Computers, Materials & Continua
DOI:10.32604/cmc.2021.017972
Article

Tech Science Press

Entropy-Based Approach to Detect DDoS Attacks on Software Defined Networking Controller

Mohammad Aladaileh[1], Mohammed Anbar[1,*], Iznan H. Hasbullah[1], Yousef K. Sanjalawe[1,2] and Yung-Wey Chong[1]

[1]National Advanced IPv6 Centre of Excellence, Universiti Sains Malaysia, Penang, Malaysia
[2]Department of Computer Sciences, Northern Border University, Ar'ar, Kingdom of Saudi Arabia
[*]Corresponding Author: Mohammed Anbar. Email: Anbar@usm.my
Received: 19 February 2021; Accepted: 24 March 2021

Abstract: The Software-Defined Networking (SDN) technology improves network management over existing technology via centralized network control. The SDN provides a perfect platform for researchers to solve traditional network's outstanding issues. However, despite the advantages of centralized control, concern about its security is rising. The more traditional network switched to SDN technology, the more attractive it becomes to malicious actors, especially the controller, because it is the network's brain. A Distributed Denial of Service (DDoS) attack on the controller could cripple the entire network. For that reason, researchers are always looking for ways to detect DDoS attacks against the controller with higher accuracy and lower false-positive rate. This paper proposes an entropy-based approach to detect low-rate and high-rate DDoS attacks against the SDN controller, regardless of the number of attackers or targets. The proposed approach generalized the Rényi joint entropy for analyzing the network traffic flow to detect DDoS attack traffic flow of varying rates. Using two packet header features and generalized Rényi joint entropy, the proposed approach achieved a better detection rate than the EDDSC approach that uses Shannon entropy metrics.

Keywords: Software-defined networking; DDoS attack; distributed denial of service; Rényi joint entropy

1 Introduction

Network security innovation is like a race between adversaries and the security communities to best each other in breaking and securing the network. Security researchers and practitioners have put much effort and made strides to overcome the threats posed by their adversaries. However, the rapid advancement of information and communication technologies, such as mobile devices and cloud computing virtualization, imposes an additional burden on network administrators in ensuring network security. Technology advancement also introduces new threats, attack methods, and attack vectors.

Many new attack detection methods have taken advantage of the SDN paradigm that separates the control plane and the data plane [1]. The separation simplifies network management by making the network programmable and the control centralized [2], allowing network administrators to manage and control the whole network via the controller [3]. However, at the same time, the control layer becomes an attractive target for DDoS attacks [4]. The exploitation of certain SDN features that makes the controller ineffective against spoofed network traffic exposes the SDN to various security issues [5].

The centralized SDN controller controls the network by creating new routing instructions or updating the existing one in the flow table of OpenFlow switches to handle new incoming traffic [6]. The OpenFlow switch inspects all incoming packets. A packet is sent to its intended destination if it matches any instructions in the switch's flow table. Otherwise, the packet is sent to the controller for further processing. Attackers exploit this process by flooding the network with spoofed IP packets to trigger a DDoS attack against the controller.

DDoS attack denies legitimate users' access to network resources by flooding the network with massive traffic comprising IP packets with spoofed sources IP addresses in a short amount of time. The sudden surge of traffic in the SDN network puts the controller into overdrive mode until its resources are exhausted [7–9]. Although the DDoS attack mechanism is well understood, the task of distinguishing DDoS attack traffic from regular network traffic is challenging, especially when attempting an early detection with high accuracy and low false-positive rate [1].

Entropy-based metrics can identify the variations in the network traffic behavior that have varying rates. This work generalized the Rényi joint entropy method to detect low-rate and high-rate DDoS attacks against the SDN controller that target single or multiple victims. The contributions of this paper are:

(a) A comprehensive study of different security issues related to the SDN controller.
(b) A generalized Rényi joint entropy metric to detect low-rate and high-rate DDoS attacks against the SDN controller regardless number of targets.
(c) A comparison of the proposed approach results with the approach that adapted the Shannon entropy metric.

We organize the rest of this paper as follows. Section 2 discusses the related work, while Section 3 elaborates the generalized Rényi joint entropy method. The discussion on the proposed detection scheme, experimental setup, and test cases are in Sections 4 to 6, respectively. Section 7 discusses the performance of the proposed approach. The result of the comparison between the proposed and existing detection approaches is in Section 8. Section 9 highlights the significance of the proposed approach's enhancement, and the analysis of the results is in Section 10. Finally, Section 11 concludes the paper.

2 Related Works

The SDN technology's adoption rate keeps trending upwards due to the popularity of big data that requires a programmable controller to configure new instructions or rules to deal with novel and diverse network traffic flows [10]. At the same time, the attempts to disrupt online services and breach online systems are becoming more common from adversaries that resort to all kinds of methods to achieve their objectives. However, the most elusive and destructive threat to computer systems and networks is DDoS attacks with varying traffic rates.

Several notable research on DDoS attack detection on SDN networks has been carried out in the past few years [11–13]. Some of the existing approaches also include the mitigation of DDoS attacks [14,15]. However, most existing detection approaches performed poorly against simultaneous low-rate and high-rate DDoS attacks. The detection accuracy severely degrades if both types of attacks occurred concurrently. Meanwhile, the detection approaches designed to detect DDoS attacks with varying attack rates suffer from low accuracy and high false-positive rate whenever multiple targets are involved. Therefore, any effort to create a new approach that could detect both low-rate and high-rate DDoS attacks regardless of the number of targets with high accuracy and low false-positive rate is a worthy endeavor. In this regard, integrating an efficient security mechanism with the controller has been shown to help address multiple SDN security challenges [16].

Despite many innovative security approaches to detect DDoS attacks against the controller, most of the existing detection approaches have limitations (drawbacks), such as unable to detect DDoS attacks with varying traffic rates in an efficient manner. Consequently, the controller remains vulnerable to the attack that could potentially collapse the entire network and prevent legitimate users from accessing network resources or services [17]. Therefore, the motivation of this research is to ensure the protection of the SDN controller from DDoS attacks with varying traffic rates (low and high), regardless of the number of attackers and victims targeted. Consequently, the proposed detection approach must achieve high detection accuracy and a low false-positive rate.

As stated before, some existing DDoS attack detection approaches utilize some features of the SDN architecture. For example, a Shannon entropy method can identify the uncertainty associated with a random variable [18,19]. An information theory-based method (joint-entropy) that depends on multiple packet header features (flow duration, source IP address, packet length, and destination port) can calculate the joint entropy value to detect DDoS attacks. Their method is effective in reducing the false-positive rate and increasing the detection accuracy. Since the joint-entropy method could identify different types of DDoS attacks, the authors employ information theory in their approach to achieve scalability, lower complexity, and higher accuracy. However, it still suffers from several weaknesses, such as ineffective on unknown DDoS attack, high detection response time, controller overloaded with new packet_in, and unable to detect low-rate or high-rate DDoS attacks with high detection accuracy rate and low false-positive rate [20].

An entropy metric is used in an approach that combines information distance with a generalized Rényi entropy for detecting low-rate DDoS attacks against the SDN controller. The probability distribution is used as the metric to detect the DDoS attack by setting a specific window size for the incoming packets and then periodically extracts the packet features from the flow table (switch table). The difference in the probability distributions indicates the existence of a DDoS attack in the network. The experiments carried out by the authors showed that the generalized entropy combined with the information distance is accurate in detecting low-rate DDoS attacks [1]. However, there are several issues with the approach.

