applied sciences

MDPI

Article

Effectiveness of an Entropy-Based Approach for Detecting Low- and High-Rate DDoS Attacks against the SDN Controller: Experimental Analysis

Mohammad Adnan Aladaileh [1], Mohammed Anbar [1,*], Ahmed J. Hintaw [2], Iznan H. Hasbullah [1], Abdullah Ahmed Bahashwan [1], Taief Alaa Al-Amiedy [1] and Dyala R. Ibrahim [3]

[1] National Advanced IPv6 Centre of Excellence, Universiti Sains Malaysia, Gelugor 11800, Malaysia
[2] Department of Computer Techniques Engineering, Alsafwa University College, Karbala 56001, Iraq
[3] Cyber Security Department, Amman Arab University, Amman 11953, Jordan
* Correspondence: anbar@usm.my

Abstract: Software-defined networking (SDN) is a unique network architecture isolating the network control plane from the data plane, offering programmable elastic features that allow network operators to monitor their networks and efficiently manage them. However, the new technology is security deficient. A DDoS attack is one of the common attacks that threaten SDN controllers, leading to the degradation or even collapse of the entire SDN network. Entropy-based approaches and their variants are considered the most efficient approaches to detecting DDoS attacks on SDN controllers. Therefore, this work analyzes the feasibility and impacts of an entropy-based DDoS attack detection approach for detecting low-rate and high-rate DDoS attacks against the controller, measured in terms of detection rate (DR) and false-positive rate (FPR), triggered by a single or multiple host attacks targeting a single or multiple victims. Eight simulation scenarios, representing low and high DDoS attack traffic rates on the controller, have been used to evaluate an entropy-based DDoS attack detection approach. The experimental results reveal that the entropy-based approach enhances the average DR for detecting high-rate DDoS attack traffic compared with low-rate DDoS attack traffic by 6.25%, 20.26%, 6.74%, and 8.81%. In addition, it reduces the average FPRs for detecting a high DDoS attack traffic rate compared with a low DDoS attack traffic rate by 67.68%, 77.54%, 66.94%, and 64.81.

Keywords: software-defined networking; entropy; attack detection; controller; dynamic threshold; static threshold; distributed denial of service

check for updates

Citation: Aladaileh, M.A.; Anbar, M.; Hintaw, A.J.; Hasbullah, I.H.; Bahashwan, A.A.; Al-Amiedy, T.A.; Ibrahim, D.R. Effectiveness of an Entropy-Based Approach for Detecting Low- and High-Rate DDoS Attacks against the SDN Controller: Experimental Analysis. *Appl. Sci.* **2023**, *13*, 775. https://doi.org/10.3390/app13020775

Academic Editor: Christos Bouras

Received: 21 November 2022
Revised: 31 December 2022
Accepted: 2 January 2023
Published: 5 January 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

SDN is among the most innovative communication technologies developed and will eventually replace conventional networks in managing network traffic flows. In addition, SDN assists data centers in controlling costs by boosting network traffic management efficiency and entirely controlling network features to meet ever-changing network business needs by isolating the data layer from the control layer [1]. The controller allows applications to develop programmes to manage network flow [2].

SDN has many advantageous features, such as network programmability, enabling the fast deployment of SDN networks, and dynamic management. In contrast, traditional networks take longer to deploy and face challenges in meeting requirements to add a new host to the network [3,4]. Figure 1 compares SDN and a traditional network architecture.

The controller is an essential feature of the SDN architecture, which is responsible for controlling the entire network operations through persistent monitoring of network devices and routing network traffic flow by generating new rules or modifying existing table instructions in the switch according to new incoming packet features and the packet flow behavior [5]. Further, an SDN controller has proactive or reactive modes to deal with network traffic packets. In their attempt to secure an SDN network from DDoS attacks,

researchers [6] have discovered that preinstalling rules in the switch table to process incoming packets in a proactive mode has a more significant effect on SDN performance than a reactive mode. In contrast, in a reactive mode, rules are created and installed inside a switch table whenever incoming packets match the switch table's rules [7].

