches. Hence, in this paper we attempt to replicate the results of two approaches and compare them so as to find the better approach. These approaches are: algorithmic approach and the second is the machine learning approach.

Keywords*—Software Defined Networks (SDN), Distributed Denial of Service (DDoS), IDS, Machine learning, DDoS Mitigation.*

I. INTRODUCTION

SDN has completely changed the working of the network and made it more efficient by allowing centralized control over the network. Being centralized it is prone to some severe attacks and one of them is DDoS. It is the major attack that has a huge impact on the performance of a network. It affects the network flow between the switches and controllers and brings down the whole network [1]. Because of the critical issues faced by the network it becomes necessary to mitigate this attack.

Software Defined Networks (SDN) is a revolutionary technique in the networking field. It basically separates the data plane from the control plane and provides a centralized control over the complete networking system with the help of a controller.

Data Plane is where the actual packets flow. The control plane mainly monitors the whole system and controls the network. The main components of the data plane are the switches and the routers whereas the main components of the control plane are the controller and its 3 interfaces viz. South Bound API, North Bound API and the East-West bound API.

Nowadays, network security threats are increasing [13]. There are various new attacks that can cause critical damage to nodes in a network. Some of the attacks are Spoofing, DoS, Man in the Middle, Eavesdropping etc. Although SDN has brought an efficient change in the networking world there are some shortcomings to the architecture. This architecture has a significant amount of vulnerabilities and security threats. This architecture is prone to many attacks like man in the middle, eavesdropping, DDoS, etc. Amongst them the most common and severe is the DDoS. More about this has been explained in the further section.

