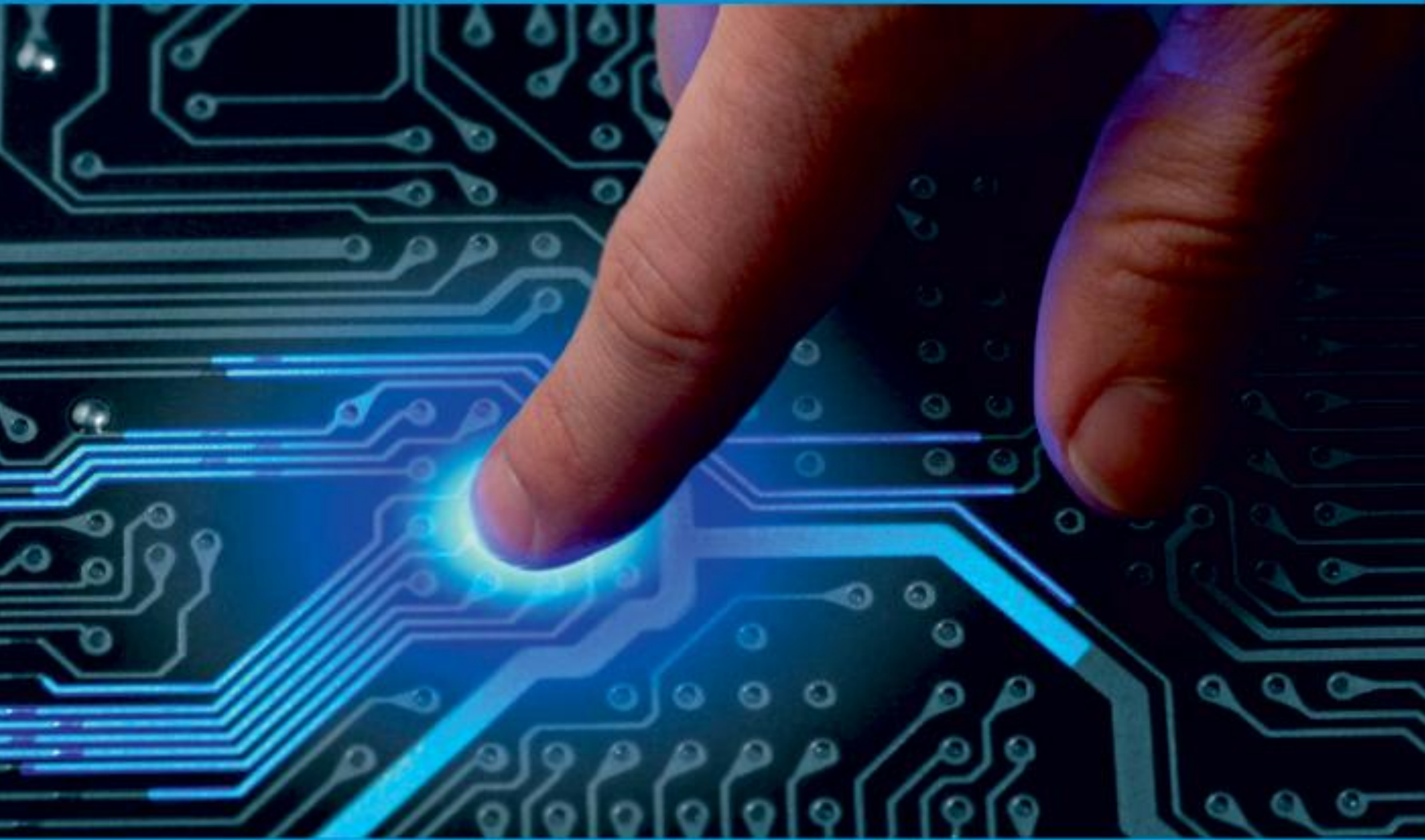
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |
|| Volume 9, Issue 6, June 2021 ||
| DOI: 10.15680/IJIRCCE.2021.0906160 |

DDoS Detection Using Machine Learning under SDN Context

Aishwarya Nagane, Akshay Mundada, Shrishail Patil

UG Student, Dept. of Computer Science &Engineering, JSPM's Bhivarabai Sawant Institute of Technology and Research, Pune, India