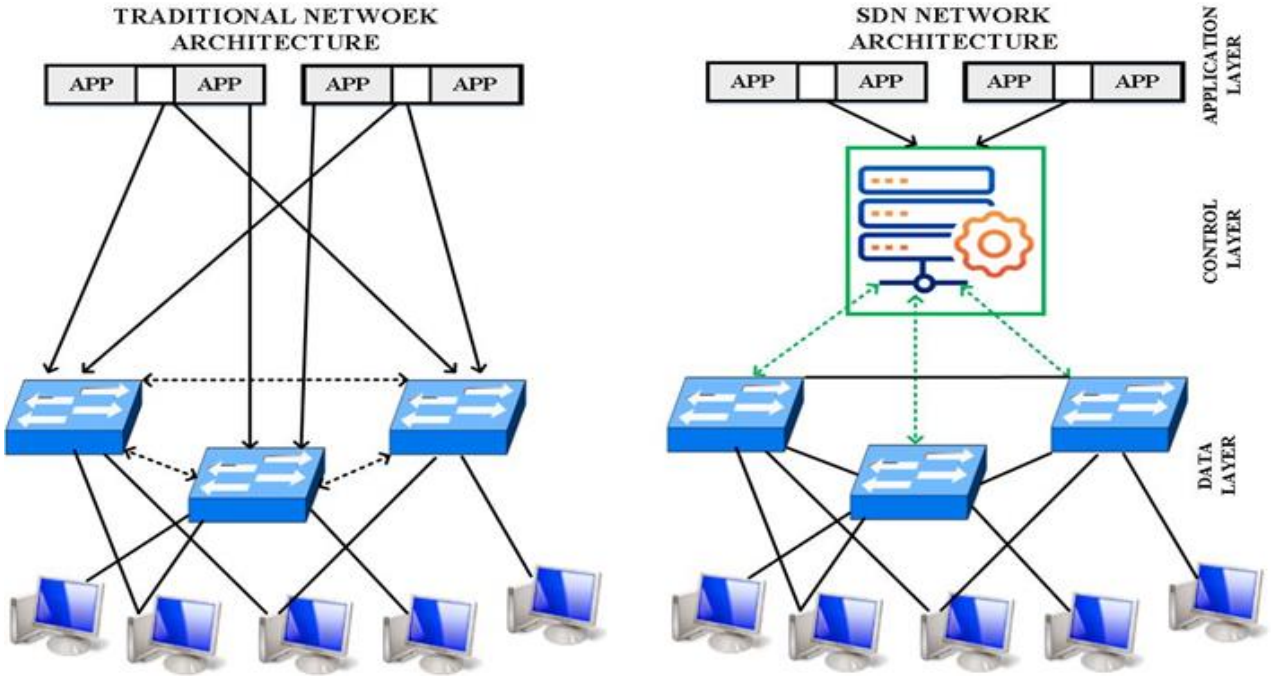


Figure 1. SDN vs. traditional network architecture.

Additionally, the controller has various roles, employing different modules to collect statistical information concerning network traffic and identify tasks for each network component [8]. Furthermore, an SDN controller gathers the required information from the network packets and then applies additional analysis to discover DDoS attacks. Nonetheless, a centralized controller has challenges and issues that affect network performance in terms of security, reliability, and scalability [9].

The integration of an SDN controller in the network could potentially bring many new security challenges, especially when the centralized controller acts as an operating system. Any unaddressed threat to the centralized controller may lead to a network breakdown. For instance, in DDoS attack scenarios, the attackers flood a network by sending a massive number of spoofed IP packets to the controller, thereby congesting and overwhelming the controller, resulting in the exhaustion of network resources and the collapse of the entire SDN networks [10].

Because security is an essential feature of any network, coupled with the importance of SDN controllers in the SDN architecture, network security has received much attention from network security researchers [11]. Although SDN offers several advantages that contribute to protecting a network from malicious attacks, its flexibility and programmability attract the attention of adversaries seeking to disrupt or destroy the network by targeting the SDN controller [12]. This paper evaluates the effectiveness of the entropy-based DDoS attack detection method, focusing on the ability to detect attacks with varying attack traffic rates (such as a high attack traffic rate and a low attack traffic rate) targeted directly at the controller and triggered by a single or multiple attack hosts that target a single or multiple victims.

Security challenges in SDN are increasing, specifically in a controller. A DDoS attack is among the most dangerous attacks that could threaten an SDN controller [13] due to its ability to cripple an entire network. The basic idea of a DDoS attack is that attackers send enormous amounts of packets to unique IP address destinations from distinct IP address sources to flood entire network devices, preventing legitimate users from obtaining

their desired computing services [14]. DDoS attackers often spoof the source IP addresses by launching attacks from multiple forged source IP addresses to evade detection [15]. Attackers may also use different traffic rates (i.e., low and high rates) to launch their attacks, making it difficult for the controller to differentiate between attack traffic flow and regular network traffic flow. Therefore, this study aims to detect DDoS attacks targeting the SDN controller. The study's contribution is an analysis of the impact of an entropy-based mechanism to detect low-rate and high-rate DDoS attacks that multiple or single hosts trigger toward a single or multiple host victims with a high DR and a low FPR in various network scenarios.

The remainder of the study is structured as follows: Section 2 presents related work, followed by Section 3, which explains DDoS attack behavior in the SDN. The details of an entropy-based DDoS attack detection approach are in Section 4. Section 5 presents the results and the discussion. Section 6 provides a comparative analysis, and Section 7 concludes this paper with insights on future research directions.

2. Related Work

This section presents relevant studies that proposed detecting DDoS attacks in SDN based on the entropy method.

Fan et al. [16] suggested a fusion entropy method for calculating the randomness of network traffic, which was evaluated and verified using eight simulation scenarios [3]. The proposed approach detects DDoS attacks by comparing an entropy value with a threshold value. The suggested method sets a threshold, which assists in increasing DRs and lowering FPRs. However, the dataset and the number of features used to detect DDoS attacks were unclear, and this study only focused on high-rate attacks.

Mousavi et al. [17] proposed an entropy-based detection method that analyzes network traffic flows to ascertain the probability of the incoming packets' flow in the controller. This approach appears to be lightweight and effective in spotting early-stage threats. Nonetheless, while the suggested method seeks to detect attacks as early as possible, significant drawbacks limit its effectiveness since it has trouble detecting varying rates of DDoS attacks with a high DR and a low FPR.

A DDoS attack can be seen as an outlier by the variation in the probability distribution of incoming network traffic flow. Therefore, Sahoo et al. [18] proposed an attack detection method by combining information distance and generalized entropy to detect low-rate DDoS attacks on the controller. The proposed method experiment showed that it effectively detects low DDoS attack traffic rates by combining generalized entropy with the information distance. However, the proposed method was not very successful at detecting high traffic rates because of the fluctuations in attack traffic rates of the network traffic flow.

Perez-Diaz et al. [19] presented a flexible method to detect and mitigate low-rate and high-rate DDoS attack traffic in SDN networks with similar behavior to normal traffic. The proposed strategy relies on intrusion detection and prevention systems (IDS and IPS). The proposed approach employs six machine learning models for DDoS classification in the IDS. One issue is that the proposed method has a fixed threshold that is ineffective in detecting low-rate DDoS attack traffic against multiple victims.

Finally, Jiang et al. [20] proposed an entropy-based DDoS defense mechanism (EDDM) that thwarts attacks on legitimate network users in flash crowd scenarios by tracking attack traffic flows. The EDDM consists of three phases drawing upon traffic statistics gathered inside a given window size employed to calculate an entropy value for detecting DDoS attacks. The entropy value in sFlow is compared with a static threshold to determine the traffic packet rate targeting a single victim. However, a lag exists in processing new packets, and the multiple-victim attack detection accuracy is low.

Table 1 summarizes related work on attack detection methods and analyzes their weaknesses and strengths according to their approaches.

