Advances and Applications in Mathematical Sciences
Volume 22, Issue 5, March 2023, Pages 1013-1023
© 2023 Mili Publications, India

ISSN 0974-6803

COMPARATIVE STUDY OF DYNAMIC THRESHOLD BASED DISTRIBUTED DENIAL OF SERVICES ATTACK DETECTION TECHNIQUES IN SOFTWARE DEFINED NETWORK

BINEET KUMAR JOSHI and MAHESH CHANDRA JOSHI

Research Scholar, Department of IT
Kumaun University
Nainital, Uttarakhand, India
E-mail: bineetjoshi@gmail.com

Professor, Department of Mathematics
Kumaun University
Nainital, Uttarakhand, India
E-mail: mcjoshi69@gmail.com

Abstract

A Distributed Denial of Service (DDoS) attack attempts to make a server or network inaccessible to its legitimate users. Entropy-based approaches are very popular to detect DDoS in Software Defined Network (SDN). An important aspect of this approach is to identify the threshold value to declare that incoming data flow is malicious or legitimate. The threshold value may be chosen as static or dynamic. This paper attempts to provide an overview of the current advances in the research that has been conducted over the last few years on DDoS detection approaches, which utilise dynamic threshold values. The comparison results show that solutions based on dynamic thresholds have low false positive and high detection rate at the cost of high computational resource overhead.

1. Introduction

Software Defined Networks (SDN) have evolved as a game-changing networking paradigm capable of meeting the rising requirements of future networking. In comparison to traditional networking architectures, the essential feature of the SDN architecture is the separation of the control and

2020 Mathematics Subject Classification: 68M25, 68M11.

Keywords: Dynamic Threshold, DDoS, SDN, Entropy.

Received April 9, 2022; Accepted January 13, 2023

data planes. This control plane behaves as if it were an operating system, capable of transmitting commands and making modifications via its interface. While centralised control can be considered as a significant benefit of SDN, it may also represents a single point of failure if it is rendered unreachable by a DDoS attack. SDN divides the control plane from the forwarding plane and enables network administrators to take control of the control plane (Xia et al., [1]).

Distributed Denial of Service (DDoS) attacks are well-known types of cyber-attacks which overwhelm the resources of a network or a computer by flooding them with traffic. The attacker's two primary objectives are bandwidth exhaustion and the unavailability of resources to intended users (Douligeris and Mitrokotsa, [2]). While SDN's capabilities can be used to defend against these attacks, it is critical that the centralised architecture of SDN is protected from DDoS attacks. For this goal, researchers have developed a variety of methodologies like entropy-based statistical approaches, knowledge base techniques, and machine learning.

Entropy quantifies the randomness of a network. Claude Shannon developed the term "uncertainty measurement" in 1948 (Shannon, 1948). By examining the entropy value, it is possible to identify a DDoS attack if network activities deviates from regular network behaviour. To identify DDoS attacks using entropy, we need a threshold value (Mousavi and St-Hilaire, [4]). An attack can be declared if the estimated entropy exceeds or falls below a threshold. Thus, selecting the right threshold value is critical for entropy-based DDoS detection systems. A threshold value may be static, based on the window width and IP header attributes, or dynamic, based on the time and nature of the traffic (Oshima et al., [5]).

We examined and offered a comparative study of recent breakthroughs in DDoS detection research based on the dynamic threshold in this work. The effects of using dynamic threshold values on the DDoS detection algorithm's performance are discussed. To our knowledge, this is the first study that tries to assess the role of choosing a dynamic threshold on entropy-based DDoS attack detection approaches in SDN.

2. Software Defined Networks

Software-Defined Networking term was coined to describe the concepts and efforts surrounding Stanford University's academic projects (Kreutz et al., [6]). SDN's fundamental principle is the segregation of the control and data planes, which enables organisations to considerably innovate in terms of network design. This means the programmability of SDN networks has greatly increased. Network traffic handling and SDN-enabled device configuration improve with this (Nunes et al., [7]).

