Proposed statistical-based approach for detecting distribute denial of service against the controller of software defined network (SADDCS)

Mohammad A. AL-Adaileh*, *Mohammed* Anbar*, *Yung-Wey* Chong 1, and *Ahmed* Al-Ani1

[1]National Advanced IPv6 Centre, Universiti Sains Malaysia, 11800 Gelugor, Penang, Malaysia

Abstract Software-defined networkings (SDNs) have grown rapidly in recent years be-cause of SDNs are widely used in managing large area networks and securing networks from Distributed Denial of Services (DDoS) attacks. SDNs allow net-works to be monitored and managed through centralized controller. Therefore, SDN controllers are considered as the brain of networks and are considerably vulnerable to DDoS attacks. Thus, SDN controller suffer from several challenges that exhaust network resources. For SDN controller, the main target of DDoS attacks is to prevent legitimate users from using a network resource or receiving their services. Nevertheless, some approaches have been proposed to detect DDoS attacks through the examination of the traffic behavior of networks. How-ever, these approaches take too long to process all incoming packets, thereby leading to high bandwidth consumption and delays in the detection of DDoS at-tacks. In addition, most existing approaches for the detection of DDoS attacks suffer from high positive/negative false rates and low detection accuracy. This study proposes a new approach to detecting DDoS attacks. The approach is called the statistical-based approach for detecting DDoS against the controllers of software-defined networks. The proposed approach is designed to detect the presence of DDoS attacks accurately, reduce false positive/negative flow rates, and minimize the complexity of targeting SDN controllers according to a statistical analysis of packet features. The proposed approach passively captures net-work traffic, filters traffic, and selects the most significant features that contribute to DDoS attack detection. The general stages of the proposed approach are (i) da-ta preprocessing, (ii) statistical analysis, (iii) correlation identification between two vectors, and (iv) rule-based DDoS detection.

1 Introduction

The Internet has grown rapidly on heterogeneous network structures with complicated networking protocols. Thus, conventional networks are now complex, network traffic is difficult to manage, and maintaining network security is significantly critical [1].In

* Corresponding author: m_aladaileh2003@nav6.usm.my and anbar@nav6.usm.my

addition, the rapid development of information and communication technologies has facilitated the exchange of enormous amounts of data and the sharing of network assets; this change has exposed these networks to attacks Moreover, network threats are on the rise [2].

Software-defined network (SDN) architecture [3], [4] has emerged as a new and novel method that meets network requirements in terms of network management and flexibility. SDNs are designed to establish high-level abstraction on top of hardware and software infrastructure. A fundamental characteristic of SDN architecture is the ability to isolate the control plane from the data plane. Therefore, the advantage of SDNs is centralized network control.

The present study illustrates the architecture of the proposed approach, which is called the Statistical-Based Approach For Detecting DDoS Against Controllers Of Software-Defined Networks (SADDCS) that aims to detect the presence of DDoS attacks against SDN controllers based on the statistical analysis of TCP and UDP features. This paper is organized as follows. Section 2 presents the existing studies pf detection techniques and its limitations. Section 3 describes the proposed SADDCS approach. Section 4 provides the conclusion and the future works.

2 Related Work

SDNs provide many advantages over traditional networks, but SDN also has some of drawbacks such as security threats due to depending the SDN on a centralized controller to monitor over the entire network. Hence, any threat leads to the creation of a single point of failure. One of the most widely known threats is the Distributed Denial of Service (DDoS) attack. This attack aims to exhaust network resources by sending a huge number of packets to the controller, which in turn causes network congestion. That is, a DDoS attack is considered as a one of the most dangerous threats security on SDN networks[5]. SDNs can be extremely affected by DDoS attacks because SDN controller is main part, which controls and manages all network actions. Thus, a breakdown of a controller might lead to a network collapse. Many techniques have been proposed to secure SDNs against DDoS attacks by detecting and mitigating this type of attacks. Entropy is known as a measure of randomness variable [6]. The detection based entropy works based on calculating the distribution of packets in a network according to different variables in the network, such as source IP address, source port or some other values of packet characteristics [7]. Therefore, entropy-based metrics are used in traffic analysis and anomaly detection. Mousavi and St-Hilaire [8] proposed a lightweight detection method to identify DDoS attacks to controllers in early stages. The method collects network statistics from the flow table and calculates entropy, which compares entropy value with a specific threshold in a fixed window size. However, time characteristic of this method is not considered during anomaly traffic detection, because it causes an excessive overhead in SDN controller. A hybrid mechanism based on security analysis is proposed in [9] to defend against DDoS attacks. This mechanism involves the use of a trust value and an entropy concept for detection purposes. The trust value is assigned by a trust value server, the trust value is higher than the attacker and lower than the legitimate users based on client access behavior. This mechanism allows a SDN controller to identify malicious users by monitoring their access behavior.