Table 1. Summary of work related to DDoS detection approaches against SDN.

Author (Year)	Method	Strengths	Drawbacks
Fan et al. [16]	Entropy	- Detecting high DDoS attack traffic rate with a high detection rate	- Low attack detection rate for detecting low-rate attack traffic
Mousavi et al. [17]	Entropy	- Lightweight method - Detecting high-rate DDoS attack traffic with a high detection rate	- Low attack detection rate for detecting low-rate attack traffic
Sahoo et al. [18]	Generalized entropy	- Detects high-rate DDoS attacks targeting a single victim efficiently	- False-positive rate increases during different attack traffic rates - Low attack detection rate for detecting low-rate attack traffic targeting multiple victims
Perez-Diaz et al. [19]	IDS based on machine learning models	- DDoS attack classification	- Ineffective in identifying low-rate DDoS attacks that target multiple victims
Jiang et al. [20]	Entropy	- Avoids the dropping of legitimate packets	- Delay in processing new packets - Low attack detection rate for detecting low-rate attack traffic that targets multiple victims

3. DDoS Attack Behavior

A low-rate DDoS attack has characteristics similar to normal network traffic in traffic patterns [21]. Conversely, a high-rate DDoS attack is distinguishable from normal traffic. In addition, low-rate DDoS attacks targeting multiple or single victims are more challenging to detect with low FPR and high DR.

In DDoS attack scenarios, an attacker typically spoofs the source IP addresses of the generated packets with many unique IP addresses, resulting in many spoofed packets without matching rules in the switch table's flow entries (flow table). Consequently, the process forces the switch to forward all the packets to a controller for additional processing to develop new instructions for dealing with the incoming packets. Making matters worse, an attacker constantly generates and sends new spoofed packets into the network until the SDN controller becomes exhausted.

As for the controller's performance under a DDoS attack, the efficiency is remarkably affected due to treating and managing all new incoming packets that lead to denying legitimate users from accessing services or resources, which could result in an entire SDN network's collapse [5].

The role of a detection approach is to identify DDoS attack behavior using observations of the entire SDN network traffic flows from the hosts toward the destination. However,

other existing detection approaches might observe all the network traffic flow incorrectly, which is one of the reasons for their inability to detect low-rate and high-rate DDoS attacks with a high DR and a low FPR [22]. Therefore, to overcome the abovementioned issues, the incoming network traffic must be collected from the hosts to be analyzed and used as input for the detection approach. This study also aims to analyze the entropy algorithm's impact on detecting low-rate and high-rate DDoS attacks against the SDN controller that target a single and multiple victims' hosts with a high DR and a low FPR.

4. Entropy-Based DDoS Attack Detection Approach

Entropy is an algorithm for calculating the probability of a random variable occurring during a specific period [15,23]. The entropy algorithm is most commonly used to detect DDoS attacks based on analyzing traffic statistics collected from network traffic flows [24]. This study employed the entropy algorithm to compute network traffic packet randomness by using one packet header feature of the network traffic flow, like the destination IP and IP address and the source or destination port. In addition, entropy-based statistics are utilized for analyzing network traffic flows based on the packet header features to detect abnormal packets in the network traffic flows [17,24].

Randomness is measured during the abnormal packet detection stage to calculate the probability of an attack in the network. The attack probability is calculated as a percentage, as shown in Equation (1):

$$p_{xi} = \frac{x_i}{n} \tag{1}$$

where x_i is the frequency of each unique source IP address of the total number among all source IP addresses that occurred in the total number of n packets during time t.

As stated before, an entropy algorithm is a statistical means to compute incoming packet randomness in network traffic flows to detect DDoS attacks of various traffic rates (i.e., low or high attack traffic rate), which is this work's primary goal. The entropy algorithm depends on the probability calculation of the source IP address, and the presence of randomness in the behavior of packets is considered a sign of DDoS attacks. The formula for the entropy-based detection approach is expressed in Equation (2) [25].

$$H(X_i) = -\sum_{i=1}^{n} P(x_i) \log_2 P(x_i) \tag{2}$$

$P(x_i)$ denotes the probability of a specific feature from the packet header features within the time interval t, n represents the total number of features in network traffic at a given time, and $H(x_i)$ denotes the entropy value. In the DDoS attack detection approach, the entropy calculating the incoming traffic packets' probability to the source IP address based on the IP frequencies $i = 1, 2, \ldots, n$, $P(x_i) > 0$.

Attack and normal traffic have different probability distributions derived by computing the source of packet header features' probabilities and are considered a variable of entropy, which, in turn, is used to measure the randomness and uncertainty in the IP source address variable. The higher the uncertainty, the higher the entropy, which is a factor contributing to detecting DDoS attacks in a network. Indeed, the probability is considered an indicator of an attack against the controller. Thus, if a controller receives a large volume of packets, the probability value will be high, indicating abnormal behavior in the network traffic. Therefore, the probabilities of source IP addresses $P(x_i)$ that launch the attack towards a distinct destination in 5 s are used as input to calculate the entropy value using Equation (2). Figure 2 presents the entropy-based detection approach's flowchart.