In traditional networks, equipment is often configured with embedded control logic. If the policy needs to be updated, everything must be manually adjusted utilizing the manufacturer's specific commands, which would be a significant expense. Traditional switches make it difficult to apply new inventive policies since they have propriety issues. However, thanks to the centralised controller, policy modification is a fast operation. The old network provides less testing space for the new policies, but SDN has more extensive testing chances.

SDN offers tools to resist DDoS attacks, but attackers targeted SDN itself. Security experts have been highly concerned about DDoS detection in recent years. Many researchers are working on developing an effective DDoS attack detection method and have proposed strategies to mitigate the effects of DDoS attacks (Sagar et al., [8]).

3. Distributed Denial of Service Attack

A DDoS assault is a type of cyber-attack that targets a specific online service with the intent of disabling it through the use of massive amounts of traffic from various sources (Mirkovic and Reiher, [9]). Attackers create "botnets," or networks of compromised machines, by spreading malicious software via a variety of techniques, such as e-mails or phoney software. Once a device is infected, it is managed from the outside, without the knowledge of the system's owners, and is utilised as an army to launch attacks against any target.

In February 2018, GitHub was the target of a 1.35 Tbps DDoS attack. Another important instance is a DDoS attack utilising the Mirai botnet, which peaked at 1.1 Tbps in volume and disrupted a considerable portion of the internet's services in October 2016. According to Kaspersky Lab, 2021 will see a doubling of DDoS assaults compared to the fourth quarter of 2020, as well as an 80 percent increase over the same quarter last year (Kaspersky, [10]). Three primary methods for detecting DDoS are briefly discussed (Joshi et al., [11]).

3.1. Machine Learning-Based methods

As suggested by (Singh and Bhandari, [12]) "Machine learning provides defence systems with an ability to self-learn from a large set of data to identify hidden patterns and make decisions requiring no explicit instructions."

3.2. Methods Relying on Knowledge-Based Techniques

Knowledge-based algorithms analyse traffic for DDoS detection using publicly available datasets or information about related assaults. These methods build detection skills by analysing existing DDoS attack traffic signatures. This approach identifies and detects DDoS assaults by correlating the geographical and temporal characteristics of DDoS attack traffic.

3.3. Statistical Techniques

DDoS attack traffic has characteristics that separate it from normal traffic. DDoS can be detected using statistical qualities of IP packet header fields, such as source IP address entropy. These methods generate a numerical model of typical traffic and then analyse incoming traffic statistically to determine whether it fits the model or not.

4. Dynamic Threshold Based DDoS Detection Techniques

Finding the right threshold values to distinguish regular and abnormal traffic can be considered the most crucial component of DDoS detection approaches. The static threshold's downside is that it generates a large number of false alerts, making network managers' jobs more difficult. As a result, the usage of dynamic thresholds in statistical analysis approaches is growing. Dynamic threshold settings are validated in relation to the time and nature of the traffic. This section examines recent work on DDoS attack detection and mitigation in SDNs using dynamic threshold values.

The dynamic entropy model was created using the notion of alive communication and integrates information entropy with the characteristics of netflow conversation. The authors (Jian-Qi et al., [13]) make a comparison between their method and the static entropy-based detection method. In comparison to the static entropy-based technique, the dynamic entropy-based model seems to have a low false positive rate.

To identify DDoS, the researchers (Fouladi et al., [14]) use an approach based on projecting future traffic features and chaos theory, as well as an exponential filter and a dynamic threshold mechanism. The dynamic threshold was calculated by combining an exponential filter with the normalised time series of unique destination IP addresses. The authors claim that the method has high prediction accuracy as well as a low false positive rate.

The authors (Hong et al., [15]) investigates the dynamic DDoS attack threshold in the SDN context. The authors present a viable DDoS detection and defence strategy by utilising SDN features. Based on the collected traffic status, the proposed model computes the entropy of the network environment and assesses a dynamic threshold based on network conditions to determine if the environment is vulnerable to DDoS attacks.

