International Conference on Smart Systems and Inventive Technology (ICSSIT 2018)
IEEE Xplore Part Number: CFP18P17-ART; ISBN:978-1-5386-5873-4

Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques

V.Deepa[1], K.Muthamil Sudar[2], P.Deepalakshmi[3]
Department of Computer Science and Engineering
School of Computing
Kalasalingam Academy of Research and Education, Krishnankoil
vkdeepa94@gmail.com[1], k.muthamilsudar@klu.ac.in[2], deepa.kumar@klu.ac.in[3]

Abstract- **Software Defined Network (SDN) provides a promising solution over traditional networks by decoupling the control plane and network plane. With the help of this feature, controller can get global view of the entire network. Since the controller acts as a core part of the SDN environment, there is a serious threat towards the controller in terms of security. A Distributed Denial of Service (DDoS) attack is the most potential attack in SDN environment. DDoS attack prevents the authorized user to access the available resources for infinite amount of time. In this paper, we have proposed the hybrid machine learning model to protect the controller from DDoS attacks. And our experimental results clearly manifest that the hybrid machine learning model provides more accuracy, detection rate and less false alarm rate compared to simple machine learning models.**

Keywords: **Software Define Network, Machine Learning(ML), Hybrid Machine learning, Distributed Denial of Service (DDoS), Support Vector Machine(SVM), Self Organized Map (SOM).**

I. INTRODUCTION

SDN[1] architecture was developed with a great mission to overcome the drawbacks available in existing traditional network architecture. SDN architecture separates the network control from forwarding devices and enables the controller to become directly programmable. This helps the network administrators to adjust the network traffic flow dynamically. Due to its centralized nature, controller can get a global view of the network. With the help of these strong features, SDN environment can provide high reliability, simplicity and flexibility.

But, still there are some problems that need to be addressed in terms of security. Due to its centralized nature, controllers are subjected to major potential attacks. In order to protect the controllers, security mechanisms such as statistical-based, machine learning-based have been proposed. The major threat in networking environments is DDoS (Distributed Denial of Service) [2] attack. The main aim of DDoS attacks is to prevent the legitimate user to access the service for a long time. In this attack, attacker tries to compromise the multiple numbers of hosts to send a huge amount of traffic intentionally towards a legitimate user. This leads to unavailability of service for large amount of time. A host which is under the attacker control is called bot. A group of controlled computers is known as botnet.

In this paper, we have designed a DDoS detection mechanism based on hybrid machine learning techniques. The structure of the paper is organized as follows. Section II discusses some of the related works. Section III describes about the DDoS attack in SDN environment. Section IV is about our proposed algorithm with experimental setup detailed in Section V. Section VI discusses about performance of proposed work and Section VII states conclusion and some future work.

II. RELATED WORKS

In this section, we analyze some related work, focusing on detection of DDoS attacks in SDN.A.Saboor et al[3] proposed the detection of DDoS attack based on correlation algorithm and IAFV algorithm. They used different time series with sliding windows for improving the detection rate.Yavuz CANBAY et al. [4] studied the Genetic Algorithm (GA) and K-nearest Neighbor (KNN) and combined the model to detect the attacks. Experimental hybrid system provided more accurate results compared to conventional KNN classifier.

Saurav Nanda et al. [5] used Bayesian Network and achieved an accuracy of 91.68 % which indicates that out of 278,598 attacks, their model was able to accurately predict 254,834 attacks. Gisung Kim, et.al[6] proposed a hybrid learning model to detect the DDoS attack and to protect the OpenFlow switches. They found that their model work well for unknown attacks also.

Ahmad Y. Javaid et al. [7] used deep learning methods to detect the DDoS attack in SDN environment. They had collected the traffic from home wireless network (HWN) scenario. And they got 96.65% accuracy. Lohit Barki et al.[8] have used different machine learning techniques such as Naive Bayes, K-nearest neighbor, K-Means, K-medoids to detect the DDoS attack. They found that Naïve Bayes model work well compared to other considered algorithms with highest accuracy. From the literature survey, we have identified that the hybrid models may produce high performance in terms of accuracy and false alarm rate.