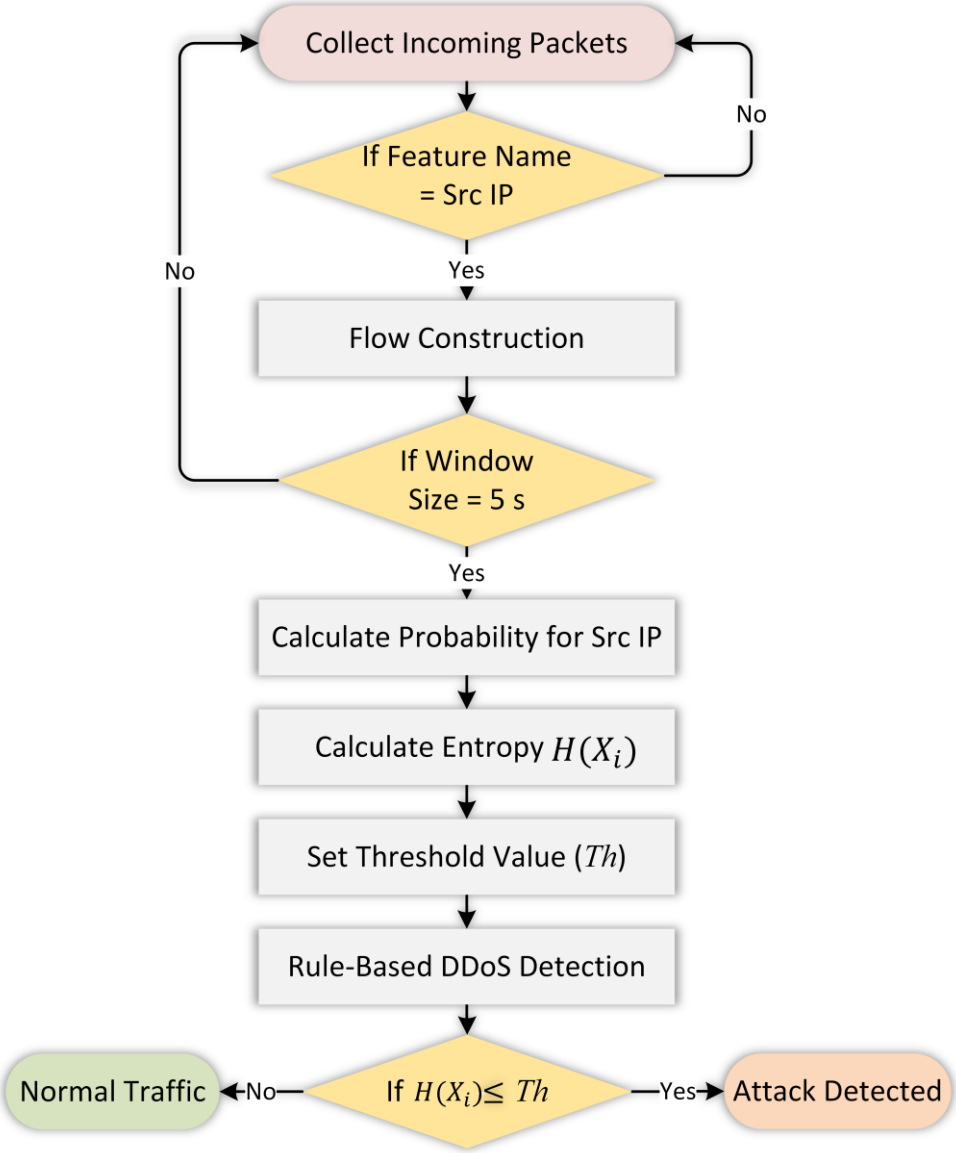


Figure 2. Detection approach process.

5. Experimental Scenarios

This work analyzed the impact of an entropy-based approach in detecting DDoS attacks using a statistical traffic analyzer. The analyzer calculates entropy that depends on one feature of the packet header features within a specific time t (window size), which is compared with a predefined threshold via preparation and configuration of multiple simulation scenarios and later evaluated using various evaluation metrics.

The primary purpose of analyzing the impact of the entropy-based technique is to evaluate and detect various DDoS attack traffic rates (high or low attack traffic rates) against an SDN controller with high DRs and low FPRs. Therefore, this section presents the simulation scenarios employed to assess the entropy-based approach's performance and analyze the entropy method's impact on detecting a low DDoS attack traffic rate compared with a high DDoS attack traffic rate.

The entropy-based detection approach's performance assessment employs eight simulation scenarios with low and high attack traffic rates [26]. Based on this, there are different assumptions regarding the single host's attack scenarios and the multiple hosts' attack scenarios against a controller targeting a single or multiple victim(s).

Each simulation scenario run lasts 30 min, with the average result recorded every 5 min. Thus, the window size is divided into n slots, and each slot is equal to m seconds. The computation of the time slot is shown in Equation (3) [3].

$$Time\ slots(n) = (5 * 60)/m = 300/5 = 60 \quad (3)$$

In addition, the network traffic is aggregated every m seconds, where m is a configurable variable. Hence, the entropy-based detection method is run every 5 s to check for the existence of DDoS attacks in the aggregated traffic. This work determined the parameter m = 5 s through trial-and-error experiments.

In the scenarios, a single or multiple hosts' attacks triggered low-rate and high-rate DDoS attacks against the controller targeting multiple or single victim hosts. The attacker used a unique source IP address to launch a DDoS attack against the victim(s). Based on that, a low DDoS attack traffic rate was sent at a rate of 0.2 s per packet, with a total number of attack packets sent in 1 s equal to 5 packets for a single host's attack and 15 packets for multiple hosts' attack. Meanwhile, a high DDoS attack traffic rate was sent at a rate of 0.03 s per packet, meaning that the total number of attack packets sent in 1 s equals 33 packets triggered by a single host's attack, while multiple hosts' DDoS attacks will send 166 packets to the victim (S). Table 2 shows the distributed number of packets for high- and low-rate DDoS attack traffic and normal traffic during 1 s.

Table 2. Distribution of packets' numbers for various DDoS attack traffic rates with the normal traffic.

Attack Source	Number of Low DDoS Attack Traffic (5 s/Packet per Attacker's Host)	Number of High DDoS Attack Traffic (5 s/Packet per Attacker's Host)	Number of Normal Packets (5 s/Packet per Legitimate Host)
Single Host's Attack	5	33	63
Multiple Hosts' Attack	15	166	61

The experiment was conducted on a workstation running a 4.20 GHz Intel® Core i7-7700 CPU with 16 GB of RAM and a 250 GB SSD hard drive running the Ubuntu Linux 14.04 operating system. The network topology consisted of 64 hosts, an OpenFlow switch, and a POX controller. Additionally, Mininet version 3.7 (32-bit) virtualized the prototype network scenarios to emulate network elements.

