Volume XXII 2019
ISSUE no.1
MBNA Publishing House Constanta 2019

Scientific Bulletin of Naval Academy

Detecting the DDoS attack for SDN Controller

To cite this article: D. Glăvan, C. Răcuciu, R. Moinescu and N. F. Antonie, Scientific Bulletin of Naval Academy, Vol. XXII 2019, pg. 144-150.

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-19-I1-019

Detecting the DDoS attack for SDN Controller

Dragoș Glăvan, Ciprian Răcuciu, Radu Moinescu, Narcis-Florentin Antonie
Military Technical Academy “Ferdinand I”- Systems Engineering for Defense and Security
dragos.glavan@gmail.com

Abstract: A Software Defined Network (SDN) is an architecture used to form agile and flexible networks. SDN's goal is to improve network control, allowing service providers to respond rapidly to changing requirements. In a SDN, an administrator or a network engineer can configure the traffic from a centralized control console without having to touch individual network switches. Due to the fact that the control plan is entered by SDN as a network manager, a Single of Failure Point (SPoF) is also introduced. If SDN can not be reached by network devices, the network will crash. Distributed Denial of service (DDoS) attack is a way to make SDN Controller inaccessible. In this paper are presented the potential vulnerabilities of SDN Controller that can be exploited for DDoS attack as well as the presence of methods of detection and attenuation of these attacks.

1.INTRODUCTION

Software Defined network is a new network management model that decouples the command plan and data plan, the control plan being often called the SDN Controller. The global behavior of the network is dictated / directed by SDN Controller. This separation has simplified the network management since the configuration and management are only applied to the Controller. Then, the Controller has the responsibility to apply the change to the whole networks. As far as network security is concerned, SDN introduces a Single Point of Failure (SPoF). Network performance depends on the controller, which is the main brain of the network. The DDoS attack is one of the methods by which the SDN Controller can be attached and through which resources could be overwhelmed (for example, SYN Flood and ICMP Flood).

Organizing a DDoS attack costs only 7$ per hour, while target companies may lose thousands or even millions of dollars. The cost varies depending on the type / importance of the victim, for state or multinational resource-funded sites, the solutions to combat this type of attack are very costly, you need a very good solution given the importance of the information provided on the site.

Usually, the DDoS attack involves sending a large number of packets at a given time. These malicious packages have the same port and destination address and have a typical dimension different from the legitimate package size. These features have been studied in numerous papers that propose methods to detect and attenuate the DDoS attack, but the attack time is rarely used.

The purpose of this paper is to develop a method of detecting and mitigating DDoS attacks for SDN Controller, in the first part there are the vulnerabilities that can be exploited by such an attack.

2.SDN OPERATION

This chapter will present the SDN operation and the vulnerabilities that can be exploited by DDoS attacks on the SDN Controller. It also analyzes the DDoS attack characteristics to formulate the solution for detecting and attenuating DDoS attacks.

2.1 SDN Operation

In current SDN, the OPenFLow protocol is widely used, it is responsible for secure channel communication between the OPenFlow Switch and the OpenFlow Controller. OpenFlow Controller manages a flow table that contains match field and instruction regarding the flow. OpenFlow Switch manages its own flow table that given by the OpenFlow Controller.

Basic SDN operation is to transfer traffic for a packet in the network. The illustration of basic SDN operation is illustrated in figure 1. Every time a new packet is coming, it will look the match information in its flow tables. If a match is found, the packet will be directly forwarded according the instruction that are in the table. If a match is not found, the packet will be sent to the Controller. Controller then looks up a match in its flow tables. If a match is found, the Controller will decide a new rule for the packet based on instruction field on its flow table. Otherwise, the packet will be dropped. The new rule is then applied to the flow tables in the network devices so the network device will know how to do to the similar packet.