UG Student, Dept. of Computer Science &Engineering, JSPM's Bhivarabai Sawant Institute of Technology and Research, Pune, India

Assistant Professor, Dept. of Computer Science &Engineering, JSPM's Bhivarabai Sawant Institute of Technology and Research, Pune, India

ABSTRACT: Software-Defined Networking is the future of networking that decouples data and control layers from network devices for centralized network management. SDN provides excellent network management and security, allowing you to program your network in a convenient and easy-to-use manner. However, SDN is vulnerable to attacks. DDOS attacks are the most dangerous and threaten the network because they overload the network, block access to network servers with a large number of packets, and use network resources to avoid answering additional incoming calls question. It is well known that the number of DDOS attacks only increases in cloud environments. The proposed method combines statistical and machine learning techniques to effectively detect and block DDOS attacks on SDN. This method is implemented using Ryu controller and mini-network simulator with OpenFlow SDN protocol. The algorithm implemented for machine learning provides 99.26% accuracy and 100% detection rate when detecting and protecting DDOS attacks from software-defined networks.

KEYWORDS: DDoS Detection, Machine Learning, Software Define Network.

I. INTRODUCTION

The trend towards cloud computing has grown rapidly in industry and academia in recent years, thanks to the key opportunities that traditional networks can provide. Cloud networking trends. SDN is a networking technology that improves network performance and management, provides centralized network management, and allows you to program network devices. (Xiaetal. (2015)).

SDN separates network device control and baud rate and allows SDN controllers to program control layers. The SDN architecture consists of three layers: an infrastructure layer with network devices such as switches and hosts, a control layer that implements controllers, and an application layer for network applications. SDN is used to monitor and manage the network from a single location. This makes it easy to change and manage network devices on your network. The internship improves scalability, performance, control, and provides flexibility and cloud management. Software-Defined Networked Clouds are deployed on cloud computing networks to enhance network security and control and Network as a Service (NAAS) (Yanetal. (2016)).

II. LITERATURE SURVEY

1) Authors Xu and Liu (2016) presented a parallel algorithmic technique for modifying the flow monitoring of network switches to quickly identify potential victims, malicious traffic, and suspicious attackers. The author experimented with their designs, and the author's claim is well supported by the graphics and article results. However, there is not enough detail in this article about the modeling tools and techniques used to obtain results obtained to achieve high accuracy in asymmetric flow detection.
2) Wang et al. (2019) proposes four feature extraction methods, including collecting traffic and bitrate data, symmetric and asymmetric power fluctuations, and the number of packets outgoing from the network. The proposed algorithm is implemented using the Ryu controllerand simulated using Mininet. The results showed that the response time of the controller to DDOS attacks is reduced.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906160 |

3) The approach of Bushan and Gupta (2019) is to tune the software-defined size of the network flow table to protect against DDOS attacks. This is because most DDOS attacks fill table records and block new records. Switch input. .. The architecture has two databases: blacklist resources and stream table state. The flow table status contains the network power input status for all switches. The blacklist status stores the original IP addresses of malicious attack traffic entering your network. When the flow table is full, find the closest switch to pass traffic and do not set the size of the flow table. This method actually allows malicious traffic on the network. This can be dangerous to the network and there is no early warning system. The author experimented with this method and presented the results, implemented it using Pox controller, a Python-based driver, and created a simulation environment using Mininet. Since there is no strategy for early detection of limitations, assessments are documented and detailed in order to reproduce and reproduce the experiment.
4) Myint Oo et al. (2019) proposes a machine learning algorithm based on an extended support vector machine. In this study, the ASVM algorithm predicts DDOS attacks on SDN by collecting data and classifying parameters during the feature extraction phase. This method aims to reduce the time for testing and training machine learning algorithms to work. The implementation takes place in an open daylight control and simulation environment implemented with mininet, and the ASVM method claims the authors have a recognition accuracy of 97% and the shortest test and training time. The author’s argument is well supported by the graphical results of the article.
5) Dehkordie et al. (2020) applies a combination of entropy-based learning and machine learning methods. The author’s approach consists of three stages: traffic data collection, entropy threshold and ML classifier. It collects data, applies a static threshold based on entropy to increase only malicious traffic, and then applies those records using machine learning algorithms. Experiments were performed using reflector drivers, and network modelling and topology were performed by Mininet. The results show that this approach provides better accuracy and predicts DDOS detection results.