First, it is difficult to set the dynamic threshold because of varying attack traffic rates in the traffic flow. Second, relying on the switch's table instead of the SDN controller to extract the traffic statistics may result in some data loss. Third, the presence of DDoS attacks with varying traffic rates increases the false-positive rate of the approach. Furthermore, the proposed detection approach only depends on a single packet header feature to collect traffic flow statistics, which increases the false-positive rate.

Furthermore, a support vector machine (SVM) is used to propose a DDoS attack detection approach to distinguish between normal and attack traffic. The flow status collected by the controller is used to build the proposed approach. Since the SVM method depends on the statistical theory to classify the network traffic using six features, the controller has an additional burden and strain to process all incoming traffic packets to detect or prevent any potential DDoS attack. Hence, a low false-positive rate is evidence of an improved DDoS attack detection ratio [21]. However, this method demands more resources to compute and process network traffic flow that exhausts the SDN controller resources.

A novel detection technique called SAFETY was proposed for early detection and mitigation of TCP SYN flooding attack by harnessing the programmability and comprehensive visibility of the SDN through an entropy method to determine the randomness of the flow [22]. The entropy is calculated using the destination IP address and few attributes of the TCP flags. The authors performed extensive evaluation that shows significant improvement to the average response time and average attack detection time. However, this method is only suited to handle a single victim, and when multiple concurrent victims are involved, it destabilizes the network.

Time-Based Detection and Defense Scheme Against DDoS (TDDAD) approach detects DoS attacks against the SDN controller based on time features using three modules: statistics collection module, feature extraction module, and attack detection module by BPNN. Attackers exploit the OpenFlow (OF) switch's inability to control incoming packets after overwhelming the controller with many packets that deplete its resources. The objectives of TDDAD are to detect and defend against DDoS attacks in real-time effectively and swiftly since any detection approach that relies on the packet's content feature to detect an attack will be incapacitated once the switch or controller loses control [23]. However, not only is it difficult to predict the attacks, but it could also inadvertently exhaust the controller's resources, especially when dealing with low-rate DDoS attacks targeting many victims.

Authors in [24] proposed Safe-Guard Scheme (SGS) to mitigate DDoS attacks against the controller. It leverages DDoS attack detection's behavior features that depend on the cooperation between the data plane and the control plane. The proposed approach consists of two stages. The first stage detects any abnormal traffic in the data plane, and the second stage provides a dynamic defense of the controller in the control plane. However, the scheme cannot detect low-rate DDoS attacks, and it also depends on multiple controllers, which increases detection time significantly.

The literature studies showed that the studies on low-rate and high-rate DDoS attacks against SDN controllers that target single or multiple victims are very few and far between. No study has adopted a generalized Rényi method with joint entropy to detect DDoS attack traffic before.

The motivation of this research is to protect the SDN controller detect both low-rate and high-rate DDoS attacks against the SDN controller regardless of the number of targets by using Rényi joint entropy generalization without adding overhead to the SDN controller. Also, it must not misclassify abnormal traffic behavior as normal behavior.

3 Generalized Rényi Joint Entropy

The presence of randomness in UDP traffic behavior is one of the telltale signs of DDoS attacks. Some of the existing detection approaches use the Shannon entropy method [25,26] to detect the UDP traffic behavior's randomness. However, using the Shannon entropy method may result in a low detection rate and high false-positive rate, especially for low-rate DDoS attacks with multiple targets. It depends only on a single packet header feature as the input to calculate

the entropy value. Furthermore, it relies on a static threshold to decide if the network traffic flow exhibits DDoS attack behavior.

Two essential concepts in the Rényi joint entropy theory are joint entropy and Rényi. It was introduced to measure two random variables (i.e., two packet header features, such as source IP address and destination IP address) represented by x and y, respectively. The probability $p(x, y)$ defines the probability distribution of each source IP and destination IP. Furthermore, the Rényi joint entropy has been implemented with a dynamic threshold to calculate the selected features' probability values in the first stage. The dynamic threshold helps to accurately detect the randomness in the traffic behavior, leading to the detection of DDoS attacks. This stage consists of an important step that represents the core of the approach in Rényi joint entropy.

This section demonstrates Rényi joint entropy's generalized formula to detect low-rate and high-rate DDoS attacks against the SDN controller targeting a single or multiple hosts. The tradeoff between contributions from the distribution's main mass and the tail is controlled by two parameterized Shannon entropy generalizations in this research. Indeed, the two parameters (Rényi and Tsallis) are derived from Kolmogorov–Nagumo's [27] generalization of an average. The Kolmogorov-Nagumo generalization is represented by Eq. (1) [28].

$$(X)\,\phi = \phi^{-1}\left(\sum_{i=1}^{N}\sum_{j=1}^{M} p\left(x_i y_j\right)\phi\left(x_i y_j\right)\right) \tag{1}$$

where Ø denotes a function that satisfies the affine or exponential function. Due to affine transformation functions $\phi(x_i) \to \phi\gamma(x_i) = a\phi(x_i) + b$. Where a, b are real numbers, and the inverse of the affine function is defined by Eq. (2).

$$\gamma^{-1}(X_i) = \phi^{(-1)}\left(\frac{x_i - b}{a}\right) \tag{2}$$

Consequently, the Rényi entropy can be obtained from the Shannon entropy with the following transformations:

$$H_{RJ\alpha}(x) = \phi^{-1}\left(\sum_{i=1}^{N}\sum_{j=1}^{M} p\left(x_i y_j\right)\phi\left(-log_2 p\left(x_i y_j\right)\right)\right) \tag{3}$$

where $\phi(X_i) = 2^{(1-\alpha)X_i}$ *and* $\phi^{(-1)}(X_i) = \dfrac{1}{1-\alpha} log_2 X_i$.

$$H_{RJ\alpha}(x) = \frac{1}{1-\alpha} log_2\left(\sum_{i=1}^{N}\sum_{j=1}^{M} p\left(x_i y_j\right) 2^{-(1-\alpha) log_2 p\left(x_i y_j\right)}\right) \tag{4}$$

$$\mathrm{H_{RJ\alpha}}(\mathrm{x}) = \frac{1}{1-\alpha}\log_2\left(\sum_{\mathrm{i}=1}^{\mathrm{N}}\sum_{\mathrm{j}=1}^{\mathrm{M}} \mathrm{p}\left(\mathrm{x_i y_j}\right) 2^{\log_2 \mathrm{p(x_i y_j)}^{(\alpha-1)}}\right) \tag{5}$$

$$H_{RJ\alpha}(x) = \frac{1}{1-\alpha} log_2\left(\sum_{i=1}^{N}\sum_{j=1}^{M} p\left(x_i y_j\right) p\left(x_i y_j\right)^{(\alpha-1)}\right) \tag{6}$$

$$H_{RJ\alpha}(x) = \frac{1}{1-\alpha} log_2 \left(\sum_{i=1}^{N} \sum_{j=1}^{M} p\left(x_i y_j\right)^{\alpha} \right) \tag{7}$$

where $p\left(x_i y_j\right)$ is the probability of the event $(x = x_i,\ y = y_i)$, $i = 1, 2, 3, \ldots, N$ and $j = 1, 2, 3, \ldots, M$.

Eq. (7) is a general formula for Rényi joint entropy for two random variables, where α is a positive parameter that exposes the main mass, which reflects the concentration of events that often occurred. As stated before, the generalized Rényi joint entropy $H_{RJ\alpha}(x, y)$ is a statistical method for calculating the randomness of incoming network traffic flows to detect UDP DDoS attacks with varying traffic rates, which is the goal of this research. The Rényi joint entropy method depends on the probability calculation of each source IP and destination IP.

