CHAPTER ONE

INTRODUCTION

1.1 Research Background

Distributed Denial of Service (DDoS) attack has been a real threat to the network and cyber infrastructure. DDoS attacks are capable to cause huge damage in any information communication technology (ICT) infrastructure. There could be many reasons for launching DDoS attacks. These reasons may include networks disruption and financial earning (Paroutis et al., 2014).

DDoS attacks can cripple networks and services by overloading servers, networks links, and network devices such as routers and switches with illegitimate packets. These attacks can cause huge losses by either degrading the service or complete denial of service. The growing dependence of the ICT infrastructure has given a rise in the need for efficient solutions for protection against DDoS attacks (Bawany et al., 2017).

Although existing DDoS attack detection and mitigation solutions are numerous and varied, DDoS attacks continue to grow in sophistication and intensity (Yadav et al., 2016). Fast detection and mitigation of DDoS attacks have become severely challenging as attackers continue to use new methods to launch DDoS attacks (Hoque et al., 2015). The rising number of DDoS attacks has made the DDoS attack detection and mitigation the topmost priority.

The goal of Software Defined Networking (SDN) is to make the network more agile. SDN is an approach that allows network administrators to programmatically change, control and manage the behavior of the network dynamically via open interfaces, and to quickly respond to the changing of business requirements via a centralized control console. Disassociating the control plane (intelligence of the network) from the data plane where the forwarding devices such as switches are, come to achieve the goal of SDN (Nunes et al., 2014).

The rapid and recent advancements in SDN have grabbed a wide acceptance in the network community where many researchers have involved in developing the security solutions that are based on SDN network. Centralization of the SDN intelligence enables developers to directly program, manage and control the network resources. SDN-based solutions have attracted more attention since they are deployed in wide area networks (Jain et al., 2013).

1.2 Problem Statement

Detection of Distributed Denial of Service (DDoS) attacks has become one of the main Internet security challenges today. The difficulty that is faced by the DDoS attack detection system comes from two issues. First, is how to distinguish between normal packets and attack packets. Second, is how to detect different attack categories accurately and at a low cost of resources. Therefore, the detection solution must be an efficient and less complex detection solution that has low false alarms (Saboor & Aslam, 2015)

To detect such an attack, payload-based methods or flow-based methods are used. Sperotto et al. (2010) found that network overhead is maximized when

payload-based detection systems operate in the network; therefore, flow-based detection is used to minimize it. According to Alaidaros et al. (2011), payload-based methods maximize network overhead due to inspecting the content of each packet. Also, payload-based methods on deep packets have reached their limits. For that, flow-based detection methods used to minimize overhead due to having an overall lower amount of data to be processed which makes the ability to detect such an attack in a short time much easier (Vykopal, 2013).

Although flow-based methods used to decrease overhead, high overhead when these methods operate is still noticeable. Along with the performance issue (high overhead), another issue related to the performance (high false alarms rate) has appeared. There are two reasons for these two performance issues to appear. Firstly, the complexity of techniques used to detect DDoS attacks (Bawany et al., 2017; XU et al., 2017) and secondly, the parameters used by these techniques to detect DDoS attacks (Cvitić et al., 2017).

The SDN paradigm facilitates the detection of the DDoS attack due to decoupling the control plane from the data plane in its structure. This decoupling allows the systems developers to have an overview of all forwarding devices from one controller and to take immediate actions against suspicious activities in the network. Although the major advantage of SDN is the central control, it is also a failure point if it is made unreachable by a DDoS attack (Yan et al., 2016). Thus, protecting the controller in SDN from being overwhelmed by DDoS attack packets is the protection of the entire network.

Several flow-based methods for detecting DDoS attacks in SDN have been proposed but we can infer that there is lack of efficient and less complex flow-based DDoS detecting solutions that have low false alarms (Saboor & Aslam, 2015).

The related surveys of the previous researches had classified generally the DDoS detection methods in SDN into two main classifications in terms of techniques they use to detect the attack (Bawany et al., 2017; XU et al., 2017). These techniques are entropy and machine learning.