6. Results and Discussion

This section analyzes the impact of the entropy-based low-rate and high-rate DDoS attack detection approach regarding DR and FPR and discusses the experimental results obtained by implementing the DDoS attack detection approach in the following scenarios: (i) a single host with low-rate attack traffic against a single victim host (LSS), (ii) a single host with a high attack traffic rate against a single victim host (LSM), (iii) a single host with a high attack traffic rate against multiple victim hosts (LMS), (iv) a single host with a low attack traffic rate against multiple victim hosts (LMM), (v) multiple hosts with low attack traffic against a single victim host (HSS), (vi) multiple hosts with high attack traffic against a single victim host (HSM), (vii) multiple hosts with high attack traffic against a single victim host (HMS), and (viii) multiple hosts with high attack traffic against multiple victim hosts (HMM) [22].

Figure 3 illustrates the average DRs and FPRs of the entropy-based detection technique for all low-rate DDoS attack scenarios.

As observed in Figure 3, the fluctuation of DRs and FPR is because of the variations of the DDoS attack traffic rates in each scenario. The lowest FPR and highest DR are obtained when a low-rate DDoS attack is triggered by multiple host attacks that target a single victim. Meanwhile, the lowest DR and the highest FPR are obtained with a low-rate DDoS

attack triggered by a single host attack targeting multiple victims. The rationale behind the difference between the DRs and FPRs for low-rate DDoS attacks is a perceptible difference in the amount of attack traffic received by a single or multiple victims.

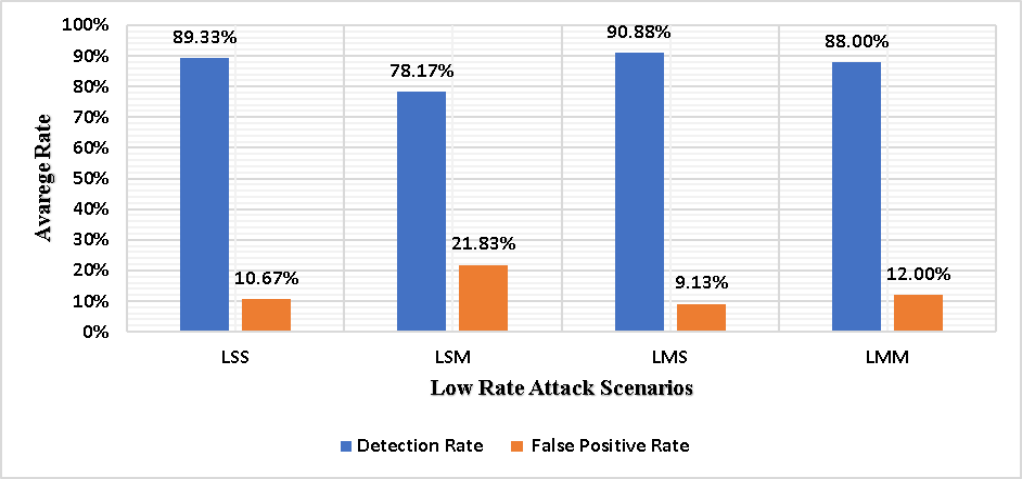


Figure 3. Average DRs and FPRs using low-rate attack scenarios in 30 min.

In addition, the high-rate DDoS attack simulation scenario aims to check the entropy-based detection technique's ability to detect high-rate DDoS attack against the controller by a single or multiple hosts' attack that targets a single or multiple victim hosts in terms of DR and FPR. Furthermore, the detection technique depends on the entropy and threshold values to detect high-rate DDoS attack traffic. Figure 4 presents the average FPR and DR for all high-rate DDoS attack scenarios.

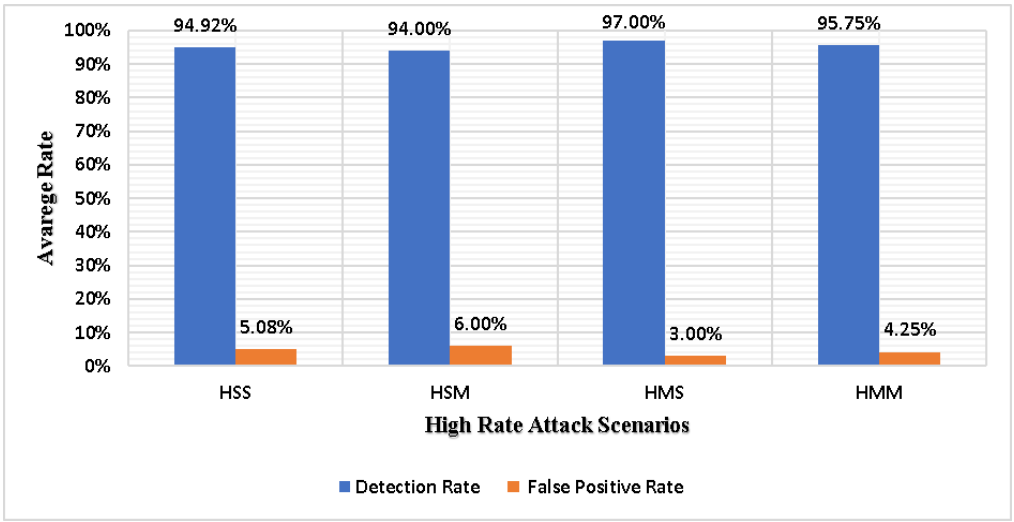


Figure 4. Average DRs and FPRs using high-rate attack scenarios in 30 min.

As shown in Figure 4, DRs and FPR fluctuate due to the high DDoS attack traffic rate variation in each scenario. The lowest FPR and highest DR are obtained when a high-rate DDoS attack is triggered by multiple host attacks targeting a single victim. Meanwhile, the lowest DR and the highest FPR are obtained when the high-rate DDoS attack is triggered by a single host attack that targets multiple victims. The rationale behind the difference between the DRs and FPRs for high-rate DDoS attacks is a perceptible difference in the amount of attack traffic that a single or multiple victims receive.