ISSN: 2233-7857 IJFGCN

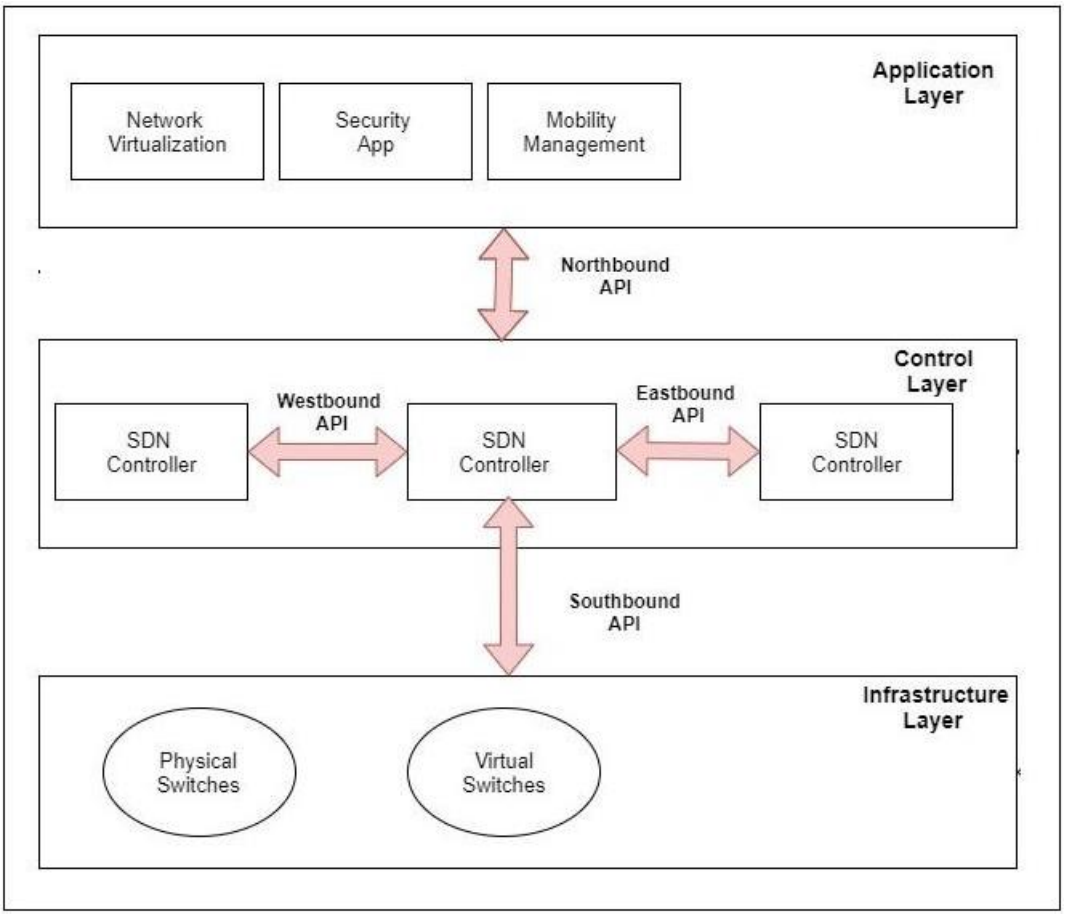


Fig. 1 SDN Architecture and its Interfaces

The rest of the paper is segregated in different sections. Section 2 contains a brief discussion of various papers. In section 3, we have given description of what is DDoS and how it affects the SDN. Section 4 contains the two approaches used for DDoS detection. It also contains methodology to mitigate the same. Section 5 has implementation details followed by result analysis of the two approaches in Section 6. Lastly section 7 discusses the conclusion and future work to be done.

II. LITERATURE SURVEY

In [2] the authors have implemented SRL, a system which provides security against TCP SYN Flood DDoS attack. The author has proposed two modules: Hashing module and Flow Aggregator module. Hashing module is used to remove fraudulent values from the flow table, while Flow Aggregator module is used to limit the number of requests to the server. Hence it successfully mitigates SYN FLOOD DDoS attack.

In [3] this paper S. S. Mohammed et al a DDoS detection and mitigation of the DDoS attack is proposed using machine learning algorithm. The Naive Bayes Algorithm is used to for the purpose of attack mitigation and detection.

Authors Y. Chen, J. Pei and D. Li, have discussed the advantages and disadvantages of process of the DDoS mitigation. And given a solution for the mitigation of the DDoS attack by modifying the decision tree algorithm [4].

In [5] authors talk about a secure architecture using deep reinforcement learning which can be used to avoid DDoS attack. The propose solution has two modules first is an Information collection module which uses the OpenFlow protocol and sends message in the network which requests the information and then analyses this information and second is a DDoS mitigation module which takes into consideration the mitigation server and the agent . The agent is a discreet host equipped with the deep reinforcement algorithm and the server runs as an application on SDN.

ISSN: 2233-7857 IJFGCN

This paper describes [6] implementation of a real time detection and mitigation of a DDoS attack. sFlow tool is used to monitor the network. By deciding threshold for packets per seconds a DDoS attack is detected if based on the decided threshold.

In [7] proposes a hybrid machine learning technique which uses the amalgamation of two ML algorithms namely SVM and SOP. It then compares the performance of these 2 algorithms.

Authors C. Buragohain and N. Medhi [8] proposes a DDoS mitigation and detection framework named FlowTrApp which is implemented using FloodLight controller in a mininet environment. UDP Flood DDoS attack is performed and this attack is detected by comparing the parameters viz. flow rate and flow duration.

In [9] the methodology used to detect the DDoS attack is by monitoring the flow of the network. For this approach the iftop tool is used.

III. DDoS Attack in SDN

Denial of Service (DoS) is the most destructive attack on the network. It focuses on denying services to other hosts in the network. It achieves this by continuously sending requests to the server. DoS attack is a type of active attack. High volume of packets is generated by the attacker which overwhelms the server.

