GENERALIZED ENTROPY-BASED APPROACH WITH A DYNAMIC THRESHOLD TO DETECT DDOS ATTACKS ON SOFTWARE DEFINED NETWORKING CONTROLLER

MOHAMMAD ADNAN AHMAD ALADAILEH

UNIVERSITI SAINS MALAYSIA

2021

GENERALIZED ENTROPY-BASED APPROACH WITH A DYNAMIC THRESHOLD TO DETECT DDOS ATTACKS ON SOFTWARE DEFINED NETWORKING CONTROLLER

by

MOHAMMAD ADNAN AHMAD ALADAILEH

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

March 2021

ACKNOWLEDGEMENT

All praise and thanks are due to ALL MIGHTY ALLAH, for giving me the strength, health knowledge and patience to complete my Ph.D.

As the Prophet MOHAMMED "Peace be Upon Him" said:'Whoever does not thank people (for their favours) has not thanked Allah (properly), therefore, I would like to express my sincere gratitude and the deepest thanks to my supervisor Dr. Mohammed F. R Anbar (main supervisor), I will always be deeply in dept for his guidance, help, stimulating suggestions and encouragement which helped me in the research and writing of this thesis. I also would like to express my gratitude to my co-supervisor Ms. Yung-Wey Chong for her help. Most importantly, none of this could have happened without my family. “My Father” Adnan Aladaileh, I really do not have the words to explain how much thankful I am for your assistance to make me who I am now, without you I am literally nothing. “My Mother” who encouraged me and prayed for me throughout the time of my studies. And lastly, thanks to my brothers Firas, Anas, Eng. Qosai and Dr. Hamza. My lovely sisters. I love you all.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

SDN	Software Defined Networking
DDoS	Distributed Denial of Service Attack
API	Application Program Interface
IP	Internet Protocol
AI	Artificial Intelligence
EWMA	Exponentially Weighted Moving Average
GEADDDC	Generalized Entropy-Based Approach with a Dynamic Threshold to Detect DDoS Attacks on Software Defined Networking Controller
EDDSC	Early Detection of DDoS Attacks in Software Defined Networks Controller
SSL	Single Host's Attack Against Controller by Targeting A Single Victim with Low Arracks Traffic Rates
SSH	Single Host's Attack Against Controller by Targeting A Single Victim with High Arracks Traffic Rates
SML	Single Host's Attack Against Controller by Targeting Multiple Victims with Low Arracks Traffic Rates
SMH	Single Host's Attack Against Controller by Targeting Multiple Victims with High Arracks Traffic Rates
MSL	Multiple Hosts' Attack Against Controller by Targeting A Single Victim with Low Arracks Traffic Rates
MSH	Multiple Hosts' Attack Against Controller by Targeting A Single Victim with High Arracks Traffic Rates
MML	Multiple Hosts' Attack Against Controller by Targeting Multiple Victims with Low Arracks Traffic Rates
MMH	Multiple Hosts' Attack Against Controller by Targeting Multiple Victims with High Arracks Traffic Rates
IDS	Intrusion Detection System
GB	Gigabyte
RAM	Random-access memory

Dest	Destination IP
Src	Source IP
Th	Dynamic Threshold for Renyi Joint Entropy
$\boldsymbol{H_{R\alpha}}$	Renyi Entropy
JESS	Joint Entropy based Security Scheme
SPRT	Sequential Probability Ration Test
FADM	Flooding Attack Detection and Mitigation
HMM-R	Hidden Markov Model- Renyi Entropy
$\boldsymbol{H_{RJ\alpha}}$	Renyi Joint Entropy

PENDEKATAN BERASASKAN ENTROPI UMUM DENGAN AMBANG DINAMIK UNTUK MENGESAN SERANGAN DDOS TERHADAP PENGAWAL PERANGKAIAN TENTUAN PERISIAN

ABSTRAK

Proliferasi teknologi telekomunikasi yang meluas dalam dekad terakhir turut menimbulkan banyak ancaman keselamatan yang semakin canggih. *Software-defined Networking* (SDN) adalah suatu seni bina rangkaian baharu yang memisahkan satah kawalan rangkaian daripada satah data yang menawarkan ciri dan fungsi yang lebih baik untuk mengesan dan menangani ancaman keselamatan tersebut. Ciri elastik yang dapat diprogramkan memungkinkan pengurusan rangkaian yang cekap dan memberi kefleksibelan kepada operator rangkaian untuk memantau dan menata rangkaian mereka. Walau bagaimanapun, teknologi baharu ini tidak bebas daripada mempunyai masalah keselamatannya tersendiri. Serangan Nafi Khidmat Teragih (DDoS) adalah salah satu ancaman utama yang sering mensasarkan pengawal SDN dan mengancam keselamatan rangkaian SDN. Oleh kerana pengawal SDN adalah komponen penting dan fokus utama SDN, apa jua masalah yang berlaku pada pengawal boleh menjejaskan bahkan meruntuhkan keseluruhan rangkaian. Oleh itu, terdapat keperluan yang mendesak untuk suatu pendekatan yang berkesan untuk mengesan serangan DDoS dengan kadar ketepatan yang tinggi dan tahap positif palsu yang rendah. Maka, tesis ini mencadangkan satu pendekatan pengesanan serangan DDoS yang cekap yang dikenali sebagai Pendekatan Berasaskan Entropi Umum dengan Ambang Dinamik untuk Mengesan Serangan DDoS Terhadap Pengawal SDN (GEADDDC). GEADDDC umumkan kaedah entropi gandingan Renyi dan menggunakan ambang dinamik untuk mengesan serangan DDoS terhadap pengawal. Pendekatan yang

dicadangkan telah dinilai dengan menggunakan lapan senario simulasi yang merangkumi kombinasi serangan DDoS dengan kadar trafik rendah atau tinggi terhadap pengawal SDN, yang dipacu daripada serangan hos tunggal atau berbilang hos, dan menyasarkan mangsa tunggal atau berbilang dalam rangkaian SDN. Keberkesanan pendekatan GEADDDC telah dibandingkan dengan pendekatan EDDSC, dan keputusan simulasi membuktikan bahawa ia mengatasi pendekatan EDDSC dari segi kadar pengesanan dan kadar positif-palsu. Pendekatan GEADDDC yang dicadangkan mengatasi purata kadar pengesanan pendekatan EDDSC sebanyak 10.62%, 1.78%, 35.81%, 3.36%, 5.72%, 0.88%, 9.49%, dan 0.73% untuk SSL, SSH, SML, SMH, MSL, MSH, MML, MMH, masing-masing. Selain itu, purata kadar positif-palsu GEADDDC telah mengalami penambahbaikan sehingga 90.20%, 76.09%, 92.07%, 71.75%, 90.73%, 75.65%, 94.01%, dan 72.00% untuk SSL, SSH, SML, SMH, MSL, MSH, MML, MMH, masing-masing, berbanding pendekatan EDDSC sedia ada.