III. Proposed Methodology

Existing network systems are vulnerable to attacks and can cause data protection problems and data protection breaches in network information packets. To help prevent network attacks on public networks, this white paper presents methods for detecting and defending against software-defined network DDOS attacks using network statistical analysis and machine learning techniques. SDN-based networking allows separation of control and data layers for network devices. A centralized management mechanism has been implemented to prevent unauthorized access to the network. All incoming network traffic has some characteristics and parameters that are defined for each stream of network packets. These attributes are collected as training capabilities and testing methods to prevent DDOS attacks on networks that use software-defined networks. The following features and parameters are monitored and combined to detect DDoS attacks.

Speed of IP Sources: This feature provides the total amount of incoming TP resources on the network in a given time interval. It is abbreviated as SSIP and is defined as:

$$SSIP = SumIPsrc / IP$$

SumIPsrc is the total number of incoming IP sources for each stream, and T is the sampling time interval. The time interval T is set to 3 seconds, so the detection system monitors and collects stream data every 3 seconds and stores the source IP address for this period. The controller needs enough attack data and legitimate traffic data so that machine learning algorithms can predict attacks. In a normal attack, SSIP is usually low, and in an attack, it is high.

Flow Count of the Traffic: All network traffic coming from the network has a certain number of flows. Normal traffic flow is less than DDOS attack traffic.

Speed of Flow Entries: This is the total number of streaming inputs to switches on the network over a given time interval. Abbreviated as SFE, it is defined as:

$$SFE = N/T$$

In the case of a DDOS attack, the number of stream entries increases significantly at regular intervals compared to the value of the stream entry rate in the stream, which is a very important property for detecting attacking traffic.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906160 |

Ratio of Pair-Flow Entries: This is the total amount of incoming traffic that goes through the switch. H. Interactive IP addresses divided by the total number of streams in period T. This is abbreviated as RPF and is defined as:

RPF = SrcIPs / N

Where SrcIP is the total number of communicating IP addresses in the network stream, and N is the total number of IP addresses. Under normal traffic conditions, the source IP address of the ith stream coincides with the destination IP address of the jth stream, and the jth stream is the same source IP address as the destination IP address of the ith stream. This is an interactive stream and does not cover DDoS traffic. During an attack, the input stream to the target host increases rapidly at time T, and the target host becomes unresponsive.

Consequently, when a DDOS attack is initiated, the total number of joint threads for the attacking traffic is drastically reduced. By dividing the total number of shared streams by the total number of streams, this discovery parameter can be extended to the network under different operating conditions.

These are 4 parameters and properties extracted from each inbound traffic stream programmed into the ryu SDN controller. Using this extracted feature data, the SVM / Decision Tree machine learning algorithm can detect malicious traffic reaching the network and classify it as normal or DDOS traffic.

IV. DESIGN SPECIFICATION

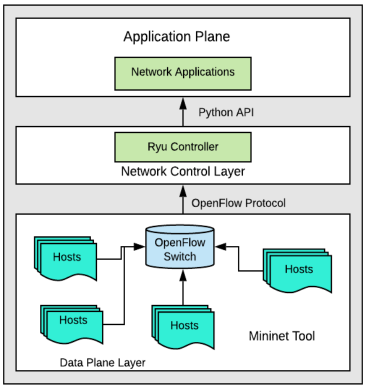


Fig. SDNFramework.

The SDN frame data field has multiple nodes/hosts created virtually as mininet networks connected to an OpenFlow switch that defines the SDN protocol, the OpenFlow protocol is the frame control plane, the control plane manages the data fields, overrides rules, defines and monitors them. Network traffic flow. Here the Ryu controller is used as a controller that provides scheduling functions and can control routing in the network. Since Ryu is a Python-based controller that uses a Python-based API to communicate with the application layer (in this case, the network application), the control plane is programmed using Python.

V. IMPLEMENTATION

The presented method uses both statistical and machine learning methods to detect and mitigate DDOS attacks in a software defined network. The implemented method requires to train the SVM ML algorithm for detecting the attack in a network. Data Collection module has to collect data of both normal traffic and attack traffic and stores the data in a CSV file for the ML algorithm to use. At first normal traffic data has to collect and then the attack traffic data, it is recommended to collect normal traffic data again after attack traffic data for better accuracy. The data is collected considering all three statistical parameters of feature extraction defined in the methodology namely speed of source IP, speed of flow entries and ratio of flowpair entries in different columns.