IDS is a system for detecting intrusions attempting to misuse data or to consume network resources. IDS collects network information from all sources, analyzes the information to identify network intrusion, and uses the information to detect DDoS attacks [10]. Thus, the use of IDS could help identify any abnormal traffic. Existing systems could be merged with different approaches to achieve network behavior with dynamic access control, such as rate bounds. A lightweight flow that is based on IDS is proposed in [11];

this method collects network statistics from OpenFlow (OF) switches periodically and employs statistical analysis for the collected information thus, the controller will process the information obtained from switches and then it sends the new rules to the switches. This proposed method can extract and collect proper information to classify flows as legitimate or abnormal traffics.

Attackers might generate low traffic flow that is similar to the normal traffic in order to trigger malicious flooding requests by connecting to different switches. A suggested an effective detection method is proposed in [12] that is designed to detect the low traffic flows by using the sequential probability ratio test (STRT). A mathematical model for estimating the impact of low-rate DDoS attacks by analyzing the vulnerability of the retransmission timeout mechanism [13]. The results showed that increasing the bottleneck buffer size in a network effectively protects against DDoS attacks. However, vulnerabilities may emerge when an attack is of different types, in which case it becomes difficult to identify.

Attackers may use a duration of time to achieve target destinations, that is, they send out attacks with a time period. Several DDoS attack detection methods do not consider time characteristics in detecting abnormal traffic. A methodology to detect SYN flooding attacks according to specific packet features is presented in [14]. Although this method is capable of large traffic flow detection, it does not consider the time characteristics of DDoS attacks. Table 1 summarizes the limitations of related works.

Table 1. Limitations of related works

Author/ Year	Limitations
Mousavi and StHilaire (2015)	-Time characteristic of this method is not considered. -Attack method handle a single host and then makes it more vulnerable.
Jantilaet al (2016)	-High false positives. -Does not distinguish DDoS attack traffic in the flash crowd traffic.
Georgi et al(2017)	- Takes long time to the attack detection - Cannot detect low traffic rate.
Dong et al (2016)	-Resources consumption in the controller.
Luo et al (2014)	- Unable to distinguish several kinds of attacks. -Consumes time during detecting low rate DDoS attacks.
Muhammad Nugraha et al (2014)	-Increase detection time.

3 Proposed Approach (SADDCS)

Detecting DDoS attacks that target SDN controller is still a challenging problem that has caught the attention of researchers and has prompted the proposal of efficient approaches to detect DDoS attacks. To achieve the study objectives, we present a set of stages for the proposed approach. The proposed approach aims to detect UDP and TCP DDoS attacks by monitoring the behavior of UDP and TCP traffic packets. The proposed approach consists of four stages, as shown in Fig 1. The first stage, i.e., data collection and preprocessing, aims to receive network traffic and filter TCP and UDP traffic. This stage consists of two steps: (a) network traffic capture and (b) network traffic filter. The second stage is the traffic statistical analysis that is generated from the switch table. This stage consists of three steps: (a) aggregated values related to entropy values, (b) aggregated values related to TCP and UDP packet header features, and (c) dynamic threshold

calculation. The third stage, i.e., correlation identification between two vectors, aims to come up with the second group of statistical features by checking the existence of a correlation between the two vectors. The fourth stage, i.e., rule-based DDoS detection, aims to detect the presence of DDoS attacks on the basis of the randomness of network traffic using the proposed rule 1 and the presence of a correlation between two vectors of statistical features using the proposed rule 2.

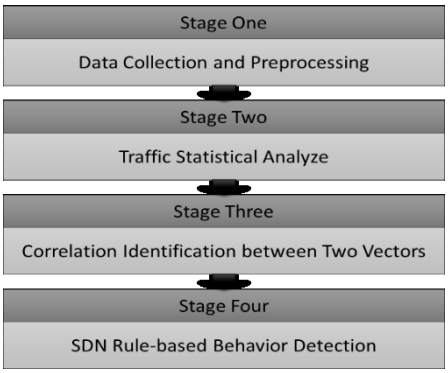

Fig.1. General Stages of Proposed Approach

3.1 Data Collection and Preprocessing

This stage aims to collect network traffic packets from switches after they are received from hosts. This stage consists of two steps: (1) network capture of all incoming packets targeting the switch and (2) network filtering that selects the significant features that contribute to the detection of TCP and UDP DDoS attacks.

3.1.1 Network traffic capture

In this step, all incoming traffic packets from hosts are received by the switches without losing any packet feature. The switch device monitors all incoming packets that match the packet with rules in the switch flow table that received rules from the controller regardless of their resource and destination IP. However, this step might include redundant features that do not contribute to the detection of DDoS attacks against SDN controllers.