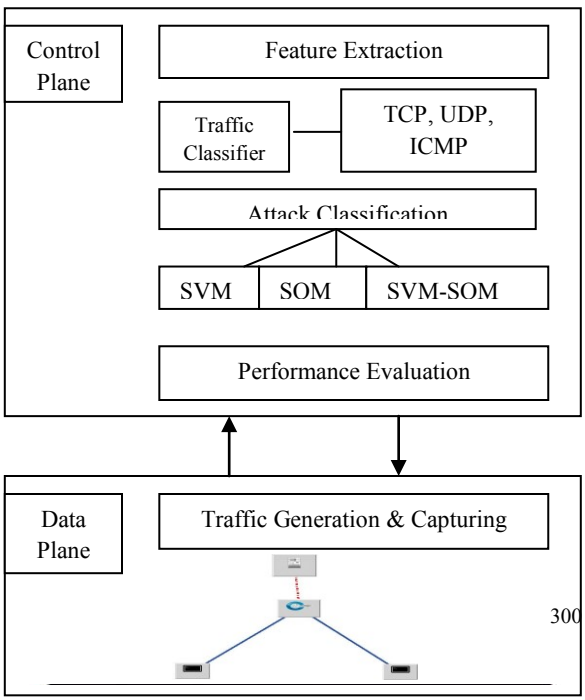
III. DDOS ATTACKS ON SDN

SDN[1] architecture consists of three layers such as Infrastructure layer, Control Layer, Application layer. Control layer i.e., controller is responsible for managing the entire traffic flow based on the abstract view. The main role of infrastructure layer is to forward the packets as per the rules and policies assigned by controller. Application layer is responsible for software related business and security applications.

Switches in the infrastructure layer contain the flow tables. Flow tables are made up of flow rules. These rules consist of three fields such as match, condition, action. Based upon the flow table, incoming traffic will be processed. When the packet is coming to the switch for the very first time, it will be directed towards the controller to initiate a new flow. If the flow for the incoming packet is already available, that will follow the same set of rules given in the flow table. In DDoS attack [2], one way to compromise the user is spoofing the identity of target user. This will result in flood of incoming packets with several new IP address. If those IP addresses are not matched means, the packet header will sent to the controller for processing. This will cause the legitimate request to wait for large amount of time.

IV. PROPOSED WORK

In order to handle this DDoS attack, we have proposed a combination of two machine learning based model with Support Vector Machine (SVM) and Self Organized Map(SOM). Fig 1 shows the architecture of our proposed method. SVM is a kind of supervised learning technique whereas SOM is a kind of unsupervised learning technique. Initially, we have separately implemented the SVM and SOM. And we found that SOM works well for the attack classification compared to the SVM. In order to improve the performance, we jointly implemented both SVM and SOM, which shows the better detection rate, accuracy and false rate compared to separate implementation. In this section, we discussed about working of two algorithms and our proposed hybrid machine learning algorithm.



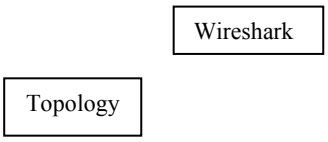


Fig 1: System Architecture of Proposed Method

Input: Captured network traffic with both attack and normal connections.
Output: An Optimal SVM Classifier.

Train the SVM classifier with training samples, when the controller starts.

Categorize the different types of packet as TCP, ICMP, UDP using traffic classifier module.

Construct an optimal hyper plane to classify the attack.
If the classifier detects the connection as attack.
Block the connection and update the rules in flow table.
Else
Allow the connection
Wait for next connection
Repeat above two steps for all the incoming connection.

Fig 2: SVM Algorithm

Input: Captured network traffic with both attack and normal connections.
Output: An Optimal SOM Classifier.

Train the SOM classifier with training samples, when the controller starts.

Categorize the different types of packet as TCP, UDMP, ICMP using traffic classifier module .
Construct the SOM classifier to classify the attack.
If the classifier detects the connection as attack
Block the connection and update the rules in flow table.
Else
Allow the connection
Wait for next connection
Repeat last two steps for all the incoming connection.

Fig 3 : SOM Algorithm

Input: Captured network traffic with both attack and normal connections.
Output: An Optimal SVM-SOM Classifier.

Train the SVM and SOM classifier with training samples, when the controller starts.
Categorize the different types of packet as TCP, UDMP, ICMP using traffic classifier module.
First use the SVM classifier to detect the attack
If the connection is identified as attack
Block the connection and update the rules in flow table.
Else
Forward those connections to SOM classifier module
If the connection is identified as attack by SOM module
Block the connection and update the rules in flow table.
Else
Allow the connections.
Wait for next connection
Repeat last three steps for all the incoming connection.