With a dynamic threshold detection method, the authors (David and Thomas, [16]) provide an effective statistical approach to identify attacks. The method did not use time series models. The threshold value was compared to four attributes. These threshold values change for various network situations and are updated periodically. The dynamic threshold was used because network activity and user behaviour change over time, and a fixed threshold did not account for these variations.

A Secure and AgiLe (SEAL) framework based on SDN for shielding the applications of smart city from DDoS attacks was introduced in (Bawany and Shamsi, [17]). Proactive, Active, and Passive filters were suggested and implemented to determine the dynamic threshold for several applications. This framework and its elements have been experimentally evaluated for the purpose of detecting DDoS attacks. The D-Defense module detects and mitigates data plane attacks, protecting smart city applications from DDoS attacks. This component uses a modified estimated-weighted moving average (EWMA) filter to evaluate dynamic thresholds in near real-time for various applications.

The authors (Fouladi et al., [14]) proposed a dynamic threshold that was computed with the help of a modified adaptive threshold algorithm (MATA). The original ATA uses the Exponential Weighted Moving Average (EWMA) method, which generates a significant number of false alarms. This method has a small overhead for determining the network infrastructure's baseline traffic information. It decreases false alarms significantly by generating dynamic and adaptive thresholds depend on the baseline. As a result, the false negative rate is decreased dramatically because the attack may be dismissed as soon as the DDoS Mitigation application gets the abnormal event information.

In the work (Majed et al., 2020), a dynamic threshold was used to determine the best answer from among multiple possible options. For each characteristic, the Z-score value was compared to the Coefficient of Variation (CV). To obtain Z-scores, three attributes were aggregated together, and then three values associated with those Z-scores were compared to each other to identify how extreme the Z-scores were. A light and fast statistical technique for DDoS detection has been suggested. NetFlow statistics were compiled and summarised to reduce the amount of time and effort spent gathering and processing the data.

The authors (Aryal et al., [20]) offer a new technique for detecting DDoS attacks that integrates machine learning with a statistical approach. Iteratively collected data sets were examined for dynamic threshold. A total of sixteen features were extracted, and correlation values between the features were examined using machine learning. A threshold for attacks was determined through experimentation using datasets from simulated SDN networks. For the dynamic threshold, a time sequence-based computing method was utilised to enable rapid detection of DDoS attacks occurring over a short time period.

Using a dynamic threshold, the authors (Mohammad et al., 2022) offered a method for detecting low-rate DDoS attacks on the SDN controller. The proposed technique was evaluated using four simulated cases. The proposed approach has an average detection rate of roughly 95% and a false-positive rate of between 3.3 and 4.7 percent. An exponentially weighted moving average was used to calculate the dynamic threshold (EWMA). This work is mostly concerned with detecting low-rate DDoS attacks. It cannot handle high-volume DDoS attacks.

In this research, the authors (Tsobdjou et al., [22]) offer an online system designed to identify flooding attacks in a client-server environment in a short amount of time. The detection system is comprised of five distinct parts. When the entropy fell below a threshold, suspicious behaviour was identified. The calculation of the threshold was based on Chebyshev's theorem. This research proposes a dynamic threshold technique to track changes in valid traffic. The suggested detection method outperforms previous comparable systems in terms of detection rate, false positive rate, precision, and overall accuracy.

5. Results

Table 1 shows the impact of dynamic threshold on the performance of DDoS detection algorithms. Researchers have used either the time series method or an algorithm based on attributes of data packets to find the dynamic threshold values. The performance of all the solutions has been improved in two broad ways: a decrease in false positive rates and an increase in attack detection rates. Dynamic thresholds vary with network conditions and change accordingly. It requires the use of continuous computing resources, which results in resource overhead.

Table 1. Comparisons of Solutions based on Dynamic Threshold.