3.1.2 Network traffic filtering

This step involves filtering the incoming network traffics. It consists of two main layers. The first layer aims to filter all the incoming network traffics and holds TCP and UDP packets to be used to detect DDoS attacks that relate to it. The second layer aims to extract TCP and UDP features that could be used to detect DDoS attacks.

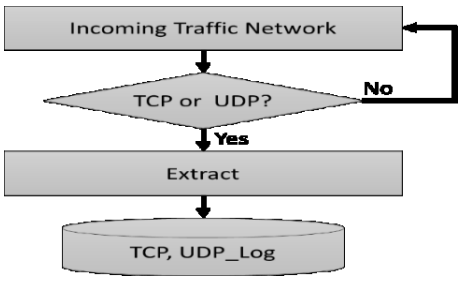

Fig. 2. Incoming network traffic filtering

Therefore, only the significant features that contribute to detect the DDoS attacks are filtered. The filtered TCP and UDP features will be stored into TCP_Log and UDP_Log files. Fig 2 shows the flow chart of network traffic filtering steps. The log files will be used as input to the next stage which is traffic statistical analyses (refer to section 0).

3.2 Traffic statistical analysis

Statistical analysis is used in SADDCS to detect different types of attacks. This stage is responsible for providing details about the selected features by calculating the aggregated values according to an analysis of TCP and UDP logs received from the previous stage. The aggregated values are divided into two groups: (1) aggregated values based on TCP and UDP packet header features, (2) aggregated values based on the entropy approach and (3) dynamic threshold. .

3.2.1 Aggregated values related to entropy values

Entropy approaches show impressive results in terms of detecting different types of attacks. Entropy is used for DDoS detection mainly because of its ability to measure randomness associated with a source IP and destination IP in the packets that are entering a network using the equation below.

$$H(X) = -\sum_{i=1}^{n} P(x_i)\, log_b\, P(x_i) \quad (1)$$

Therefore, in the case of a DDoS attack, the entropy value of the source and destination IP address increases because the attacker always spoofs its source IP address on each packet transmission or changes the destination IP address. Traffic randomness can occur if the entropy value exceeds a threshold (Th), the value of which is calculated dynamically on the basis of the adaptive threshold algorithm.

3.2.2 Aggregated values related to packet features

This step extracts the features of TCP and UDP from TCP_log and UDP_Log and performs the following statistical analysis for each log table. (i) The number of packets that have sent from one source to specific destination (Outbound). (ii) The number of packets that have received by specific destination (Inbound). Thus, the output of this step comprises two log files: (1) statistical_TCP_Log and (2) statistical_UDP_Log. Moreover, it facilitates the process of attack detection by an alert that is triggered if the number of packets exceeds a predefined threshold (t).

3.2.3 Dynamic threshold

The threshold value, which is a critical component for detecting DDoS attacks, is determined on the basis of the aggregation of the data for the adaptive threshold algorithm parameter. In increasing the accuracy of detection, the threshold value must be updated according to the incoming network traffic condition. The adaptive threshold algorithm relies on testing whether the traffic measurement over a given interval exceeds a particular threshold; it can be defined as follows:

$$X_n \geq (\alpha + 1) . \mu_{n-1} \tag{2}$$

where: X_n: number of packets in the nth time interval

α: a positive parameter (α>0) that indicates the percentage above the mean value that is considered evidence of anomalous behavior.

$\mu\_(n-1)$: mean rate estimated from measurements prior to n . The mean value (μ_n) can be computed using the Exponential Weighted Moving Average (EWMA) which represented as the following formula:

$$\mu_n = \lambda \cdot \mu_{n-1} + (1-\lambda) \cdot X_n \tag{3}$$

3.3 Correlation Identification between Two Vectors

This step aims to calculate (r), which represents the existence of a correlation between two vectors A and B. Vector A represents the data of statistical TCP_log and statistical_UDP_log while B represents the probability_TCP_log and probability_UDP_log. Pearson's correlation coefficient is adopted to calculate the value of r on the basis of the equation below.

$$r_{AB} = \frac{\left(n\sum AB - (\sum A)(\sum B)\right)}{\sqrt{((n_A \sum A^2 - (\sum A)^2)(n_B \sum B^2 - (\sum B)^2))}} \tag{4}$$

The correlation coefficient(r) ranges from −1 to 1. A value of 1 implies that a linear equation describes the relationship between (A) and (B) perfectly, with all data points lying on a line for which (B) increases as (A) increases. A value of −1 implies that all data points lie on a line for which (B) decreases as (A) decreases. Finally, a value of 0 implies that there is no linear correlation between the variables.