Although entropy and machine learning techniques have been widely used to detect DDoS attack, they have suffered from some limitations. Methods that use entropy suffer from losing the relevant information about the distribution of the analyzed feature because of the probability distribution of this feature is represented by a single value when entropy is calculated. This leads to masking of the anomaly in some cases, which may affect the accuracy as well as increasing the false alarms (False Positives). Also, the entropy-based methods need to combine with other technologies to make threshold determination and multi-element weight assignment. Thus, the increase in resource usage using this technique is still noticeable. The limitations that detection machine learning-based techniques are suffering from are that it requires a large number of training sets and need to spend long time training. Thus, the machine learning-based techniques are consuming lots of controller's resource (i.e. CPU and memory) which eventually lead to an increase in the controller's overhead. Moreover, the performance of these techniques is typically dependent upon the dataset that has been used for training (Bawany et al., 2017; XU et al., 2017).

Based on the literature in DDoS attack detection techniques, the arrival time of the packets is not used as a key parameter in detecting DDoS attacks. According to Noble and Sujitha (2015), the current methods do not consider the arrival time of packets as a relevant object to find DDoS attacks. Selection of parameters to be used is a key component for achieving an effective system of DDoS attacks detection (Cvitić et al., 2017). According to (Bhattacharyya & Kalita, 2016), number of used parameters must be as low as possible and it is necessary to use parameters that have the greatest impact when detecting network traffic anomaly.

Although authors have proposed many DDoS defense solutions to detect DDoS attacks, the solutions are failed to exist a defense solution that can detect the DDoS attacks that changing from high volume to low volume at the time of the attack. Furthermore, the low-rate attacks are difficult to detect (Behal & Kumar, 2016). Despite many solutions provided in the literature, it clearly appears that few works have considered the low-rate DDoS attacks detection in SDN (Sahoo et al., 2018).

What can be observed from the previous works conducted in the domain of detecting DDoS attacks in SDN is that the techniques used for detecting the DDoS attacks either entropy or machine learning techniques suffer from performance degradation in terms of high false alarms rates and high measured overhead. Also, we can observe that the performance of these techniques is almost the same because the parameters used by these different techniques to detect DDoS attacks in SDN are almost the same parameters. Another observation is that the existing solutions have not designed to detect the change in volume of the attack packets as the DDoS attackers move from high volume to low volume and vice versa during the time of

the attack. Further, we observe that there is a severe lack of solutions that consider detecting the low-rate DDoS attacks in SDN.

As a conclusion, there is a need to find a comprehensive, efficient and less complex DDoS detection solution that has low false alarms. In other words, the solution should simplify the complexity existed in the current techniques and use new parameters to enhance the performance. Minimizing the math computations and selecting effective parameters will positively increase detection accuracy and decrease controller resources usage as well as decreasing false alarms rate. Thus, providing a solution can detect and mitigate different DDoS types that attack at the same time using different attacking strategies with performance enhancement, is extremely required.

1.3 Research Objectives

1- To analyze parameters used by the existing solutions for detecting DDoS attacks in SDN.

2- To design the scheme to detect and mitigate Low-rate DDoS attacks, flooding DDoS attacks and DDoS attacks that changing from high volume to low volume in SDN.

3- To evaluate the performance of the proposed scheme in defending different DDoS attacks in SDN environment.

1.4 Significance of Research

The SDN paradigm simplifies the traditional network in two important ways: first, the network no longer consists of disparate elements running proprietary protocols

but instead comprises uniform switching hardware with standard functionality and interfaces and communicating using a single open protocol. Second, network control is no longer purely distributed over several elements but restricted to the controller (Guha et al., 2013).

In threat detection, the SDN paradigm offers a new level of visibility into the network which is ideally suited for traffic monitoring applications. The controller can program forwarding devices in the network to conduct fine-grained flow inspection on traffic passing through the devices. Statistics that periodically collected by the controller, afford a centralized real-time view of network state which is exposed via open Application Programming Interfaces (APIs) and allowing for automation (Ali et al., 2015).

Researchers have started focusing their work for a resolution of DDoS attacks as one of the biggest security challenges in SDN environment. In this context, the researchers have proposed several types of solutions that meant to detect DDoS using different techniques such as machine learning and entropy techniques. Obviously, many of the proposed solutions to detect DDoS attack using these different techniques have achieved a remarkable accuracy but the accuracy achieved in the available solutions has either increased the controller's overhead, false alarms or both of them at the same time. Further, the available solutions have not detected the attack packets that change from a large number to a small number of packets as well as the low rate DDoS attacks. Thus, there is a need to find a new solution that can detect the high rate and low-rate DDoS attacks with enhanced performance.