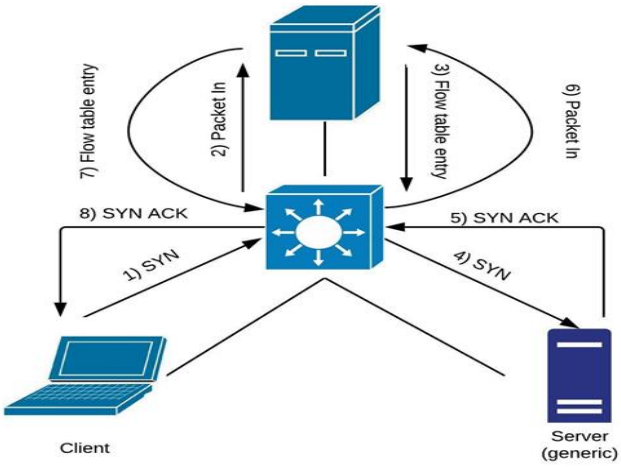
In DDoS, multiple devices are used to attack simultaneously. Due to multiple attackers, it is hard to mitigate. These attackers send large number of packets to a server.

DDoS in SDN is classified into 2 types– Control Plane DDoS and Data Plane DDoS [1]. In Control plane DDoS, the attacker focuses on the controller. It tries to bring down the controller. Once the controller is unable to function, the network is brought down. Whereas in Data plane DDoS, the attacker concentrates on the hosts in the SDN network. Data plane DDoS can be further categorized as Volumetric (ICMP, Smurf attack) and Protocol Exploitation (SYN Flood, HTTP flood attack) attacks. Volumetric attack sends a huge volume of packets. Protocol exploitation attacks try to acquire server resources. Protocol exploitation is characterized by low number of packets which focus on server resources. Protocol exploitation attacks have more effect on the servers than Volumetric attacks [1].

In this paper we focus on a TCP SYN-Flood attack.

A. TCP SYN-Flood Attack

TCP SYN-Flood attack is a type of a protocol exploitation attack in which attacker continuously sends TCP SYN packets. To understand SYN-Flood attack we first need to know about TCP handshake. A TCP handshake is a 3-way process. It is used to establish connection between 2 hosts. The steps in TCP handshake are as follows, the host sends a SYN packet to the server on specific port. The server upon receiving the SYN packet allocates resources for the host, and then sends a SYN-ACK packet back to the server. The host then sends ACK packet to complete the handshake. Now the host and the server send can communicate and exchange information. Following figure depicts a TCP handshake in SDN environment.



ISSN: 2233-7857 IJFGCN

Fig. 2 TCP Handshaking in SDN

In TCP SYN-Flood DDoS attack, the attackers send a large amount of TCP SYN packets. The server then allocates memory for each request. Server sends the SYN-ACK packet and waits for the ACK packet. The attacker simply ignores this step and the server is kept waiting. Due to this the port is kept open and server resources are wasted. Also, the flow table entries of the switches are filled with fake entries. Backward flows are also installed into the switches. The server waiting for a ACK sends SYN-ACK packets repeatedly. As the host with spoof IP address are not present in the network the controller does not install any flow entries, hence the controller gets flooded by these repetitive requests.

A TCP SYN-Flood attack not only affects the server resources but also affects the switches and controllers in SDN environment. Hence it can bring the server as well as the controller down. Due to these reasons we have selected TCP SYN-Flood attack and in further sections we discuss algorithms to mitigate this attack.

IV. DDoS Detection and Mitigation

For our comparative study we have selected two approaches which are discussed in further sections.

A. DDoS Detection

The first approach is to detect the malicious packets with the help of the Machine Learning approach [14]. In Machine learning, the machine learns from different scenarios and thus tries to predict or classify whether the network is under attack or not. The second approach is algorithmic approach in which frequency based blocking is used. The details of these algorithms are discussed below.

1) *Approach 1- Algorithmic Approach* : The DDoS attack extensively focuses on making requests to a service and blocking other users from accessing this service. In this approach, the algorithm keeps a count of requests made by a host in the network. Request count determines whether a host is legitimate or an attacker.

In a SYN-Flood attack scenario, a host sends a TCP SYN packet to the server. Upon receiving these packets, server allocates memory and is ready to provide service to the host. In SYN-Flood DDoS, attacker only sends SYN packets and does not complete the TCP handshake. The algorithm keeps track of these SYN packets.