GENERALIZED ENTROPY-BASED APPROACH WITH A DYNAMIC THRESHOLD TO DETECT DDOS ATTACKS ON SOFTWARE DEFINED NETWORKING CONTROLLER

ABSTRACT

The wide proliferation of telecommunication technologies in the last decade also gives rise to many sophisticated security threats. Software-Defined Networking (SDN) is a new networking architecture that isolates the network control plane from the data plane that offers better features and functionalities to detect and deal with those security threats. Its programmable elastic feature permits efficient network management and provides network operators with the flexibility to monitor and fine-tune their network. However, the new technology is not free from new security concerns. The Distributed Denial of Service (DDoS) attack is one of the major concerns that mainly targets the SDN controller and threatens the security of the SDN networks. Since the controller is the key and focal component of the SDN, any problem occurring at the controller may degrade or even collapses the entire network. Therefore, there is a dire need for an effective approach to detect low rate DDoS attacks with high accuracy and low false positive rate. Thus, this thesis proposes an efficient DDoS attack detection approach called Generalized Entropy-Based Approach with a Dynamic Threshold to Detect DDoS Attacks on Software-Defined Networking Controller (GEADDDC). GEADDDC generalizes the Renyi Joint Entropy algorithm and uses a dynamic threshold to detect DDoS attacks on the SDN controller. The proposed approach has been evaluated using eight simulation scenarios covering a combination of either low or high rate DDoS attack against the SDN controller, triggered from either a single host attack or multiple host attacks, and targeting either

a single victim or multiple victims in the SDN network. The effectiveness of the GEADDDC approach has been compared with the EDDSC approach, and the results prove that it outperforms the EDDSC approach in terms of the detection rate and the false positive rate. The proposed GEADDDC approach has improved the detection rate average over the EDDSC approach by 10.62%, 1.78%, 35.81%, 3.36%, 5.72%, 0.88%, 9.49%, and 0.73% for SSL, SSH, SML, SMH, MSL, MSH, MML, MMH, respectively. Moreover, the average false positive rates of GEADDDC improved to 90.20%, 76.09%, 92.07%, 71.75%, 90.73%, 75.65%, 94.01%, and 72.00% for SSL, SSH, SML, SMH, MSL, MSH, MML, MMH, respectively, compared to the existing EDDSC approach.

CHAPTER 1

INTRODUCTION

1.1 Overview

The last few decades have witnessed a proliferation and rapid growth of information and communication technology which spurred the astronomical increase of network traffic which added more complexity to the operations to process the massive data (Al-adaileh et al., 2018). Soon, the existing conventional network architecture might not be able to cope with the tremendous amount of network traffic which may lead to security and privacy issues as some packets maybe be lost or dropped in transit. This issue has grabbed the attention of many researchers to give their utmost effort to solve; even to the extent of proposing a new network architecture such as software defined networking (SDN) that was designed to be more secure and flexible, easier to manage and also programmable (He et al., 2017; Scott-Hayward et al., 2016).

SDN architecture emerged in the early 2000s (Feamster et al., 2014) to overcome the drawbacks of conventional networks (Singh & Jha, 2016). Consequently, many organizations and researchers joined the research and development effort that resulted in continuous improvement of the technology in terms of performance, scalability, reliability, security and the ability to deal with an enormous amount of network traffic (Görkemli et al., 2016; Liu et al., 2017 & Shu et al., 2016).

SDN is one of the most innovative communication technologies in recent decades that will eventually take over the role of managing network traffic flows in place of conventional networks. Furthermore, SDN helps data centers to control costs

by increasing the efficiency of managing network traffic. Cisco reported in 2018 that SDN will be partially or fully adapted by a large percentage of data centers globally to manage their network traffic flows in not so distant future (Cisco, 2018) as shown in Figure 1.1 .

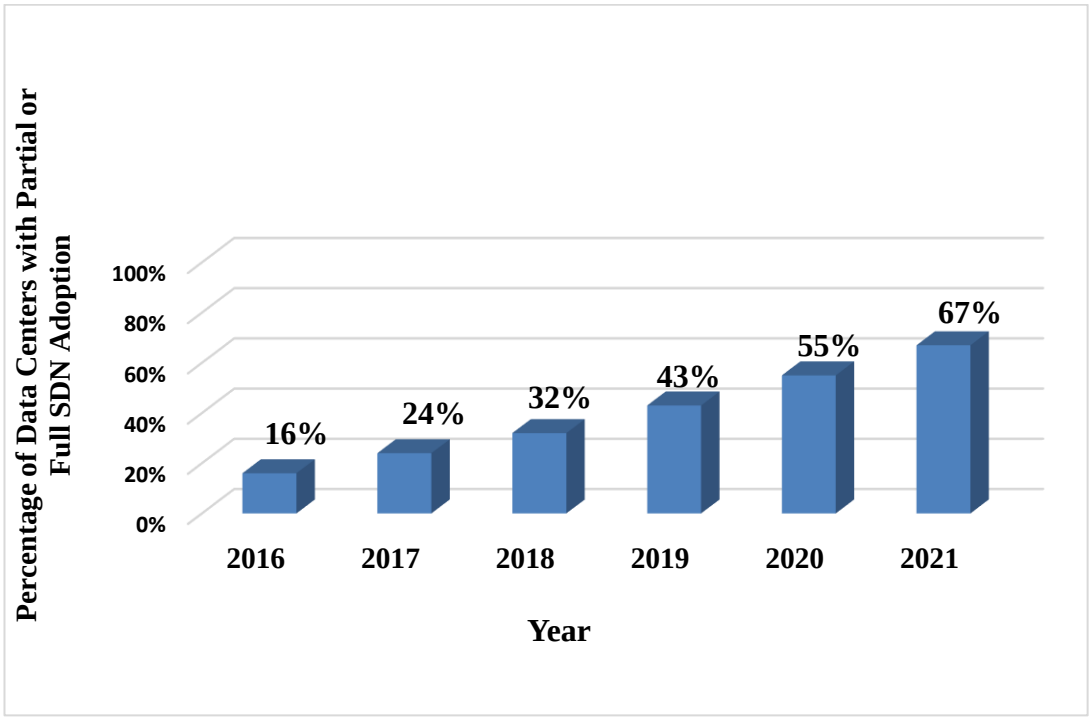

Figure 1.1 Adoption of SDN from 2016 to 2021

Figure 1.1 shows that by 2021, the majority of data centers will be using SDN technology since it makes the management and control of network traffic more efficient, thus less costly. This is a strong indicator of the importance of SDN in information technology and data exchange. Therefore, this serves as the basis for the work in this thesis to focus on making the SDN environment more secure.