4 Proposed Attack Detection Scheme

In SDN, a low-rate DDoS attack is one of the most problematic security threats to the SDN controller. The difficulty in detecting the attack stems from the resemblance of the attack traffic to normal traffic behavior. It is even more challenging to achieve high accuracy and low false-positive rate when the target involves multiple hosts. Meanwhile, the high-rate DDoS attack poses its own challenge to any detection scheme, especially when involving multiple targets. Therefore, the proposed approach aims to detect DDoS attacks on the SDN controller regardless of attack traffic rates and the number of targets by passive monitoring of UDP packets in the SDN network.

The presence of abnormal behavior in the SDN UDP traffic could be strong evidence of a DDoS attack. Several existing approaches can detect DDoS attacks by relying on certain packet header features [29–31]. However, these existing approaches cannot accurately detect low-rate DDoS attacks when varying attack traffic rates are involved. Hence, there is a need to find significant features that contribute to detecting DDoS attacks regardless of the attack intensity (i.e., low-rate or high-rate). The proposed approach assumes that leveraging a Rényi joint entropy method with significant features and dynamic threshold usage would positively affect the DDoS attack detection accuracy regardless of the attack traffic rates.

In this step, the Rényi joint entropy equation will be used to overcome the limitations of the existing DDoS detection approaches that rely on the Shannon entropy method and its variants. There are several important reasons to use the Rényi joint entropy equation: (i) it uses a smaller number of packet header features to distinguish regular traffic from attack traffic, (ii) it uses a smaller number of packet header features to detect both low-rate and high-rate DDoS attacks, (iii) it detects DDoS attacks more accurately than other approaches, (iv) it reduces false-positive error rate, (v) it is usable at various scales, in terms of several instances taken per size window, and (iv) it can measure the randomness of network packets. These features are essential for detecting DDOS attacks on the SDN controller accurately.

In this research, a generalized Rényi joint entropy is proposed based on combining two concepts: the joint entropy method and the Rényi method. The generalized Rényi joint entropy measures two random variables in the form of two packet header features, such as source IP address and destination IP address, represented by x and y, respectively. The formula for the proposed Rényi joint entropy method is as follow:

$$H_{RJ\alpha}(x) = \frac{1}{1-\alpha} log_2 \left(\sum_{i=1}^{N} \sum_{j=1}^{M} p\left(x_i y_j\right)^{\alpha} \right) \tag{8}$$

where $H_{RJ\alpha}(x, y)$ denotes a Rényi joint entropy, α denotes a positive parameter, $p(x_i, y_j)$ is the probability distribution between source IP (x) and destination (y) within the time interval $\boldsymbol{t}$.

In the proposed GEADDDC approach, the Rényi joint entropy depends on α value that can improve the detection rate by calculating the incoming traffic packets probability. The probability distribution $p(x_i, y_j)$ is calculated for each source and destination based on the IP frequencies. A Rényi joint entropy's maximum value occurred when each packet's probability distribution is equally distributed among all the hosts' destinations. On the other hand, a minimum value of Rényi joint entropy occurred when the amount of probability to all packets within a particular time window skewed towards a distinct destination host.

The Rényi joint entropy is based on the probability of each source IP (x_i) and destination IP address (y_j) recorded in the previous stage within a specific period. Eqs. (9) and (10) show the probability of x_i and y_j, respectively.

$$p_{x_i} = \frac{x_i}{n} \tag{9}$$

$$p_{y_j} = \frac{y_j}{n} \tag{10}$$

where $\boldsymbol{x_i}$ denotes the frequency of each distinct source IP within $\boldsymbol{w}$, and $\boldsymbol{y_i}$ denotes the frequency of each distinct destination IP addresses within $\boldsymbol{w}$, and $\boldsymbol{n}$ represents the total number of n packets within $\boldsymbol{w}$. Regular traffic and attack traffic have different probability distributions. By calculating the probabilities for each source IP and destination IP of packet header features, which are considered variables of Rényi joint entropy, it will measure the uncertainty and randomness in both variables (IP source address and IP destination address). Thereby, the higher uncertainty will result in higher Rényi joint entropy, which is considered one factor contributing to the detection of DDoS attacks in the network. Fig. 1 shows the flowchart of the Rényi joint entropy method.

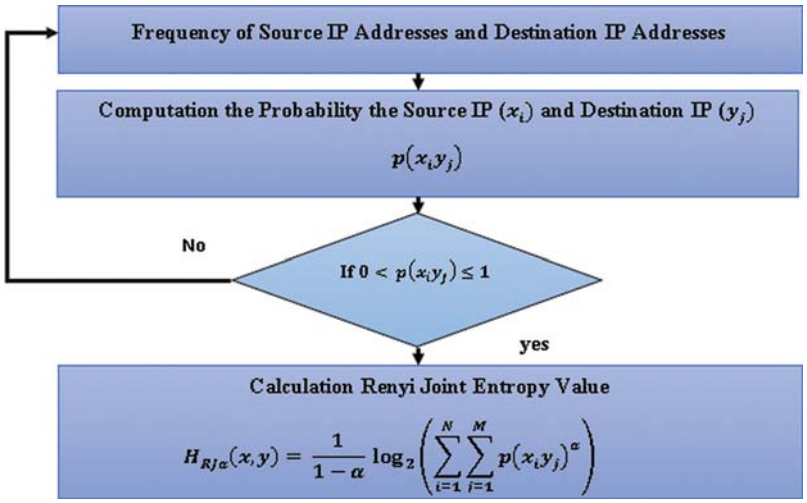

Figure 1: Joint Rényi entropy values aggregation

This stage is the first step in identifying abnormal traffic behavior by observing the Rényi joint entropy value. Therefore, the output of this stage contributes to achieving one of the research objectives.

5 Experimental Setup

The experiment was conducted on a workstation with a 2.20 GHz Intel Core i5-5200U processor and an 8 GB RAM running Ubuntu Linux 14.04 operating system. The network consists of a POX controller, an OpenFlow (OF) switch, and 64 hosts connected to the OF switch, as illustrated in Fig. 2. POX is a widely popular software-based SDN controller within academic research circles, and it is a lightweight, fast, and open-source platform running on Linux, Mac OS, and Windows. Also, Mininet version 3.7 (32-bit) provides prototype network scenarios using the process virtualization concept to emulate network elements. UDP packets with spoofed source IP addresses were used as attack packets without any payload in this work. Python programming language was used to generate packets with random source IP addresses using a random function "randrange [1–255]." Additionally, python scripts were used for generating traffic.

