Computers, Materials & Continua
DOI: 10.32604/cmc.2022.029369
Article

Tech Science Press

Dynamic Threshold-Based Approach to Detect Low-Rate DDoS Attacks on Software-Defined Networking Controller

Mohammad Adnan Aladaileh, Mohammed Anbar*, Iznan H. Hasbullah, Abdullah Ahmed Bahashwan and Shadi Al-Sarawn

National Advanced IPv6 Centre of Excellence, Universiti Sains Malaysia, Penang, Malaysia
*Corresponding Author: Mohammed Anbar. Email: anbar@usm.my
Received: 02 March 2022; Accepted: 02 April 2022

Abstract: The emergence of a new network architecture, known as Software Defined Networking (SDN), in the last two decades has overcome some drawbacks of traditional networks in terms of performance, scalability, reliability, security, and network management. However, the SDN is vulnerable to security threats that target its controller, such as low-rate Distributed Denial of Service (DDoS) attacks, The low-rate DDoS attack is one of the most prevalent attacks that poses a severe threat to SDN network security because the controller is a vital architecture component. Therefore, there is an urgent need to propose a detection approach for this type of attack with a high detection rate and low false-positive rates. Thus, this paper proposes an approach to detect low-rate DDoS attacks on the SDN controller by adapting a dynamic threshold. The proposed approach has been evaluated using four simulation scenarios covering a combination of low-rate DDoS attacks against the SDN controller involving (i) a single host attack targeting a single victim; (ii) a single host attack targeting multiple victims; (iii) multiple hosts attack targeting a single victim; and (iv) multiple hosts attack targeting multiple victims. The proposed approach's average detection rates are 96.65%, 91.83%, 96.17%, and 95.33% for the above scenarios, respectively; and its average false-positive rates are 3.33%, 8.17%, 3.83%, and 4.67% for similar scenarios, respectively. The comparison between the proposed approach and two existing approaches showed that it outperformed them in both categories.

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

1 Introduction

For decades, defending network security has been a competitive process between attackers and security practitioners. Despite the advancement of technology, innovative new attack types and the tools to trigger them keep appearing that require sophisticated countermeasures [1]. For example, DDoS attacks can cause significant network disruption and even destroy network

infrastructure [2]. However, the adoption of SDN architecture as a security measure has significantly reduced the destructive impact of DDoS attacks on the target network/victims [3,4].

The controller provides significant functions in the SDN network, including configuring flow tables (rules), being able to monitor network components by constructing secure channels, and updating an infrastructure layer's instructions flow table to identify new network traffic flows. [5–8]. Furthermore, through an open API, the controller could control the complete network flow of traffic by serving as a controller between the infrastructure and application layers [9]. Finally, the network traffic flow could be checked by the network traffic flow statistics the controller has collected to provide the attack detection approach in the traffic statistics. This way, the controller could figure out whether the network traffic flow is normal or abnormal.

Any new network technology will encounter many security issues, especially with the explosion in Internet use. However, no network technology can guarantee absolute safety or security, including the SDN. The SDN controller is an attractive target for attackers aiming to break down entire SDN network operations [10]. Nexusguard's report showed a high increase in DDoS attacks in the first half of 2021, which reached 233% compared to years prior [11].

Although the SDN network is vital in network management and provides flexibility to deal with the network traffic flows, it still faces many security issues because the centralized controller is the main component of the network serving as an operating system for all network functions. Therefore, if any threat to the controller is not addressed early, it will eventually slow down the entire network. For example, the primary objective of most DDoS attacks on SDN networks is the controller, typically achieved by bombarding it with a massive amount of spoofed IP packets to exhaust its resources, reducing its ability to process incoming packets [12,13].

Many DDoS detection approaches for DDoS attacks on SDN controllers employ the entropy algorithm, which involves examining network traffic flow behavior. The entropy method can collect statistical information on traffic flows regarding the number of packets and the packet header features. However, the existing entropy-based approaches depend on the static threshold, which could degrade the performance of low-rate DDoS attack detection, which implies a high false-positive rate. Thus, this paper's contribution is to adapt a dynamic threshold into an entropy algorithm to detect DDoS attacks on SDN controllers with a high detection rate and a low false-positive rate, regardless of the trigger source (single host attack or multiple host attacks) and the number of targets (single victim or multiple victims).

The rest of the paper is structured as follows: The related work is presented in Section 2. Section 3 discusses adapting a dynamic threshold algorithm for detecting low DDoS attack traffic rates and provides a detailed explanation of the proposed detection approach. Section 4 elaborates on the experiments and evaluation in terms of the experiment setup and simulation scenarios for evaluating the performance of the detection approach and discusses the proposed approach results. It is followed by Section 5, which compares the proposed approach with existing detection approaches in terms of attack detection rate and false-positive rate metrics. Finally, Section 6 summarizes the study's conclusion and recommends several directions for future research. for submission. It will speed up the review and typesetting process.

2 Related Work

As mentioned in Section 1, the SDN controller faces many security challenges due to its importance to the network, making it attractive as a target for attackers attempting to collapse the

network since the controller is responsible for managing all network traffic flows. Hence, any successful attack against the controller could affect the entire network, especially the one launched with varying traffic rates toward single or multiple victims within the network, which is challenging to detect low DDoS attack traffic rate with a high detection rate and low false-positive rate.

Dehkordi et al. [14] proposed a hybrid attack detection approach using the entropy method and machine learning (ML) executed on an SDN controller. The proposed approach comprises three parts: collector, entropy, and classification. The approach effectively detects DDoS attacks and attacks with a high detection rate. However, identifying an optimum threshold value is difficult when dealing with varying DDoS attack traffic rates.