Detection and Mitigation takes place after the data has been collected and the controller is set to detection state, then when the normal traffic is generated the SVM algorithm predicts it as normal traffic and when the attack traffic is generated it instantly detects the traffic as DDOS attack traffic and blocks the port from which the traffic is incoming. Once the port has been blocked the controller is set to a 120sec hard time, after which it unblocks the port. But, if the

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906160 |

attack is still active it again detects and blocks the port for another 120 seconds. After blocking thenormal traffic flow is allowed in the network from other ports. This process keeps on going as long as the attack lasts.

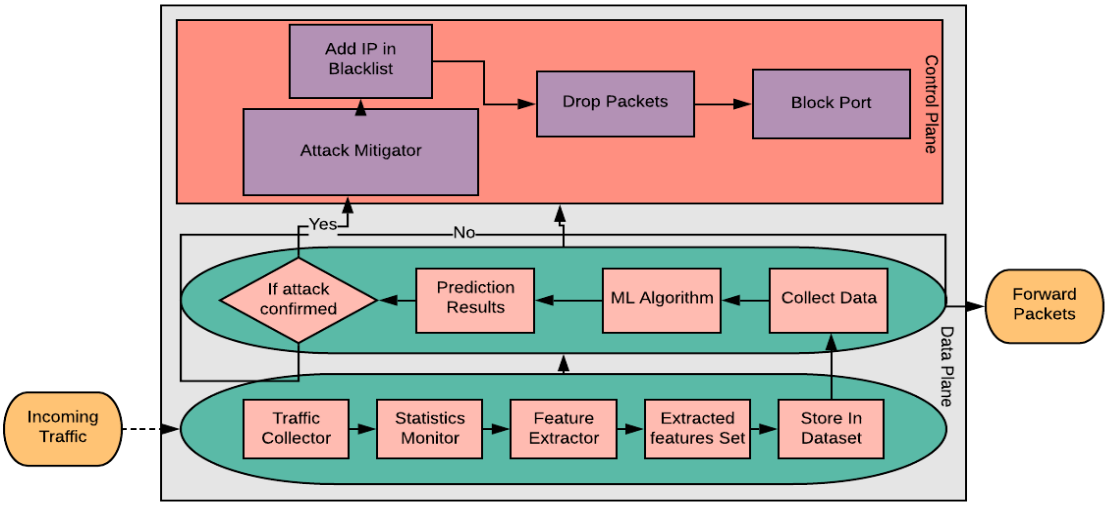


Fig. 1 Flowchart of the Presented Method.

Software-Defined Networking has many protocols and drivers, each of which works in a specific way and provides efficiency and flexibility in a specific way. The provided methods are implemented using the most popular and powerful DDOS detection and protection against software-defined network attacks.

The Openflow protocol is the most common and standard protocol in software-defined networks. This is why this project uses openVswitch. The presented method is a combination of statistical methods and machine learning, therefore the logic and methods are programmed in Python. The statistical method includes parameters such as IP source rate, ingress rate, and ingress rate of a pair of streams, all of which are programmed into the controller.

Ryu Controller is an open source Python-based programmable controller used to define the rules and logic that switches must follow in their methodology.

Mininet is a network simulator that uses controllers, switches, and hosts to create a virtual network topology. This will create one openVswitch with 10 and 25 hosts for some testing.

Hping3 is a packet generator that generates TCP / IP traffic on your network. It is mainly used for network security testing. General traffic attacks and scripts have been written to automatically generate traffic with this tool.

Iperf is also a network provider and network performance tester and is used to manually generate traffic for this task.

VI. EVALUATION

This section describes SDN testing as a general detection and mitigation process based on the accuracy and speed of detection of normal and non-essential traffic sent across the network to different ports. The first generated dataset contains over 600 generic traffic data samples and over 300 attack traffic data samples that can train and analyze SVM algorithms to predict attacks. The test was run for 300 seconds at 2 second intervals to collect traffic. SVM predicts traffic every 2 seconds.