For every TCP SYN packet, the algorithm keeps a counter value. Whenever a host sends a TCP SYN packet, its counter is increased. A threshold value is defined which is checked against the counter value. If the counter value exceeds the threshold, the host is immediately blocked. The threshold value should be high enough so that genuine users are not blocked. Generally, in a TCP SYN- Flood attack, volume of packets sent by the attackers are less as compared to volumetric attack [10]. Hence, we need choose the threshold value accordingly. If the counter value for any host exceeds the threshold value, it is blocked using a wildcard entry. This wildcard entry further prevents the host to communicate with the server.

2) *Approach 2- ML Based Approach :* Machine learning is a method which helps a machine learn by itself with the help of past experiences provided to it and the changes in the environment that the machine perceives. Machine learning has changed modern age computing and made human life simple. With the emerging new technologies like face recognition, Intrusion Detection System [11] etc. which makes use of ML algorithms has opened a whole new world of opportunities for data scientists.

As mentioned in the introduction, this section gives a brief idea of DDoS Detection using machine learning. This approach focuses on building a machine learning model and trains it using a dataset to perform detection of DDoS attack. Thus this model can be used to block the DDoS attackers before the network gets severely damaged.

ISSN: 2233-7857 IJFGCN

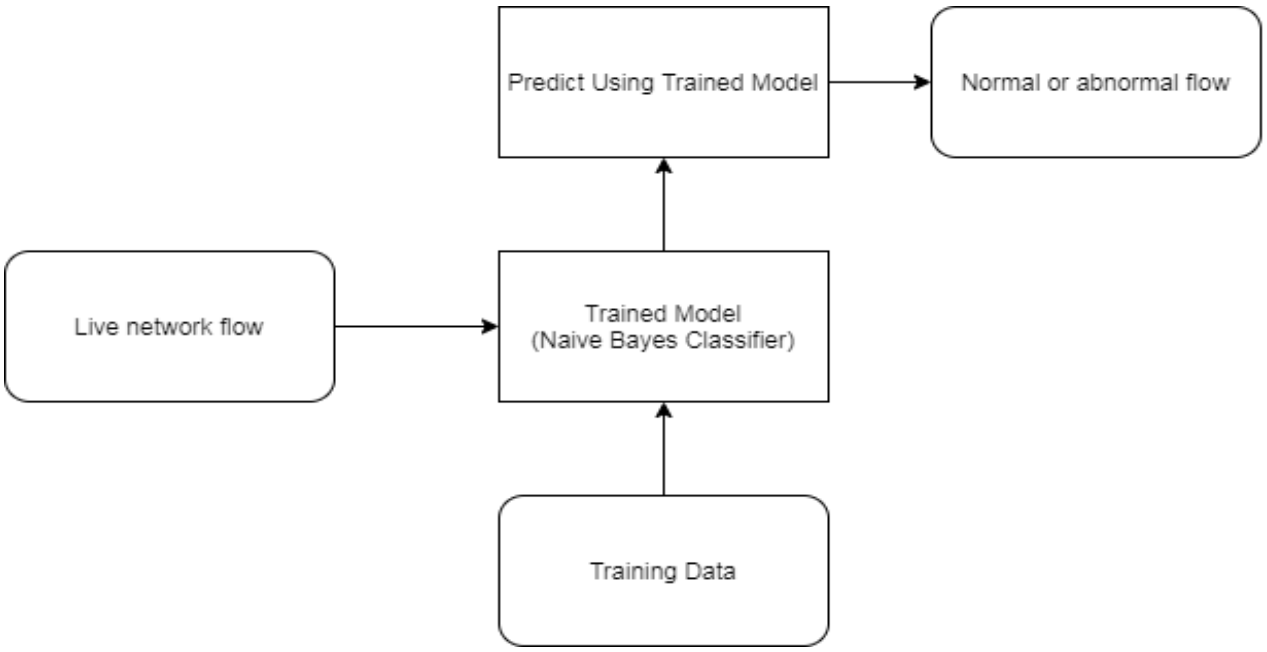


Fig. 3 Machine learning methodology

For the training purpose, the network flow is captured using Wireshark. Wireshark is an open-source tool which can be used to capture the packets from a network flow. We created a model which is based on this dataset which is captured by Wireshark. This model uses Naive Bayes Classification algorithm for attack detection. Naive Bayes is a classifier from the Bayesian algorithm family. It's a probabilistic classifier i.e. it works on the probabilistic values which is based on the Bayes Theorem and Maximum. Naive Bayes [12] works on an assumption that the effect of an attribute value on a given class is independent of the values of the other attribute i.e. features are purely independent of each other. The above assumption simplifies the computation.