Singh et al. [15] proposed a novel technique utilizing a theory-based information approach (i.e., Jensen Renyi Divergence (JRD)). The proposed approach detects high-rate and low-rate DDoS attacks in SDN-based network flows. This method has a lower computational requirement because there are fewer traffic features to calculate. The detection approach starts with time intervals and then extracts the relevant traffic features (i.e., source and destination IP, source and destination port, and protocol operated). Finally, the procedure uses source IP addresses to calculate the information theory metrics for detection. However, the proposed approach achieves lower performance, particularly for low-rate DDoS attacks.

Fan et al. [16] proposed a fusion entropy technique and a static threshold for calculating the randomness of network traffic. The proposed approach is expected to detect DDoS attacks in the SDN network environment. The proposed method was evaluated and tested using a real SDN dataset. However, the proposed approach achieves a low performance of 91.25% for the decline rate of entropy. Also, the proposed approach uses a static threshold value, which leads to low detection accuracy and high false-positive rates. In addition, the proposed method gives a lack of information about the dataset used and the features that could be used to detect DDoS attacks. Overall, this approach is limited to high-rate DDoS attacks.

Meanwhile, Perez-Diaz et al. [17] proposed a flexible technique to detect and mitigate low DDoS attack traffic rate in SDN networks with characteristics similar to regular traffic. The approach relies on intrusion detection and prevention systems (IDS and IPS). Furthermore, the proposed approach uses six machine learning models for DDoS classification executed in the IDS. However, the proposed approach uses a fixed threshold, making the prevention method highly ineffective.

Yu et al. [18] proposed a platform to detect DDoS attacks in vehicular networks that depend on the SDN environment by using machine learning (SVM). The proposed platform comprises the trigger detection model for packet-in, flow table features extraction and DDoS attack detection model. The proposed approach significantly reduces the time of DDoS attack detection. However, the proposed approach uses a predefined threshold, not considering varying attack traffic rates.

Furthermore, Cui et al. [19] proposed an attack detection approach by combining the entropy method and cognitive-inspired computing, which depend on the SVM algorithm to detect DDoS attacks. Furthermore, the proposed approach depends on the periodic statistics of network traffic flows to calculate the uncertainty of packets in the network using packet header features (source and destination IP). However, the detection rate is still insufficient and uses a fixed threshold.

Mousavi et al. [20] proposed an early detection approach that depends on an entropy algorithm relying on one header packet feature (destination IP address) for analyzing the network traffic flow statistics to calculate the uncertainty of the packets toward the controller. It decides if the network traffic flows have the DDoS attack by using a static threshold for comparing the threshold value with

the entropy value. However, the proposed approach depends on a predefined threshold value, which affects its detection rate and may cause DoS to users in obtaining network services.

Sahoo et al. [21] combining the information distance with the generalized entropy was proposed to detect a low attack traffic rate on the SDN controller. The number of packets within a predefined window size is used to calculate packets probability distribution in the network traffic flow, indicating DDoS attack existence. Despite their approach showing a high detection rate of DDoS, it faces difficulty setting a dynamic threshold corresponding to varying network traffic flows.

The previous studies on detecting DDoS attacks with varying attack rates against SDN controllers show that no existing detection approach utilizes a dynamic threshold to respond to changing network traffic flow rates. The motivation of this study is to detect low DDoS attack traffic rate on SDN controller regardless of the attack traffic rates with a high detection rate and a low false-positive rate by adapting a dynamic threshold without additional load to the SDN controller.

3 The Proposed Approach

Dynamic threshold-based approaches can detect low DDoS attack traffic rate with higher detection rates and lower false-positive rates than static threshold-based approaches, which reduces the effectiveness of the DDoS attack detection rates and increases detection false-positive rates. Static threshold-based approaches cannot distinguish between regular and low-rate DDoS attack traffic, and they cannot handle the variation in attack traffic flow rates. In addition, the simple variation of low-rate DDoS attack traffic and regular traffic may affect detection approach performance depending on a predefined threshold [22].

Consequently, a predefined static threshold is ineffective in reducing the false-positive rate. Furthermore, determining the threshold value is often time-consuming because it depends on observation and experimentation. However, dynamic thresholds are more flexible and can significantly improve DDoS detection performance because it can differentiate between low DDoS attack traffic rate and regular traffic rate. Therefore, Incoming network traffic's dynamic threshold is being calculated in this section. For the calculation of the dynamic threshold, we utilize the following statistics: (i) the amount of incoming traffic that flows toward the controller over time $\boldsymbol{t}$, (ii) the attack rate at which is directed towards the victim, (ii) the entropy value at time $\boldsymbol{t}$.

Eq. (1) calculates the randomness of these packets in the traffic flow (i.e., source/destination IP address) within a particular time t. The attack behavior and legitimate packets behavior vary, which can cause fluctuations in the calculation of the threshold [23]. The analysis of the incoming traffic finds the entropy used in the calculation of the dynamic threshold flows statistics. We calculate the dynamic threshold by adopting the exponentially weighted moving average (EWMA) method.

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

where $P(X_i)$ is the likelihood of a specific features from the packet header features, $\boldsymbol{n}$ is the total number of the features in the network traffic in a particular time, and $H(X_i)$ is the entropy value.