This need is the starting point of this study, which looks at the different parameters used to detect the DDoS attack and shows the effect of using the new

parameter (elapsed time between the successive attack packets) to detect DDoS attacks on performance.

In terms of accuracy, the scheme applied in this research proves the ability not to produce any false alarms (false positives) while it is mainly based on a concise list of what we believe that they are the most important statistical information obtained from both of OpenFlow switch and controller. This statistical information is the number of packets, number of flows, arrival times of packets and, destination IP address. The value in the new parameter elapsed time between the successive packets (calculated by subtracting the arrival times of the successive packets that are considered as suspicious packets) will give the time distance between the successive packets that try to reach the same destination as a clear indication of a DDoS occurrence. The scheme checks the number of packets in packets counter every five seconds to detect the sudden increase in network traffic. The scheme begins calculating the elapsed seconds between the successive packets once the number of packets exceeds the threshold. The scheme proves 99.27%, 99.47% and 99.85% of accuracy in distinguishing the attack packets from the normal packets in UDP flood, low-rate SYN, and mixture traffic scenarios respectively.

Moreover, this scheme monitors the network flows when the number of packets is below the threshold to detect the change in volumes of DDoS attack packets or the low rate DDoS attack attempts during the time of the attack. Also, giving a very short period of time (only five seconds) to the DDoS attack detection function to work, the scheme will detect the DDoS attack in its early stages.

In terms of CPU usage, the scheme applied in this research produces the lowest overhead measured in the network when it operates under different DDoS

attacks. The percentage of overhead measured when the network is under UDP flood DDoS attack is only 34.3%, low-rate SYN DDoS attack is only 2.5% and only 29.9% when the traffic is mixture traffic. This means decreasing the network resource usage to the lowest level compared to the available machine learning and entropy techniques based solutions.

From all the above, we demonstrated that applying the proposed scheme on the SDN POX controller will give the controller the ability to detect and mitigate the attack packets and flows in a short time. This will reflect positively on the controller resource usage and will give promising accuracy. Along with enhancing the performance, this scheme coming with, ability to detect both the attacks that change from the high volume to the low volume and the low-rate DDoS attacks. Additionally, removing the flows that contain the attack packets at the time of the attack will result in saving the memory of the switch for the new incoming packets. Besides, the correctness of differentiating the attacks packets from the legitimate packets has been shown by the scheme by lowering the false alarms produced at the time of traffic generation.

1.5 Research Scope

This research focuses on detecting DDoS attack at the SDN controller side. Since this research focuses on network flows, we do not consider the following:

1- Payload-based detection.

2- Host-based detection.

3- All SDN-based DDoS detection techniques except (machine learning and entropy).

4- All performance metrics except (CPU usage, accuracy and false alarms).

In the Figure 1.1, an illustration is provided to locate our work in the field of study. The red line in the illustration to indicates the scope of our work.