Fig 4:SVM-SOM (Hybrid) Algorithm

V. EXPERIMENTAL SETUP

To analyze the performance of proposed system, we have implemented SVM, SOM along with our proposed hybrid algorithm using SVM and SOM stated in Fig 2, Fig 3 and Fig 4 respectively to detect DDoS attack. For our simulation, we have created a custom network topology with six switches and 21 host systems as shown in Fig 5 using Mininet [9], an emulation tool, which helps to create a virtual controllers, switches, hosts and links. For the controller, we have selected POX, a mostly used, lightweight, python-based controller. Packet generation is done with the help of Scapy tool [10]. Scapy generates traffic in the form TCP, UDP, ICMP

packets from various hosts. Also, we have used Wireshark [11] tool to capture the network traffic. With the help of traffic classifier module, we separate the traffic based on the packet type. We generated two kinds of traffic namely normal traffic towards legitimate hosts and attack traffic towards the targeted host including samples for both testing and training. Table I. shows the experimental results of our implementation work based on true positive(TP), true negative(TN), false positive(FP), false negative(FN). With the help of these values, we have calculated the accuracy, detection rate and false alarm rate.

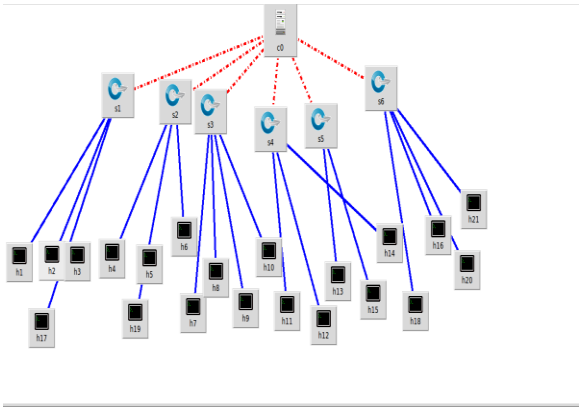


Fig 5 : Topology Setup

Algorithm	TP (%)	TN (%)	FP (%)	FN (%)
SVM	82.03	87.17	5.67	4.76
SOM	84.33	88.45	6.97	5.55
SVM-SOM	85.49	89.24	2.51	0.83

Table I: Experimental Results

VI. PERFORMANCE EVALUATION

The performance of proposed hybrid algorithm is analyzed using the parameters such as accuracy, detection rate and false alarm rate calculated using Equations 1, 2& 3 respectively. Accuracy is the percentage of correctly classified attacks for a given dataset. Detection rate is the number of attacks correctly classified over all predicted attacks. False alarm rate is a number of attacks wrongly classified.

$$Accuracy = \frac{No.of\ correctly\ predicted\ attacks}{Total\ No.of\ attacks} * 100 \quad (1)$$

$$DetectionRate = \frac{TP}{FP+TP} * 100 \quad (2)$$

$$False\ Alarm\ Rate = \frac{FP}{FP+TN} * 100 \quad (3)$$

Fig 6, 7 and 8 shows the comparison of detection rate, accuracy, false alarm rate for SVM, SOM, hybrid SVM-SOM. Since SVM is a supervised machine learning model, it should be trained with labeled data only. And it is very complex to detect the new attack. In case of SOM, it is a unsupervised machine learning model, it can able to detect the new attacks. But in case of SOM, false alarm rate will be high. In order to avoid the drawbacks in SVM and SOM, we have used hybrid model. In our model, first the traffic is passed through the SVM module and attacks are identified. To detect the new kind of attacks, resultant traffic from SVM module is again passed through the SOM module. Once the attack is detected, particular connection will be closed and rules are updated in flow table. Our proposed hybrid model provides high accuracy of 96.77%, high detection rate of 90.45%, and low false alarm rate of 0.032%.

