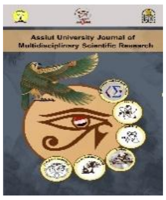
Assiut University Journal of Multidisciplinary Scientific Research (AUNJMSR)
Faculty of Science, Assiut University, Assiut, Egypt.
Printed ISSN: 2812-5029
Online ISSN: 2812-5037
Vol. 51(3): 229 – 241 (2022)
https://aunj.journals.ekb.eg/



Time Series Similarity for Detecting DDoS Flooding Attack

Fatma A. Hussain* and Dalia Nashat

Department of Information Technology, Faculty of Computers and Information, Assiut University, Assiut, Egypt.

*Corresponding Author: fatma.abdelhalem@aun.edu.eg

ARTICLE INFO

Article History:
Received: 2022-04-11
Accepted: 2022-05-16
Online: 2022-08-30

Keywords:
DDoS Flooding Attack, Time Series similarity, Dynamic Time Warping, Exponential Weighted Moving Average

ABSTRACT

Distributed Denial of Service attack (DDoS) is one of many types that hit computer networks. For security specialists, this attack is one of their main concerns. The DDoS flooding attack prevents the legitimate users from using their desired services by consuming the server resources. It includes many types depending on the targeted layer as example, SYN flooding attack and UDP attack are lunched into the network layer, while the HTTP flooding attack and DNS attack into the application layer. The DDoS flooding attack takes use of a flaw in the internet routing system by flooding the server with packets bearing faked IP addresses. Due to the internet routing infrastructure's inability to discriminate between spoofed and legitimate packets, using these spoofed IP addresses makes it difficult to detect this attack. Based on time series similarity measurement, we offer a new detection approach for DDoS flooding attacks in this paper. By computing the cost function value and by comparing this value with a modified adaptive threshold, legal and malicious traffic intervals can be clearly distinguished. Our results show the efficiency of the proposed detection approach through the obtained detection rates.

INTRODUCTION

Nobody can deny that network-based computer systems have become an essential part of our daily life especially after the COVID-2019 pandemic. These systems are extremely important in our personal and professional lives, especially now that people all around the world are working, studying, shopping, and having fun online in unprecedented numbers. On the other hand, the rise in attacks has paralleled the rapid advancement of network connectivity and service accessible technologies.

DDoS attacks have emerged as one of the most serious risks to computer networks, posing a substantial threat to a variety of network-based services. DDoS attacks drove big websites like Amazon, CNN, and Yahoo to close at the end of the twentieth century [1]. In 2015 DDoS attack made the BBC domain, their on-demand TV service, and radio player go offline for 3 hours. It also made its mark in 2016, where 274 of the DDoS attacks were observed and reached over 100 Gbps while 46 DDoS attacks registered above 200 Gbps. GitHub was hit with a DDoS attack that clocked in at 1.35 terabits per second and lasted for roughly 20 minutes in 2018. Imperva reported a DDoS attack in April 2019 that recorded its highest value per second at 580 million packets. Amazon Web Services was hit by a gigantic DDoS attack in February 2020 [2].

The DDoS flooding attacks mainly aim to exhausts the victim designated resources through flooding it with a large amount of worthless network traffic. Depending on exploiting the system vulnerabilities of the victim, DDoS attacks are launched by using multiple spoofed IP addresses. As a result, legitimate users are unable to access their intended service [3]. Therefore, it's difficult to spot these attacks because the internet routing system can't differentiate between a legal packet and one that's been faked. The DDoS flooding attacks can be launched into network-layer by using network protocols (e.g. TCP, UDP and ICMP) or into application-layer (e.g. HTTP, DNS and SMTP). SYN flooding attacks are the most prevalent network layer kind, while HTTP flooding attacks are the most common application layer type [4].

In this study, we describe a new method for detecting DDoS flooding attacks that uses time series similarity measurement to assess the similarity across network time series, allowing us to quickly discover dissimilarity intervals. Due to the dissimilarity between the signals of different attributes under the DDoS flooding attack, the former strategy yielded a high rate of detection. The systematic of the rest sections as follows, Section 2 reviews the concerned related work of this research area. Section 3 describes the DDoS flooding attack mechanism. Section 4 explains in detail the time series similarity and the used measurement. The methodology of our proposed method is introduced in Section 5. Experimental results are presented in Section 6. Section 7 concludes this work.

RELATED WORK

In the past two decades, many DDoS attack detection techniques have been introduced. Anomaly-based detection and signature-based detection are the two basic categories in which these techniques can be classified. Anomaly detection approaches rely on irregular behavior in network traffic to detect anonymous attacks, whereas signature-based methods are ineffective in detecting new or unknown attacks [5]. The anomaly-based methods can be broken down into three divisions, statistical methodologies, signal processing techniques, and machine learning techniques.