Reference	Year	Type of threshold value (s)	Methodology used to find the threshold values	Performance improvement by using dynamic values	Resource Overhead
[13]	2013	Dynamic and Static	Timing characteristics of hosts and their correlations	Yes [Higher detection rate and low false positive rate]	Yes
[14]	2020	Dynamic	Normalised time series of unique destination IP addresses	Yes [High prediction accuracy as well as a low false positive rate]	Yes

[15]	2019	Dynamic	Using traffic time window	Yes [Works well even for high data traffic]	Yes
[16]	2019	Dynamic	Dynamic threshold algorithm	Yes [Effective detection rate and accuracy]	Yes
[17]	2019	Dynamic	D-Defense module with three filters	Yes [Detects DDoS in real time for applications of smart cities and has a low false positive rate]	Yes, depending on switches directly connected to the SDN controller
[18]	2020	Dynamic	Modified adaptive threshold algorithm	Yes [False negative rate is reduced and the accuracy is Increased]	Yes
[19]	2020	Dynamic	Coefficient of Variation	Yes [Efficient to detect attacks and have low false alarm rate]	Yes
[20]	2021	Dynamic	Time sequence-based method	Yes [High accuracy and preciseness]	Yes
[21]	2022	Dynamic	Exponentially weighted moving average (EWMA) based method	Yes [False negative rate is reduced and the accuracy is Increased]	Yes
[22]	2022	Dynamic	Chebyshev's theorem	Yes [Better detection rate, false	Yes

				positive rate, precision and overall accuracy]	
[23]	2022	Dynamic	Confidence Interval along with average entropy with standard deviation	Yes [Better detection rate, fast and accuracy]	Yes

6. Conclusion

In this work, we compared the recent solutions to detect DDoS attacks in SDN using dynamic threshold. Developing a method for DDoS attack detection with high accuracy and low false alarms is a desire of every cyber security researcher. Our studies have identified that using dynamic threshold for DDoS attack detection is one way to achieve it. Furthermore, it has been observed that using time series analysis or its variants results in the detection of these attacks with high accuracy. Although it may lead to higher resource (memory, processor, or bandwidth) utilization. This paper will help researchers to identify the appropriate algorithm for choosing the dynamic threshold as per their work requirements. It is a challenge for researchers to reduce the resource overhead while maintaining a high attack detection rate.

References

[1] W. Xia, Y. Wen, C. H. Foh, D. Niyato and H. Xie, A Survey on Software-Defined Networking, IEEE Communications Surveys and Tutorials 17(1) (2015), 27-51. https://doi.org/10.1109/comst.2014.2330903

[2] C. Douligeris and A. Mitrokotsa, DDoS attacks and defense mechanisms: a classification, IEEE, (2003). https://doi.org/10.1109/isspit.2003.1341092

[3] C. E. Shannon, A mathematical theory of communication, Bell System Technical Journal 27(3) (1948), 379-423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

[4] S. M. Mousavi and M. St-Hilaire, Early Detection of DDoS Attacks Against Software Defined Network Controllers, Journal of Network and Systems Management 26(3) (2017), 573-591. https://doi.org/10.1007/s10922-017-9432-1

[5] S. Oshima, T. Nakashima and T. Sueyoshi, DDoS Detection Technique Using Statistical Analysis to Generate Quick Response Time, IEEE, (2010). https://doi.org/10.1109/bwcca.2010.153

[6] D. Kreutz, F. M. V. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolky and S. Uhlig, Software-Defined Networking: A Comprehensive Survey 103(1), Institute of Electrical and Electronics Engineers (IEEE), (2015). https://doi.org/10.1109/jproc.2014.2371999

[7] B. A. A. Nunes, M. Mendonca, X. N. Nguyen, K. Obraczka and T. Turletti, A survey of software-defined networking: past, present, and future of programmable networks, IEEE Communications Surveys and Tutorials 16(3) (2014), 1617-1634. https://doi.org/10.1109/surv.2014.012214.00180

[8] A. Sagar, B. K. Joshi and N. Mathur, A Study of Distributed Denial of Service Attack in Cloud Computing (DDoS), Edition on Cloud and Distributed Computing: Advances and Applications, HCTL Open Science and Technology Letters (STL) 2 (2013), 1-7.