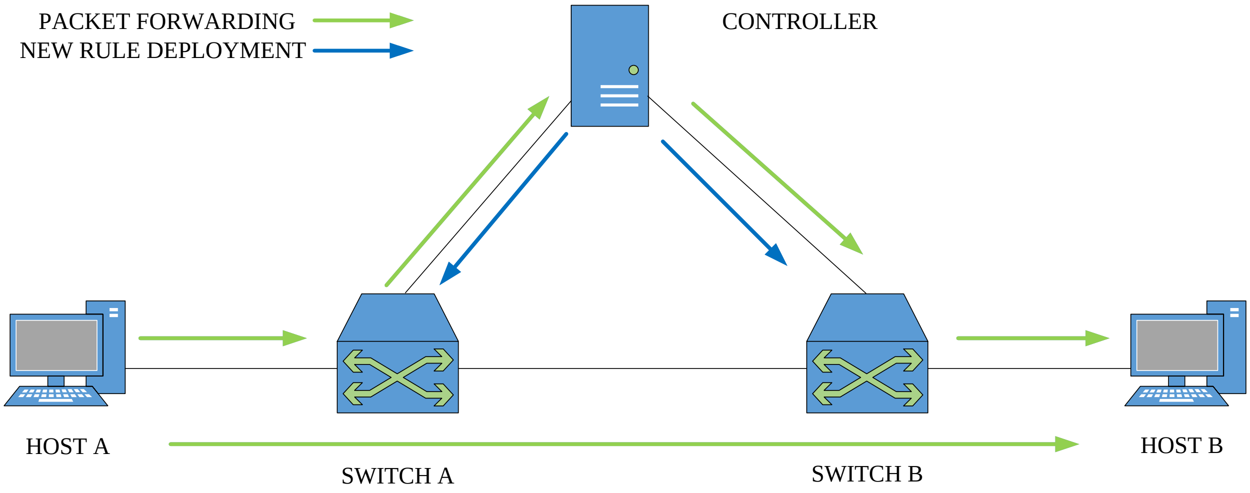

Figure 1 Basic SDN Operations

2.2 Vulnerability of SDN Controller

Communication to the Controller is done through a secure line. This secure line make the effort to take full control of the Controller is quite difficult. However, regarding basic SDN operation, an attacker can exploit the new packet mechanism to make the Controller unreachable. Due to memory size, flow table size in Controller and Network Devices is limited. Attackers send a huge number of packets that have spoofed addresses. Since the addresses are unknown, the packet will be forwarded to the Controller. If the arrival rate of packets reaching the Controller is high, the Controller will have all its resources bound into processing the malicious packets. A high rate malicious packet can completely overwhelm the Controller and make it unreachable to the legitimate traffic. This can cause the collapse of SDN architecture of the network.

Also, one very important thing is that this type of attack takes time to get a malicious package. Sometimes, DDoS attackers use a periodic attack that occurred at some point in time. This method can be used in the detection method to rise the detection time before attackers reach their target.

2.3 Related Work

Many researches have conducted in this field. Muhammad Nugraha uses a statistical method to detect DDoS attack based on the number of packet characteristic. The proposed method uses sFlow to collect the flow and apply the threshold to define the DDoS packet. However, this method only considers the number of the attack packets. The time characteristic of DDoS attack is not counted on the proposed method. Dokyeong Lee introduced centralized monitoring using Snort to detect DDoS mitigation. However, time was not considered in the proposed method and Controller was not the victim of DDoS Attack.

Rodrigo Braga presents a lightweight method for DDoS attack detection. The proposed method in this paper extract feature of interest with low overhead compared to traditional approaches. This method utilizes the SDN Controller which provides a programmable interface to facilitate the handling of switch information. However, this paper did not mention the effect of DDoS attack on SDN Controller. Nguyen Tri in his paper presents the impact of DDoS attack on SDN Controller. This paper also presents how to manage the limitation of the flow table. But the method on detecting and mitigate of DDoS attack is not the domain of this proposed solution. Sayed Mohammad Mousavi presents the detection method of DDoS using entropy method. The method in this paper monitors the IP destination of the incoming packets to SDN Controller. When the packet IP destination is directed toward particular hosts, the entropy value will decrease into certain value. If the value passes the threshold value, the DDoS attack will be detected. This method also did not consider the time characteristic of DDoS attack.

3. SOLUTION DESIGN

This chapter describes the design of the proposed solution for detecting and attenuating the DDoS attack. Also, the parameters used to evaluate the performance of the method used will be explained.

3.1 DDoS Attack Scenarios

DDoS attack scenario is illustrated in figure 2. In this experiment four switches are used, a switch is connected to the Controller to make a secure connection, and the other three switches have their own network containing the number of hosts. Some host of the network members become the agent for DDoS attack. The agent host then is used to generate malicious packets to attack flow table resource on each switch and finally, attacks flow table in the Controller.