7. Comparative Analysis

This section compares the performance of the entropy-based detection approach by comparing the results of low-rate DDoS attack scenarios with high-rate DDoS attack rate scenarios in terms of DRs and FPRs by executing single-host and multiple-host attack scenarios that target a single or multiple victims. The evaluation metrics used in the benchmarking are DRs and FPR [22]. Those metrics are widely employed to assess an IDS that detects DDoS attacks in SDN and traditional networks. Figures 5 and 6 show the average DRs and FPRs of high and low DDoS attack traffic rates for all scenarios.

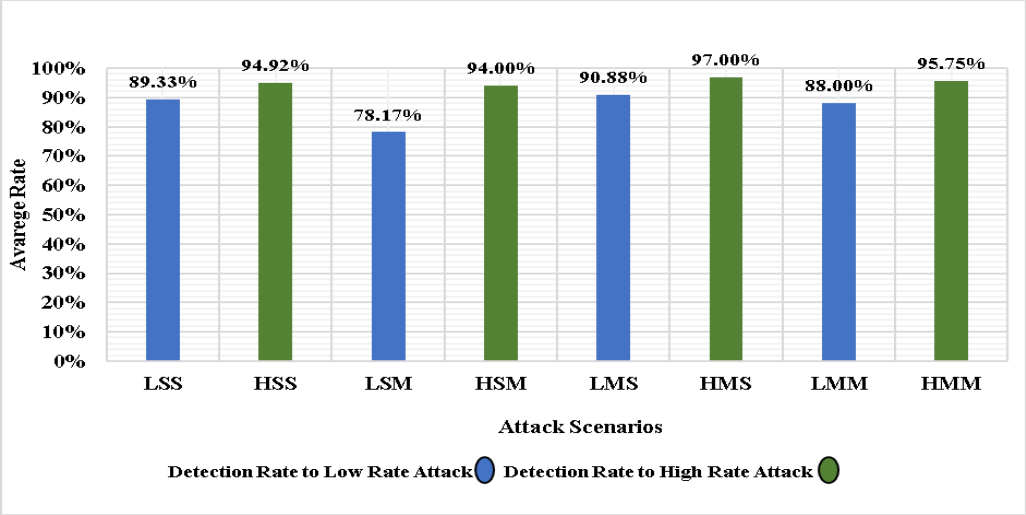


Figure 5. Comparison of the average DR of low-rate and high-rate attacks in using simulation scenarios.

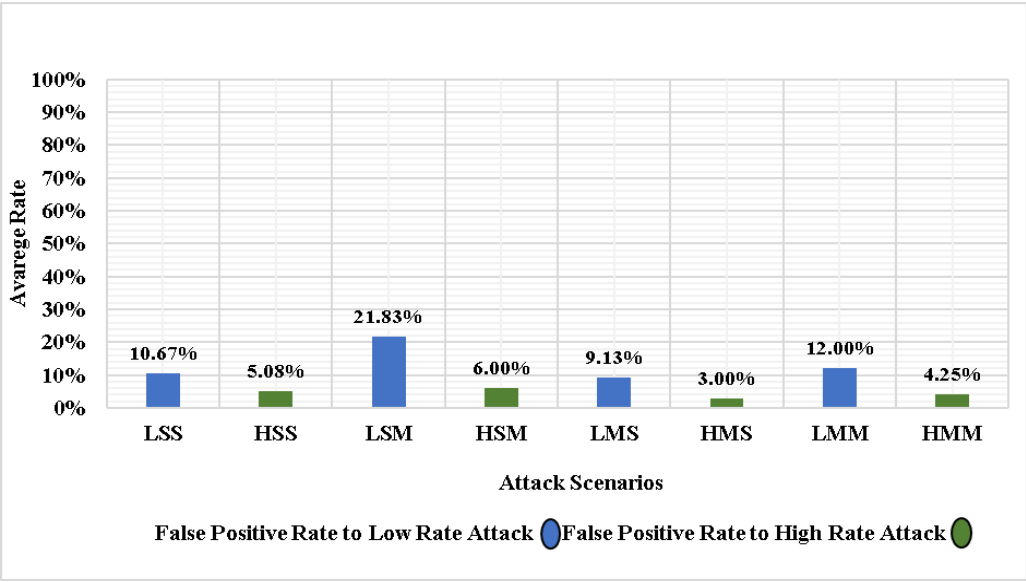


Figure 6. Comparison of the FPR of low-rate attack and high-rate attack in using simulation scenarios.

Figures 5 and 6 present the performance of the entropy-based detection approach in discerning low-rate and high-rate DDoS attacks. The detection approach clearly outperformed others in detecting high-rate DDoS attacks of the average DR and the average FPR in all simulation scenarios because the detection approach can collect more statistics on new incoming network traffic since it has a high traffic rate, which increases the amount of statistical information about the incoming traffic flows. At the same time, the detection approach is affected by a low DR and a high FPR in detecting low-rate DDoS attack traffic against controllers that target multiple victims.

The number of attack sources that increase or decrease their attack traffic rates (spoofing source IPs) determines the DDoS attack rates on a network. The DDoS attack could be triggered by a single host's attack (single attacker) or multiple hosts' attacks (multiple attackers), affecting the attack DR and FPR. Based on that, the entropy-based detection approach proved its ability to detect high-rate DDoS attack that targets a single or multiple victims with a high DR and a low FPR by depending on incoming network traffic statistics, which can change its values per the network traffic flows within a period t (window size).

Figure 7 shows the entropy-based detection approach's enhancement for detecting low-rate and high-rate DDoS attacks focusing on a single or multiple victims using the DR and FPR metrics. By comparing high and low DDoS attack traffic rates, detection results in the following: a low attack rate with a high attack rate triggered by a single host's attack that targets a single victim (L/HSS), a low attack rate with a high attack rate triggered by a single host's attack that focuses on multiple victims (L/HSM), a low attack rate with a high attack rate triggered by multiple hosts' attacks that target a single victim (L/HMS), and a low attack rate with a high attack rate triggered by multiple hosts' attacks that target multiple victims (L/HMS).