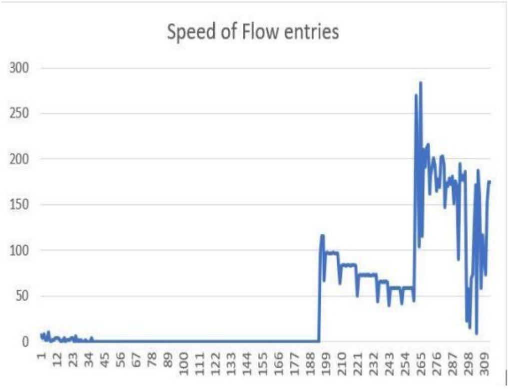
CASE STUDY I

In this experiment, normal traffic is sent from all ports, an attack is sent from network port / host 1, and inbound traffic is captured every 3 seconds. The network topology is created using a mini-network with an OpenFlow switch with 10 hosts per network.

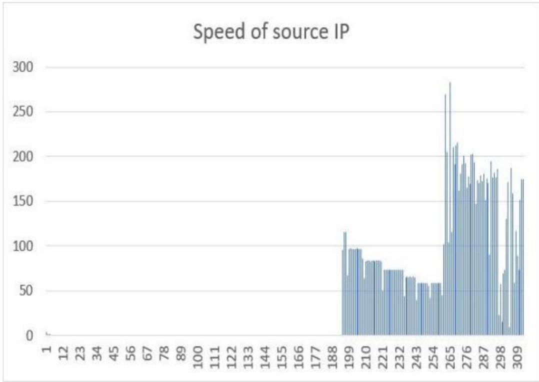
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906160 |

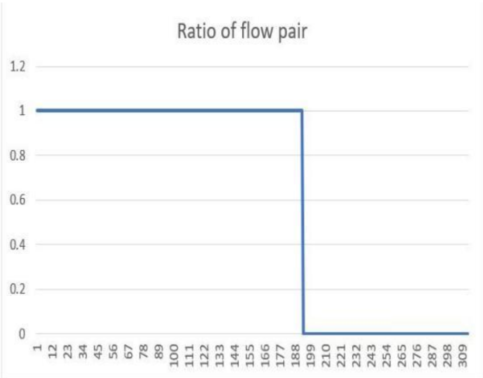


(A) SFE

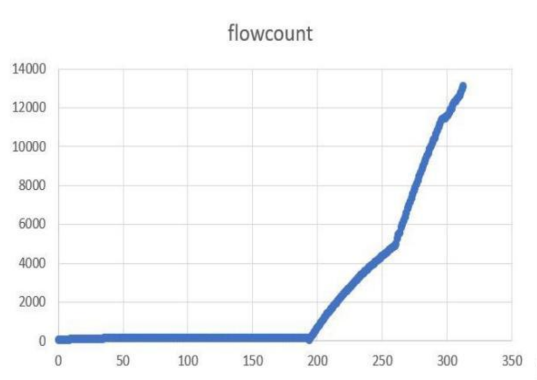


(B) SSP

On maps A and B, the X-axis is the amount of data, and the Y-axis is the number of input layers and IP sources. The graph shows how the speed of incoming resources and IP increases as the attack traffic is sent over the network, and the straight line shows the normal traffic flow on the network.



(A) RFIP



(B) Flowcount

Diagram A shows the flow pair ratios for attack traffic coming from the network, while Chart B shows the total flow for normal traffic and attack traffic.SVM machine learning algorithm predicting the traffic as normal traffic. The SVM machine learning algorithm predicts traffic when DDOS attack traffic and the protection process starts immediately, blocking port 1 for attack traffic.