1.2 Background

This section elaborates on SDN and SDN controller, followed by the discussion of the main security challenges of SDN.

1.2.1 Software Defined Networking

The SDN achieves complete control of the network properties to meet the requirements of the ever-changing network business need. On the contrary, the current networks (traditional networks) fulfil the network requirements by configuring all actions and control using proprietary vendor-centric hardware which typically involves proprietary software that makes it difficult for administrators to gain full control of the entire network without falling into vendor lock-in situation. Therefore, there are needs to restructure the network to keep up with the latest developments of the network technology such that switches are responsible for forwarding packets and receive instructions instead of using their own resources (service providers) to process new incoming packets.

SDN is a new network architecture that has been introduced to change the approach on managing the network and it provides innovative solutions to conventional network problems. Consequently, there are several factors that differentiate SDN from traditional network. One of the main differences between the two is the concept of separation of control plane from data plane. The separation provides the SDN with the ability to centrally and flexibly manage the entire network using a centralized controller (Xia et al., 2015; Kreutz et al., 2015; Scott-Hayward et al., 2016) (refer to Section 2.2.1).

Since the controller is the most important part of the SDN network, some researchers draw parallel between the SDN controller and the human brain that constantly control and monitor network traffic flow behaviour to ensure the network is functioning properly and smoothly (Görkemli et al., 2016) (refer to Section 2.2.2.). However, the SDN controller has become an attractive target for attackers whose aim is to deny legitimate users from gaining access to network services. A successful attack on SDN controller is extremely dangerous, especially for less prepared network operators, due to the ability of the controller to control the entire network via programming the controller. The network centralization feature of the SDN architecture provides anyone with access to the servers that host the control software to potentially gain control the entire network (Kreutz et al., 2013). Figure 1.2 shows an overview of the three layers in SDN architecture (Zhang et al., 2018).

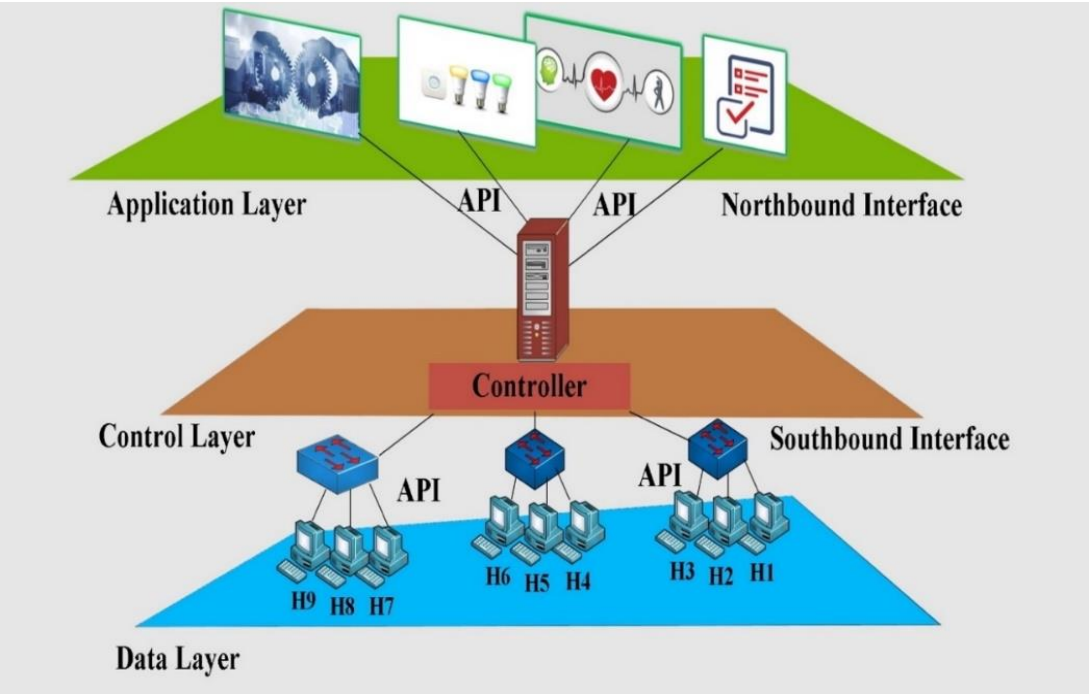

Figure 1.2 SDN Architecture

As shown in Figure 1.2, SDN consists of three layers: the data, control and application layers. The data layer is responsibles to handle all new incoming packets by forwarding them to their respective destination according to the rule in the flow table, or if there are no matching rules, they will be forwarded to the controller via a secure channel (Kreutz et al., 2015). The control layer is responsible to manage the entire network through a logically centralized controller by constantly analysing the network traffic flows that arrived from the data layer. The controller will create a flow instruction that matches the new traffic behavior to prevent disruption in the network processes and then install flow entries in the flow table (infrastructure layer) (Khan et al., 2016; Salman et al., 2016). The application layer consists of programs that have specific task to communicate behaviours and needed resources with the SDN controller through north-bound interface APL. The application layer manages different services and security applications (Xia et al., 2015).

1.2.2 Security Challenges of Software Defined Networking

There are many challenges facing the SDN network such as DoS, DDoS and saturation attacks; scalability; and availability (Ahmad et al., 2015). There are also security challenges that specifically affected the SDN controller such as scalability, flexibility, reliability, availability, controller failure and policy distribution (Chen et al., 2016; Hakiri et al., 2014; Jammal et al., 2014; Karakus & Durresi, 2017).

The importance of the controller to the SDN network makes it an attractive target to attackers who wish to disrupt the network. Two examples of attacks that could disrupt or cause total collapse of a network are Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

DDoS attack is one of the more serious threats to SDN network (refer to Section 2.2.1(d)) that is capable of bringing down the entire network which will deny legitimate users from accessing network services or resources. DDoS is one of the most common type of attacks that is used by attackers to target SDN controllers (Haque et al., 2017). Attackers have several methods at their disposal to execute DDoS attack against the SDN controller in order to deny legitimate users from accessing network services or resources. One of the methods is by rendering the network inoperable by flooding the network or the controller with a large volume of packets or traffic to the point where the controller's resources are exhausted and unable to process any more incoming packets.

Another method is to bombard a single host or multiple hosts in the network with large volume of well-crafted packets with spoofed Source IP address so that they do not have matching rules in the flow table which will force the switches to forward all incoming packets to the controller for further processing. Eventually the controller resources will be exhausted and will affect its ability to process incoming packets that will result in degradation and even collapse of the entire network. If the situation persists, legitimate users will be denied from accessing network services or resources (Dharma et al., 2015). Figure 1.3 illustrates the behaviour of DDoS attack in SDN network (Douligeris & Mitrokotsa, 2004).