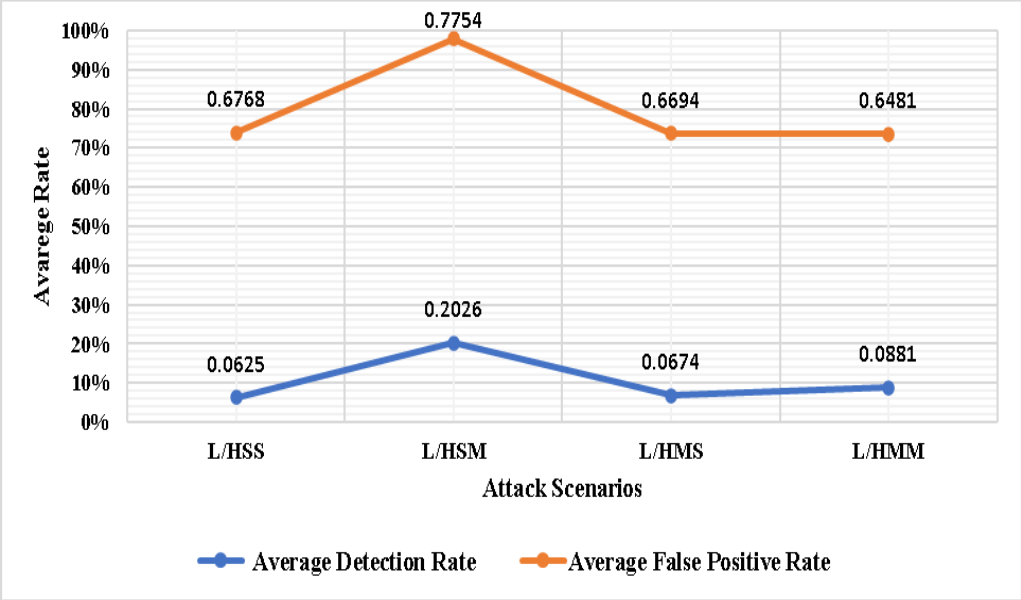


Figure 7. Enhancement of the proportion of detecting low-rate DDoS attacks to high-rate DDoS attacks by the entropy-based detection approach using simulation scenarios.

Figure 7 demonstrates that the entropy-based detection approach enhances the average DDoS attack DRs for detecting a high DDoS attack traffic rate compared with a low DDoS attack traffic rate by 6.25%, 20.26%, 6.74%, and 8.81%. In addition, the entropy-based detection approach reduces the average FPRs for detecting a high DDoS attack traffic rate compared with a low DDoS attack traffic rate by 67.68%, 77.54%, 66.94%, and 64.81 for L/HSS, L/HSM, L/HMS, and L/HMM, respectively.

8. Conclusions and Future Research Directions

The performance of the entropy-based detection approach shows significant results based on the resulting DR and FPR in detecting high-rate and low-rate DDoS attacks against the SDN controller, which triggers a single host's or multiple hosts' attacks irrespective of whether a target is a single or multiple victims. The simulation scenarios were used to assess the performance of the entropy-based detection technique in spotting different DDoS attack traffic rates in terms of DR and FPR.

The DRs and FPRs of the low-rate DDoS attack traffic are evaluated and compared with the high-rate DDoS attack traffic by adopting an entropy-based detection technique in terms

of average DR and average FPR. In addition, the results obtained from the comparison of low-rate DDoS attack traffic and high-rate DDoS attack traffic demonstrated that the entropy-based detection approach detects high DDoS attack traffic rates with a high DR and a low FPR in all simulation scenarios. Future research could add security layers through the infrastructure layer to increase the network traffic analysis granularity.

Author Contributions: M.A.A., T.A.A.-A. and D.R.I.; Methodology, M.A.A., M.A., A.A.B. and D.R.I.; Software, M.A.A., M.A., A.J.H., I.H.H., A.A.B. and D.R.I.; Validation, M.A.A., M.A., I.H.H. and T.A.A.-A.; Formal analysis, M.A.A., M.A., I.H.H. and A.A.B.; Investigation, M.A.A., M.A., I.H.H., A.A.B., T.A.A.-A. and D.R.I.; Resources, M.A.A., M.A., A.J.H., I.H.H., A.A.B., T.A.A.-A. and D.R.I.; Data curation, M.A.A., M.A., A.J.H. and T.A.A.-A.; Writing—original draft, M.A.A., M.A. and I.H.H.; Writing—review & editing, M.A.A., M.A., A.J.H. and I.H.H.; Visualization, M.A.A. and M.A.; Supervision, M.A.A.; Project administration, M.A.A. All authors have read and agreed to the published version of the manuscript.

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

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: For this article's experimental data and results, you can contact us at anbar@usm.my.

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

Conflicts of Interest: The authors declare no conflict of interest to report regarding the present study.