Many statistical approaches such as entropy, principal components analysis, hidden Markov models, mutual information, correlation, and covariance have been used for network anomalies detection [6]. The method in [7] offered a statistical method for dealing with DDoS mitigation. Using Markov decision processes with multiple objectives, It is used to discover the best Moving Target Defense strategy by resolving the shuffling efficacy vs. cost trade-off. Based on a statistical measurement (Odds Ratio), authors in [8] could detect the DDoS flooding attacks by exploring the odds ratio to determine the risk factor of any incoming traffic to the server.

Signal processing techniques have been employed by several researchers to detect anomalies in network traffic. Authors of [9] provided a detection approach for estimating the self-similarity of OpenFlow traffic characteristics, with Hurst exponents used to evaluate the degree of self-similarity. They discovered that regular OpenFlow traffic has a low degree of self-similarity, whereas attacks have a high degree of self-similarity. In [10], the authors used

Multifractal Detrended Fluctuation Analysis and a modified adaptive threshold to detect aberrant behavior of the time series TCP protocol. They calculated each interval's local fluctuations and compared their results with the modified threshold to efficiently detect attack intervals. In [11], the authors developed a new approach for detecting TCP DoS/DDoS attacks. They separated TCP traffic into control and data planes and used the Dynamic Time Warping (DTW) technique to align them.

Authors in [12] employed a machine learning based technique to deal with the problem of DDoS attack detection, by integrating sequential feature selection with the multilayer perceptron to choose the best features during the training phase (MLP). In SDN environment, an intrusion detection system based on Deep Learning is presented to mitigate DDoS attacks [13]. Lucky et al. proposed a machine learning strategy to detect DDoS attacks [14]. Their method was trained with a small number of features. For anomaly identification, authors in [15] presented a novel time-based method that employs an autoencoder.

DDoS FLOODING ATTACK

The main idea behind the DDoS flooding attacks is to exhaust the victim designated resources by flooding it with huge numbers of useless network traffic by using multiple spoofed IP addresses. There are various types of DDoS flooding attacks, including UDP, ICMP, HTTP, and SYN flooding attacks. As a case study, we'll focus on the SYN flooding type.

Mainly, the SYN flooding attackers exploit a known TCP weakness at the connection sequence (i.e. three-way handshake). Where they send a high rate requests of half-open connection (SYN packets), therefore overwhelming the victim server by consuming its resources.

A series of packets is exchanged between the client and the server during the usual establishing of a TCP connection. The first packet (SYN packet) is a connection-starting request from the client to the server. The server responds with a SYN- ACK packet for acknowledging the client's request. Finally, the connection is established when the client sends an ACK message back.

During SYN flooding attacks, the victim server is overwhelmed with repeated SYN packets from the attacker with faked IP addresses. As a result, the server's resources are depleted while waiting for the ACK packets to complete the connection, which will never be transmitted, resulting in a denial of service. As a result, early detection of a DDoS attacks has become more vital as a key building component in the development of an integrated security system.

As mentioned, under the SYN flooding attack there are a significant difference between the request packet numbers and the response packet numbers. Thus an obvious dissimilarity is found between the request and the response time series. To estimate the similarity of the request and the response time series, the Dynamic Time Warping is applied. So the cost function value of the optimal alignment of the former series can be computed for each time interval in the traffic to detect the attack intervals accurately.

TIME SERIES SIMILARITY

Measuring similarity of two time series plays a vital role in time series analysis, where it is involved into a diverse range of time series analysis tasks such as, clustering, classification, segmentation, prediction, anomaly detection [16]. For example in medical signal analysis the similarity measurement is the prior stage before the disease clustering and prediction stage [17]. Many different measures exist for time series similarity, these measures can be roughly categorized into: time-rigid measures (Euclidean distance), time-flexible measures (dynamic time warping), feature-based measures (Fourier coefficients), and model-based measures (auto regression and moving average model). Among the mentioned measurements, the DTW is probably the most popular and established ones in addition to its applicable to accommodate the deformation of time series [18], therefore we choose Dynamic Time Warping for our detection method.

One of the most extremely efficient similarity measurements is the Dynamic Time Warping (DTW). It is a well-known algorithm which is used in time series analysis to measure the similarity between two given (time-dependent) sequences, which is estimated through finding an optimal alignment between those two signals under certain restrictions.

It was first introduced in the 1960s, and it was intensively researched in the 1970s through its application to voice recognition. It's currently being used in a variety of applications, including online signature matching, sign language, gesture recognition, data mining, and time series clustering [19].