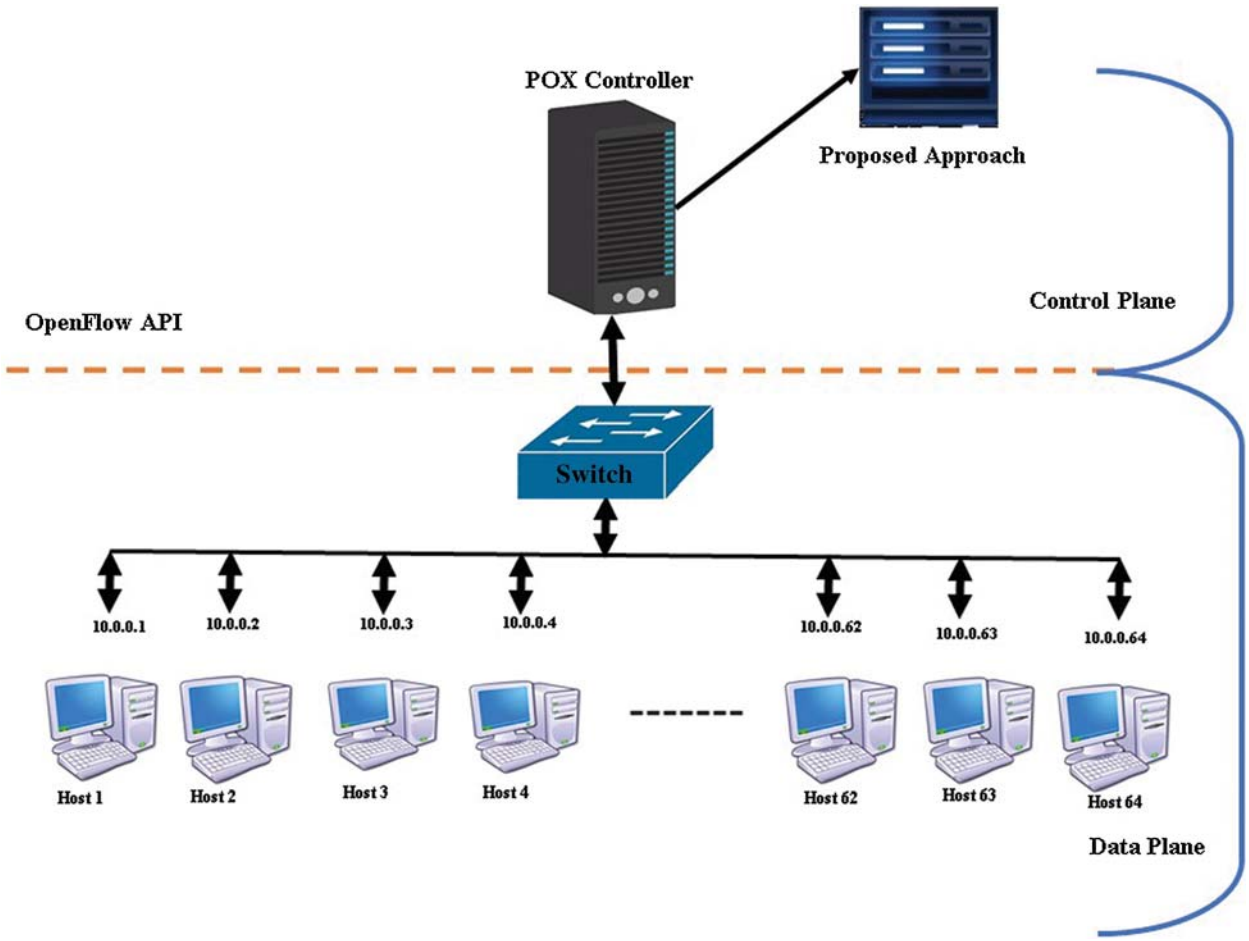

Figure 2: Experimental testbed SDN topology

Eight simulation scenarios were used to validate the proposed GEADDDC approach. Different assumptions are made regarding the attack scenarios in terms of attack source quantity (single or multiple attack hosts) and the number of targets (single or multiple victim hosts).

(a) In the single-source attack, one attacker generates spoofed attack packets with a unique source IP address.
(b) In the multi-source attacks, three attackers generate spoofed attack packets with unique source IP addresses.
(c) Attack traffic flows are launched towards the SDN controller.
(d) Attack traffic uses UDP packets with spoofed source IP addresses to simulate attack traffic flows.
(e) All network hosts are in working condition, and the network is stable throughout the attack.

Each simulation scenario runs for 30 min The average result in terms of detection rate and the false-positive rate were reported every 5 min. The 5 min window size is divided into n time slots where each slot is equal to m s. Eq. (11) shows the calculation of the time slot.

$$TimeSlots\,(n) = (5 \times 60)\,/m = 300/5 = 60 \tag{11}$$

where ***m*** is a configurable value, which indicates that the network traffic will be aggregated each ***m***, and then the proposed approach will check the aggregated traffic for the existence of a DDoS attack. In this research, ***m*** is equal to 5 s based on experimental observation. In general, the proposed approach will report the result in terms of detection rate and false-positive rate six times (30/5).

6 Test Cases

The experiment examines the proposed approach's effectiveness in detecting low-rate and high-rate DDoS attacks against the controller targeting single or multiple hosts using two simulation cases with four different scenarios. The first case simulates a DDoS attack on an SDN controller from a single source with four different scenarios: (i) Single-source attack on a Single victim host with Low-rate attacks (SSL), (ii) Single-source attack on a Single victim host with High-rate attacks (SSH), (iii) Single-source attack on Multiple victim hosts with Low-rate attacks (SML), and (iv) Single-source attack on multiple victim hosts with High-rate attacks (SMH). The second case simulates DDoS attack on SDN controller from multiple sources with four different scenarios: (i) Multi-source attack on Single victim host with Low-rate attacks (MSL), (ii) Multi-source attack on Single victim host with High-rate attacks (MSH), (iii) Multi-source attack on Multiple victim hosts with Low-rate (MML), and (iv) Multi-source attack on Multiple victim hosts with High-rate attacks (MMH).

All scenarios were simulated on the Mininet platform to cover all possible DDoS attack iterations against the SDN controller, including a different number of attack sources, attack targets, and attack rates. At the same time, evaluate the proposed GEADDDC approach's efficiency to detect different types of attacks. Fig. 3 depicts the evaluation scenarios used to evaluate the proposed approach.

The first and second test scenarios also have different attack intensities. For single-source attacks, one host generates attack traffic while the rest generate regular traffic. In the case of multiple sources attack, three hosts are designated as attackers that generate attack traffic. Eq. (12) is used to calculate the intensity of attack traffic.

$$AttackTrafficRatio = \frac{AttackPacket}{PacketTotal} \times 100 \tag{12}$$

where *AttackPacket* represents the number of attack packets per second launched by the attacker within a specific window size. *PacketTotal* represents the total number of regular packets plus the total number of attack packets per second within a similar window size.

