# Detection of Distributed Denial of Service Flooding Attack Using Odds Ratio

Dalia Nashat[1], Fatma A. Hussain[1], and Xiaohong Jiang[2]
[1]Faculty of Computers and Information, Assiut University, Assiut, Egypt
[2]School of Systems Information Science, Future University Hakodate, 116-2
Kamedanakano-cho, Hakodate, Hokkaido, 041-8655, Japan

**Computer networks are vulnerable to many types of attacks while the Distributed Denial of Service attack (DDoS) serves as one of the top concerns for security professionals. The DDoS flooding attack denies the services by consuming the server resources to prevent the legitimate users from using their desired services. The hardness of detecting this attack lies in sending a stream of packets to the server with spoofed IP addresses, so that the internet routing infrastructure cannot distinguish the spoofed packets. Based on the odds ratio (OR) statistical measurement, in this work we propose a new detection method for the DDoS flooding attacks. By exploring the odds ratio to determine the risk factor of any incoming traffic to the server, the legitimate and attack traffic packets can be easily differentiated. Experimental results demonstrate the efficiency of the presented detection method in terms of its detection probability and detection time.**

***Index Terms*—DDoS Attack, TCP Protocol, TCP SYN Flooding Attack, Case-Control Studies, Odds Ratio**

## I. INTRODUCTION

Network-based computer systems have undergone a phenomenal growth in recent years. It becomes an essential part of our daily life since it has many benefits for our personal and professional activities. Its benefits has been increasing since the COVID-2019 pandemic, where people worldwide are now working, studying, shopping, and having fun online like never before. It is notable, however that these networks are vulnerable to malicious attacks which exploit security bugs in network protocols during their connection to the internet. Therefore, intrusion detection becomes highly desirable for efficient defence systems in computer networks.

One of the chief hindrances which influences the availability of networks services is the Distributed Denial of Service attack (DDoS). This attack basically aims to deny the services to the legitimate users. The attack scenario start when the attackers use a group of infected machines (i.e botnets) to overwhelm the victim by a huge number of packets potentially hundreds of thousands or more. Therefore the bandwidth of the server is flooded and its resources are consumed [1]. Distributed Denial of Service attack (DDoS) enforced popular web sites like Yahoo, Amazon, and CNN to close in year 2000 [2]. Hong Kong Occupy Central reported a DDoS attack of 500 gigabits per second in 2014. March 2018 NETSCOUT reported that its detection system confirmed a 1.7 Tbps memcached reflection/amplification attack on an unnamed U.S.-based service provider. Also in 2018, as reported in [3] GitHub was hit with a sudden DDoS onslaught of 1.35 terabits per second. January 2019 Imperva client sustained a 500 million packets per second DDoS attack. April 2019 Imperva reports a DDoS attack that peaked at 580 million packets per second [4].

One of the most common DDoS attack types is the TCP SYN flooding attack, where the DDoS attacks use TCP protocol with percent over than 90% [5], [6], [7]. In Q1 2020, the leading attack type is the DDoS flooding types specially the SYN flooding, where its percentage was over than 92.57% [8]. Therefore, in this paper we use the SYN flooding as case study to demonstrate the efficiency of the proposed detection method. In the SYN flooding attacks, the attackers exploit the limitation of the TCP protocol (three-way handshakes) by maintaining half-open connection to send a huge number of SYN requests to the server (victim). This limitation is due to the TCP connection timeout since the connections remain in half-open until receiving response or backlog queue limit is reached. During the attack the server receives many half open connection thus the server is exhausted and all new requests are dropped.

Although the DDoS attack risks has been increasing, we can avoid most of the financial losses by detecting that attack at an early stage. The detection of the TCP SYN flooding attack becomes more difficult due to the limitation of the internet infrastructure in differentiate a legitimate SYN packet from a spoofed one. Currently, several defense mechanisms have been proposed for the SYN flooding attacks such as Syn cookies [9], Syn cache [10], Synkill [11], Syn proxying [12]. However to locate the flooding sources, the former mechanisms have to rely on the expensive IP traceback such as, hop-by-hop tracing, ICMP-based traceback, and Packet marking [13].

Beside the defence mechanisms, there are many techniques used to detect the DDoS attack which based on different methods such as statistical based methods, or machine learning based methods, or signal processing based methods. In [14], authors proposed a statistical approach to mitigate the DDoS attack . Depending on the multi-objective Markov decision processes, this approach is used to find the optimal Moving Target Defense (MTD) strategy by solving the trade-off problem between the effectiveness and cost of shuffling. An intrusion detection system against DDoS attacks in SDN environments is proposed [15]. This method is based on

Manuscript received November 8, 2021; revised December 23, 2021. Corresponding author: Dalia Nashat (email: dnashat@aun.edu.eg).

