An SVM Based DDoS Attack Detection Method for Ryu SDN Controller

Shideh Yavary Mehr
Byrav Ramamurthy
University of Nebraska-Lincoln
Lincoln, Nebraska, U.S.A.
{syavarymehr,byrav}@cse.unl.edu

ABSTRACT

Software-Defined Networking (SDN) is a dynamic, and manageable network architecture which is more cost-effective than existing network architectures. The idea behind this architecture is to centralize intelligence from the network hardware and funnel this intelligence to the management system (controller) [2]-[4]. Since the centralized SDN controller controls the entire network and manages policies and the flow of the traffic throughout the network, it can be considered as the single point of failure [1]. It is important to find some ways to identify different types of attacks on the SDN controller [8]. Distributed Denial of Service (DDoS) attack is one of the most dangerous attacks on SDN controller. In this work, we implement DDoS attack on the Ryu controller in a tree network topology using Mininet emulator. Also, we use a machine learning method, Vector Machines (SVM) to detect DDoS attack. We propose to install flows in switches, and we consider time attack pattern of the DDoS attack for detection. Simulation results show the effects of DDoS attacks on the Ryu controller is reduced by 36% using our detection method.

KEYWORDS

SDN, Ryu, DDoS attack, SVM

ACM Reference Format:
Shideh Yavary Mehr and Byrav Ramamurthy. 2019. An SVM Based DDoS Attack Detection Method for Ryu SDN Controller. In *The 15th International Conference on emerging Networking EXperiments and Technologies (CoNEXT '19 Companion), December 9–12, 2019, Orlando, FL, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3360468.3368183

1 INTRODUCTION

Software defined networking (SDN) has become widespread in the network research community and industry due to its characteristics such as scalability and flexibility. SDN creates a centralized control system to manage the overall network resources. In SDN, security has been the source of some concern [1] - [3]. Recent SDN-based security solutions are implemented at centralized controllers and their focus mostly are on increasing the control flexibility of SDN instead of strengthening the controller [1] , [4]. Existing SDN solutions are mainly based on specific aspects of network security. Most of them do not satisfy the general network security requirements [12]. SDN is vulnerable to different types of attacks, such as spoofing, tampering, information disclosure, and distributed denial of service (DDoS) [6]. Among these attacks, DDoS has the most devastating effect as it can cause service degradation of the SDN performance and further a lunching a DDoS attack is extremely simple. Increasing latency and dropping legitimate packets and, very big losses can caused degradation of the SDN performance [7], [8]. Since in SDN, the switches have less intelligence they cannot detect the malicious flows. Therefore, it is more difficult to mitigate DDoS attack. In this case the controller cannot realize if the incoming packets are from attacker or from burst flows [3] - [8]. Many earlier solutions are based on defining rules for dropping malicious packets, blocking suspicious traffic, prioritizing scheduling and so on [12]. These solutions may require some additional hardware or extra control packet, etc. Also, they are not cost effective [3] [6]. In this work, first we implement a successful DDoS attack using Mininet emulator. Then, we show how adding some flows in the switches, reduce DDoS attack by 36%.

2 METHODOLOGY

We use Python-based open source controller Ryu. Ryu supports various protocols. We simulate DDoS attack on SDN using Mininet emulator. Our topology consists four hosts, three switches and one controller (see Fig. 1). Mininet creates SDN elements such as controller, switches, and hosts and can share them with the other networks. Ryu provides software components with well defined API. It is easy for developers to create new network management and control applications. In this work, we use a machine learning method (SVM) to detect the DDoS attack. First, we collect traffic data from the packet-in messages and extract some values, such as source IP address, source port, and destination IP address, destination port. We use entropy to measure the distribution of these values and train the model by normal and abnormal traffic data. By comparing with some other machine learning algorithms [5]. We found that SVM is a better framework in terms of detecting the DDoS attack on Ryu SDN controller [5], [7].

3 IMPLEMENTATION

In order to simulate the DDoS attack in realistic traffic we use two different hosts and simulate the attacks from them. We used Mininet emulated virtual network which is installed on a virtual machine and it is connected with remote RYU controller running on another virtual machine. We wrote a script to generate normal traffic from

CoNEXT '19 Companion, December 9–12, 2019, Orlando, FL, USA

ACM ISBN 978-1-4503-7006-6/19/12…$15.00
https://doi.org/10.1145/3360468.3368183

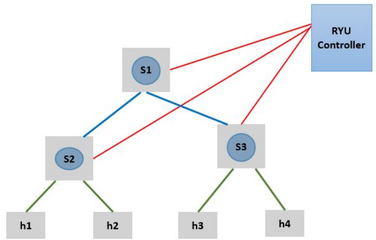

Figure 1: System Component Architecture

2 different hosts at random durations. To simulate malicious traffic, we use another script with randomly spoofed IPs with a high packet rate of 25 packets per second. Then, we use a machine learning technique to identify normal traffic and malicious traffic [9], [10]. SVM is a learning algorithm that classifies incoming traffic patterns as normal or malicious. SVM supports multi-class classification. The idea is a multi-class problem is broken-down into binary problems. Then these classifiers are trained [9], [11].