3.4 SDN Rule-based Behavior Detection

This stage is a core stage in the proposed SADDCS approach. It aims to propose rules to detect DDoS attacks against SDN controllers according to the statistical analysis. The assumption is that DDoS attacks can be detected if one of the statistical analysis results exceeds the threshold. The rules are as follows.

3.4.1 Rule 1: Entropy-based rule

The first proposed rule will be applied to probability_TCP_log or probability_UDP_log. The entropy value that matches the proposed rule will be identified as DDoS attack. For probability_TCP_log and probability_UDP_log the following rules will be applied:

If Entropy (probability_TCP_log)) >Th or Entropy (probability_UDP_log.)) >Th, then they have accessed suspicious traffic behavior.

3.4.2 Rule 2: Correlation-based rule

The second proposed rule will be applied to probability_TCP_log and statistical_TCP_log or probability_UDP_log and statistical_UDP_log. The correlation coefficient (r) value that match the proposed rule will be identified as DDoS/DoS attack. For probability_TCP_log and probability_UDP_log the following rules will be applied:

If correlation (statistical_TCP_log, probability_TCP_log)) >Th or If correlation (statistical_UDP_log, probability_UDP_log)) > Th, then they have accessed suspicious traffic behavior.

4 Conclusion and Future Work

SDN controllers are important in SDNs, and several approaches have been proposed to secure SDNs controllers against DDoS attacks. However, these approaches suffer from various limitations, such as additional overhead for SDN controllers, high false positive rates, and the need for external resources to detect DDoS attacks. Therefore, the proposed approach intends to capture network traffic, to filter traffic, and to select the most significant features that contribute to the detection of DDoS attacks. Moreover, the SADDCS approach is designed on the basis of a statistical approach, entropy variation based on statistical TCP and UDP packet header feature, a correlation between statistical_TCP, UDP_Log and probability of packets, and rule-based behavior DDoS detection. The main stages of SADDCS are (i) data preprocessing, (ii) statistical analysis, (iii) correlation identification between two vectors, and (iv) rule-based DDoS detection. In the future, an implementation of the proposed approach will be presented and an evaluation of it against existing approaches will be done.

References

1. J. Chen, X. Zheng, and C. Rong, “Survey on software-defined networking,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9106, no. 1, pp. 115–124, (2015).
2. D. Kreutz and F. Ramos, “Software-Defined Networking: A Comprehensive Survey,” arXiv Prepr. arXiv …, p. 49, (2014).
3. A. Samson and N. P. Gopalan, “Software Defined Networking,” Proc. Int. Conf. Informatics Anal. - ICIA-16, pp. 1–6, (2016).
4. S. . A. Scott-Hayward, S.a , Natarajan, S.b , Sezer, “Survey of Security in Software Defined Networks,” Surv. Tutorials, vol. 18, no. 1, pp. 623–654, (2016).
5. H. D. Zubaydi and M. Anbar, “Review on Detection Techniques against DDoS Attacks on a Software-Defined Networking Controller,” (2017).
6. A. X. Liu, “l An Advanced Entropy-Based DDOS Detection Scheme Jie Zhang, Zheng Qin, Lu Ou, Pei Jiang , JianRong Liu,” pp. 67–71, (2010).
7. M. Jackson, D. Nelson, and S. Stirk, Lecture Notes in Computer Science. (2005).
8. S. M. Mousavi and M. St-Hilaire, “Early detection of DDoS attacks against SDN controllers,” 2015 Int. Conf. Comput. Netw. Commun. ICNC 2015, pp. 77–81, (2015).
9. Y. Jiang, X. Zhang, Q. Zhou, and Z. Cheng, “An Entropy-Based DDoS Defense Mechanism in Software Defined Networks,” in International Conference on Communicatins and Networking in China, pp. 169–178, (2016)

10. A. S. Syed Navaz, V. Sangeetha, and C. Prabhadevi, “Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud,” Int. J. Comput. Appl., vol. 62, no. 15, pp. 975–8887, (2013).
11. G. A. Ajaeiya and A. F. B. Ids, “Flow-Based Intrusion Detection System for SDN,” pp. 787--793, (2017).
12. P. Dong, X. Du, H. Zhang, and T. Xu, “A detection method for a novel DDoS attack against SDN controllers by vast new low-traffic flows,” 2016 IEEE Int. Conf. Commun. ICC 2016, (2016).
13. J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, “On a mathematical model for low-rate shrew DDoS,” IEEE Trans. Inf. Forensics Secur., vol. 9, no. 7, pp. 1069–1083, (2014).
14. M. Nugraha, I. Paramita, A. Musa, D. Choi, and B. Cho, “Utilizing OpenFlow and sFlow to Detect and Mitigate SYN Flooding Attack TT -,” J. Korea Multimed. Soc., vol. 17, no. 8, pp. 988–994, (2014).