After the model is built, it is used for detection purpose. Whenever packets flow through the network, they are captured and then analysed whether they are normal or abnormal using this built model[16 17].

B. DDoS Mitigation

DDoS detection algorithms identify the attacker in the network. DDoS Mitigation module blocks these attackers from accessing the services. Once an attacker is identified the mitigation module informs the controller about the attacks. The IP address of the attacker and the IP address of the victim is noted. Flow table of the switches are modified by removing flows related to the source IP address. New flows are added which block the attacker from sending packets to the server. All the packets from the attacker's IP are dropped. In this way the attacker is isolated and further attack is stopped.

V. IMPLEMENTATION DETAILS

Following softwares are used for the simulation of the DDoS attack detection and mitigation.

1) *Wireshark* : Wireshark is an open-source tool which can be used to capture the packets from a network flow. As mentioned earlier it is used to capture the packets from network flow. It is also used to analyse the network flow.

2) *Pox Controller* : Pox controller is an open source python-based controller which supports OpenFlow. It follows the Publish Subscribe model.

3) *Mininet* : Mininet is used as a network emulator to create virtual SDN topologies. It supports the OpenFlow protocol.

ISSN: 2233-7857 IJFGCN

4) *Hping3* : Hping3 is a tool to generate traffic in a network. It is able to generate a high volume of packets to simulate DDoS attack. It is mostly used for penetration testing. It can perform various types of attack like ICMP flood attack, TCP SYN-Flood attack, HTTP flood attack etc.

5) *Scikit-learn* : Scikit-learn is used for machine learning. It is a library for python programming language which is used for implementation of machine learning process, algorithms etc.[15].

6) *Virtual Box* : Virtual Box is an open source software which enables us to create virtual machines.

VI. RESULT EVALUATION

For simulation of SYN-Flood DDoS attack we used the tool hping3 to generate packets. We created a simple topology with 4 hosts. Attack was performed on host 4 with IP address 10.0.0.4. We have used the Pox controller. Wireshark was used for packet capturing. Also, further result analysis and graph generation is accomplished with Wireshark. Mininet emulator is implemented in a virtual environment. This virtual environment is created using VirtualBox.

A. Testing Scenario

A simple topology is created with 4 hosts. Host h4 with IP address 10.0.0.4 is the victim. Attack is performed by host h1 using spoofed IP address. The spoof IP address is generated randomly. For our testing scenario only 1 attacker was used. TCP SYN-Flood attack is generated by hping3. Attack is performed on the port 80 of host h4.

B. Results

Following results are generated using Wireshark's IO Graph.

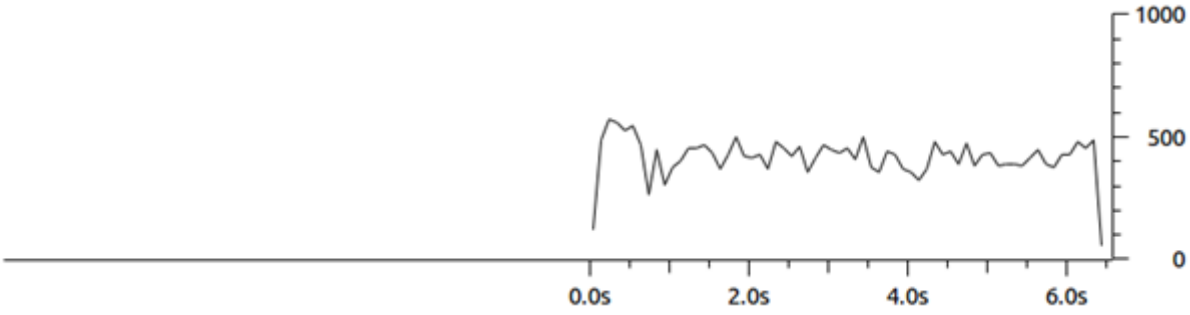


Fig. 4 DDoS Attack Traffic

This is the attack traffic generated during a SYN-Flood DDoS attack. This traffic is generated by a single attacker.