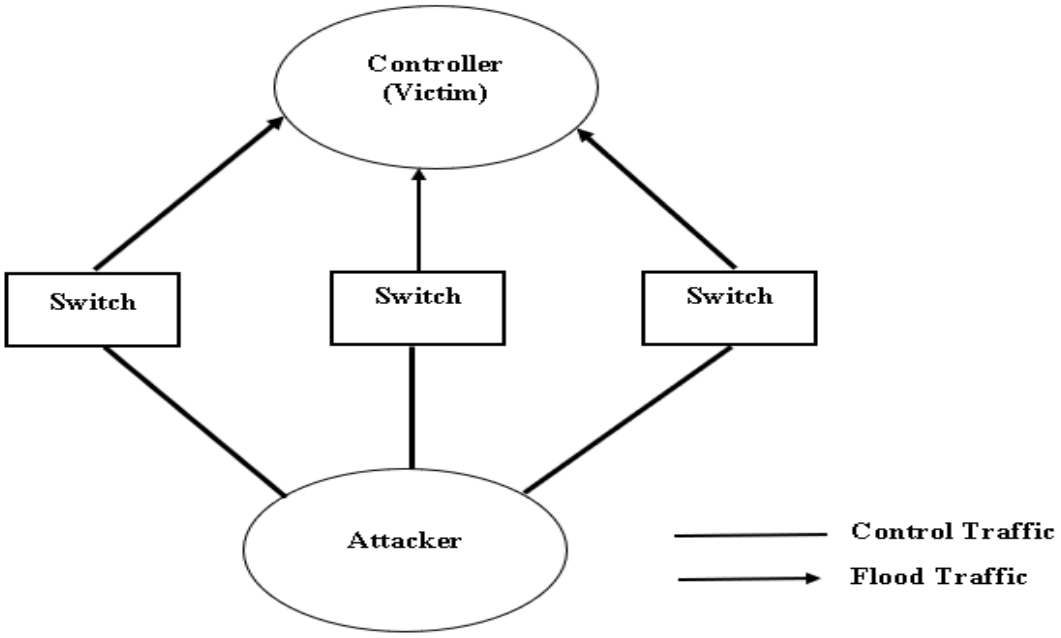

Figure 1.3 Architecture of DDoS Attacks

There are various methods that attackers could use to deplete the controller resources such as flooding the network with crafted packets with spoofed source IP addresses; and attacking the network with low and high traffic rate to evade detection and to force the controller into intensive tasks of processing those spoofed packets for detection or protecting the network from attacks (Devare et al., 2014; Scott-Hayward et al., 2016). Therefore, it is crucial for the controller to be able to handle both high and low rate incoming packet traffic.

1.3 Research Motivation

The adoption rate of SDN architecture keeps increasing due to the importance of managing big data nowadays which requires programmable controller to configure new instructions or rules to process new incoming traffic flows and flexibility with diverse network traffic flows (Masoudi & Ghaffari, 2016). At the same time, the destructive attempts to disrupt the SDN controller is becoming more common practice

of attackers that use DDoS attack. DDoS attacks have various DDoS traffic attack rates which are the most serious network threats, it also has significant implication on data integrity and economy. Statista Research Department 2016 reported that the SDN revenue is expected to exceed USD 28.1 billion by 2022, as shown in Figure 1.4 (Statista, 2016). This indicates the usefulness of SDN in minimizing capital expenditure and operational costs and it will be even more efficient as time goes by which attract more organizations to invest in the technology. However, the popularity of SDN makes it an attractive target to the attackers that wish to disrupt or bring down the network.

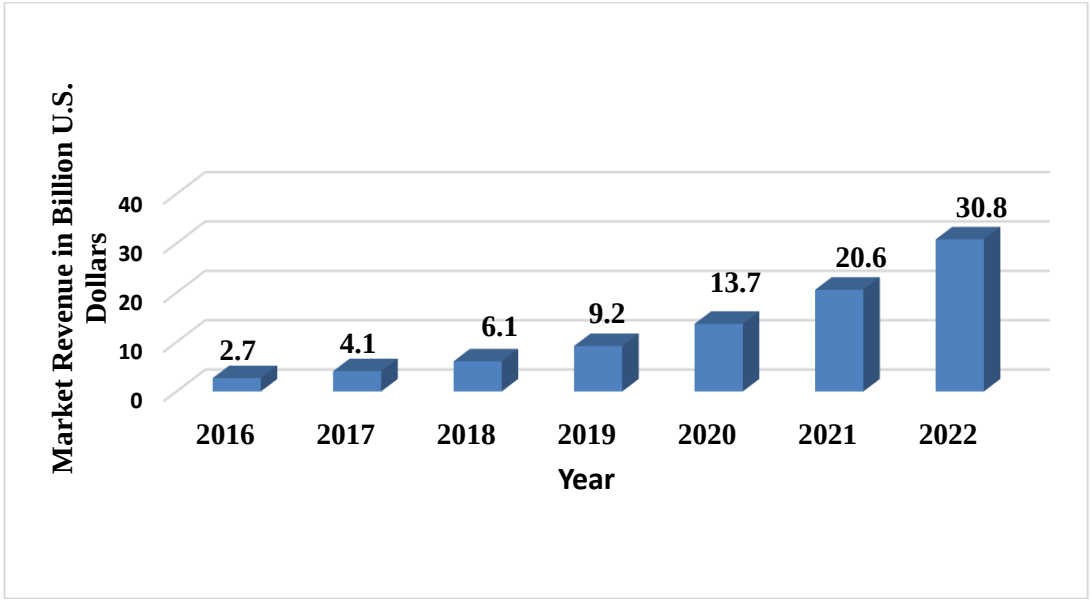

Figure 1.4 Software-Defined Networking (SDN) Market Revenue Worldwide From 2016 to 2022

Recently, several significant research has been carried out on the security of the SDN (Bouras etal., 2017; Duy et al., 2018; Huang et al., 2017). Some of the approaches such as (He et al., 2017; Peng et al., 2018) are related to the detection and mitigation of DDoS attack on SDN. However, most of the approaches performed poorly with simultaneous low and high rate DDoS attacks. Their performance will

degrade if both attacks occurred at the same time. Meanwhile, the approaches designed to detect DDoS attacks with varying attack rates suffer from low accuracy and high false positive rate whenever multiple targets in the network are involved. Therefore, any effort to propose a new approach that could detect DDoS attacks regardless of attack traffic rate and the number of targets with high accuracy and low false positive rate is a worthy endeavour. In this regard, the integration of an efficient security mechanism with the controller has been proven to help address different security challenges of SDN (Salman et al., 2016).