[9] J. Mirkovic and P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communication Review 34(2) (2004), 39-53. https://doi.org/10.1145/997150.997156

[10] Kaspersky, (2021, May 26), Kaspersky research finds DDOS attacks tripled year-on-year in Q2 2020. Usa.Kaspersky.Com. https://usa.kaspersky.com/about/pressreleases/2020_kaspersky-research-finds-ddos-attacks-tripled-year-on-year-in-q2-2020

[11] B. Kumar Joshi, N. Joshi and M. Chandra Joshi, Early Detection of Distributed Denial of Service Attack in Era of Software-Defined Network, IEEE, (2018). https://doi.org/10.1109/ic3.2018.8530546

[12] M. P. Singh and A. Bhandari, New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges, Computer Communications 154 (2020), 509-527. https://doi.org/10.1016/j.comcom.2020.02.085

[13] Z. Jian-Qi, F. Feng, Y. Ke-xin and L. Yan-Heng, Dynamic entropy based DoS attack detection method, Computers and Electrical Engineering 39(7) (2013), 2243-2251. https://doi.org/10.1016/j.compeleceng.2013.05.003

[14] R. F. Fouladi, O. Ermiş and E. Anarim, A DDoS attack detection and defense scheme using time-series analysis for SDN, Journal of Information Security and Applications, 54 (2020), 102587. https://doi.org/10.1016/j.jisa.2020.102587

[15] G. C. Hong, C. N. Lee and M. F. Lee, Dynamic Threshold for DDoS Mitigation in SDN Environment, 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), (2019, November). https://doi.org/10.1109/apsipaasc47483.2019.9023229

[16] J. David and C. Thomas, Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic, Computers and Security 82 (2019), 284-295. https://doi.org/10.1016/j.cose.2019.01.002

[17] N. Z. Bawany and J. A. Shamsi, SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks, Journal of Network and Computer Applications 145 (2019), 102381. https://doi.org/10.1016/j.jnca.2019.06.001

[18] N. Haymarn Oo, A. Cahyadi Risdianto, T. Chaw Ling and A. Htein Maw, Flooding attack detection and mitigation in SDN with modified adaptive threshold algorithm, International Journal of Computer Networks and Communications 12(3) (2020), 75-95. https://doi.org/10.5121/ijcnc.2020.12305

[19] H. Majed, H. Noura, O. Salman, M. Malli and A. Chehab, Efficient and Secure Statistical DDoS Detection Scheme, Proceedings of the 17th International Joint Conference on E-Business and Telecommunications Published, (2020). https://doi.org/10.5220/0009873801530161

[20] B. Aryal, R. Abbas and I. B. Collings, SDN enabled DDoS attack detection and mitigation for 5G networks, Journal of Communications 16(7) (2021).

[21] M. A. Aladaileh, M. Anbar, I. H. Hasbullah, A. A. Bahashwan and S. Al-Sarawn, Dynamic Threshold-Based Approach to Detect Low-Rate DDoS Attacks on Software-Defined Networking Controller, Computers, Materials and Continua 73(1) (2022), 1403-1416. https://doi.org/10.32604/cmc.2022.029369

[22] L. D. Tsobdjou, S. Pierre and A. Quintero, An Online Entropy-based DDoS Flooding Attack Detection System with Dynamic Threshold, IEEE Transactions on Network and Service Management 19(2) (2022), 1679-1689. https://doi.org/10.1109/TNSM.2022.3142254

[23] D. V. Nhat, L. D. Huy, C. Q. Truong, B. T. Ninh and D. T. T. Mai, Applying Dynamic Threshold in SDN to Detect DDoS Attacks, International Conference on Advanced Technologies for Communications (ATC), (2022). https://doi.org/:10.1109/ATC55345.2022.9943031