4 DETECTION

We used SVM as a classifier to detect DDoS attacks. SVM has low false positive rates and it tries to maximize the margins by discovering a suitable hyperplane. It generates a precise classification and has a good accuracy [3] - [5]. Some existing research on DDoS attacks has been analyzed by extracting the flow status information[10], [11]. In order to classify two different types of data (normal and malicious) some parameters such as "Speed of source IP", "Standard deviation of flow packets", "Standard deviation of flow bytes", "Speed of flow entries", "Ratio of pair flow entries" are used [11], [10]. Figure 2 shows the throughput comparison for the cases with DDoS attack detection and without DDoS attack detection.

5 MITIGATION

When the number of malicious packets start to increase exponentially in a certain time, then flow collector will notify the Ryu controller. In this case, the Ryu controller adds new rules to all forwarding devices. Based on these rules, all the forwarding devices send back all the malicious packets to the flow collector. Also we use time pattern of DDoS attack to prevent the DDoS attack.

6 CONCLUSIONS

In this work, we implemented a SVM based solution for attack detection. We highlighted the important attributes that can be used in effectively detecting the DDoS attack in its early stages like the number of packets and time in seconds. Experiments with our prototype implementation showed the effect of attack detection. In the future, we plan to extend our work in improving feature correlation, traffic generation, and real-time performance.

7 ACKNOWLEDGEMENT

This material is based upon work supported by the National Science Foundation under Grant No. CNS-1817105.

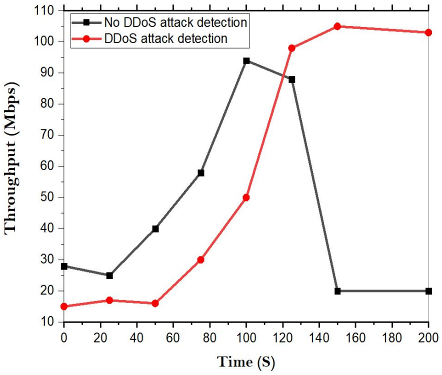

Figure 2: Throughput Comparison

REFERENCES

[1] K. Kalkan, G. Gur, and F. Alagoz, "Defense Mechanisms against DDoS Attacks in SDN Environment", IEEE Communications Magazine, vol. 55, no. 9, pp. 175-179, 2017.

[2] Y. Yu, L. Guo, Y. Liu, J. Zheng, and Y. Zong, "An Efficient SDN-Based DDoS Attack Detection and Rapid Response Platform in Vehicular Networks", Access IEEE, vol. 6, pp. 44570-44579, 2018.

[3] S. Ezekiel, D. Mon Divakaran, and M. Gurusamy, "Dynamic attack mitigation using SDN", 27th International Telecommunication Networks and Applications Conference (ITNAC), pp. 1-6, 2017.

[4] I. Abdulqadder, D. Zou, I. Aziz, and B. Yuan, "Modeling software defined security using multi-level security mechanism for SDN environment", IEEE 17th International Conference on Communication Technology (ICCT), pp. 1342-1346, 2017.

[5] Q. Y. Gong, and F. R. Yu, "Effective software-defined networking controller scheduling method to mitigate DDoS attacks," Electronics Letters, vol. 53, no. 7, pp. 469–471, 2017.

[6] N. Gde Dharma. M. F. Muthohar. J. Prayuda, K. Priagung. and D. Choi, "Time-based DDoS detection and mitigation for SDN controller." in 17th APNOMS, pp. 550-553, 2015.

[7] R.Wang, J. Jia, and L. Ju, "An entropy-based distributed DDoS detection mechanism in software-defined networking", 2015 IEEE Trustcom/BigDataSE/ISPA, pp. 310–317, 2015.

[8] Y. Xu and Y. Liu, " DDoS attack detection under SDN context", In: IEEE INFOCOM 2016—The 35th Annual IEEE International Conference on Computer Communications, pp.1–9, 2016.

[9] M. Alazab, "Profiling and classifying the behavior of malicious codes," Journal of Systems and Sofware, vol. 100, pp. 91–102, 2015.

[10] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS Attack Detection Method Based on SVM in Software Defined Network", Security and Communication Networks, Volume 2018, Article ID 9804061, 2018.

[11] R. T. Kokila, S. T. Selvi, and K. Govindarajan, "DDoS detection and analysis in SDN-based environment using support vector machine classifier, in Proc. 6th Int. Conf. Adv. Comput. (ICoAC), pp. 205–210, 2014.

[12] Z. You, Y. Feng, K. Sakurai, "Packet in Message Based DDoS Attack Detection in SDN Network Using OpenFlow", Proc. 5th International Symposium on Computing and Networking, CANDAR 2017, pp. 522-528.