Many security solutions have been proposed to detect DDoS attacks on the controller, but most have limitations (drawbacks), such as not able to detect attacks with varying traffic rates. Consequently, the controller remains vulnerable to the attack that could potentially collapse the entire network and deny legitimate users from accessing network resources or services (Abdelaziz et al., 2017). Thus, the motivation of this research is to protect the SDN networks; and specifically to detect DDoS attacks with varying traffic rates (e.g. a low traffic attack rate and high traffic attack rate) that target the controller and triggered by attacks originating from both single and multiple hosts that targeting one or more victims in the network. Consequently, the proposed approach is expected be able to detect the DDoS attacks with a high detection rate along with a low false positive rate.

1.4 Problem Statement

Several existing approaches to detect DDoS attacks on SDN controller have been proven to be successful in detecting the types of attack that use fixed-rate traffic and target a single victim (Cui et al., 2016; Mao et al., 2018; Mousavi & St-Hilaire, 2015). Furthermore, most of these approaches have the ability to detect DDoS attack

with high traffic rates quite accurately and with low false positive rate. However, some of DDoS attack detection approaches are not able to differentiate between legitimate network traffic and low rate DDoS attack traffic (Ajaeiya et al., 2017; Boite et al., 2017).

Meanwhile, the majority of existing approaches suffer from drawbacks that affect the detection rate which leads to a high false positive rate and low detection rate due to several reasons. First, some of these approaches, such as the EDDSC approach (Mousavi & St-Hilaire, 2018), were designed to detect attacks that target a single host with a high detection rate and low false positive rate but have a low detection rate and high false positive rate to attacks that target multiple hosts, especially when triggered by low rate attacks on the controller. Furthermore, the approaches ignored attacks' sources that are triggered from a single host or multiple hosts. However, some of the approaches are capable of detecting low rate DDoS attack on SDN controller with high detection rate and low false positive rate, such as HMM-R scheme (Wang et al., 2018), but only for low rate DDoS attack that targets single victim. The existing approaches only focus on the detection of either low rate DDoS attacks or high rate DDoS attacks; and none consider both low and high rate DDoS attacks.

Most of the detection approaches depend on entropy method, such as (Boite et al., 2017; Mousavi & St-Hilaire, 2018). However, entropy-based approaches share the same drawbacks with approaches that rely on a single packet header feature which degrades the detection rate and increase false positive rate. Even though entropy variant approaches, such as (Kalkan et al., 2018; Mao et al., 2018), rely on two features, they still suffer from low attack detection rate and high false positive rate,

therefore incapable to detect low rate DDoS attack on the controller that that targets multiple victim hosts (Ajaeiya et al., 2017; Boite et al., 2017; Wang et al., 2018).

Furthermore, entropy-based detection approaches (Mousavi & St-Hilaire, 2018) also share the common drawbacks with approaches that use static threshold: low DDoS attacks detection efficiency, especially when there are various attack traffic rates targeting the controller that increase the false positive detection rate and reduce the detection rate.

The problem statement can be summarized as follows:

- The existing detection approaches are inefficient to detect DDoS attacks on SDN controller, especially when low rate DDoS attack traffic targets multiple victim hosts, to achieve a high detection rate and low false positive rate (Ajaeiya et al., 2017; Boite et al., 2017; Wang et al., 2018).
- The majority of existing detection approaches rely on one packet header feature to detect DDoS attacks on SDN controller triggered from a single host and targeted single or multiple victim hosts; thus have low detection rate and high false positive rate (Boite et al., 2017; Mousavi & St-Hilaire, 2018).
- Some of the existing detection approaches to detect DDoS attacks on SDN controller that use two packet header features are incapable of detecting low rate DDoS attacks launched against multiple victim hosts to achieve high detection rate and low false positive rate (Kalkan et al., 2018; Mao et al., 2018).
- Most of the existing detection approaches rely on static threshold values which are inefficient in detecting DDoS attacks with varying attack traffic rates to achieve high detection rate and low false positive rate (Mousavi & St-Hilaire, 2018; Kalkan et al., 2018).

1.5 Research Objectives

The main goal of this thesis is to propose a generalized entropy-based approach with a dynamic threshold to detect DDoS attacks on software defined networking controller with high detection rate and low false positive rate regardless of the attacks' traffic flow rates (low or high) and the source of the attack (single or multiple hosts) that target single victim host or multiple victim hosts. The following objectives are formulated to achieve the main goal of this thesis:

1. To generalize an information theory-based algorithm to detect DDoS attack on SDN controller based on two features of the packet header.
2. To adapt a dynamic threshold that is adaptable to varying incoming traffic rates to reduce the number of false positive and to obtain higher detection rate.
3. To propose a rule-based detection mechanism to efficiently detect DDoS attacks on SDN controller.

1.6 Research Scope and Limitations

The proposed approach is motivated to propose an efficient UDP DDoS attack detection approach against the controller by using the SDN environment, and by filtering the UDP packet and selecting the source IP and destination IP the controller collects the network traffic statistics to analyse these incoming traffic packets at the SDN controller for the proposed approach to be executed efficiently whether the attack traffic is high or low traffic attack rate, the proposed approach is limited to select the implementation environment through simulating all the scenarios according to the chosen environment.

In this research, the SDN environment features, the packet traffic attack type, the protocol type and the proposed approach evaluation metrics (the detection rate and false positive rate) are the scope of this research. However, the conventional network traffic cannot be measured in SDN simulation environment, payload packet in the attack traffic case because process all payload information requires a considerable amount of resources for computation (collect data) and it is very time consuming so a conventional network environment simulation are out of scope. Table 1.1 summarizes the scope and limitations of the study.

Table 1.1 Research Scope and Limitations

No	Items	Scope of Research
1	Network architecture	SDN
2	Protocol	UDP
3	Attack type	UDP flooding DDoS attack
4	Target layer	SDN controller
5	Evaluation Dataset	Simulated dataset
6	DDoS traffic rate	Low and high UDP DDoS traffic attack rate
7	Evaluation metrics	Detection rate and false positive rate

1.7 Research Contributions

The main contribution of this research is proposing a generalized entropy-based approach with a dynamic threshold to detect DDoS attacks on software defined networking controller with high detection rate and low false positive rate regardless of the attacks' traffic flow rates (low or high) and the source of the attack (single or multiple hosts) that target a single victim host and multiple victim hosts. The contributions of this research in relation to the previously stated research objectives are summarized as follows:

1) An information theory-based algorithm to detect low or high rate DDoS attacks on SDN controller that target either single or multiple hosts. Generalized Renyi Joint Entropy is proposed based on two features of the packet header (source IP and destination IP).
2) A dynamic threshold to reduce false positive rate and increase the detection rate of the DDoS attack detection approach which adapts to variations in the rates of the attack traffic. The dynamic threshold used the generalized Renyi Joint Entropy value as the input.
3) A rule-based mechanism for detecting DDoS attack against the SDN controller. The rule-based DDoS attack detection is used Renyi Joint Entropy values and dynamic threshold values that proposed in the first two objectives. The DDoS attack will be detected if the value of Renyi Joint Entropy below the dynamic threshold.