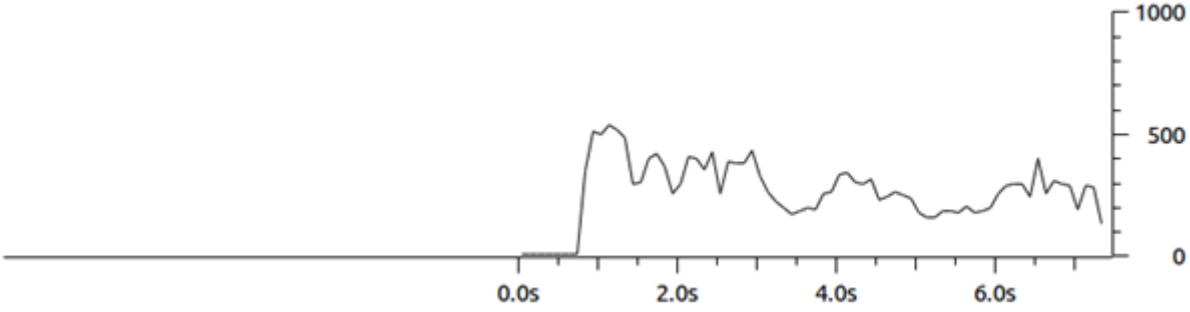


Fig. 5 Mitigation traffic for for Algorithmic Approach

This is the traffic generated during SYN-Flood DDoS attack while implementing the first mitigation module.

ISSN: 2233-7857 IJFGCN

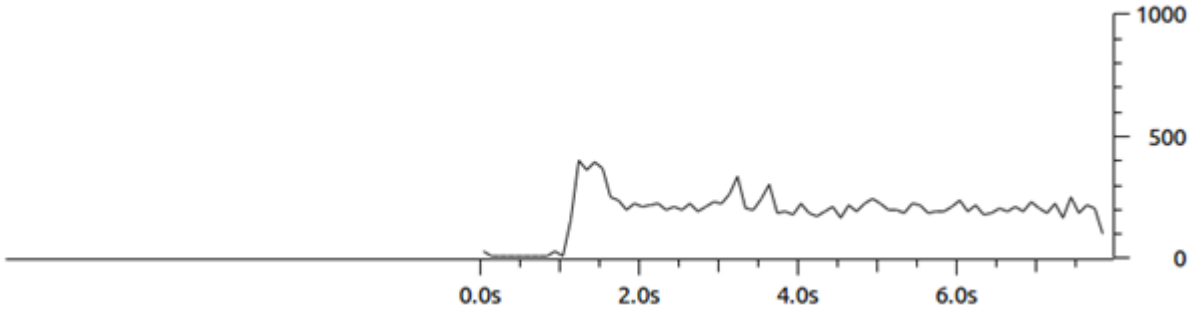


Fig. 6 Mitigation traffic for ML Based Approach

This is the traffic generated during SYN-Flood DDoS attack while implementing the second mitigation module.

C. Result Analysis

Above figures show packet flow through the network when mitigation module is implemented. As we can see in both the cases, the packets count is reduced gradually.

As we can observe ML-Based Approach has better results in mitigating SYN-Flood DDoS. ML based approach is faster in detecting the attack. Both the algorithms were given same threshold value. The threshold value is used to define the maximum number of abnormal packets permitted by a host. This threshold value is necessary for false positive cases.

Both the approaches are given all the packets to evaluate. Performance of ML based approach can further be increased by sampling of packets. In sampling of packets, only a subset of packets is send to the mitigation module for detecting. This reduces the load on the module.