DTW has also been employed in the field of network security, in [20] it is used to compare the similarity of malware binaries to worm executable signatures to determine whether the malware belongs to a specific worm class. DTW is commonly used to determine the degree of similarity between two signals.

Given two time series $X = (x_1, x_2, \dots x_M), M \in N \, and \, Y = (y_1, y_2, \dots . y_K), K \in N,$ which are taking values from some feature space Ψ. To compare these series $X, Y \in \Psi$, four basic steps should be taken into account.

Step 1: The local distance measure of these signals is needed as defined in Eq.(1)., [21]

$$d: \Psi \times \Psi \rightarrow \mathrm{R} \geq 0 \qquad (1)$$

The task of optimal alignment of the signals is turning to a task of arranging all signals points by minimizing the cost function. Thus, it is common to call the distance function d as the "cost function". It is axiomatic that d has a small value (low cost) when the signals are similar while its value gradually increases (high cost) according to the amount of difference in the signals.

Step 2: The distance matrix $C \in R^{M \times K}$ is built which representing all pairwise distances between X and Ysignals. The distance matrix also called the local cost matrix for the alignment of the two series X and Y as in Eq.(2).

$$d: \Psi \times \Psi \rightarrow \mathrm{R} \geq 0 \qquad (2)$$

$$\mathrm{C_{i,j}} = \left\| x_i - y_j \right\|, i \in [1:M] \, , j \in [1:K]$$

Step 3: The alignment path is found which runs through the low-cost areas on the cost matrix. This path is a sequence of points $p = (p_1, p_2, \dots . p_L)$ with $p_l = \left(p_i, p_j\right) \in [1\colon M] \times [1\colon K]\; for\; l \in [1\colon L]$ which must satisfy the following three condition:

1. Boundary condition: to ensure that the start and end warping path points must be the first and the last points of the aligned sequences, $p_1 = (1{,}1)\;\; and\, p_K = (M, K)$.
2. Monotonicity condition: to preserve the time-ordering of points, $$m_1 \leq m_2 \leq \cdots m_L \;\; and\, k_1 \leq k_2 \leq \cdots k_L$$
3. Step size condition: to limit the warping path from long jumps while align sequences, $$p_{l+1} - p_l \in \;(1, 0), (0, 1), (1, 1).$$

Step 4: The total cost $c_p(X, Y)$ of the former warping path p between X and Y with respect to the local cost measure C is defined as in Eq.(3).:

$$C_p(X, Y) = \sum_{l=1}^{L} C(x_{ml}, y_{kl}) \qquad (3)$$

The warping path that has a minimal cost associated with alignment is the optimal one (p^*). To determine it, every possible warping paths between X and Y should be tested, which means an exponential complexity in the lengths M and K. To overcome this problem an algorithm based on Dynamic Programming is employed. The Dynamic Programming section of DTW technique uses the DTW distance function in Eq.(4).

$$dtw(X, Y) = C_{p^*}(X, Y) = \min C_p(X, Y),\;\; p \in P^{M \times K} \qquad (4)$$

Where $P^{M \times K}$ is the set of all potential warping paths, then it constructs D (accumulated cost matrix) matrix, which is defined as follows:

First row:

$$D(1, j) = \sum_{k=1}^{j} c(x_1, y_k),\; j \in (1\colon K).$$

First column:

$$D(i, 1) = \sum_{k=1}^{i} c(x_k, y_1),\; i \in (1\colon M).$$

Other elements:

$$D(i, j) = C\left(x_i\,, y_j\right) + \min \begin{cases} D(i-1\,, j-1) \\ \;\; D(i-1\,, j) \\ \;\; D(i\,, j-1) \end{cases} \qquad i \in [1, M], j \in [1, K]$$

The warping path could be set once the accumulated cost matrix is established by the simple backtracking from the point $p_{end} = (M, K)$ to the $p_{start} = (1,1)$ [21]. After that the cost function is computed as the total distance of the warping path. This implies that if one is only interested in the value $DTW(X, Y) = D(M, K)$, the storage requirement is $O(K)$.

METHODOLOGY

This section, introduces in details the two main modules of the proposed method for detecting the SYN flooding attack, the Dynamic Time Warping technique and the Adaptive Threshold.