The relationship between the research gaps, objectives, and contributions are shown in Table 1.2 below.

Table 1.2 Relationship Between Research Gaps, Research Objective, and Contributions

Research Gap(s)	**Research Objective(s)**	**Research Contribution(s)**
Existing DDoS attack detection approaches that rely on a single packet header feature have low detection rate and low false positive rate.	Objective # 1	Contribution # 1
Existing DDoS attack detection approaches that rely on two packet header features not able to detect low traffic rate to achieve high detection rate and low false positive rate.	Objective # 1 Objective # 3	Contribution # 1 Contribution # 3

Table 1.2 Relationship Between Research Gaps, Research Objective, and Contributions (Cont.)

Research Gap(s)	Research Objective(s)	Research Contribution(s)
Existing DDoS attack detection approaches unable to detect low rate DDoS attacks that target multiple victims to achieve high detection rate and know false positive rate.	Objective # 1 Objective # 3	Contribution # 1 Contribution # 3
Existing DDoS attack detection approaches rely only on static threshold value which makes them inefficient in detecting DDoS attacks with variations in attack traffic rates.	Objective # 2	Contribution #2

As shown in Table 1.2, the problem statement is summarized into research challenges, where each research challenge is solved by one or more objectives through proposing different contributions resulting from these objectives.

1.8 Research Steps

This research is conducted based on several phases of theoretical and experimental analysis to find a better security approach to detect DDoS attacks on SDN controller. To achieve the goal of detecting DDoS attacks, including those with a mix of low and high traffic rates, with high detection rate and low false positive rate; and to fulfil the objectives of this study as mentioned in Section 1.5, the research process is divided into four phases: (i) reviewing the literature, (ii) proposing a new approach to detect DDoS attack on SDN controller, (iii) designing and implementing the proposed approach, and (iv) testing and evaluating the proposed approach. The four phases of the research are illustrated in Figure 1.5.

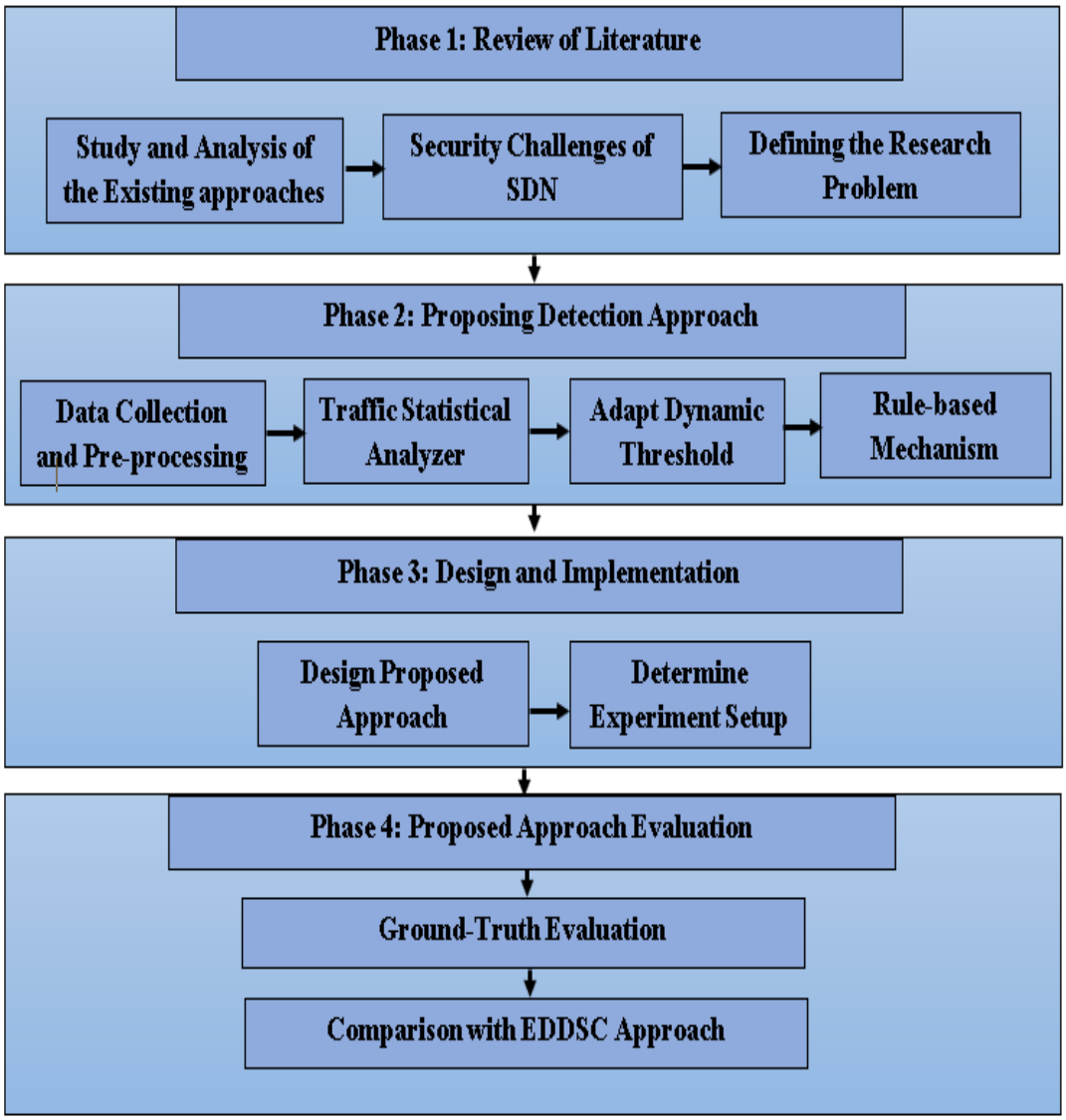

Figure 1.5 Research Steps

The first phase, several literatures have been studied to gain understanding of the challenges that await any effort to secure the SDN controller; and to clarify the research problems by analysing any issues related to existing detection approaches. It is hoped that by identifying the limitations of the existing approaches, the gap and problems of this research will be established.

The second phase, the solution to the research problem is proposed. The solution consists of four stages to detect DDoS attacks with high detection rate and low false positive rate. The proposed approach employs network traffic statistical

analyser, adapt the dynamic threshold, and uses a rule-based detection approach to achieve the research goal.

The third phase involves the design and implementation of the proposed approach to achieve the research goal. This phase implements all methodology and the four stages proposed in the second phase to detect DDoS attack against the SDN controller.