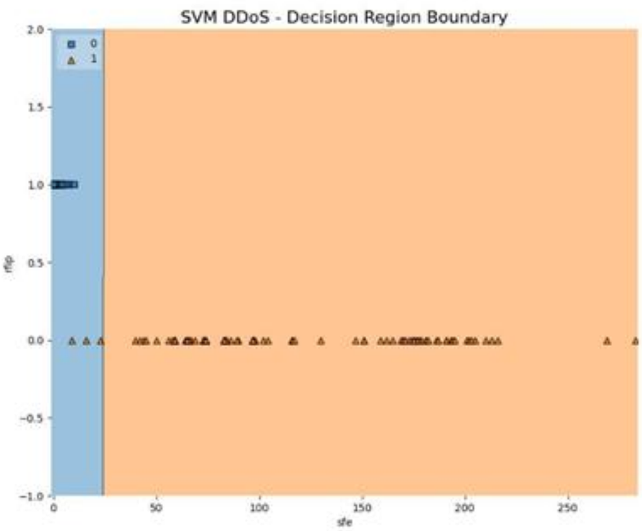


Fig. SVM Decision Boundary

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

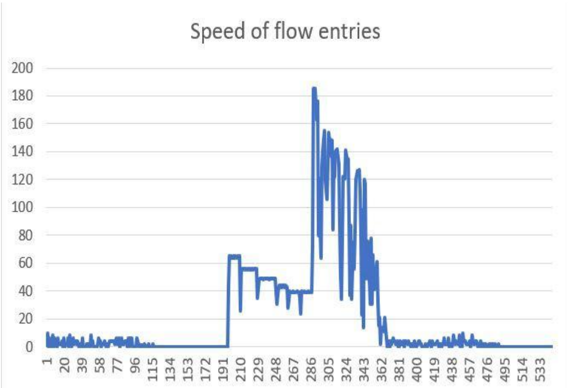
|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906160 |

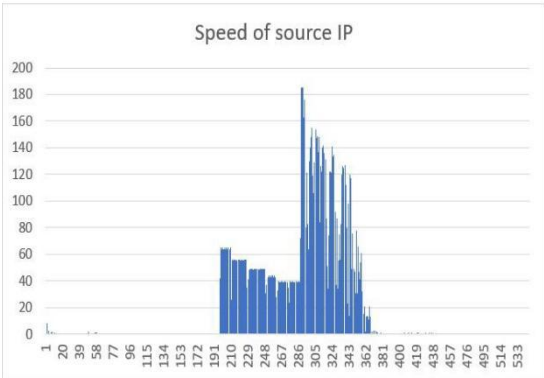
The image above shows the decisions made by the SVM-ML algorithm. The blue area represents normal traffic, and the orange area represents attacking traffic from the network. The accuracy value of the presented method is 98.71%, and the cross-validation value between the training data and the collected test data is 99.57%. The traffic detection rate of DDOS attacks in the network, achieved by this method, was 92.8% and 0% of false positives. This means that normal traffic is not considered attack traffic.

CASE STUDY I I

In this experiment, normal traffic is sent from all ports, an attack is sent from port / host 8 on the network, and inbound traffic is captured every 2 seconds. The network topology is created using a mini-network with an OpenFlow switch with 25 hosts on the network.

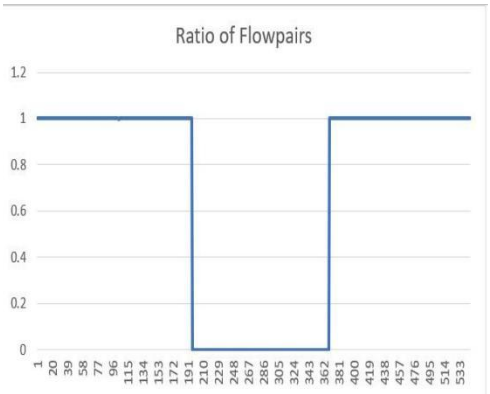


(A) SFE

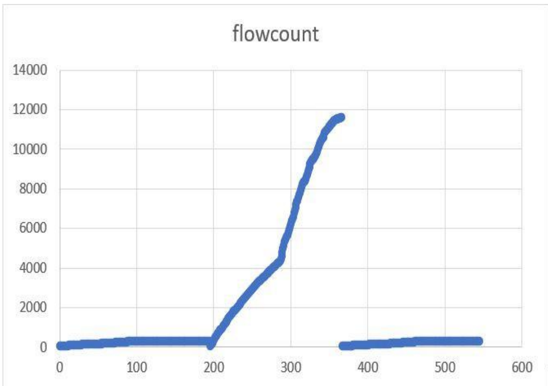


(B) SSP

On maps A and B, the X-axis is the amount of data and the Y-axis is the input rate and the source IP address. The graph shows how the speed of the incoming and outgoing IP address increases as the attacking traffic travels over the network, and the straight lines represent the normal traffic flow on the network. Graph A shows the relationship between racing pairs.