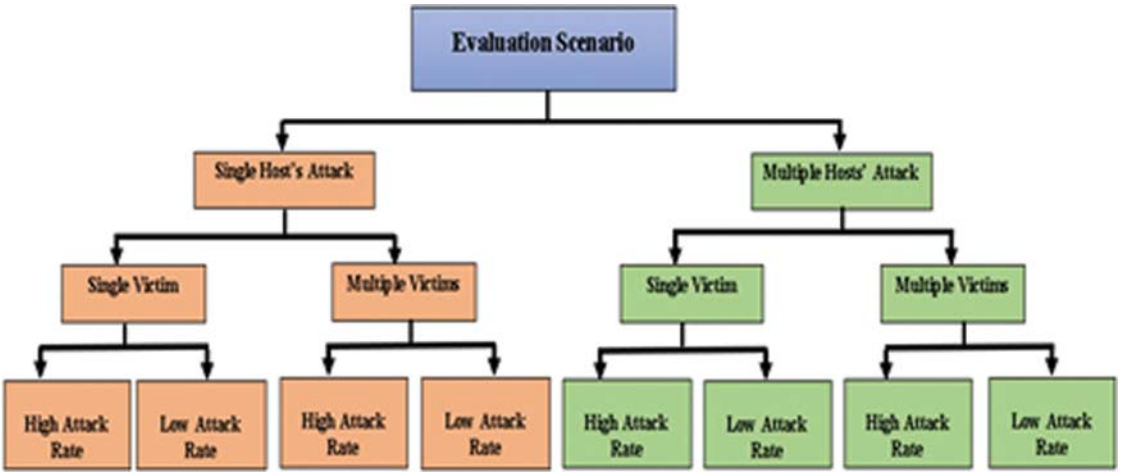

Figure 3: Test strategy

7 Results

This work's main objective is to increase the detection rate of DDoS attacks on the SDN controller and reduce the false-positive detection rate. Therefore, to quantify the proposed GEAD-DDC approach's performance, it is compared with an existing DDoS attack detection approach, the Early Detection of DDoS Attacks in Software Defined Networks Controller (EDDSC) approach [26]. The two approaches are compared in terms of average detection rate and false-positive detection rate for low-rate and high-rate DDoS attacks on the SDN controller. EDDSC is selected as a comparison since it uses the Shannon entropy metric to detect DDoS attacks. Each simulation scenario depends on the number of traffic packets per second during a specific time period t [32]. For results representations, the packet distribution is reported every 5-min (300 s) window. Therefore, the simulation will report 60 traffic flows, where each flow is aggregated in a 5-s window size. The average detection rate and a false-positive rate of 60 traffic flows is reported every five minutes for 30 min duration.

7.1 Single-Source Attack Test Scenarios

Single-source attack test scenarios measure the proposed approach's ability to detect both low and high-rate DDoS attacks against the SDN controller from a single host attack towards single or multiple victim hosts with a high detection rate and low false-positive rate. These scenarios are divided into four scenarios, as described in Section 7. Tab. 1 summarizes the number of normal traffic, attack traffic, and attack proportion from the network traffic for these scenarios collected in a 5-min window.

For the sake of results representations, the packet distribution is reported every five minutes (300 s) windows. Therefore, the proposed approach will report 60 traffic flows, where each flow is aggregated in a 5-s window size. The average detection rate and a false-positive rate of 60 traffic flows will be reported every five min. As shown in Tab. 1, the number of normal traffic sent in

five minutes is equal in all single host attack scenarios (18,900 packets). Meanwhile, the number of attack packets depends on the traffic rate, i.e., a low-rate or high-rate attack traffic. Based on Tab. 1, the number of attack packets in a low-rate DDoS attack is 1,500 packets within five min. Meanwhile, the number of attack packets in a high-rate DDoS attack is 10,000 packets. Thus, the attack traffic proportion for low-rate and high-rate attack traffic is 7% and 34%, respectively.

Table 1: Single host's attack scenarios characteristics

Scenarios/5 min	Total number of normal traffic	Total number of attack traffic	Attack percentage (%)
SSL	18900	1500	7
SML	18900	1500	7
SSH	18900	10000	34
SMH	18900	10000	34

7.2 Multi-Source Attack Scenarios

Multi-source attack test scenarios measure the proposed approach's ability to detect low-rate and high-rate DDoS attacks from multiple attackers that target single or multiple victims with a high detection rate and low false-positive rate. These scenarios are divided into four scenarios, as described in Section 7. Tab. 2 summarizes the number of normal traffic, attack traffic, and attack traffic proportion from the network traffic for these scenarios collected in a 5-min window.

Table 2: Multiple hosts attacks scenarios characteristics

Scenarios/5 min	Total number of packets in normal traffic	Total number of packets in attack traffic	Attack percentage (%)
MSL	18300	4500	19
MML	18300	4500	19
MSH	18300	30000	62
MMH	18300	30000	62

As shown in Tab. 2, the number of normal traffic packets sent in 5 min is equal in all multiple host attack scenarios, which are 18,300 packets. These packets are collected from the simulated network as explained in Section 5. For the sake of result representation, the packet distribution is reported for each 5-min time window. Therefore, the proposed approach will report 60 traffic flows where each flow is aggregated in a 5-s window. The average detection rate and a false-positive rate of 60 traffic flows will be reported for each 5-min window. Meanwhile, the total number of normal packets in a 5-min window is 18300 packets. Furthermore, the size of the attack traffic will be fluctuating due to the diversity in the attack traffic rates (e.g., low or high). The number of packets for a low-rate DDoS attack per second is 15 packets or 900 packets in one minute and 4,500 packets within five minutes. Meanwhile, the number of attack packets for a high-rate DDoS attack is 99 packets per second or 2,000 packets per minute and 30,000 packets per five

minutes. Thus, the attack traffic proportion for low-rate and high-rate attacks are 19% and 62%, respectively.

The approach's main aim is to detect low-rate and high-rate DDoS attacks against the controller triggered by multiple attackers that target single or multiple victim hosts effectively with a high detection rate and low false-positive rate. Fig. 4 shows the average detection rates and the average false-positive rates of the proposed GEADDDC approach for all scenarios.

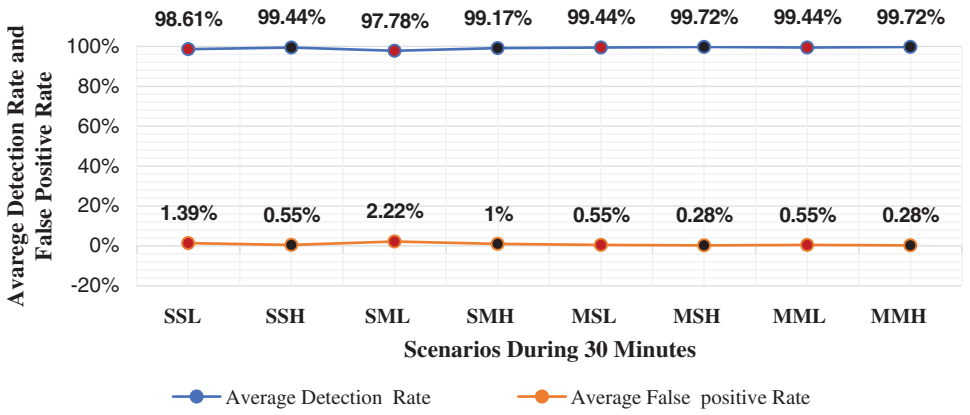

Figure 4: Summary of the average detection rates and false-positive rates using GEADDDC for all scenarios in 30 min

Fig. 4 shows the average detection rates and the average false-positive rates of the proposed GEADDDC approach for all eight test scenarios. The fluctuation of detection rates and false-positive rates is due to the variation of each scenario's attack traffic rates. The highest detection rate and lowest false-positive rate occurred when multiple attackers triggered a high-rate DDoS attack on single or multiple victims. Meanwhile, the lowest detection rate and the highest false-positive rate occurred when a single attacker triggered a low-rate DDoS attack on single or multiple victims. The detection rates' difference is because of the different amount of attack traffic received by the victims.

8 Comparison with Existing Approaches

The GEADDDC approach's performance has been compared with the EDDSC approach [26], which depends on the entropy method. Since entropy is the basis for all entropy variant approaches, it shares the common drawbacks of static threshold usage and single packet header feature usage. The comparison uses the simulation scenarios (refer to Section 7). The evaluation metrics used in the benchmarking are detection rate and false-positive rate, which are the same metrics used in the EDDSC approach. These evaluation metrics are also widely used to evaluate intrusion detection systems in detecting DDoS attacks. Tab. 3 below summarizes the average evaluation metrics results for all simulation scenarios using the GEADDDC approach and the EDDSC approach. Furthermore, Fig. 5 presents the enhancement of GEADDDC over the EDDSC approach regarding the detection rate and false-positive rate metrics.