This study calculates a dynamic threshold by adopting the EWMA method [24]. Consequently, the dynamic threshold in this work relies on network traffic flow statistics that have been collected by controller and Entropy value, which reduces the time needed to calculate a suitable threshold for

the proposed approach. Therefore, the DDoS attack detection effectiveness depends on the threshold value. Eq. (2) is the original EWMA equation.

$$EWMA_i = (1 - \alpha) \cdot EWMA_{i-1} + \alpha \cdot Y_i \quad (2)$$

where, $EWMA_i$ is the current value of the $EWMA$, $EWMA_{i-1}$ is the previously estimated $EWMA$ value and the initial threshold value adopted in this research based on the calculation by [25]. The process of calculating the dynamic threshold is as shown in Fig. 1.

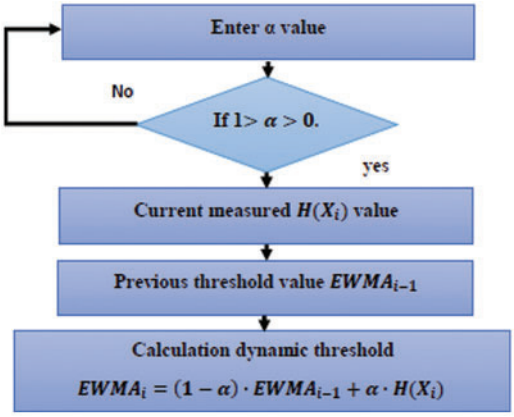


Figure 1: Dynamic threshold calculation process

The core contribution of this paper is the adaptation of the dynamic threshold to minimize the false positive rate and increase the detection rate for a low DDoS attack traffic rate detection approach regardless of the attack's trigger sources (single host attack or multiple host attacks) and the number of victim targets (single victim or multiple victims). The dynamic threshold used the entropy value as the input.

Most DDoS attack detection methods are entropy-based [26–28]. However, entropy-based approaches share the same drawbacks with approaches that rely on a static threshold which degrades the attack detection rate and increases the false positive rate. Therefore, they struggle to detect low DDoS attack traffic rate on SDN controller that target single or multiple victim hosts. According to the proposed approach, using an entropy method with a dynamic threshold would significantly improve the accuracy for detecting low DDoS attack traffic rate regardless of the attack's trigger sources that targeted a single victim host or multiple victim hosts.

Finding the optimal dynamic threshold requires running multiple scenarios to see the effect of the entropy-based attack detection methods. These scenarios cover the attacks launched from a single host or multiple hosts on controller that targets a single victim host or multiple victim hosts. Consequently, since the behaviors of the incoming attack traffic flows are changing in network traffic flow by diverse attack sources based on specific window size, the $EWMA$ is adopted to find a suitable dynamic threshold value. According to Eq. (2), the dynamic threshold calculation depends on each of the following:

$\boldsymbol{\alpha}$ is one of $EWMA$ parameters with a value between 0 to 1, so the new threshold will be more precise based on the experiments to limit the value of false-negative error; however, this choice is somewhat arbitrary [24].

$EWMA_{i+1}$ is an estimated value (previous value) for $EWMA_i$ with the value sets to 1.31 based on [25], which provides an accurate value to calculate the first value of $EWMA_i$. $H(X_i)$ is currently measured, herein, the $H(X_i)$ value has been adopted for each window size to suit all attack traffic rates in terms of the attack traffic intensity, whether it was a high DDoS attack traffic rate or a low DDoS attack traffic rate.

After calculating dynamic threshold value, the comparison between the incoming traffic flows' randomness and the dynamic threshold will be made. The next stage is a key to deciding if there is a DDoS attack by using a rule-based detection approach. Fig. 2 illustrates the flow of the dynamic threshold process.

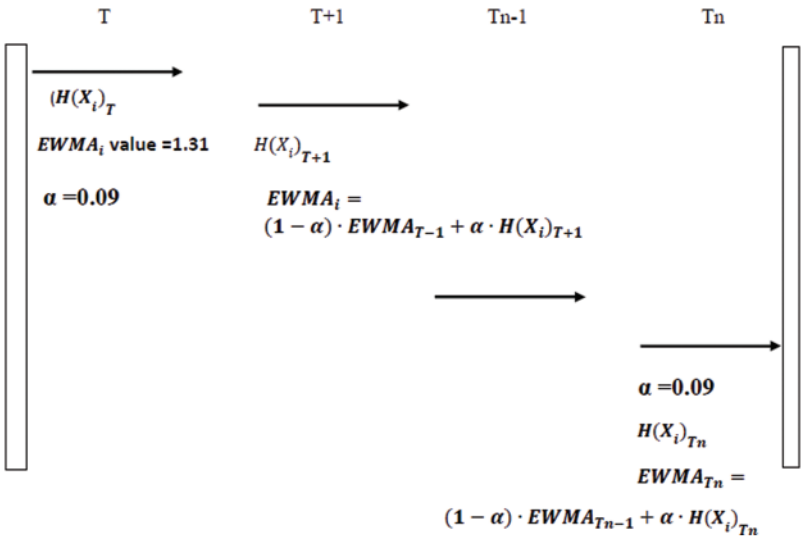


Figure 2: Dynamic threshold flowchart

Based on Fig. 2, the α value is 0.09, the initial value of $EWMA_{i-1} = 1.31$ and the $H(X_i)$ value corresponds to the currently measured value $EWMA_i = (1\text{-}0.09) * 1.31 + (0.09\text{-}H(X_i))$. This value is for the first incoming flow, so for the subsequent incoming flow, $EWMA_{i-1}$ and $EWMA_0$ based on the previous value of the $EWMA_{i+1}$ will be based on the current value of entropy $EWMA_{i-1}$.