(A) RFIP



(B) Flowcount

If there is attacking traffic on the network, it will decrease and Chart B shows normal traffic flow and attacking traffic. The SVM machine learning algorithm predicts that the traffic is attacking DDOS traffic and the protection process starts immediately, blocking port 8 through which the attacking traffic arrives.

The image above shows the decisions made by the SVM-ML algorithm. The blue area represents normal traffic, and the orange area represents attacking traffic from the network.

The accuracy value obtained using the presented method is 99.26%, which corresponds to the value of cross-validation with training and testing data. The data obtained is 99.75%.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906160 |

The traffic detection rate for DDOS attacks in the network, achieved by this method, is 100% and 0% false positives. This means that normal traffic is not considered attack traffic.

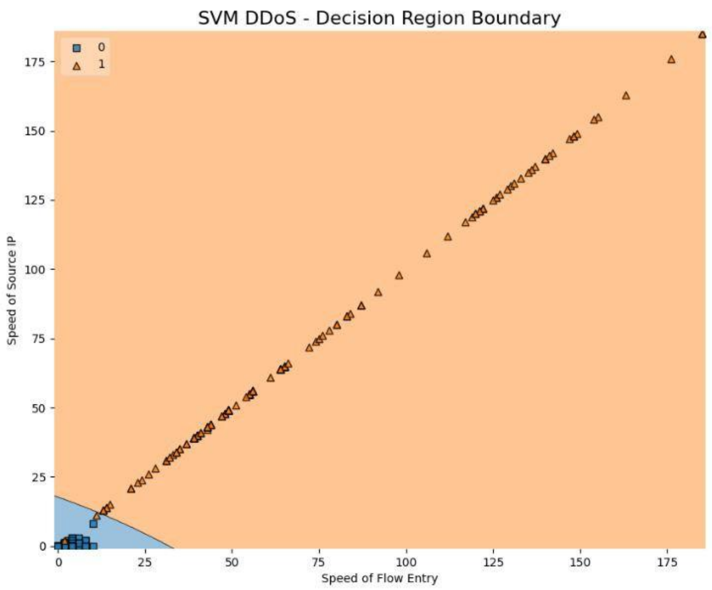


Fig. SVM Decision Boundary

VII. CONCLUSION

Software-Defined Networks provide the ability to programmatically design and operate networks not found in traditional networks. The main goal of this work is to detect and respond to DDOS attacks in the cloud using SDN. The applied method is a combination of the SVM algorithm with statistical functions such as the source IP address for machine learning to detect and predict DDOS attacks on the network, the stream reception rate, the number of streams and the ratio of stream pairs. Experience shows that the method provided by 0f can provide 99.26% accuracy and 100% malicious traffic detection rate without false traffic predictions. However, security is not a complete test and can always be compromised in the same way if there are flaws in the way it is implemented. Attacks from trusted IP sources can be used by SVMs to send unexpected and malicious traffic across the network.

REFERENCES

1. Ahmad, I., Namal, S., Ylianttila, M. and Gurtov, A. (2015). Security in software defined networks: A survey, IEEE Communications Surveys Tutorials 17(4): 2317–2346. JCR Impact Factor: 22.973 (2019).
2. Alshamrani, A., Chowdhary, A., Pisharody, S., Lu, D. and Huang, D. (2017). A defence system for defeating ddos attacks in sdn based networks, Proceedings of the 15th ACM International Symposium on Mobility Management and Wireless Access, MobiWac '17, Association for Computing Machinery, New York, NY, USA, p. 83–92. ERA Ranking: B.
3. Bhushan, K. and Gupta, B. B. (2019). Distributed denial of service (ddos) attack mitigation in software defined network (sdn)-based cloud computing environment, Journal of Ambient Intelligence and Humanized Computing 10(5): 1985–1997. JCR Impact Factor: 1.910 (2019).
4. Dehkordi, A. B., Soltanaghaei, M. and Boroujeni, F. Z. (2020). The ddos attacks detection through machine learning and statistical methods in sdn, The Journal of Supercomputing pp. 1–33. JCR Impact Factor: 2.600 (2019).
5. Wang,Y.,Hu,T.,Tang,G.,Xie,J.andLu,J.(2019). Sgs: Safe-guard scheme for protecting control plane against ddos attacks in software-defined networking, IEEE Access 7:34699–34710.JCR Impact Factor: 4.640 (2019).