Fig. 5 presents the improvements of GEADDDC over EDDSC in terms of average detection rate and average false-positive rate. GEADDDC approach enhances the average DDoS attack detection rates by 10.62% (SSL), 1.78% (SSH), 35.81% (SML), 3.36% (SMH), 5.72% (MSL),

0.88% (MSH), 9.49% (MML), and 0.73% (MMH). In addition, GEADDDC approach reduces the average false-positive rates by 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, and MMH, respectively.

Table 3: Average performance metrics of GEADDDC approach *vs*. EDDSC approach

Scenarios	Detection approach	Average detection rate (%)	Average false-positive rate (%)
SSL	EDDSC	89.14	14.19
	GEADDDC	98.61	1.39
SSH	EDDSC	97.70	2.30
	GEADDDC	99.44	0.55
SML	EDDSC	72.00	28.00
	GEADDDC	97.78	2.22
SMH	EDDSC	95.95	3.54
	GEADDDC	99.17	1.00
MSL	EDDSC	94.06	5.93
	GEADDDC	99.44	0.55
MSH	EDDSC	98.85	1.15
	GEADDDC	99.72	0.28
MML	EDDSC	90.82	9.18
	GEADDDC	99.44	0.55
MMH	EDDSC	99.00	1.00
	GEADDDC	99.72	0.28

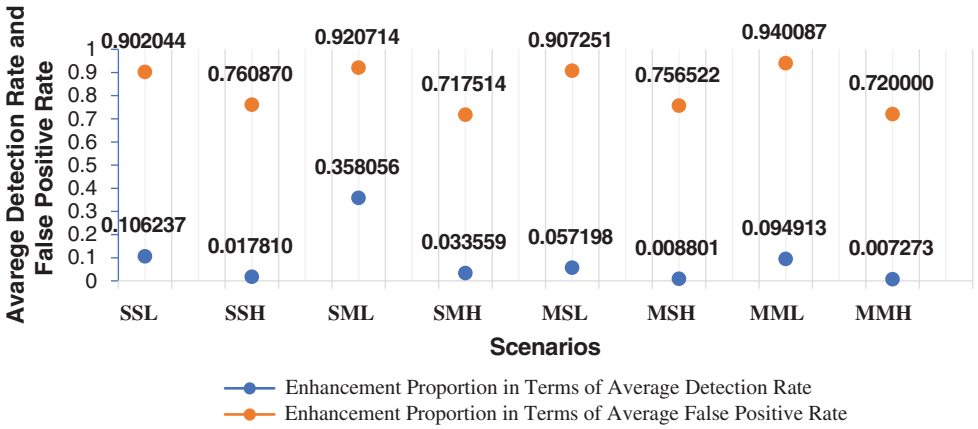

Figure 5: Average detection rate and average false-positive rate enhancement of GEADDDC over EDDSC approach for eight simulation scenarios

9 Significance of Enhancement

In the previous section, GEADDDC was compared with EDDSC in terms of detection rate and false-positive rate. The results reveal that GEADDDC has enhanced the detection rate and

false-positive rate compared with EDDSC. This section discusses whether the enhancement is significant or not using a T-test to measure the enhancement's significance. According to [25], the T-test compares the significant variance among the means of two groups. It considers one of the statistical inferences by using the parametric method that observes distribution parameters' inferences by the variables' probability distributions.

As mentioned, the T-test defines the variance's significance among the means of two groups by calculating the probability of error by specifying the error value P-value. $p < 0.05$ means there is a difference among two means groups (average detection rate and average false-positive rate) which is considered statistically significant. Otherwise, the difference between the means is not significant. Consequently, the hypothesis has been formulated for statistical significance as follows:

- H_0: GEADDDC does not significantly enhance the DDoS attack detection in terms of average detection rate and average false-positive rate.
- H_1: GEADDDC enhance the DDoS attack detection significantly in terms of average detection rate and average false-positive rate.

Tab. 4 summarizes the T-test findings, while Fig. 3 above exhibits the enhancement proportion for the detection rate and false-positive rate using the GEADDDC approach compared with the EDDSC approach.

Table 4: T-test findings

Detection rate	Metric	Scenario	P-value	Significance	H1	H0
GEADDDC with EDDSC	Average detection rate	SSL	0.002597882	Significant	Accepted	Rejected
		SSH	0.001090822	Significant	Accepted	Rejected
		SML	1.91422E-07	Significant	Accepted	Rejected
		SMH	0.001013595	Significant	Accepted	Rejected
		MSL	3.60435E-05	Significant	Accepted	Rejected
		MSH	0.018159544	Significant	Accepted	Rejected
		MML	0.000573114	Significant	Accepted	Rejected
		MMH	0.045966062	Significant	Accepted	Rejected
GEADDDC with EDDSC	Average false-positive rate	SSL	0.002593721	Significant	Accepted	Rejected
		SSH	0.001056421	Significant	Accepted	Rejected
		SML	1.92711E-07	Significant	Accepted	Rejected
		SMH	0.00029573	Significant	Accepted	Rejected
		MSL	5.07866E-05	Significant	Accepted	Rejected
		MSH	0.017749527	Significant	Accepted	Rejected
		MML	0.000568622	Significant	Accepted	Rejected
		MMH	0.04511974	Significant	Accepted	Rejected

As shown in Tab. 4, the T-test results reveal that the GEADDDC approach has significantly improved the existing approach in terms of the detection rate and false-positive rate.

10 Discussion

GEADDDC was proposed as an approach to detect low and high-rate DDoS attacks against SDN controller regardless of attack sources (single or multi-source attacks) and targets (single or multiple victim hosts) with high detection rate and low false-positive rate. The proposed GEADDDC approach was evaluated using eight different simulation scenarios (experiment plans) to measure two metrics: average detection rate and average false-positive rate. Then, the results were compared with the EDDSC approach using the same configuration in all simulation scenarios to determine whether the proposed approach achieves the stated aims (i.e., high detection rate and reduce false-positive rate).

The experiment results prove that the proposed GEADDDC approach performs better than the existing EDDSC approach in detecting DDoS attacks on the SDN controller. Consequently, GEADDDC has a higher detection rate and lower false-positive rate in detecting the attack than EDDSC.

Tab. 3 revealed the comparison proposed approach results that fulfill a high average detection rate and a less false-positive rate when using SSL, SSH, SML, SMH, MSL, MSH, MML, and MMH. For low and high-rate DDoS attacks against the SDN controller targeting a single victim or multiple victims, the proposed approach collects new incoming traffic flow statistics more efficiently than other existing approaches by using two packets header features. The use of two packet header features increases the network statistics available for decision-making. On the contrary, the reliance on a single packet header by the EDDSC approach limits network traffic statistics, which results in a lower DDoS attack detection rate of EDDSC. The following subsections discuss the results obtained in detail.

10.1 Detection Rate

The experiment results reveal that the GEADDDC approach has an accurate DDoS attack detection based on the detection rate; thus, it fulfills the requirement of a high detection rate of low/high-rate DDoS attacks against the SDN controller. GEADDDC approach is compared with the existing EDDSC approach, which uses the entropy method; and is considered the reference for entropy variant-based detection approaches.