5.1 Implementation Strategy

Our implementation strategy is applied on the SYN flooding attack. Where the two desired time series are extracted from them by counting the SYN and ACK attributes numbers. By decomposing the network traffic into two main signals (SYN signal, and ACK signal) and by using the Dynamic Time Warping technique, we can estimate how similar they are. (DTW) thus finding the best alignment between them. The suggested method starts with action of attribute selection in which we determine the SYN and ACK packets number from datasets during a two-second timeframe. Thus, the desired time series will be as follows,

$$x_i = SYN \quad y_i = ACK \qquad (5)$$

where i is the interval index, and it starts from $i = 1$ to $i = M$. We chose SYN and ACK packet number variations as our experimented signals since they are a clear indicator of attack activity. During the regular span of time, the difference of the SYN, and ACK number is slight which means a high similarity degree of these signals. Unlike their similarity degree during the attack period where, the SYN number grows significantly while the number of ACK packets drops. Therefore, during the detection time, the SYN and ACK number received from clients is tallied. The distance (cost) matrix CM of the signals (x, and y) is built over segments (non-overlapping) of identical length N as illustrated,

$$S = int\left(\frac{M}{N}\right)$$

According to internet traffic measurements, TCP connections take 12-19 seconds to complete [22], We use N = 10 to give us a total observation time of about 20 seconds. Depending on the euclidian distance, the cost matrix C is computed for each segment (interval) as in Eq.(6).

$$C \in R^{N\times N}: \quad \mathrm{C}_{\mathrm{i,j}} = \left(x_i - y_j\right)^2, i \in [1{:}N], j \in [1{:}N] \qquad (6)$$

Then the accumulated cost matrix $A_{i,j}$ is computed from the former signals where the first element of A is $A(1,1) = C(1,1)$ and the other elements are as in Eq.(7).:

$$A(1, j) = \sum_{j=2}^{N}\left(C(1, j) + A(1, j-1)\right)$$

$$A(i,1) = \sum_{j=2}^{N}\big(C(i,1) + A(i-1,1)\big) \qquad (7)$$

$$A(i,j) = C(i,j) + \min\begin{cases} A(i-1\,,j-1) \\ A(i-1\,,j) & i,j \in [1,N] \\ A(i\,,j-1) \end{cases}$$

For this case there is no need to compute the warping path as last accumulated cost matrix value is sufficient for the detection strategy. Therefore we use the value $CF = A(N,N)$ as our cost function value to compare it with the threshold

5.2 The Adaptive Threshold

We use the adaptive threshold for determining whether the cost function values suggest an attack interval or not. The necessity for an adaptable threshold with internet traffic has emerged as a significant influencing issue, as internet traffic varies substantially over time intervals depending on client activity. An adaptive threshold based on the fluctuation RMS (root mean square) is presented to avoid detection being dependent on the access patterns of sites [23]. The adaptive threshold algorithm checks if the cost function values CF for a given interval surpass a threshold, which is adaptively set based on mean number estimation of the signals' Euclidian distance. This estimate is made by averaging prior data with an exponential weighted moving average (EWMA), as shown in Eq.(8).

$$avCF_n = \beta \times avCF_{n-1} + ((1-\beta) \times X_n \qquad (8)$$

where β is the factor of the EWMA, X_n is the total of all the Euclidian distance of the signals(x,y) in the n^{th} segment. If the condition is satisfied as in Eq.(9)., the alert will be signaled at time n.

$$CF_n \geq (\alpha + 1) \times avCF_{n-1} \qquad (9)$$

CF_n is the cost function value in the n^{th} time interval, and $avCF_{n-1}$ is the estimated mean rate based on measurements taken before n. Where $\alpha > 0$ is the percentage over the mean value that we regard to be an indication of abnormal behavior. In addition to the first value of $avCF_1$ equals the summation of the Euclidian distance of the signals (x,y) over the first segment, we chose the values of $\alpha\ and\ \beta$ equal 0.5 and equal 0.99. Using this threshold gives high false positive rate, so we adjust the adaptive threshold as follows:

- A new value Dav_n (the modified threshold) is calculated as the mean of.
$$avCF_n, avCF_{n-1}, \ldots .\, avCF_1$$
- The alert will be signaled at time n if the condition is satisfied Eq.(10).
$$CF_n \geq (\alpha + 1) \times Dav_n \qquad (10)$$

Through modifying the adaptive threshold, we are able to achieve the desired result.

PERFORMANCE EVALUATIONS

We carry out the experimental evaluation on two distinct datasets to assess the efficiency of our technique: ESynFlood dataset [24], and CICDDoS2019 dataset [25].

6.1 Datasets

Based on the following three traces ESyn, CICF, and CICS, our experimental test is carried out. The first traces ESyn On May 25, 2016, where 30 attacker nodes sent SYN flooding attack packets to an internal web server node at a rapid rate. The scenario begins at 10:52 on the CyberVAN testbed, with the distributed SYN flooding attack beginning at 11:25 and ending at 11:35, effectively preventing access to smf's website. SYN flooding attack with high volume rate begins from 1800 to 2900 second. On January 12th from time 10:30 to time 17:15, the CICF trace was captured and its SYN flooding attacks periods are launched between 13:29 and 13:34. CICS trace began at 09:40 and terminated at 17:35, with SYN flooding attack intervals ranging from 11:28 to 17:35.