VII. CONCLUSION AND FUTURE WORK

In this paper, we have discussed about SDN and DDoS attack in SDN. We have implemented two DDoS detection and mitigation approaches. This approaches are applied on a simple topology. Further DDoS attack is performed and the efficiency of these two algorithms is analyzed. Our aim of comparing these two algorithms was to find out the best out of them which will detect and mitigate the DDoS attack which causes some serious threats to the controller. We have observed that ML approach works better than the algorithmic approach in this scenario. In future we would like to work on increasing the efficiency of the machine learning approach.

REFERENCES

[1] C. Dharmadhikari, S. Kulkarni, S. Temkar and S. Bendale, “A Study of DDoS attacks in Software Defined Networks”, in IRJET, vol. 6 issue 12. 2019.
[2] Ubale, Tushar & Jain, Ankit. (2018). SRL: An TCP SYNFLOOD DDoS Mitigation Approach in Software-Defined Networks. 956-962. 10.1109/ICECA.2018.8474561.
[3] S. S. Mohammed et al., "A New Machine Learning-based Collaborative DDoS Mitigation Mechanism in Software-Defined Network," 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Limassol, 2018, pp. 1-8.
[4] Y. Chen, J. Pei and D. Li, "DETPro: A High-Efficiency and Low-Latency System Against DDoS Attacks in SDN Based on Decision Tree," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6.
[5] Y. Liu, M. Dong, K. Ota, J. Li and J. Wu, "Deep Reinforcement Learning based Smart Mitigation of DDoS Flooding in Software-Defined Networks," 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, 2018, pp. 1-6.
[6] B. H. Lawal and A. T. Nuray, "Real-time detection and mitigation of distributed denial of service (DDoS) attacks in software defined networking (SDN)," 2018 26th Signal Processing and Communications Applications Conference (SIU), Izmir, 2018, pp. 1-4.\

ISSN: 2233-7857 IJFGCN

[7] V. Deepa, K. M. Sudar and P. Deepalakshmi, "Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques," 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2018, pp. 299-303.
[8] C. Buragohain and N. Medhi, "FlowTrApp: An SDN based architecture for DDoS attack detection and mitigation in data centers," 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), Noida, 2016, pp. 519-524.
[9] R. M. Thomas and D. James, "DDOS detection and denial using third party application in SDN," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, 2017, pp. 3892-3897.
[10] N. Dayal and S. Srivastava, "Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN," 2017 9th International Conference on Communication Systems and Networks (COMSNETS), Bangalore, 2017, pp. 274-281
[11] Siddhant Shah, Shailesh Bendale,"An Intuitive Study:Intrusion Detection Systems and Anomalies, How AI can be used as a tool to enable the majority", in 5G era. ICCUBEA, 2019
[12] S. Ray, "A Quick Review of Machine Learning Algorithms," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 2019, pp. 35-39.doi: 10.1109/COMITCon.2019.8862451
[13] S. P. Bendale and J. Rajesh Prasad,"Security Threats and Challenges in Future Mobile Wireless Networks",2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, 2018, pp.146-150.
[14] Mr. Ajinkya Patil, Mr. Pratik Jain, Mr. Ravi Ram, Mr. Venkatesh Vayachal, Prof. S. P. Bendale,"Detection of Distributed Denial-of-Service (DDoS) Attack on Software Defined Network (SDN)," 2018, IRJET ISO 9001:2008 Certified Journal,2018, e-ISSN: 2395-0056,p-ISSN: 2395-0072.
[15] Scikit-learn available [Online]: https://scikit-learn.org/stable/
[16] Dhumane, A., & Prasad, R. (2015). Routing challenges in internet of things. CSI Communications.
[17] Dhumane, A. V., Prasad, R. S., & Prasad, J. R. (2017). An optimal routing algorithm for internet of things enabling technologies. International Journal of Rough Sets and Data Analysis, 4(3), 1–16.

ISSN: 2233-7857 IJFGCN