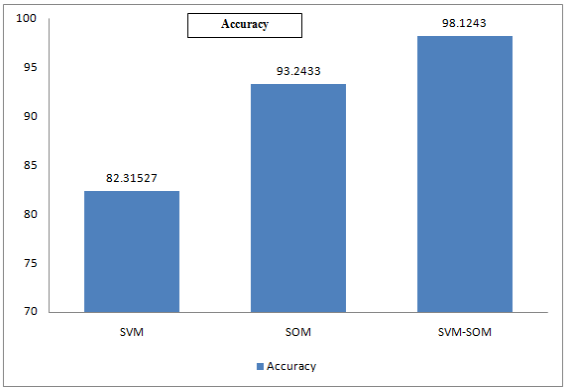


Fig 6: Comparison of Accuracy for SVM, SOM, SVM-SOM

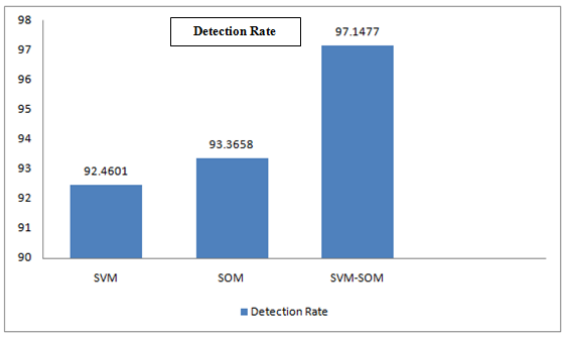


Fig 7: Comparison of Detection rate SVM, SOM, SVM-SOM

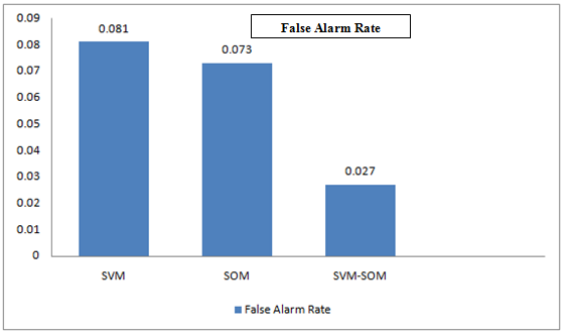


Fig 8: Comparison of False Alarm Rate for SVM, SOM, SVM-SOM

VII. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a hybrid machine learning model to detect DDoS attack in SDN environment. We also analyzed our proposed work based on the three performance metrics such as accuracy, detection rate, and false alarm rate. SOM, an unsupervised machine learning algorithm, which works well for detection of attacks compared to SVM algorithm. But by using our proposed hybrid machine learning model (SVM- SOM), we have achieved more accuracy, detection rate and low false alarm rate compared to simple machine learning model. In future, we will try to implement ensemble machine learning models to detect DDoS attack in data plane by imposing the security rules in the flow table.

VIII. REFERENCES

[1] Kreutz, Diego, et al. "Software-defined networking: A comprehensive survey." Proceedings of the IEEE 103.1 (2015): 14-76.

[2] Zargar, SamanTaghavi, James Joshi, and David Tipper. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." IEEE communications surveys & tutorials 15.4 (2013): 2046-2069.

[3] Yavuz CANBAY and Seref SAGIROGLU, "A Hybrid Method for Intrusion Detection" In IEEE 14th International Conference on Machine Learning and Applications",2015.

[4] A.Saboor and B.Aslam, " Analyses of Flow Based Techniques to Detect Distributed Denial of Service Attacks" In Proceedings of 12th International Bhurban Conference on Applied Sciences & Technology (IBCAST), 13th-17th Jan,2015. pp 354-362.

[5] Saurav Nanda, Faheem Zafari, CasimerDeCusatis, Eric Wedaa and Baijian Yang, "Predicting Network Attack Patterns in SDN using Machine Learning Approach", In IEEE Conference on Network Virtualization and Software Defined Networks (NFV-SDN),2016.

[6] Gisung Kim, Seungmin Lee, Sehun Kim "A novel hybrid attack detection method integrating anomaly detection with misuse detection", - journal on Expert Systems with Applications – [Online] Available : www.elsevier/locate/eswa,

[7]Niyaz, Quamar, Weiqing Sun, and Ahmad Y. Javaid. "A deep learning based DDoS detection system in software-defined networking (SDN)." arXiv preprint arXiv:1611.07400 (2016).

[8]Barki, Lohit, et al. "Detection of distributed denial of service attacks in software defined networks." Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on. IEEE, 2016.

[9] http://mininet.org/

[10] http://scapy.net/

[11]http://www.wireshark.org/