6.2 Normal Traces Behavior

Before applying DTW, we extracted the desired time series signals from the former traces traffic attributes over time intervals of two seconds. Where, each trace is decomposed into two signals. Figure 1 shows all the signals of the former traces at the normal case, where each subfigure presents how close the structure or the attributes number to both of SYN and ACK signals. The ESyn trace contains normal intervals that start from time interval 0 to 912 before the attack and end at time interval 1212 to 2611 after the attack. As an example, Figure 1(a) presents the normal intervals from 0 to 100. It is noticed from these intervals that the behavior of the SYN signal is extremely similar to the ACK signal behavior where their values are almost identical in some intervals.

The normal intervals of CICF trace are from time 0 to 748 before the attack and from time 896 to 1038 after it. Figure 1(b) shows the extracted two signals (SYN, and ACK) from interval 0 to 100, it is clear that their difference in behavior is negligible. Regarding CICS trace, its normal intervals before the attack begin from 0 to 431 and from 666 to 11452 after it. By comparing the behavior of the SYN signal and the ACK signal from interval 0 to 100 as shown in Figure 1(c), we also find that they are so far similar to each other, as happened with the CICF trace signals.

6.3 Attack Traces Behavior

The ESyn's SYN flooding attack periods are shown in Figure 2(a), where we can see that the SYN signal contains pulses with high rate that start at interval 913 and end at interval 1211. It is also noticed that the difference between the SYN signal and the ACK signal is very high, which means a very high dissimilarity.

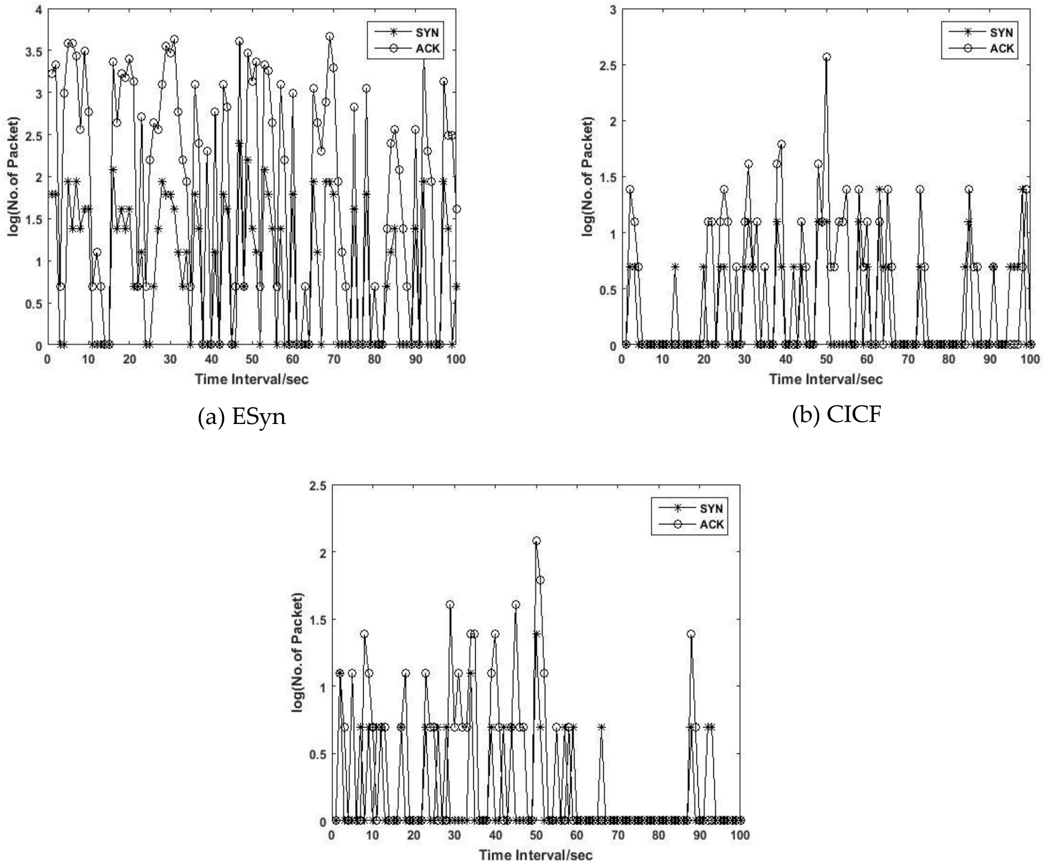
Figure 2(b) shows a high-rate SYN flooding attack of the CICF trace, which starts at interval 749 and ends at interval 897. As illustrated in Figure 2(c), a very high rate SYN flooding attack get start from interval 432 to interval 665 for the CICS trace. It is clear that the behavior of the SYN signal and the ACK signal of the former traces is differ dramatically as shown in Figure 2(b) and Figure 2(c) respectively.