This study proposes a new rule-based attack detection to detect low DDoS attack traffic rate on the controller based on a statistical analysis of incoming network traffic flows. The rule is based on the entropy $H(X_i)$ value and the dynamic threshold value within a specific window size. As stated in Section 3, a DDoS attack exists if is less than or equal to *Th*; otherwise, the incoming network traffic flow will be considered regular traffic.

4 Experiments and Evaluation

This section describes the experiments on low-rate DDoS attack detection approach adaptation of a dynamic threshold with entropy, evaluates the attack detection approach, and compares the results with the existing entropy-based attack detection approach [20] and information theory algorithm-based attack detection approach. This experiment uses a virtual SDN environment to implement and evaluate the dynamic threshold-based low-rate DDoS attack detection approach.

4.1 Experiment Setup

This section describes the setup of the experiment. The quantitative research evaluation uses Mininet version 3.7 (32-bit) to simulate DDoS attack detection approaches covering different attack scenarios. Furthermore, selecting the implementation tool software and hardware in the testbed and setting up the simulation environment depends on the detection approach requirements. Tab. 1 presents the detail of the topology of the experimental setup.

Table 1: Description of the attack detection approach topology

Number of hosts	64
IP ranges	10.0.0.1–10.0.0.64
Attack type	UDP
Attacker OS	Kali
Normal users' OS	Ubuntu
Controller type	POX

The workstation used for the experiment runs a 64-bit Microsoft™ Windows 10 operating system on hardware with 2.6 GHz Intel™ Core® i7-6700HQ CPU and 16 GB RAM.

4.2 Experiment Setup

This section describes the simulated scenarios that have been used to evaluate the performance of the proposed approach, compared with the existing DDoS detection approaches, and the evaluation metrics used to measure the effectiveness of the proposed approach for detecting low DDoS attack traffic rates on the SDN controller.

This study tests several attack scenarios, such as attack sources (single or multiple attack hosts) and targeted victims (single or multiple victim hosts). The average of each scenario's result will be reported every five minutes for 30 minutes. Furthermore, the five minutes are divided into n slots, so each slot is equal to $\boldsymbol{m}$ second, where $\boldsymbol{m}$ is a configurable value for calculating the network traffic with $\boldsymbol{m}$ seconds. Eq. (4) is the formula used to calculate the time slot [29].

$$Timeslots\,(\boldsymbol{n}) = (5 * 60)\,/\boldsymbol{m} \tag{4}$$

In this study, based on trial and error, the distribution of the packet is reported every 5-minute (300 sec) window. Therefore, the proposed approach will report the result of 60 traffic flows, where each flow is a 5-second window aggregate. Therefore, the average detection rate and false-positive rate of 60 traffic flows will be reported every five minutes.

In addition, a low-rate DDoS attack packet is sent at a rate of 5 packets/sec (1 packet every 0.2 seconds), as stated in [30]. As a result, the attack ratio in a 5-second time window is calculated using Eq.(5) [21].

$$AttackTrafficRatio = \frac{Attack\ Packet}{packet\ total} \times 100\% \tag{5}$$

As shown in Tab. 2, the attack packet is sent at a five packets/sec rate, almost the same as the normal traffic rate (one packet/sec). For reference, the total number of normal packets sent per second is 63 in the single attacker scenario since the testbed comprises 63 hosts (non-attackers); or 61 in

the multiple attacker scenario (non-attacking hosts) since the testbed comprises three attacker hosts. Therefore, for a single attacker scenario, the total number of attacks and normal packets sent in five seconds is 25 and $63 \times 5 = 315$, respectively, regardless of the number of targets (single or multiple victims). As for the multiple attacker scenario, the total number of attacks and normal packets sent in five seconds is 75 and $61 \times 5 = 305$, respectively, regardless of the number of targets (single or multiple victims). However, due to the SDN characteristics that only forward a packet with a unique source IP address to the controller, only 63 or 61 packets are sent to the controller. As a result, using Eq. (5), the attack ratio within the 5-second window is 7% and 19%, respectively.

Table 2: Single attacker traffic specifications against single or multiple targets using low-rate attack traffic

	# Attack packet	# Normal packet	Ratio
Single attacker	25	315	7%
Multiple attackers	75	305	19%

4.3 Result

In this study, the number of attack packets depends on the rate of attack traffic. For example, based on Tab. 2, in five minutes, the number of attack packets in a low-rate DDoS attack triggered by a single host is 1,500, and the number of regular traffic is 18,900 packets. Meanwhile, when triggered by multiple hosts, the number of attack packets is 4,500 within five minutes, and the number of regular traffic is 18,300 packets within the same period.

The single and multiple hosts attack scenarios aim to check the performance of the proposed approach in detecting low-rate DDoS attacks against the controller that targets single or multiple victims. The proposed approach depends on entropy and dynamic threshold values to detect low-rate DDoS attacks. Fig. 3 shows the average values for each entropy and dynamic threshold values every 30 minutes; where SSL denotes a single host's low-rate attack targeting a single victim host, SML is a single host's low-rate attack targeting multiple victim hosts, MSL is multiple hosts' low-rate attacks targeting a single victim host, and MML is multiple hosts' low-rate attack targeting multiple victim hosts.

As observed from Fig. 3, the entropy values are slightly lower but very close to the dynamic threshold values within 30 minutes of the experiment, which indicates the presence of low-rate DDoS attacks in the network according to the rule-based attack detection.

Indeed, the detection approach reports the packet distribution of each five-minute window size. Thus, the detection approach reports the findings of 60 network traffic flows according to Eq. (4), where each flow is the aggregate of packets within a 5-second window. The average detection rate and the average false-positive rate of 60 flows are reported every five minutes for 30 minutes. The proposed approach has been evaluated in terms of detection rate and false-positive rate. Figs. 4a–4d illustrates the proposed approach's detection rate and false-positive rate in detecting low-rate DDoS attack traffic.