References

1. De Assis, M.V.O.; Novaes, M.P.; Zerbini, C.B.; Carvalho, L.F.; Abrao, T.; Proenca, M.L. Fast Defense System Against Attacks in Software Defined Networks. *IEEE Access* **2018**, *6*, 69620–69639. [CrossRef]
2. Ahmad, S.; Mir, A.H. Scalability, Consistency, Reliability and Security in SDN Controllers: A Survey of Diverse SDN Controllers. *J. Netw. Syst. Manag.* **2021**, *29*, 1–59. [CrossRef]
3. Aladaileh, M.A.; Anbar, M.; Hasbullah, I.H.; Bahashwan, A.A.; Al-sarawn, S. Dynamic Threshold-Based Approach to Detect Low-Rate DDoS Attacks on Software-Defined Networking Controller. *Comput. Mater. Contin.* **2022**, *73*, 1403–1416. [CrossRef]
4. Jafarian, T.; Masdari, M.; Ghaffari, A.; Majidzadeh, K. A survey and classification of the security anomaly detection mechanisms in software defined networks. *Clust. Comput.* **2021**, *24*, 1235–1253. [CrossRef]
5. AL-Adaileh, M.A.; Anbar, M.; Chong, Y.W.; Al-Ani, A. Proposed statistical-based approach for detecting distribute denial of service against the controller of software defined network (SADDCS). *MATEC Web Conf.* **2018**, *218*, 02012. [CrossRef]
6. Salman, O.; Elhajj, I.; Kayssi, A.; Chehab, A. SDN Controllers: A Comparative Study. In Proceedings of the 2016 18th Mediterranean Electrotechnical Conference (MELECON), Lemesos, Cyprus, 18–20 April 2016; pp. 1–6. [CrossRef]
7. Al-Amiedy, T.A.; Anbar, M.; Belaton, B.; Kabla, A.H.H.; Hasbullah, I.H.; Alashhab, Z.R. A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things. *Sensors* **2022**, *22*, 3400. [CrossRef]
8. Priyadarsini, M.; Bera, P. Software defined networking architecture, traffic management, security, and placement: A survey. *Comput. Netw.* **2021**, *192*, 108047. [CrossRef]
9. Urrea, C.; Benítez, D. Software-Defined Networking Solutions, Architecture and Controllers for the Industrial Internet of Things: A Review. *Sensors* **2021**, *21*, 6585. [CrossRef]
10. Bouras, C.; Kollia, A.; Papazois, A. SDN & NFV in 5G: Advancements and Challenges. In Proceedings of the 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), Paris, France, 7–9 March 2017; pp. 107–111. [CrossRef]
11. Zubaydi, H.D.; Anbar, M.; Wey, C. Review on Detection Techniques Against DDoS Attacks on a Software-Defined Networking Controller. In Proceedings of the 2017 Palestinian International Conference on Information and Communication Technology (PICICT), Gaza, Palestine, 8–9 May 2017; pp. 10–16.
12. Haque, M.R.; Tan, S.C.; Yosoff, Z.; Nisar, K.; Kaspin, R.; Haider, I.; Nisar, S.; Rodrigues, J.P.C.; Chowdhry Muhammad, B.S.; Uqaili, A.; et al. Unprecedented Smart Algorithm for Uninterrupted SDN Services During DDoS Attack. *Comput. Mater. Contin.* **2022**, *70*, 875–894.
13. Singh, M.P.; Bhandari, A. New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges. *Comput. Commun.* **2020**, *154*, 509–527. [CrossRef]
14. Cui, Y.; Qian, Q.; Guo, C.; Shen, G.; Tian, Y.; Xing, H.; Yan, L. Towards DDoS detection mechanisms in Software-Defined Networking. *J. Netw. Comput. Appl.* **2021**, *190*, 103156. [CrossRef]

15. Aladaileh, M.A.; Anbar, M.; Hasbullah, I.H.; Sanjalawe, Y.K. Information Theory-based Approaches to Detect DDoS Attacks on Software-defined Networking Controller a Review. *Int. J. Educ. Inf. Technol.* **2021**, *15*, 83–94. [CrossRef]
16. Fan, C.; Kaliyamurthy, N.M.; Chen, S.; Jiang, H.; Zhou, Y.; Campbell, C. Detection of DDoS Attacks in Software Defined Networking Using Entropy. *Appl. Sci.* **2022**, *12*, 370. [CrossRef]
17. Mousavi, S.; St-Hilaire, M. Early Detection of DDoS Attacks Against Software Defined Network Controllers. *J. Netw. Syst. Manag.* **2018**, *26*, 573–591. [CrossRef]
18. Sahoo, K.S.; Puthal, D.; Tiwary, M.; Rodrigues, J.; Sahoo, B.; Dash, R. An Early Detection of Low Rate DDoS Attack to SDN Based Data Center Networks Using Information Distance Metrics. *Futur. Gener. Comput. Syst.* **2018**, *89*, 685–697. [CrossRef]
19. Perez-Diaz, J.A.; Valdovinos, I.A.; Choo, K.K.R.; Zhu, D. A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning. *IEEE Access* **2020**, *8*, 155859–155872. [CrossRef]
20. Jiang, Y.; Zhang, X.; Zhou, Q.; Cheng, Z. An Entropy-Based DDoS Defense Mechanism in Software Defined Networks. *Int. Conf. Commun. Netw. China* **2016**, *1*, 169–178.
21. Koay, A.M.Y. Detecting High and Low Intensity Distributed Denial of Service (DDoS) Attacks. Ph.D. Thesis, Victoria University, Wellington, ON, New Zealand, 2019.
22. Aladaileh, M.A.; Anbar, M.; Hintaw, A.J.; Hasbullah, I.H.; Bahashwan, A.A.; Al-Sarawi, S. Renyi Joint Entropy-Based Dynamic Threshold Approach to Detect DDoS Attacks against SDN Controller with Various Traffic Rates. *Appl. Sci.* **2022**, *12*, 6127. [CrossRef]
23. Bromiley, P. Shannon entropy, Renyi entropy, and information. *Stat. Inf. Ser.* **2004**, *2004*, 1–8.
24. Aladaileh, M.A.; Anbar, M.; Hasbullah, I.H.; Chong, Y.W.; Sanjalawe, Y.K. Detection Techniques of Distributed Denial of Service Attacks on Software-Defined Networking Controller–A Review. *IEEE Access* **2020**, *8*, 143985–143995. [CrossRef]
25. Bahashwan, A.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H.; Aladaileh, M.A. Propose a Flow-Based Approach for Detecting Abnormal Behavior in Neighbor Discovery Protocol (NDP). In Proceedings of the International Conference on Advances in Cyber Security, Penang, Malaysia, 24–25 August 2021; Volume 15, pp. 401–416.
26. Aladaileh, M.; Anbar, M.; Hasbullah, I.H.; Sanjalawe, Y.K.; Chong, Y. Entropy-Based Approach to Detect DDoS Attacks on Software Defined Networking Controller. *Comput. Mater. Contin.* **2021**, *69*, 373–391. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.