6.4 Cost Function

We apply the DTW approach on the extracted SYN and ACK signals from the preceding three traces to test its efficiency under the SYN flooding attack. We find that the cost function values (CF) of the mentioned signals fluctuate from some periods to others since it simulates the normal and in the attack intervals of the original traces behavior. Figure 3(a) shows the cost function values (CF) that were calculated over ten-step intervals from ESyn signals. When looking at the CF values, it's clear that some of them almost insignificant compared to others. These values reflect the normal periods before and after the attack, whereas they spike dramatically during the attack period.

This is seen in Figure 3(a), where the values of CF begin to rise substantially at interval 92 and continue to rise and fall abruptly and repeatedly throughout the attack periods until interval 122. Figure 3(b) and Figure 3(c) show the CF values of the CICF and CICS traces signals over ten-step intervals respectively. We can easily see that the CF values are significantly higher during the attack intervals than during the normal intervals. As a result, based on these values, we can easily distinguish attack periods from normal ones, since these values simulate the original traces behavior accurately.

To detect attack intervals, we compare the cost function values of the ESyn trace with the modified threshold. Using the above comparison, we are able to attain a 100% detection rate with no false positives. To validate these results we apply the DTW approach with the modified threshold on CICF and CICS traces, and we obtain the same ratios. The proposed method has been shown to be effective because it outperforms earlier detection methods in [12, 13, 14, and 15] that used the same dataset (i.e. CICDDoS2019). Although the first four techniques basically depend on training step, their detection rate is between 98% and 99.9. Also, it outperform the methods [8, and 10] in the number of the used attributes, as it has used less number of attribute. Table 1 presents this comparison.



(a) ESyn

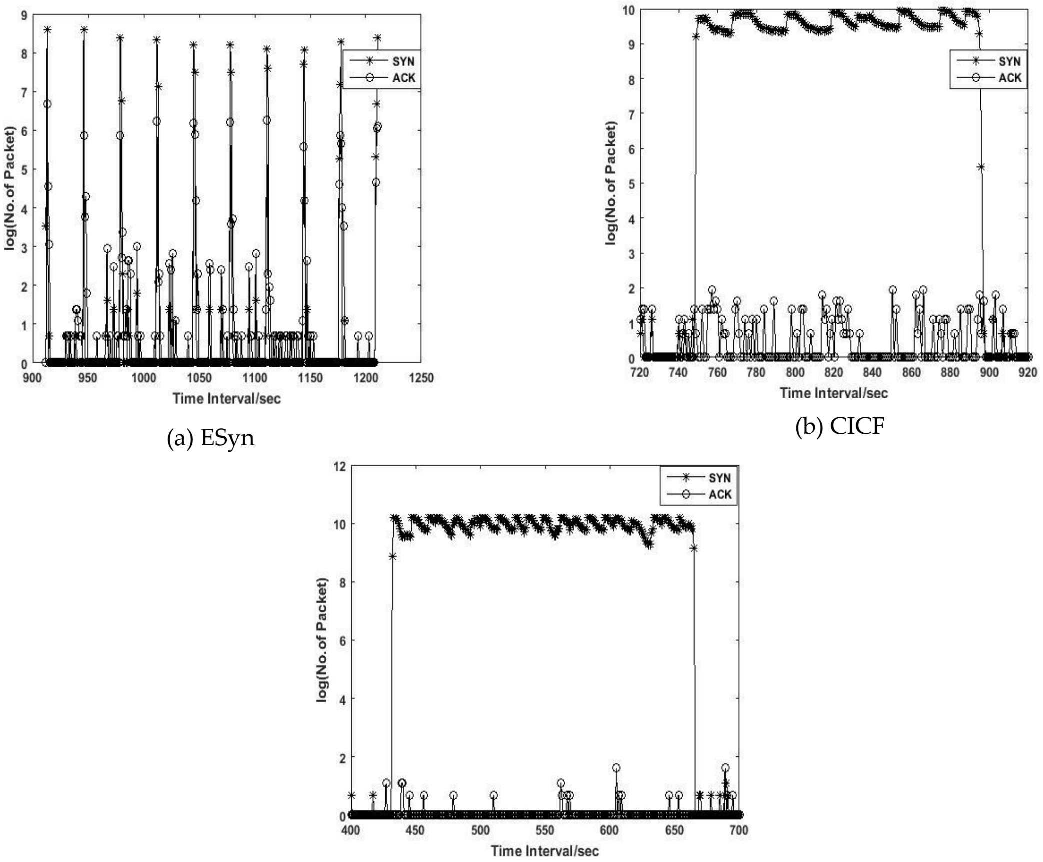
(b) CICF

(c) CICS

Figure 1*:* The normal behavior of the two signals.