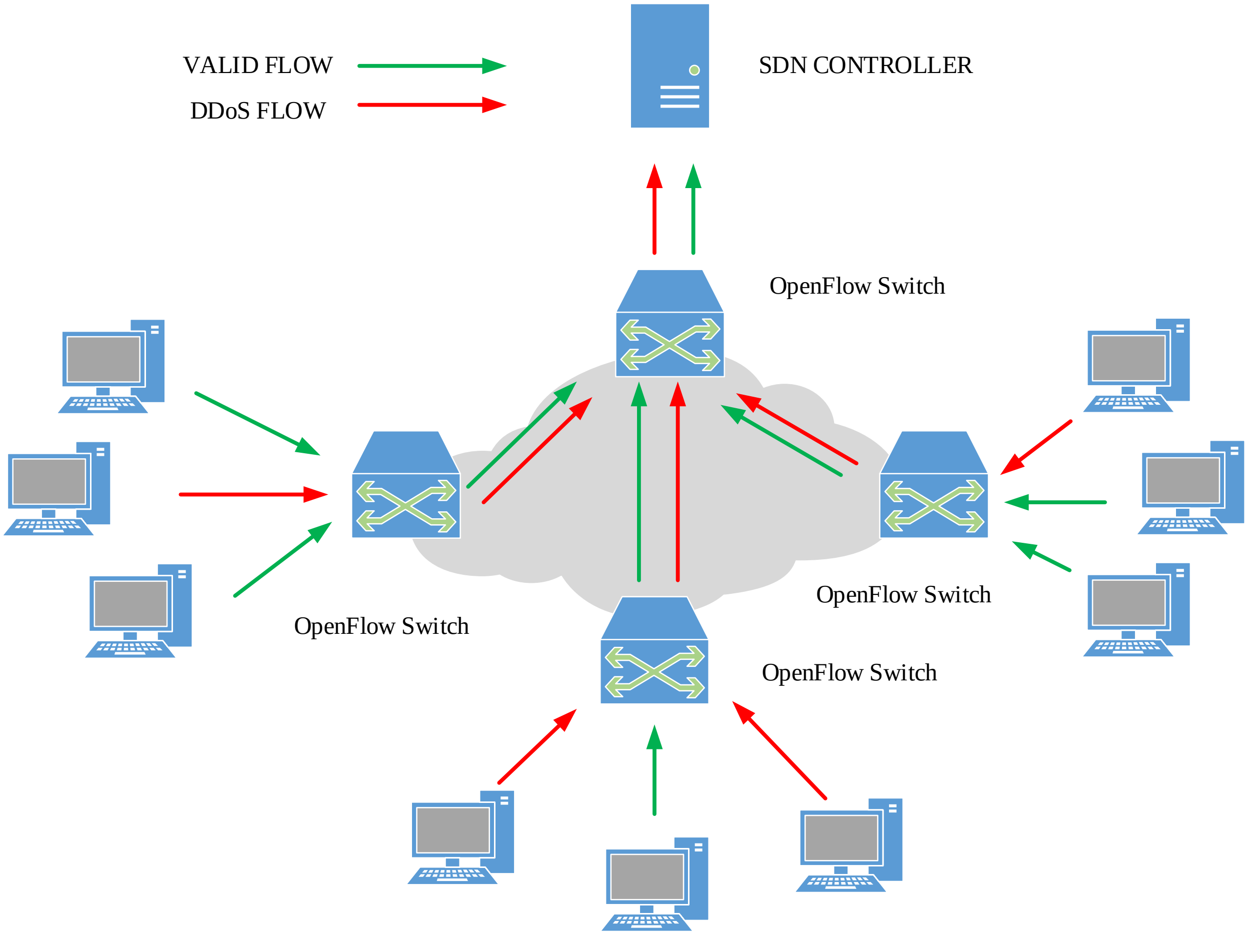

Figure 2 DDoS Attack Scenario

3.2 The Proposed DDoS Detect Method

The main purpose of this method is to detect and mitigate DDoS attacks on the SDN Controller. This method takes into account the destination address and the time it takes to achieve a high-rate traffic and time attack pattern. To detect DDoS attacks, time duration is used, and to prevent future attacks using a time attack pattern. For the destination address parameter, we use assumption that every packet coming to the Controller is a new packet. Every new packet will be check for a valid destination address. If the destination address is not valid or unknown in the network, the Controller will forward the packet to the flow collector. A flow collector is a new module that we implement in SDN Controller to store the non-valid packet for further inspection. A flow collector applies statistic method to analyze the non-valid packet that sent by the Controller.

Figure 3 illustrates our DDoS detection scenario. When the accumulation of non-valid packet is increasing significantly within a certain time, flow collector will send a notification to the Controller. The Controller then applies new rule for every network device to forward the non-valid packet directly to the flow collector. The flow collector is then applied further processing to the clustering time pattern of DDoS. This pattern then will be used to prevent the next DDoS attack. If P_{nv} is assumed to be the number of invalid packets entering the control stream, R is the invalid packet size on the time window, t represents the time window, then the proposed method can be formulated as follows:

$$R = \lim_{\Delta t \to 0} \frac{\Delta Pnv}{\Delta t} \tag{1}$$

From the experiment, we will define the best T (threshold) value so when R value exceeds the T, the flow Controller will send DDoS notification to the Controller for further processing.

3.3 Evaluation Design

This scenario will be implemented using a virtual machine that runs Ubuntu. Mininet is used to emulate the topology of SDN network and OpenDayLight as the Controller. If the proposed method is to be evaluated, the system resources used (CPU, the number of flow entries) in the OpenFlow Switch and SDN Controller. We will use system monitoring tools in Linux to measure the system resource usage.

