CHAPTER 1: INTRODUCTION

This chapter discuss about the underlying background of the research, followed with overview of SDN and then hypothesis on how to improve the method on the previous paper.

1.1. Problem Backgroud

In this section, a basic understanding of how OpenFlow works and what its shortages are needed before we explain how OpenFlow can be utilized in DDoS mitigation. With OpenFlow, the control plane of the switch is implemented in a separate machine, the OpenFlow controller. The controller and switch communicate via the OpenFlow protocol. The controller can install flows on the switch and the switch forwards traffic according to these flows [1]. This research will explore the utilization of OpenFlow in the detection and mitigation of network level attacks.

There are many Denial of Service attack methods being used to degrade the performance or availability of targeted services on the internet. Usually, these methods can be classified as network level attack or application level attacks. Network level attacks generally produce large volumes of network traffic that are detectable by their packet rate or bandwidth rate. The examples for this type of attack are amplification and flood attacks. Application level attacks misuse software in a malicious way, aiming to exhaust resources to process any further requests. These attacks are generally harder to detect on the network level as they show no clear deviation from legitimate traffic [1]. Common examples here are expensive search queries and exhaustion of connection pools. An OpenFlow rule match against properties in link, network and transport layers of the TCP/IP model and is therefore not suited to detect application level attacks with characteristics present in higher layers.

A number of methods have been researched in the field of detecting malicious activity using OpenFlow. These methods vary from the detection of infected hosts on the local network by comparing flows to deterministic sampling using OpenFlow to inspect certain traffic classes. [1]

One of the DDoS detection methods in SDN that has been researched is on the previous paper. This previous method using statistical approach by comparing the threshold from size of traffic subtracted by mean off traffic and the three of the standard deviation, and if

the threshold is higher than the three of the standard deviation, the traffic will be detected as DDoS attack. But as the researcher told that the thresholds that used in the previous research are mostly based on simulations that may not be well suited for real world scenarios. [1]

Because the previous method just using threshold deviation from 60 pool of packet flow from switches, so when there is a sudden increase of traffic it will be detected as an DDoS.

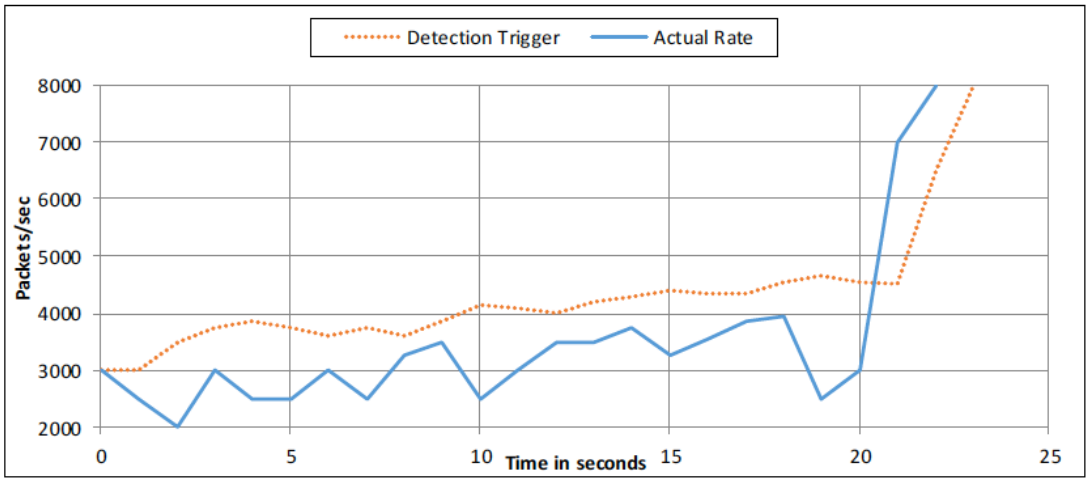

Figure 1 The DDoS detection in the existing method [1]

In real world, the traffic can suddenly increase because of normal usage. It can be happened when there are some activities like send or receive big files between hosts. The traffic can be seen in Figure 3. This case will increase the false positives as normal traffic will have detected as DDoS attack. This is the shortage of the previous method.

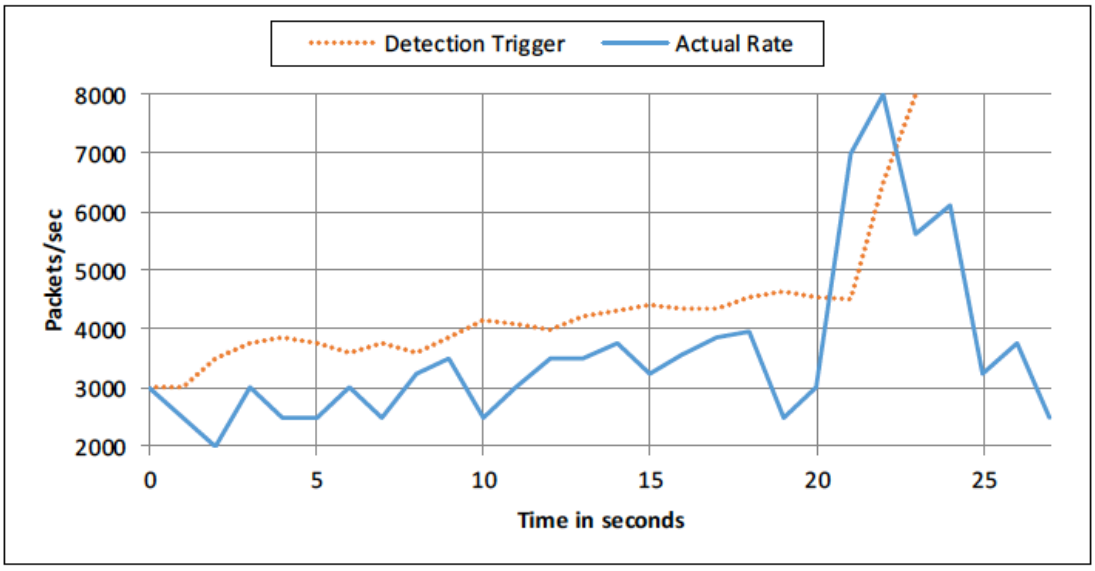

Figure 2 The real traffic on minute 20th - 25th, detected as a DDoS [1]