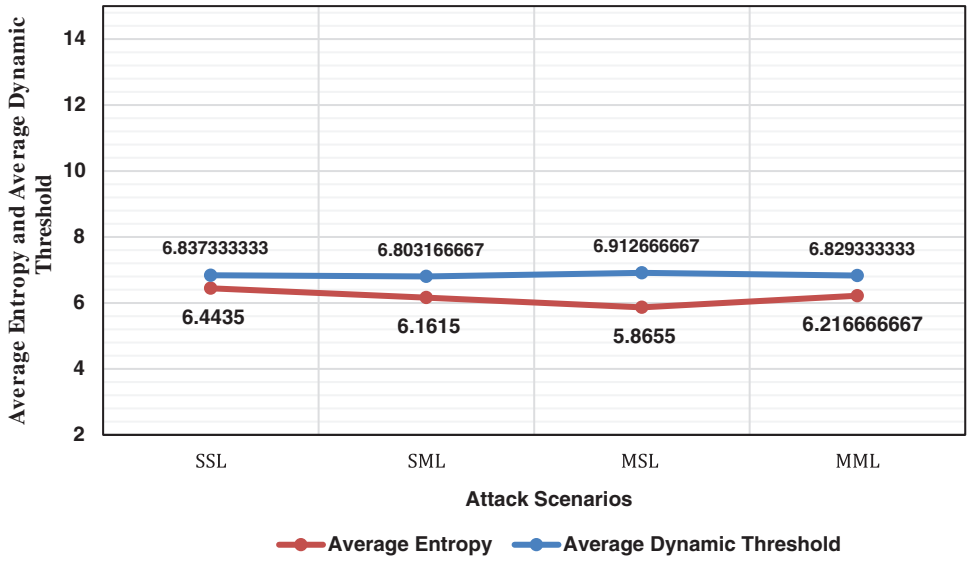
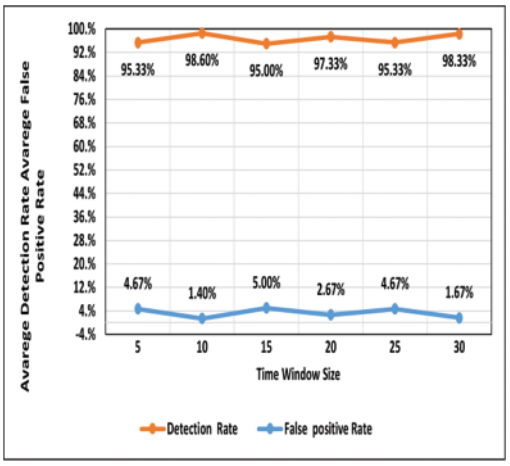
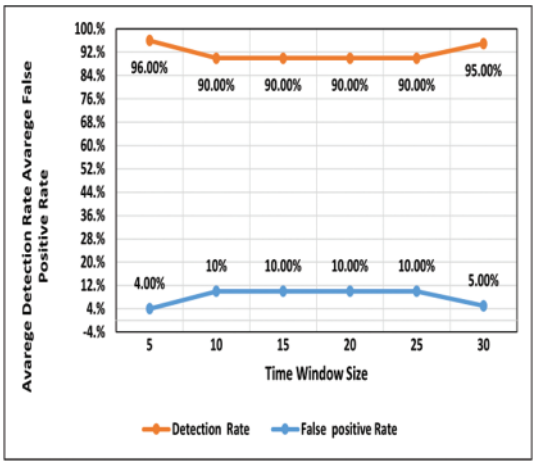


Figure 3: Average entropy and dynamic threshold values of each attack scenario

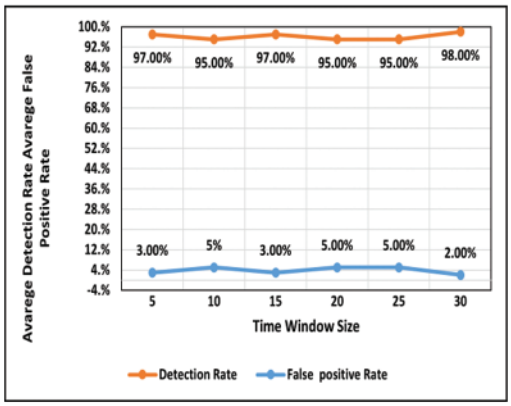


(a) Average values of detection rate and false-positive rate of scenario SSL

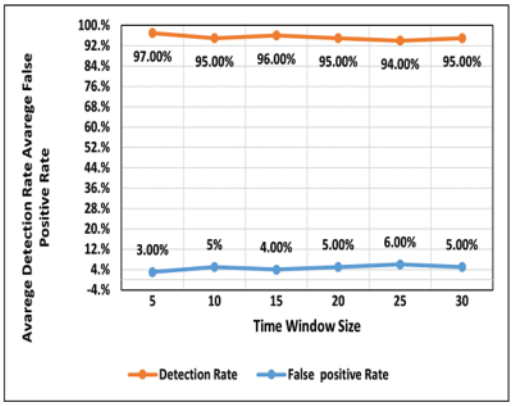


(b) Average values of detection rate and false-positive rate of scenario SML

Figure 4: (Continued)



(c) Average values of detection rate and false-positive rate of scenario MSL



(d) Average values of detection rate and false-positive rate of scenario MML

Figure 4: (a) Average values of detection rate and false-positive rate of scenario SSL (b) Average values of detection rate and false-positive rate of scenario SML (c) Average values of detection rate and false-positive rate of scenario MSL (d) Average values of detection rate and false-positive rate of scenario MML

The figures above show that the DDoS attack traffic rate is low (0.2/sec), similar to regular traffic. Thereby, the proposed approach shows the ability to detect low-rate DDoS attacks with a range between 94% to 98%, which means the proposed approach can accurately detect low-rate DDoS attacks against the controller. Meanwhile, the false-positive rates range between 1.67% to 10%. The proposed approach's effective performance is due to adopting a dynamic threshold that changes based on the attack rates according to the network traffic rates. Fig. 5 below presents the average detection and false-positive rates in 30 minutes.