The comparison results reveal that the EDDSC approach has a moderate to high attack detection rate for low-rate and high-rate DDoS attacks against the SDN controller with multiple targets compared with the proposed approach for all simulation scenarios. The reasons are that the EDDSC approach uses an entropy method that depends on one packet header feature (i.e., destination IP address) and relies on a static threshold to detect DDoS attacks. Furthermore, EDDSC fails to detect the presence of both low-rate and high-rate DDoS attacks with single or multiple targets in the network traffic flow. However, the detection rate is lower when the low-rate DDoS attack targeted multiple victim hosts (i.e., 72% and 90.82% for SML and MML scenarios, respectively.

In contrast, the proposed approach depends on two packet header features (source IP and destination IP addresses), allowing it to collect more network statistics on incoming traffic flows. The extra information available provides more accurate attack detection by the generalized Rényi entropy method. The proposed method measures the network traffic randomness resulting from DDoS attacks. High traffic randomness is one of the symptoms of DDoS attacks that spoofed IP addresses. Also, the proposed approach uses a dynamic threshold to enhance the detection of both low-rate and high-rate DDoS attacks that target single and multiple victim hosts. The

threshold depends on the number of incoming traffic flows towards the controller within a specific time, attack traffic rate toward the victim, and Rényi joint entropy value within a specific time by adapting the Exponentially Weighted Moving Average (EWMA) method. Consequently, a comparison of GEADDDC and EDDSC is necessary to evaluate the attack detection performance. Fig. 6 shows the comparison of the GEADDDC approach and EDDSC approach in terms of average detection rate.

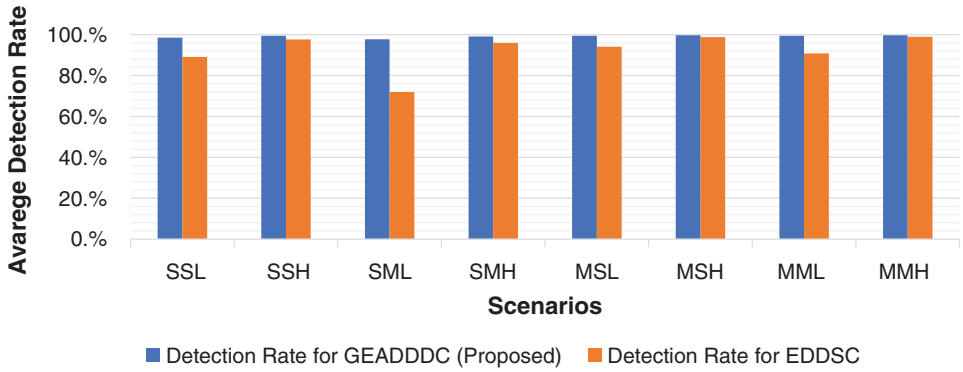

Figure 6: Comparison of average detection rate of GEADDDC and EDDSC using simulation scenarios

Fig. 6 shows that the GEADDDC approach has higher detection rates in all scenarios compared to the EDDSC approach. The high detection rates highlight the proposed approach's improved performance in terms of attack detection rate, especially in detecting low-rate DDoS attacks on multiple targets.

10.2 False-Positive Rate

EDDSC approach has high false-positive rates in all scenarios compared with the proposed approach in detecting both low-rate and high-rate DDoS attacks against the controller that targets single or multiple victim hosts. The comparison in Tab. 3 reveals that GEADDDC approach had reduced the false-positive rates in all scenarios (1.39%, 0.55%, 2.22%, 1.00%, 0.55%, 0.28%, 0.55%, 0.28%) compared to EDDSC approach.

The reduction in the false-positive rate is due to dynamic threshold usage instead of a static threshold. A dynamic threshold is more flexible and improves DDoS attack detection significantly because it can detect low-rate and high-rate DDoS attack traffic. Furthermore, the proposed approach utilizes the Rényi Joint Entropy algorithm, which depends on two packet header features instead of one, to analyze incoming traffic flow statistics for the randomness of incoming traffic. Fig. 7 shows the comparison between the GEADDDC approach and EDDSC approach in terms of average false-positive rates.

Fig. 7 clearly shows that the GEADDDC approach outperformed EDDSC with reduced average false-positive rates in all scenarios. The lowest average false-positive rate in this figure highlights the performance of the proposed approach for both low-rate and high-rate DDoS attacks that target single or multiple victims. The high average false-positive rate of EDDSC (i.e., 28 %) is mainly due to static threshold usage and reliance on a single packet header feature (i.e., destination IP address).

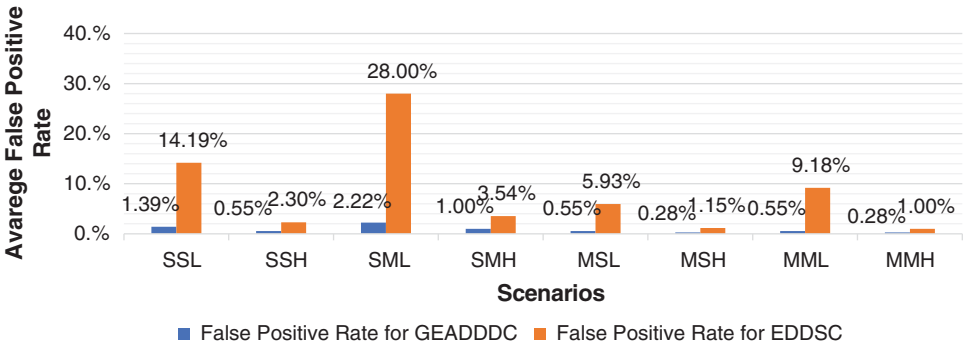

Figure 7: Comparison of average false-positive rate of GEADDDC and EDDSC using simulation scenarios

11 Conclusion

Centralized network management and programmable network control are possible in the SDN environment because of the network data plane's decoupling from the control plane. However, a massive and sudden increase in incoming traffic from multiple sources at varying rates could overload the SDN controller that leads to resource exhaustion. Consequently, attackers could exploit certain SDN features to launch DDoS attacks towards the controller. DDoS attacks could severely affect the controller's operation resulting in reduced performance or collapse of the whole SDN network. Therefore, finding an effective detection approach to detect DDoS attacks using traffic flow statistics must be considered.

Unfortunately, most existing detection approaches to detect DDoS attacks against the controller with single or multiple targets have difficulties detecting low-rate and high-rate attacks with high accuracy and low false-positive rate. Therefore, there is a need for an effective approach to detect both low-rate and high-rate DDoS attacks against the SDN controller regardless of the number of targets and the number of attackers with high accuracy and low false-positive rate.

Generalized Entropy-based Approach with a dynamic threshold to detect DDoS attacks against a software-defined networking Controller (GEADDDC) has been proposed in this research to address the need. GEADDDC has four main stages: (i) data collection and preprocessing, (ii) Rényi joint entropy calculation, (iii) dynamic threshold, and (iv) rule-based DDoS attack detection stages. The experiment results prove that the GEADDDC effectively detects low-rate and high-rate DDoS attacks against the SDN controller that targets single or multiple victims. GEADDDC achieved it by generalizing the Rényi joint entropy to calculate incoming traffic's randomness using a statistic analyzer at the controller. Some potential future work includes exploring the feasibility of detecting additional types of DDoS attacks, such as TCP sync, ICMP, and HTTP flooding attacks; detecting DDoS attacks during flash crowd events; and integrating the proposed approach with other network security approaches.

Acknowledgement: We would like to express our gratitude to Universiti Sains Malaysia (USM) for all the support and facilities that enable the completion of this research.