CONCLUSION

In this paper, we proposed the Dynamic Time Warping as a detection method for the DDoS flooding attack. The suggested method regarded the network traffic features as signals and used signal similarity estimation to detect the DDoS flooding attacks. We use simulations on the datasets (i.e. ESynFlood, and CICDDoS2019), to demonstrate that by using the DTW method with the modified threshold the attack intervals could be detect efficiently. The suggested method is distinguished by its simplicity and low complexity cost, as well as its high detection accuracy.

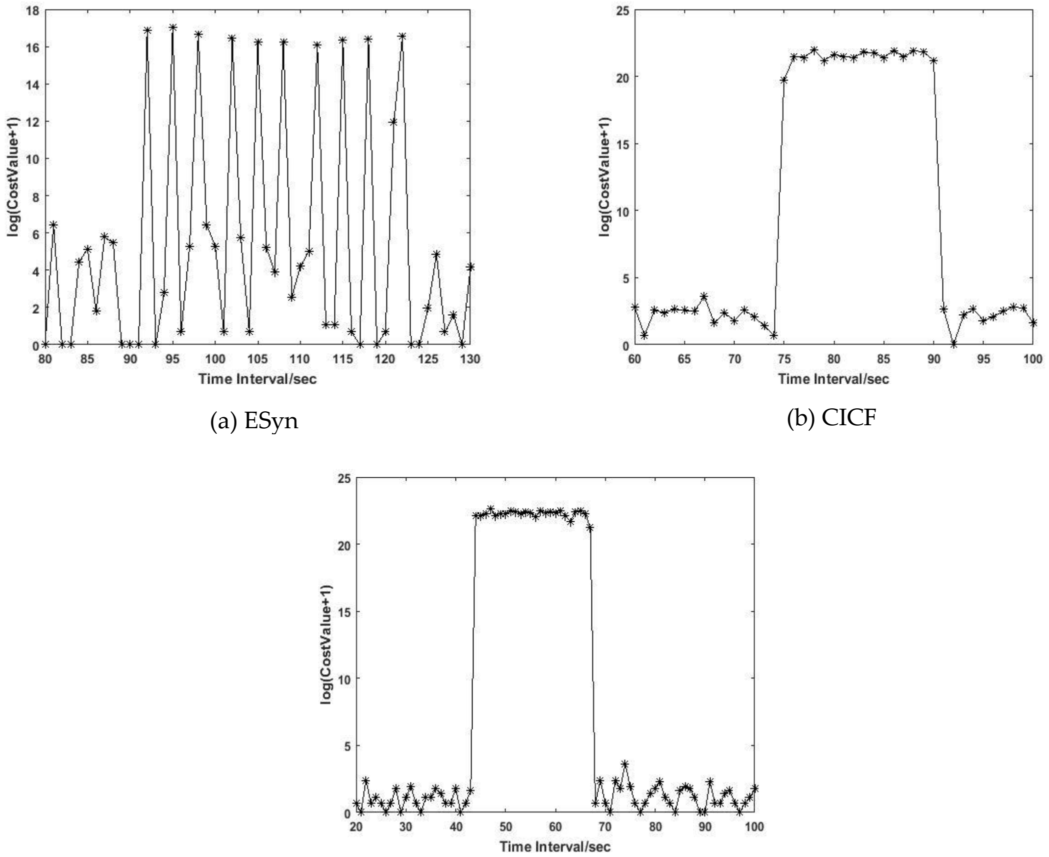


(a) ESyn

(b) CICF

(c) CICS

Figure 2: The attack behavior of the two signals.



(a) ESyn

(b) CICF

(c) CICS

Figure 3: Cost Function Values of the signals.

Table 1: CICDDoS2019 Dataset Comparisons.

Method	Technique	Features	Detection	False+
[8]	Odds ratio	4	100%	0
[10]	MFDFA	3	100%	0
[12]	Deep Learning	77	99%	0.01
[13]	Lightweight model	3	99.93%	0.1
[14]	Auto-encoder	20	99%	Unknown
[15]	Tensor based	64	99%	0.01
Our Method	Time Series Similarity	2	100%	0

REFERENCES

[1] Chakrabarti, A. and Manimaran, G., 2002. Internet infrastructure security: A taxonomy. IEEE network, 16(6), pp.13-21.

[2] https://www.cloudns.net/blog/significant-ddos-attacks-recent-years/

[3] CERT Coordinate Center, Denial of Service Attacks, http://www.cert.org/tech tips/denial of service.html.