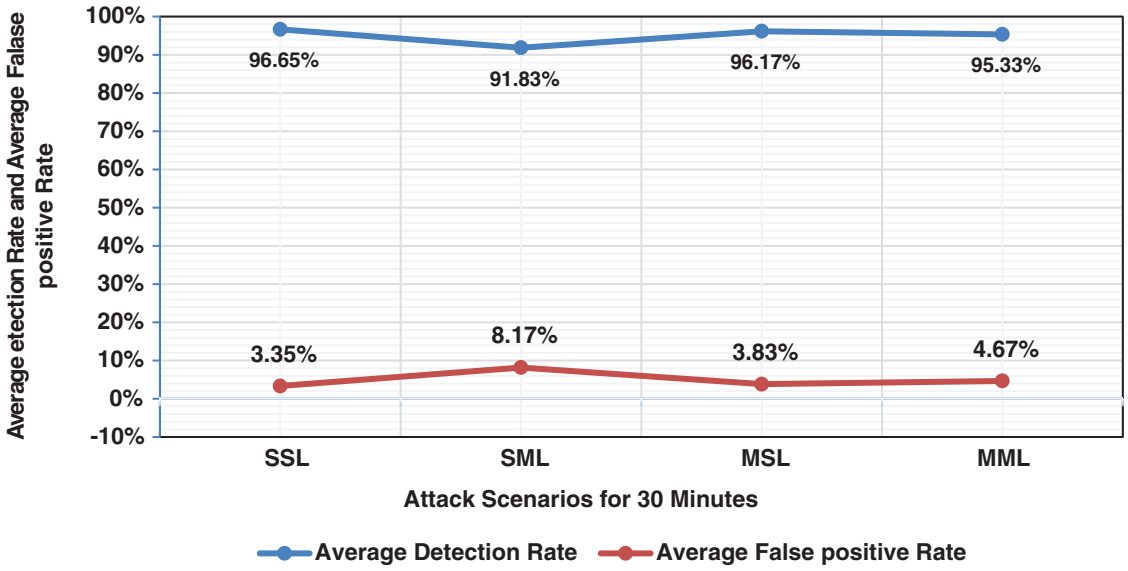


Figure 5: Summary detection approach results in terms of the average detection rates and false-positive rates

As observed in Fig. 5, when multiple hosts attacked a single host victim, both detection rate and low false-positive rate are high. However, the false-positive rate is high, and the detection rate is low when a single host attacks to multiple victims. The difference in detection rates and false-positive rates is because a single host attack distributes its attack traffic on more than one victim; therefore, the amount of attack traffic received by a single victim *vs*. multiple victims is noticeable.

5 Comparison

This section compares the proposed approach and the existing entropy-based approaches by [15,20]. The approach [20] has been used as a comparison by all entropy variant approaches to evaluate the overall performance of the proposed detection approach that depends on the entropy method. Furthermore, the approach [15] has been used as a comparison to the proposed approach that depends on information theory algorithm to detect DDoS attacks based on analysis of the network traffic statistics collected from network traffic flows. By executing single or multiple host attack scenarios designed to detect low-rate DDoS attacks on single or multiple targets. The evaluation metrics used are detection rate and false-positive rate, which are widely used in measuring the performance of DDoS attack detection approaches against SDN controllers.

The experimentation results show a high detection rate for detecting low-rate DDoS attacks against SDN controllers compared with the existing approaches because it relies on a dynamic threshold instead of a static threshold to detect DDoS attacks, which fulfills the aim of this study. Fig. 6 shows the proposed approach has an accurate ability low attack rate detection triggered from single host attack or multiple hosts attacks toward a single victim or multiple victims.