Funding Statement: This work was supported by Universiti Sains Malaysia under external grant (Grant Number 304/PNAV/650958/U154).

Conflict of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. S. Sahoo, D. Puthal, M. Tiwary, J. J. P. C. Rodrigues, B. Sahoo *et al.,* "An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics," *Future Generation Computer Systems*, vol. 89, no. 11, pp. 685–697, 2018.

[2] H. Farhady, H. Lee and A. Nakao, "Software-Defined Networking: A survey," *Computer Networks*, vol. 81, no. 14, pp. 79–95, 2015.

[3] S. A. Scott-Hayward, S. A. Natarajan and S. B. Sezer, "Survey of security in software defined networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 623–654, 2015.

[4] R. Wang, Z. Jia and L. Ju, "An entropy-based distributed DDoS detection mechanism in software-defined networking," in *IEEE Trustcom/BigDataSE/ISPA*, Washington, NW, US: IEEE, vol. 1, pp. 310–317, 2015.

[5] A. Hussein, I. H. Elhajj, A. Chehab and A. Kayssi, "SDN security plane: An architecture for resilient security services," in *IEEE Int. Conf. on Cloud Engineering Workshop*, Berlin, Germany, pp. 54–59, 2016.

[6] I. Ahmad, S. Namal, M. Ylianttila and A. Gurtov, "Security in software defined networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2317–2346, 2015.

[7] M. A. ALAdaileh, M. Anbar, I. H. Hasbullah, C. Y. Wey and Y. k. Sanjalawe, "Detection techniques of distributed denial of service attacks on software-defined networking controller—A review," *IEEE Access*, vol. 8, no. 13, pp. 143985–143995, 2020.

[8] A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi, H. Sastry and S. Goundar, "DDoS attacks, new DDoS taxonomy and mitigation solutions-A survey," in *Int. Conf. on Signal Processing, Communication, Power and Embedded System*, Odisha, India, pp. 793–798, 2016.

[9] Y. Xu and Y. Liu, "DDoS attack detection under SDN context," in *IEEE INFOCOM 2016-the 35th Annual IEEE Int. Conf. on Computer Communications*, San Francisco, CA, US, vol. 2016, 2016.

[10] R. Masoudi and A. Ghaffari, "Software defined networks: A survey," *Journal of Network and computer Applicationst. Applications*, vol. 67, no. 15, pp. 1–25, 2016.

[11] C. Bouras, A. Kollia and A. Papazois, "SDN & NFV in 5G: Advancements and challenges," in *20th Conf. on Innovations in Clouds, Internet and Networks*, Paris, France, pp. 107–111, 2017.

[12] P. T. Duy, D. Thi, T. Hien and V. Pham, "A role-based statistical mechanism for DDoS attack detection in SDN," in *5th NAFOSTED Conf. on Information and Computer Science*, Vietnam, pp. 177–182, 2018.

[13] X. Huang, X. Du and B. Song, "An effective DDoS defense scheme for SDN," in *IEEE Int. Conf. on Communications*, Paris, France, pp. 1–6, 2017.

[14] D. He, S. Chan, X. Ni and M. Guizani, "Software-defined-networking-enabled traffic anomaly detection and mitigation," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1890–1898, 2017.

[15] H. Peng, Z. Sun, X. Zhao, S. Tan and Z. Sun, "A detection method for anomaly flow in software defined network," *IEEE Access*, vol. 6, pp. 27809–27817, 2018.

[16] O. Salman, I. H. Elhajj, A. Kayssi and A. Chehab, "SDN controllers: A comparative study," in *18th Mediterranean Electrotechnical Conf.*, Cyprus, pp. 1–6, 2016.

[17] A. Abdelaziz, A. Fong, A. Gani, U. Garba, S. Khan *et al.,* "Distributed controller clustering in software defined networks," *PLoS One*, vol. 12, no. 4, pp. 1–19, 2017.

[18] M. A. Al-adaileh, M. Anbar, Y. Chong and A. Al-ani, "Proposed statistical-based approach for detecting distributed denial of service against the controller of software defined network (SADDCS)," in *MATEC Web of Conf., MATEC Web Conference*, Anyer, Indonesia, vol. 218, pp. 1–8, 2018.

[19] Y. Jiang, X. Zhang, Q. Zhou and Z. Cheng, "An entropy-based DDoS defense mechanism in Software Defined Networks," in *Int. Conf. on Communicatins and Networking in China*, Cham, China: Springer, vol. 1, pp. 169–178, 2016.

[20] J. Mao, W. Deng and F. Shen, "DDoS flooding attack detection based on Joint-entropy with multiple traffic features," in *17th IEEE Int. Conf. on Trust, Security And Privacy In Computing And Communications/12th IEEE Int. Conf. on Big Data Science And Engineering*, Cham, New York, US: Springer, vol. 11, pp. 237–243, 2018.

[21] 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*, vol. 2018, no. 4, pp. 1–8, 2018.

[22] P. Kumar, M. Tripathi, A. Nehra, M. Conti and C. Lal, "SAFETY: Early detection and mitigation of TCP SYN flood utilizing entropy in SDN," *IEEE Transactions on Network and Service Management*, vol. 15, no. 4, pp. 1545–1559, 2018.

[23] J. Cui, J. He, Y. Xu and H. Zhong, "TDDAD: Time-based detection and defense scheme against DDoS attack on SDN controller," in *Australasian Conf. on Information Security and Privacy*, Perth, WA, Australia: Springer International Publishing, vol. 10946, 2018.

[24] Y. Wang, T. Hu, G. Tang, J. Xie and J. Lu, "SGS: Safe-guard scheme for protecting control plane against DDoS attacks in software-defined networking," *IEEE Access*, vol. 7, no. 11, pp. 34699–34710, 2019.

[25] M. Kia, "Early detection and mitigation of DDoS attacks in software defined networks," Master's dissertation. Ryerson University of Toronto, ON, Canada, 2015.

[26] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against software defined network controllers," *Journal of Network and Systems Management*, vol. 26, no. 3, pp. 573–591, 2018.

[27] M. Masi, "A step beyond Tsallis and Rényi entropies," *Physics Letters A*, vol. 338, no. 3–5, pp. 217–224, 2005.

[28] P. Bereziński, B. Jasiul and M. Szpyrka, "An entropy-based network anomaly detection method," *Entropy*, vol. 17, no. 4, pp. 2367–2408, 2015.

[29] S. Khan, A. Gani, A. W. Abdul Wahab and P. K. Singh, "Feature selection of denial-of-service attacks using entropy and granular computing," *Arabian Journal for Science and Engineering*, vol. 43, no. 2, pp. 499–508, 2017.

[30] H. Zubaydi, M. Anbar and Wey, "Review on detection techniques against DDoS attacks on a software-defined networking controller," in *2017 Palestinian Int. Conf. on Information and Communication Technology*, Gaza, Palestine: IEEE, pp. 10–16, 2017.

[31] A. Bahashwan, M. Anbar and N. Abdullah, "New architecture design of cloud computing using software defined networking and network function virtualization technology," in *Int. Conf. of Reliable Information and Communication Technology*, Cham: Springer, pp. 705–713, 2019.

[32] N. Hoque, D. K. Bhattacharyya and J. K. Kalita, "FFSc: A novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis," in *2016 8th Int. Conf. on Communication Systems and Networks*, Bangalore, India, vol. 9, pp. 2032–2041, 2016.