1.2. Problem Statement

The previous method only detects a DDoS attack by comparing traffic subscribed by mean compare with three of the standard deviation in 60 sliding windows, so when there is a sudden increase traffic will be detected as an attack although it is just a sudden increase in normal traffic. When normal traffic is detected as DDoS attack then false positive will be increased.

1.3. Hypothesis

Ryu controller is one of the SDN OpenFlow controller based on python language. In this experiment we will use this type of controller by programming it by using the existing method and then add new mechanism by detecting its randomness to detect DDoS attack in SDN.

The previous DDoS detection in SDN only uses three of standard deviation threshold mechanism from 60 pool of packet flow from switches, which if there is a sudden increase of traffic then it will be detected as a DDoS attack although actually it is normal traffic. To improve the detection, we propose the modification of the previous method by checking the randomness of the traffic after detected as a DDoS attack.

Entropy is one of statistical method that used to measure randomness. Shannon identified the concept of entropy in 1948. Entropy is a quantity, a measure of the uncertainty of a random variable. Let an information source have n independent symbols each with probability of choice p_i. Then, the entropy H can be calculated using the equation 1 [2]:

$$H = -\sum_{i=1}^{n} p_i log_2 p_i \quad (1)$$

The function of the basic properties of entropy is defined as a concave function of the distribution. The entropy value equals 0 when p = 0 or 1. Similarly, the entropy is maximum when p= 1/2. This property easily can be used in network traffic monitoring. If network traffic changes from normal to abnormal status such as when the DDoS attacker sends a bulk of packets with the same port number to saturate a certain port, the entropy of this port number will be decreased. By contrast, under normal conditions, the entropy of the port number will be increased. This phenomenon can be applied to various network information such as source IP address, destination IP address, source port, destination port, total number of packets, and even in the data clustering schemes [2].

Asvani Kumar in his dissertation analyzed the network traffic of selected five days from the DARPA data-set and plotted the time series [3]. He tuned and filtered The DARPA data-set to test the DDoS attacks detection schemes. The calculated result are seen on Table 1.

Table 1 DARPA calculation from Asvani Kumar [3]

Data-set	Packet Rate	Packet size Entropy	eSD
DARPA/MIT	871	0.7003755	0.6230978

In this research, we will use the packet size entropy threshold from DARPA data-sheet provided by Asvani Kumar above in our experiment.

Another reason why we consider to combine between previous method and entropy for the new method is because if we only use entropy for bandwitdh attack then some normal traffic such as video or audio streaming that has tendency as a flat size traffic will be detected as DDoS attack although just a low traffic. The flat traffic has low randomness than normal traffic, so the entropy is also lower than the normal one.

1.4. Objectivities

The objectives of this research are:

a. To improve the detection accuracy of DDoS attack in SDN network
b. To Reduce false positive from existing the method on the previous paper.

1.5. Scope and Delimitation

In this research, we use assumption that algorithm complexity time course is not counted and only for simple scale network testing.

The following are the scope and delimitation used in this thesis:

a. The mininet simulator is used to test and design the network
b. The victim's PC have selected.
c. The type of attack used is Bandwidth or traffic attack

1.6. Importance of the Study

This thesis makes contributions which we believe that the use of SDN for security research community would benefit from such as :

a. To learn the SDN ability to detect DDoS attack by utilizing its controller.
b. To propose an improved method to differentiate legitimate traffic from attack traffic.

1.7. Thesis Organization

This thesis is divided into 6 chapters: the problem, review of literatures and studies, research methodology, experimental design, analysis of the simulation result and conclusion and recommendation.

The first chapter describes introduction, problem background, problem statement, hypothesis, objectives, scopes and delimitation, important of the study, thesis organization and summary of the chapter.

Chapter 2 explain the review of literatures and studies. The studies about SDN and DDoS attack is discussed with some DDoS detection method that already exist today.

Chapter 3 provides of research methodology of the steps which make up the new method while chapter 4 discuss the experimental design on how we design the experiment.

Chapter 5 describes analysis of the simulation results. In this chapter, a model based and simulation on the new method which were run to assess the accuracy of the new method will be analysis.

Finally, chapter 6 discuss conclusion of this research and offers recommendations for improvements to this work.

1.8. Summary

The previous method just uses three of standard deviation threshold mechanism from 60 pool of packet flow from switches, which if there is a sudden increase of traffic then it will be detected as a DDoS attack although actually it is normal traffic. To improve the detection, we propose the modification of the previous method by checking the randomness of the traffic after detected as a DDoS attack.

One of statistical method that used to measure randomness is entropy. Shannon identified the concept of entropy in 1948. Entropy is a quantity, a measure of the uncertainty of a random variable. In this research to improve the previous method, entropy mechanism is added to the previous method to detect the randomness of traffic.