[4] Mao, Z.M., Sekar, V., Spatscheck, O., Van Der Merwe, J. and Vasude van, R., 2006, September. Analyzing large DDoS attacks using multiple data sources. In Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense (pp. 161-168).

[5] Rakas, S.V.B., Stojanovic, M.D. and Markovic-Petrovic, J.D., 2020. A Review of Research Work on Network-Based SCADA Intrusion Detection Systems. IEEE Access, 8, pp.93083-93108.

[6] Hoque, Nazrul, Dhruba K. Bhattacharyya, and Jugal K. Kalita. "Botnet in DDoS attacks: trends and challenges." IEEE Communications Surveys & Tutorials 17.4 (2015): 2242-2270.

[7] Zhou, Y., Cheng, G., Jiang, S., Zhao, Y. and Chen, Z., 2020. Costeffective moving target defense against DDoS attacks using trilateral game and multi-objective Markov decision processes. Computers & Security, 97, p.101976.

[8] Dalia Nashat, Fatma A. Hussain, and Xiaohong Jiang. Detection of Distributed Denial of Service Flooding Attack Using Odds Ratio. Journal of Networking and Network Applications. 2021, Volume 1, Issue 2, pp. 67-74. https://doi.org/10.33969/JNaNA.2021.010204.

[9] Li, Z., Xing, W., Khamaiseh, S. and Xu, D., 2019. Detecting saturation attacks based on self-similarity of OpenFlow traffic. IEEE Tran actions on Network and Service Management, 17(1), pp.607-621.

[10] Nashat, Dalia, and Fatma A. Hussain. "Multifractal detrended fluctuation analysis based detection for SYN flooding attack." Computers &Security 107 (2021): 102315.

[11] Diab, Diab M., et al. "Denial of service detection using dynamic time warping." International Journal of Network Management (2021): e2159.

[12] WWang, M., Lu, Y. and Qin, J., 2020. A dynamic MLP-based DDoS attack detection method using feature selection and feedback. Computers & Security, 88, p.101645.

[13] Elsayed, M.S., Le-Khac, N.A., Dev, S. and Jurcut, A.D., 2020, August. Ddosnet: A deep-learning model for detecting network attacks. In 2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM) (pp. 391-396). IEEE.

[14] Lucky, G., Jjunju, F. and Marshall, A., 2020, December. A Lightweight Decision-Tree Algorithm for detecting DDoS flooding attacks. In 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 382-389). IEEE.

[15] Salahuddin, M.A., Bari, M.F., Alameddine, H.A., Pourahmadi, V. and Boutaba, R., 2020, November. Time-based Anomaly Detection using Autoencoder. In 2020 16th International Conference on Network and Service Management (CNSM) (pp. 1-9). IEEE.

[16] Zhang, Miaomiao, and Dechang Pi. "A new time series representation model and corresponding similarity measure for fast and accurate similarity detection." IEEE Access 5 (2017): 24503-24519.

[17] Kianimajd, A., Ruano, M.G., Carvalho, P., Henriques, J., Rocha, T., Paredes, S. and Ruano, A.E., 2017. Comparison of different methods of measuring similarity in physiologic time series. IFAC-PapersOnLine, 50(1), pp.11005-11010.

[18] Zhang, Zheng, Ping Tang, and Thomas Corpetti. "Time Adaptive Optimal Transport: A Framework of Time Series Similarity Measure." IEEE Access 8 (2020): 149764-149774.

[19] Khakse MM, Shandilya P. An Efficient and elastic approach for partial shape matching using DTW. International Journal of Engineering Trends and Technology (IJETT) 2013.

[20] Naval, Smita, et al. "Exploring worm behaviors using dtw." Proceedings of the 7th International Conference on Security of Information and Networks. 2014.

[21] Senin P. Dynamic time warping algorithm review. Information and Computer Science Department University of Hawaii at Manoa Honolulu, USA. 2008 Dec;855(1-23):40.

[22] Thompson, K., Miller, G.J. and Wilder, R., 1997. Wide-area Internet traffic patterns and characteristics. IEEE network, 11(6), pp.10-23.

[23] Nashat, D., Jiang, X. and Kameyama, M., 2010. Group Testing Based Detection of Web Service DDoS Attackers. IEICE transactions on communications, 93(5), pp.1113-1121.

[24] Bowen, T., Poylisher, A., Serban, C., Chadha, R., Chiang, C.Y.J. and Marvel, L.M., 2016, November. Enabling reproducible cyber research four labeled datasets. In MILCOM 2016-2016 IEEE Military Communications Conference (pp. 539-544). IEEE.

[25] Sharafaldin, I., Lashkari, A.H., Hakak, S. and Ghorbani, A.A., 2019, October. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-8). IEEE.