The fourth phase mainly concerned with performance evaluation to measure the level of fulfilment of the research objectives. The performance of the proposed approach is evaluated by analysing the experimental results of the implementation of the proposed approach. The proposed approach is tested and evaluated in terms of its effectiveness in detecting DDoS attacks and its ability to reduce false positive rate. It is then compared with existing attack detection approaches.

1.9 Thesis Organization

This thesis is structured into six main chapters as follow:

Chapter 2 discusses the background of the research based on the study of the literatures that are related to this work. This chapter critically reviews the existing solutions for the detection of DDoS attacks on SDN controller. Moreover, this chapter comprehensively discusses any drawbacks of previous researches in the literatures.

Chapter 3 explains the integrated stages of the proposed approach as well as the method for the detection of DDoS attacks on SDN controller with high detection rate and low false positive rate.

Chapter 4 presents the design and implementation of the proposed approach, including the design principles of the test-bed, elaboration of each phases, and the evaluation strategy to measure the performance of the proposed approach.

Chapter 5 reports the experiments and their results. It also presents a comprehensive analysis of the results and evaluates the performance of the proposed approach in comparison with the existing approaches that have similar scope with this research.

Chapter 6 presents the conclusions drawn from our work and provides suggestion for future research direction.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The previous chapter discussed the problems in detecting DDoS attack against the SDN controller. This chapter presents a comprehensive literature on detection approaches of DDoS attack against the SDN controller. In addition, this chapter analyses and considers the critical issues related to the detection of DDoS attack on SDN controller in order to find a more comprehensive and effective detection approach.

This chapter is organized as follows Section 2.2 provides a research background, which is divided into three main subsections First, Subsection 2.2.1 introduces the SDN technology. Second, Subsection 2.2.2 explains an information theory to detection of DDoS attack against controller in SDN. Third, Subsection 2.2.3 presents the use and effect of threshold in detecting DDoS attacks. In addition, Section 2.3 provides a review of the related works. Section 2.4 discusses the critical review of related work. This chapter is summarized in Section 2.5.

2.2 Background

In recent years, many researchers and enterprises have attempted to secure networks from attacks, but were confronted with many drawbacks including, but not limited to management, scalability, security, flexibility, dependability, and reliability. Consequently, the traditional network architecture is commonly characterized as complex and rigid due to the difficulty in controlling or transforming the network to satisfy changing business requirements (Xia et al., 2015). Thus, to overcome these

limitations a new network architecture is need that is more flexible, programmable, scalable, manageable and configurable (Smeliansky, 2014). In the early 2010 SDN started to look like a viable alternative solution to confront the limitation of traditional network architecture (Sarika & Prakash, 2019).

2.2.1 Software Defined Network

Software Defined Networking (SDN) is a new and better network architecture than traditional network architecture in controlling network traffic flows as well as having elasticity and flexibility to be programmed for efficient network management. The SDN offers network administrators ease of management and programmability by decoupling the control plane from the data plane (Abdelaziz et al., 2017; Scott-Hayward et al., 2016). Furthermore, SDN offers many advantageous features such as network programmability which enables the SDN networks to be deployed quickly and managed dynamically compared to the traditional networks which took a long time to be deployed and harder to manage to meet the requirements for a new host on the network (Chen et al., 2015; He et al., 2017). Figure 2.1 depicts the comparison between the SDN and the traditional network architecture; and also illustrates the location of control plane in the traditional network, which is in the same device and location as the data plane (ALAdaileh et al., 2020).

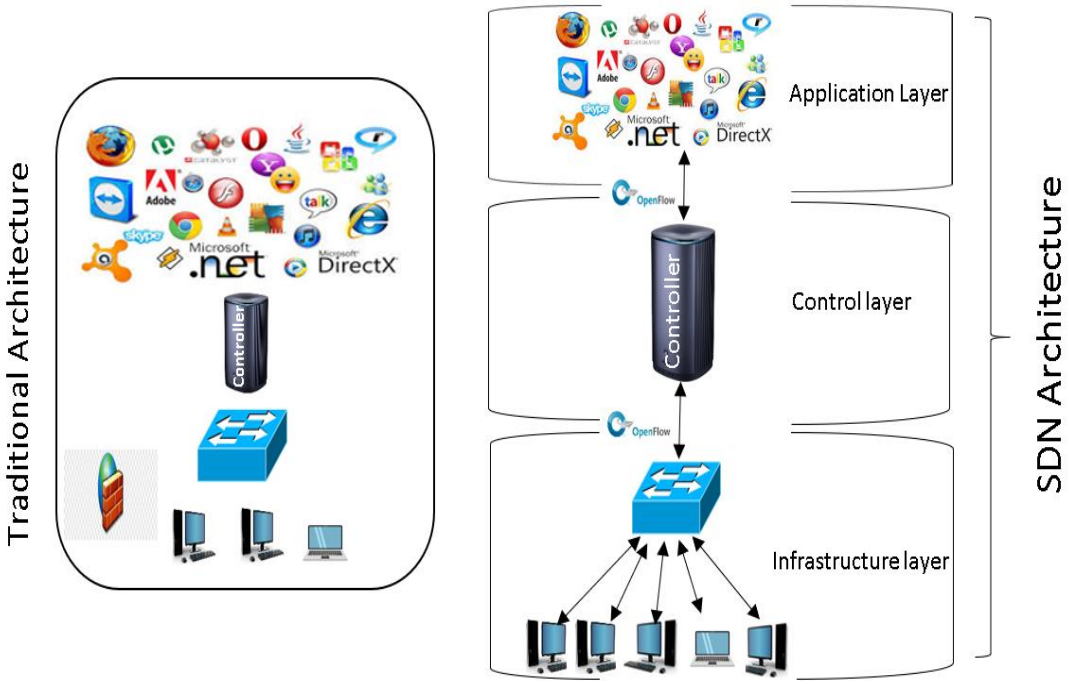

Figure 2.1 Traditional Networks vs SDN Architecture

The SDN depends on a centralized controller to control the entire network, it enables the applications to have a network-wide view by establishing centralized visibility to manage network the traffic flow (Khan et al., 2016; Xia et al., 2015). Moreover, it also provides the capability to virtualize the entire network infrastructure that will further simplify the task of configuring and managing the network. SDN promises to reduce the network complexity by dividing the data plane from the control plane (Kreutz et al., 2013; Abdullah Gani et al., 2016; Yoon et al., 2015). Table 2.1 presents the benefit of the SDN versus the traditional network.