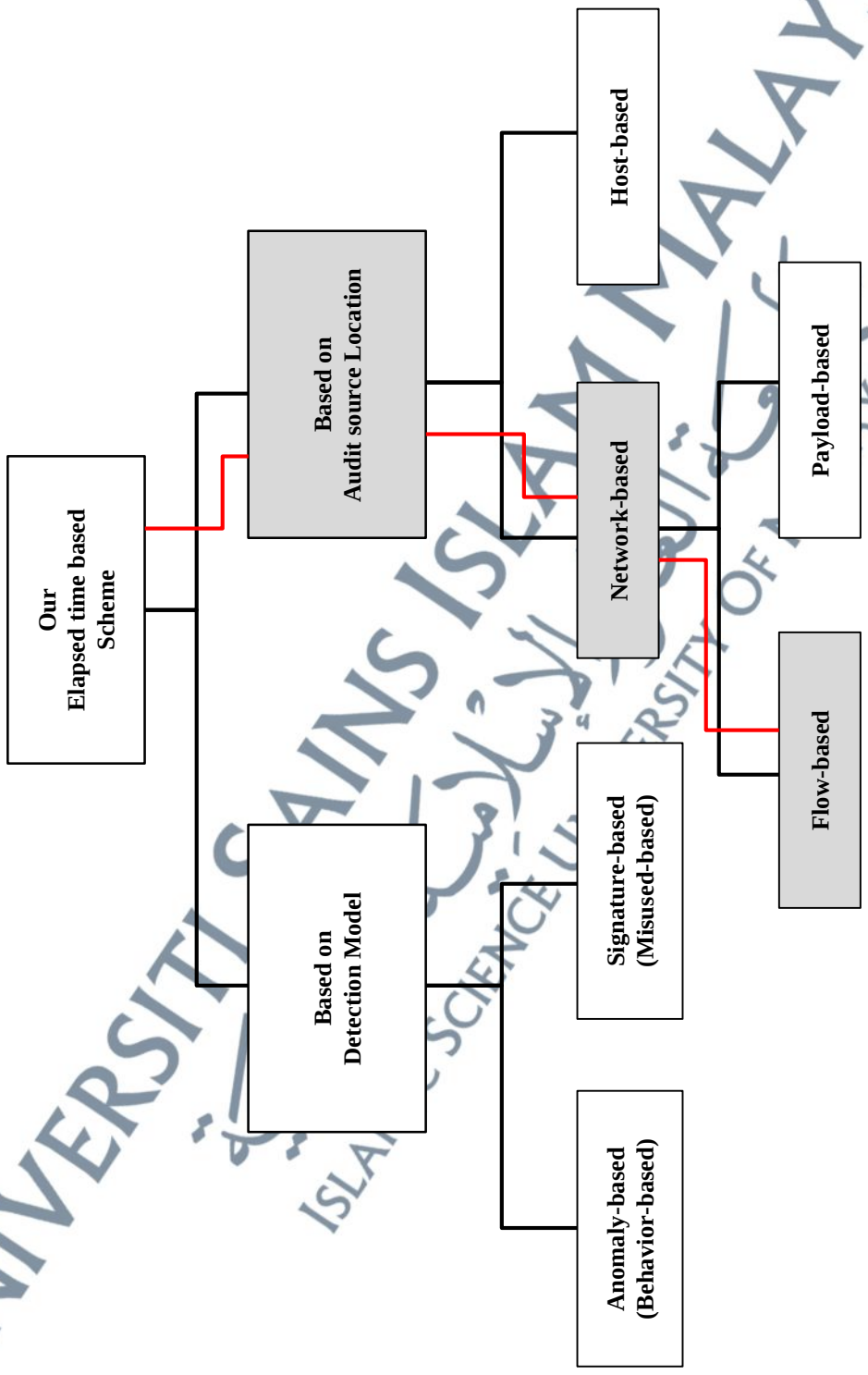

Figure 1.1: Research Scope

1.6 Organization of the Thesis

The thesis is organized into five chapters. The first chapter presents the research background, problem statement, research objectives, significance of research and scope of research.

The second chapter provides an explanatory explanation about DDoS and its most used types, SDN and its components, benefits of SDN and DDoS attacks in SDN. The gaps in the literature, pros and cons of previous works and the motivation behind the proposed and designed scheme are discussed.

The third chapter explains the requirements and tools utilized in this research. The research methodology was discussed in chapter three. Firstly, it introduced the performance evaluation techniques. Then, details of the selected network simulator were presented. Moreover, chapter three discussed the simulation experiments design, experiments hardware and software, validation and verification, and the network performance evaluation metrics.

Chapter four introduced a new scheme for detecting DDoS attacks based on the elapsed time between the successive attack packets and mitigating them based on changing the values of the Idle-timeout and hard-timeout of the flows that contain these packets to terminate these flows at the time of detection. The three phases of the proposed scheme were presented in this chapter. In phase one, we discussed in details how we collect the statistical information from both the SDN controller and the OpenFlow switch. Then, phase two discussed in details how the detection function in the proposed scheme works. Finally, the mitigation function was

explained in phase three. The algorithm of detecting and mitigating DDoS attacks was presented.

Chapter five discussed implementing and evaluating the proposed phases of the scheme in chapter four. This chapter presented three extensive experiments to evaluate the performance of the proposed scheme under different experimental scenarios and different traffic circumstances.

Finally, the sixth chapter concludes the thesis and gives the recommendations for future research.