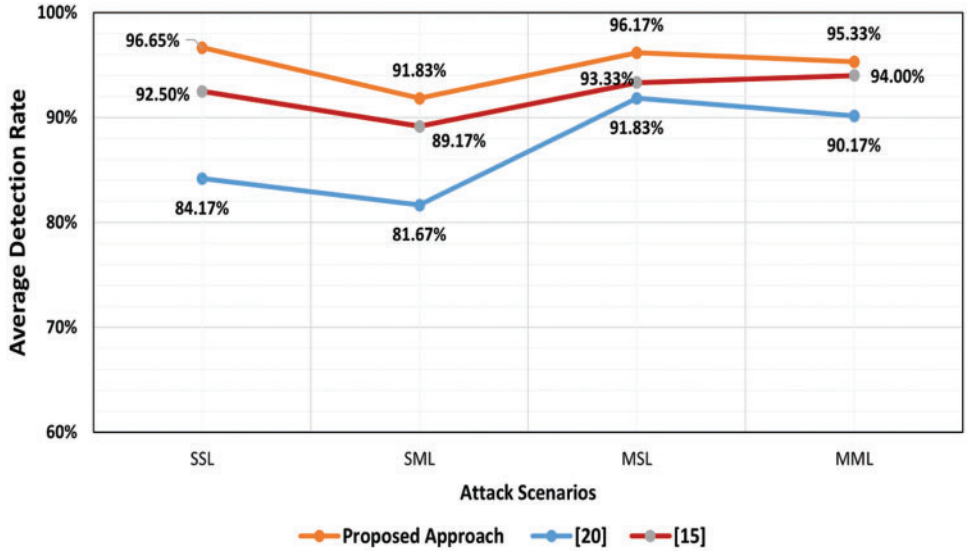


Figure 6: Average detection rate of proposed approach *vs*. existing approaches

As observed in Fig. 6, the proposed approach has a better detection rate than the existing approaches. It has a higher detection rate because the statistical analysis for the network traffic depends on packet header features (destination IP address) to calculate the randomness of the packet flow using an entropy algorithm and a dynamic threshold to detect the low-rate DDoS attack. In contrast, the existing approaches depend on a static threshold to analyze the network traffic, reducing its detection

rate in this experiment. Fig. 7 shows the average false-positive rate of proposed approach *vs*. existing approaches.

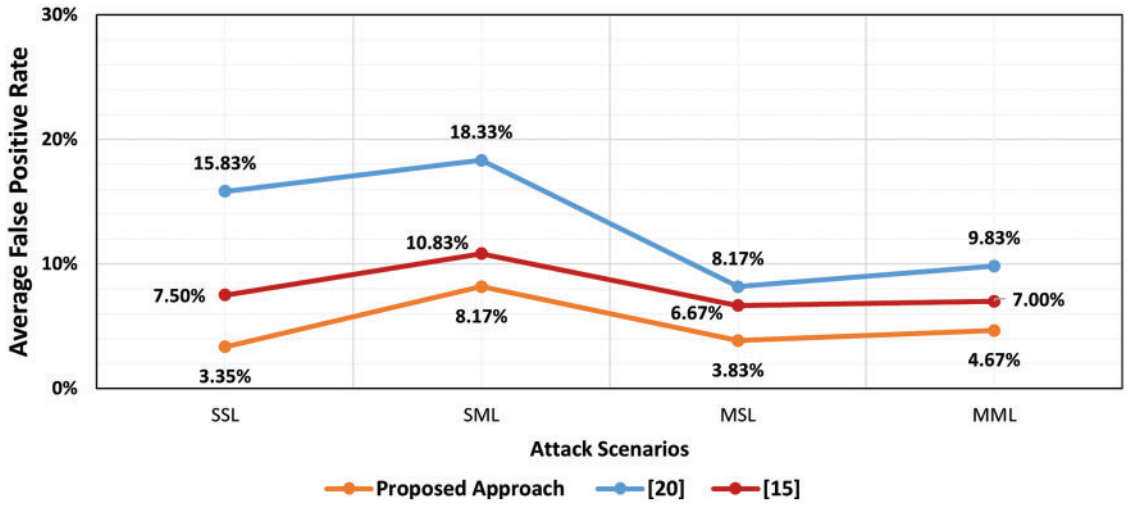


Figure 7: Average false-positive rate of proposed approach *vs*. existing approaches

As shown in Fig. 7, the proposed approach performed better than the existing approaches regarding the false-positive rate. The proposed approach has a lower false-positive rate due to a combination of an entropy algorithm, a dynamic threshold, and a rule-based detection in detecting low-rate DDoS attacks in network traffic flows. In contrast, the existing approaches depend on a static threshold to analyze the network traffic, reducing its DDoS attack detection rate in this experiment.

6 Conclusion

This paper proposed an approach to detect low DDoS attack traffic rate on the SDN controllers that target single victim or multiple victims. It used an entropy method to improve the attack detection rate and reduce the false-positive rate by adapting a dynamic threshold and proposing a new rule-based detection mechanism. The performance of the proposed approach was evaluated using four simulation scenarios using a low attack traffic rate. The results of the four simulation scenarios show considerable improvements in terms of attack detection rate and false-positive rate. In addition, the comparison of the proposed approach with the existing approaches showed that the proposed approach overcomes the limitations of the existing approaches and outperforms it in all evaluation metrics. Finally, future work could incorporate a dynamic threshold to detect high DDoS attack traffic rate with high detection rates and low false positive rates.

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).

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

References

[1] M. Al-adaileh, M. Anbar, Y. Chong and A. Al-ani, "Proposed statistical-based approach for detecting distribute denial of service against the controller of software defined network (SADDCS)," *1st International Conference on Industrial, Electrical and Electronics*, Anyer, Indonesia, vol. 218, pp. 1–8, 2018.

[2] A. A. Bahashwan, M. Anbar, I. H. Hasbullah, Z. R. Alashhab and A. Bin-Salem, "Flow-based approach to detect abnormal behavior in neighbor discovery protocol (NDP)," *IEEE Access*, vol. 9, pp. 45512–45526, 2021.

[3] S. Al-Mashhadi, M. Anbar, R. A. Jalal and A. Al-Ani, "Design of cloud computing load balance system based on SDN technology," *Lecture Notes in Electrical Engineering*, vol. 603, no. January, pp. 123–133, 2020.

[4] A. A. Bahashwan, M. Anbar and N. Abdullah, "New architecture design of cloud computing using software defined networking and network function virtualization technology," *Lecture Notes in Electrical Engineering*, Cham, vol. 1073, no. September, pp. 705–713, 2019.

[5] W. Li, W. Meng and L. F. Kwok, "A Survey on openflow-based software defined networks: Security challenges and countermeasures," *Journal of Network and Computer Applications*, vol. 68, no. 2, pp. 126–139, 2016.