In order to evaluate the detection performance, Alarm rate (FA) and Detection Rate measurement (DR) are used and are calculated as follows:

$$DR = \frac{TP}{TP+FN} \tag{2}$$

$$FA = \frac{FP}{TN+FP} \tag{3}$$

Where:

- TP = True Positive, attack flow classified as attack;
- FN = False Negative, attack flow classified as legitimate;
- FP = False Positive, legitimate flow classified as attack;
- TN = True Negative, legitimate traffic classified as legitimate.

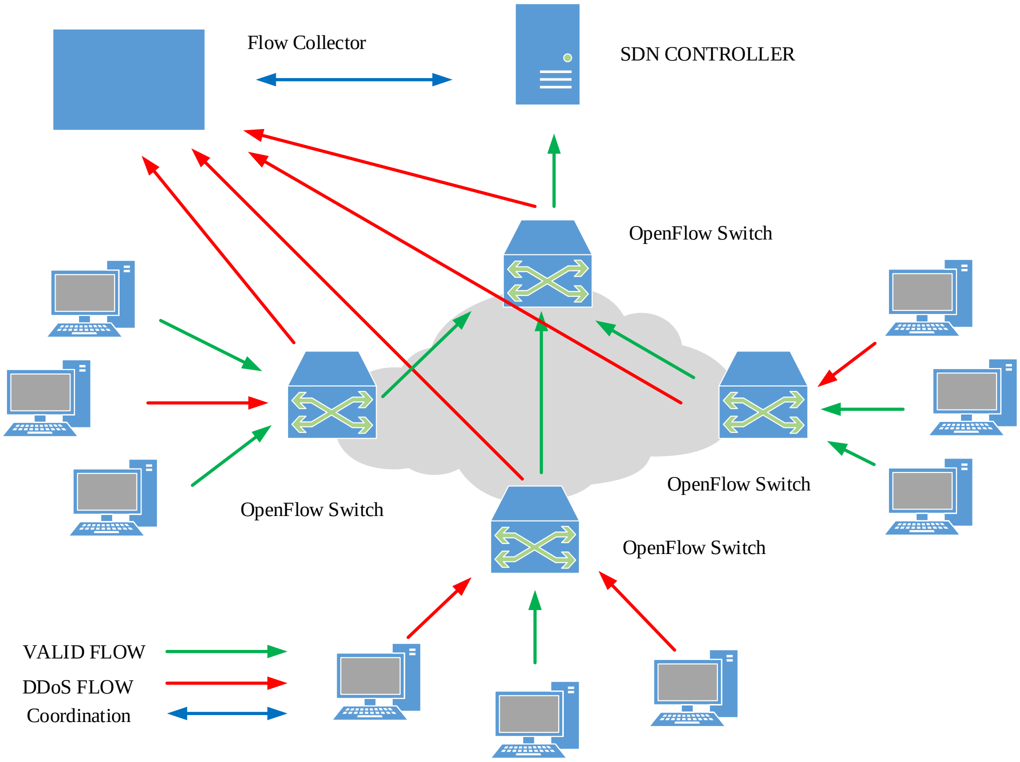

Figure 3 Proposed DDoS Detect Method Scenario

4. CONCLUSION

The most serious threats to big companies are DDoS attacks. The frequency of these attacks makes all types of businesses vulnerable because they exceed the capabilities of traditional protection methods. Attacks on sites and government resources protected by anti-DDoS solutions are more expensive because they are at high risk and more difficult to attack. On a site that offers DDoS services, the cost of such an attack on a site without protection varies between $ 50-100 and in the case of a protected site, the cost of the attack is about $ 400.

In this paper, we analyzed the vulnerabilities of SDN Controller that can be exploited by a DDoS attack. This method does not only consider the malicious package to detect the DDoS attack, also consider the DDoS attack time feature.

The scenario of the experiment was described and how the performance assessment of the proposed method is being assessed.

5.REFERENCES

[1] M. Nugraha, I. Paramita, A. Musa, D. Choi, and B. Cho, *Utilizing OpenFlow and sFlow to Detect and Mitigate SYN Flooding Attack TT*, Aug. 2014.

[2] H. T. N. Tri and K. Kim, *Resource Attack Based On Flow Table Limitation in SDN*, 2012.

[3] S. M. Mousavi and M. St-hilaire, *Early Detection of DDoS Attacks against SDN Controllers*, 2015.

[4] G. Y. Bang, D. K. Lee, and D. Choi, *A Protection Method on SDN using sFlow and Snort for SYN Flooding Attack*, 2014.

[5] J. J. M. Dover, *A denial of service attack against the Open Floodlight SDN Controller*, December 2013.