Table 2.1 SDN vs Traditional Network

Criteria	Software-defined networking	Traditional Network
Network management	Easy	Difficult
Global network view	Easy	Difficult
Maintenance cost	Low	High
Time for update/error handling	Quick	Slow
Attack detection and mitigation	Easy	Difficult
Authenticity of controller and applications	Important	Not Applicable
Integrity and consistency of forwarding table and network state	Important	Important
Availability of controller	Important	Not Applicable
Resource utilization	High	Low

SDN isolates the characteristic of control from data planes that allow network configurations to be made that could further enhance and improve the performance, as well as open the path for security innovations on the network architecture and operations (Shin et al., 2016). Moreover, it provides instant network status which makes efficient control and flow handling procedures possible while keeping the control plane flexible and intelligent (Dabbagh et al., 2015).

Indeed, SDN performance importance lies with the improvement of the network security to detect the abnormal traffic behaviour (malicious packets) by the utilization of the SDN characteristics to control incoming traffic flows. The emergence of SDN offers an opportunity for enhancing the network performance by allowing a

centralized controller to manage and control the traffic flows of the entire network, as shown in Figure 2.2 (Sezer et al., 2013). The SDN manages the entire network via application programming interfaces (APIs) located between the layers to connect the networks together (Iyengar et al., 2014). In contrast, the traditional network works as one package which causes difficulty in managing the data traffic and performance and decreases the effectiveness of management (Rawat et al., 2017).

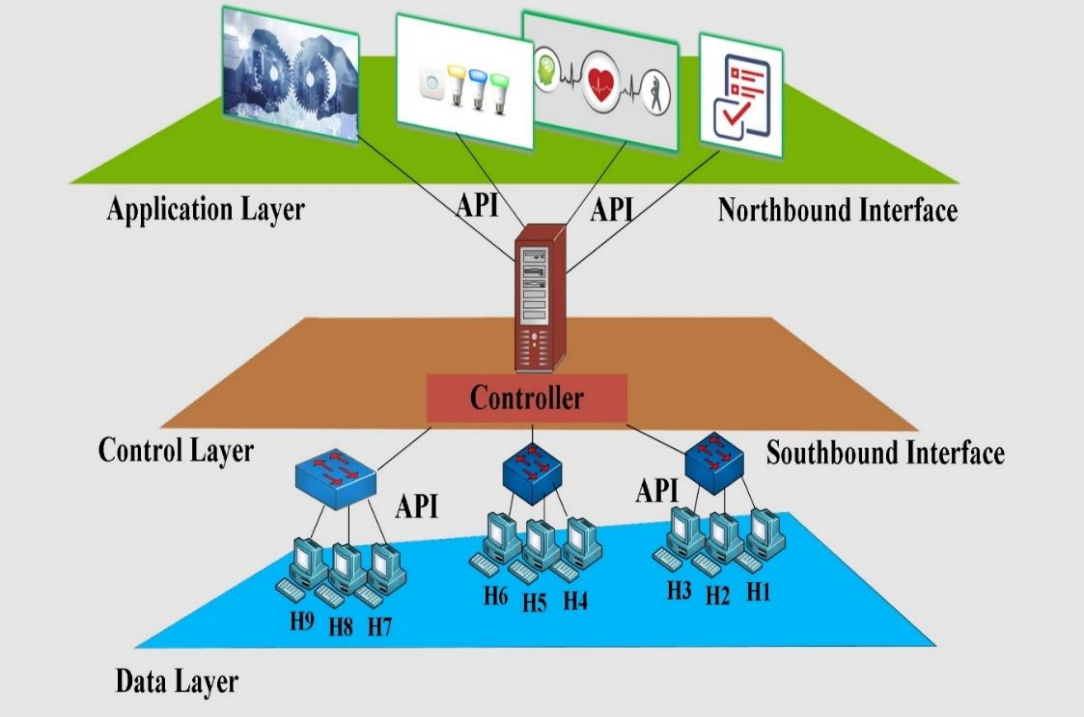

Figure 2.2 General SDN Layered Architecture

As depicted in Figure 2.2, the data layer consists of devices (switches, routers, access points) that contain a flow entries table (rules/instructions). Thereafter, the data plane is responsible for receiving incoming packets from hosts or external sources via the switches that first check the incoming packets against the existing switch table instructions. If there are no matching rule in the existing flow table, the packet will be

forwarded to the controller through a secure channel (OpenFlow protocol) (Kreutz et al., 2015).

Additionally, the controller is responsible for the operations between the data plane and an application plane by processing new incoming packets and create new instructions to deal with subsequent incoming packets. Thus, it acts as the brain of the SDN network since it is managed entirely by the centralized controller (Abdullah Gani et al., 2016). The control layer is responsible for managing and processing all the network devices and deals with the new incoming packets proactively or reactively which offers a high flexibility to make flow by flow decisions while considering QoS requirements and network traffic conditions (Salman et al., 2016).

In fact, bandwidth consumption and latency of frequent communication affect control layer scalability significantly (Shin & Gu, 2013). As aforementioned, the controller is the most significant and important element in the SDN architecture based on its ability to control the entire network through monitoring and processing the incoming traffic flows. Moreover, the SDN controller is also responsible for dictating the network policies that define all packet forwarding rules that are installed in the switches; as well as updating the rules in switches whenever the network configuration changed. So it is not a stretch to consider the controller as the brain of the SDN (Rawat et al., 2017). Consequently, due to its vital role, a failure or problem occurring at the controller may degrade and even collapse the entire SDN network.

2.2.1(a) Software-Defined Networking Controller

The SDN controller plays many considerable roles in the network such as configuring flow table; monitoring networking devices by establishing secure

connections; and updating instructions to the flow table in the infrastructure layer (switch's table) to identify new traffic flow (Tri & Kim, 2014). In addition, the controller could manage the entire traffic flow by assuming the role of a manager between the infrastructure layer and application layer through open API southbound, northbound and east/westbound interfaces (Jarraya, Madi, & Debbabi, 2014), and decides whether the traffic flow is normal or abnormal by making use of the network traffic flow statistics collected by the controller as a baseline input (information) to an attack detection method.

On the other hand, the SDN controller deals with the network traffic packets either in a proactive or reactive mode. (Salman et al., 2016) stated that the proactive mode has greater effect on the SDN performance than the reactive mode in protecting the SDN network from malicious attacks because the rules are pre-installed in the switch table (flow rule) to process the packets, whereas in the reactive mode, the rules will only be created and installed to the switch whenever new incoming packets do not have matching rules in the switch table.

Furthermore, the controller is a key component in any effort to improve the network performance. The controller plays different roles by using various modules to gather statistical information about network traffic and identifies the tasks for each part in the network (Gorkemli et al., 2016).

Particularly, the controller simplifies network operations by utilizing the centralized control feature for improving the network through monitoring network devices and routing a flow path according to the flow entry (rules/instructions) in the switch's flow table. Furthermore, SDN controller collects the required information from the network packets for analysis to detect DDoS attacks. However, the