[6] V. Patil, C. Patil and R. N. Awale, "Security Challenges in software defined network and their solutions," *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Delhi, India, vol. 1, pp. 1–5, 2017.

[7] H. T. N. Tri and K. Kim, "Resource attack based on flow table limitation in SDN," in *Proc of the Korea Information Processing Society Conf.*, Korea, pp. 215–217, 2014.

[8] S. Scott-Hayward, G. O'Callaghan and S. Sezer, "SDN security: A survey," in *2013 IEEE SDN For Future Networks and Services (SDN4FNS)*, Trento, Italy, pp. 1–7, 2013.

[9] Y. Jarraya, T. Madi and M. Debbabi, "A survey and a layered taxonomy of software-defined networking," *2013 IEEE SDN For Future Networks and Services (SDN4FNS)*, vol. 16, no. 4, pp. 1955–1980, 2014.

[10] A. Shaghaghi, M. A. Kaafar, R. Buyya and S. Jha, "Software-defined network (SDN) data plane security: Issues, solutions, and future directions," in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, Springer, Cham, pp. 341–387, 2020.

[11] Nexusguard, "DDoS Threat Report FHY 2021," *Nexusguard* [Online], 2021 https://blog.nexusguard.com/threat-report/ddos-threat-report-fhy-2021. [Accessed: 22-Jan-2022].

[12] O. Olakanmi and K. Odeyemi, "Throttle: An efficient approach to mitigate distributed denial of service attacks on software-defined networks," *Security and Privacy*, vol. 158, no. 4, pp. 1–16, 2021.

[13] M. ALAdaileh, M. Anbar, I. Hasbullah, C. Wey and Y. Sanjalawe, "Detection techniques of distributed denial of service attacks on software-defined networking controller-a review," *IEEE Access*, vol. 8, pp. 143985–143995, 2020.

[14] A. Banitalebi Dehkordi, M. R. Soltanaghaei and F. Z. Boroujeni, "The DDoS attacks detection through machine learning and statistical methods in SDN," *Journal of Supercomputing*, vol. 77, no. 3, pp. 2383–2415, 2021.

[15] J. Singh and S. Behal, "A novel approach for the detection of DDoS Attacks in SDN using information theory metric," in *Proc. of the 2021 8th Int. Conf. on Computing for Sustainable Global Development, INDIACom 2021*, Delhi, India. no. March pp. 512–516, 2021.

[16] C. Fan, N. M. Kaliyamurthy, S. Chen, H. Jiang, Y. Zhou *et al.,* "Detection of DDoS attacks in software defined networking using entropy," *Applied Sciences (Switzerland)*, vol. 12, no. 1, pp. 370, 2022.

[17] J. A. Perez-Diaz, I. A. Valdovinos, K. K. R. Choo and D. Zhu, "A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning," *IEEE Access*, vol. 8, pp. 155859–155872, 2020.

[18] Y. Yu, L. Guo, Y. Liu, J. Zheng and Y. Zong, "An efficient SDN-based DDoS attack detection and rapid response platform in vehicular networks," *IEEE Access*, vol. 6, pp. 44570–44579, 2018.

[19] J. Cui, M. Wang, Y. Luo and H. Zhong, "DDoS detection and defense mechanism based on cognitive-inspired computing in SDN," *Future Generation Computer Systems*, vol. 97, no. 2, pp. 275–283, 2019.

[20] S. 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.
[21] K. S. Sahoo, D. Puthal, M. Tiwary, J. 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. 4, pp. 685–697, 2018.
[22] A. A. Bahashwan, M. Anbar, S. Manickam, I. H. Hasbullah and M. A. Aladaileh, "Propose a flow-based approach for detecting abnormal behavior in neighbor discovery protocol (NDP)," *International Conference on Advances in Cyber Security, Penang Malaysia*, vol. 15, pp. 83–94, 2021.
[23] M. A. Aladaileh, M. Anbar, I. H. Hasbullah and Y. K. Sanjalawe, "Information theory-based approaches to detect DDoS attacks on software-defined networking controller a review," *International Journal of Education and Information Technologies*, vol. 15, pp. 83–94, 2021.
[24] P. Čisar and S. M. Čisar, "EWMA statistic in adaptive threshold algorithm," in *2007 11th Int. Conf. on Intelligent Engineering Systems*, Hungary Budapest, pp. 51–54, 2007.
[25] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in *2015 Int. Conf. on Computing, Networking and Communications (ICNC)*, Anaheim, California, USA, pp. 77–81, 2015.
[26] Y. Hande and A. Muddana, "A survey on intrusion detection system for software defined networks (SDN)," *International Journal of Business Data Communications and Networking*, vol. 16, no. 1, pp. 28–47, 2020.
[27] J. Boite, P. A. Nardin, F. Rebecchi, M. Bouet and V. Conan, "Statesec: Stateful monitoring for DDoS protection in software defined networks," in *2017 IEEE Conference on Network Softwarization (NetSoft)*. Bologna, Italy: EEE, pp. 1–9, 2017.
[28] W. Wang, X. Ke and L. Wang, "A HMM-R approach to detect L-DDoS attack adaptively on SDN controller," *Futur Internet*, vol. 10, no. 9, pp. 83, 2018.
[29] M. Aladaileh, M. Anbar, I. H. Hasbullah, Y. K. Sanjalawe and Y. Chong, "Entropy-based approach to detect DDoS attacks on software defined networking controller," *Computers, Materials & Continua*, vol. 69, no. 1, pp. 373–391, 2021.
[30] M. Kia, "Early detection and mitigation of DDoS attacks in software defined networks," Master's Thesis, Ryerson University, Toronto, ON, Canada, 2015.