Deep Learning technique as it combines the Recurrent Neural Network (RNN) with autoencoder. To detect the DDoS attack, Lucky et al. presented a machine learning approach. By using a robust features selection approach their method was trained with a minimal number of features [16]. In [17] a novel time-based anomaly detection system is presented, where that system leverages an autoencoder. By using concepts of machine learning supervised classification, a tensor based framework is proposed for DDoS attack detection [18].

Also many signal processing techniques have been used to detect anomalies in network traffic [19]. Based on self-similarity, authors in [20] proposed a detection method for SYN flooding attack, but this method is applicable to a certain network size also it has high amount of calculation. In [21], authors could detect the abnormal behavior in the TCP protocol time series based on Multifractal Detrended Fluctuation Analysis (MFDFA) in addition to an adaptive threshold. They computed the local fluctuations for each interval and compared its value with a modified adaptive thresholds thus they could detect the attack intervals efficiently.

In this paper we present a new detection method that can detect the DDoS flooding attack easily based on the odds ratio that can determine whether the incoming traffics within a time interval represent a risk factor or not. Experimental results demonstrate the efficiency of the presented detection method in terms of its detection probability and detection time. The rest of this paper is organized as follows. Section 2 presents the background of this work. The proposed method is described in Section 3. Section 4 presents the performance evaluation. Section 5 concludes this work.

## II. Background

### A. Odds Ratio

The odds ratio (OR) is one of the several statistical measurements of association that have become increasingly important in epidemiology studies specially in the case control study. Where the researchers often use it to quantify the relationship between an exposure and an outcome among two groups. It also used in the clinical research and decision-making as an effect-size statistical measurement. As it is particularly useful because it gives a clear and direct information to the clinicians about which treatment approach has the best odds to benefit the patient, where the odds ratio is used to determine the effect size of a difference in the interventions of two drug [22], [23].

The diagnostic study in [24] used the odds ratio to find out whether there were various probabilities to operate larger number of surgeries for breast cancer depending on the needle biopsy. Author in [25], used the odds ratio measure to determine the influence odds of the occupational exposures on the low back pain. For the diagnostic performance the odds ratio is used as a single indicator [26]. In [27] the odds ratio is used as an analytic measures in the physical therapy. To quantify the relations between the smoking and the histologic subtypes of lung cancer, the researchers used the odds ratio [28].

The odds ratio was used in the network security applications. In [29] a genetic epidemiology approach to cyber-security was proposed for creating tools to determine the probability of a network being susceptible to a threat. Also they use odds ratio to evaluate the association between the presence of a given network service and the infection by a given threat. To evaluate the real life performance of Antivirus software and the human risk factors of malware attacks, a computer security clinical trail was performed with real users in non-laboratory conditions similar to clinical trail in medicine. Where the odds ratio was used for performing the risk analysis to assess if particular user characteristics and demographics increase the odds of malware attack or not[30]. In [31] the odds ratio is used to find the characteristics that are more likely to be related to booters than to other websites, so generate a booter blacklist.

As we mentioned, the odds ratio was used in some network security applications, however it was used in a limited scope where its using restricted in the statistical analysis only. The present work is pioneer to apply this measurement as a detection method for the flooding DDoS attack problem.

The odds ratio (OR) is a statistical measure that used in the case-control studies to estimate the strength of the association between an exposure and an outcome, so determine if a particular exposure is a risk factor for a particular outcome or not [32]. These studies are designed to help in determining whether an exposure is associated with an outcome or not (i.e., disease or condition of interest)[32]. They are an analytic type of the epidemiological observational studies, where the study population is divided into two groups who either have or do not have a particular health outcome or a disease status (i.e., cases, and controls sequentially), in addition to the exposure status of both is prior assessed as illustrated in Fig. 1 [33].

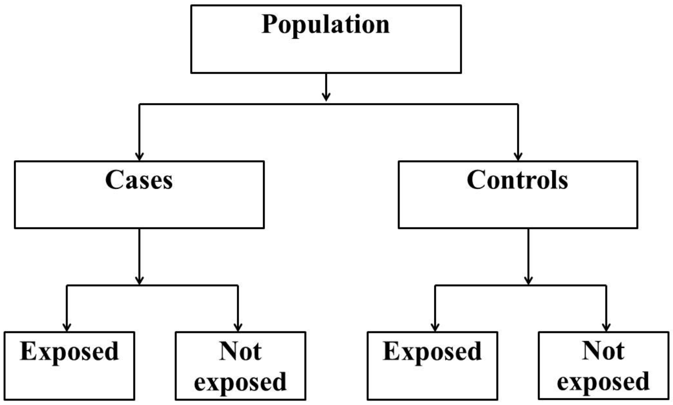

*Fig. 1: Case Control studies [33]*

The case-control studies are often used to determine the extent of the influence of an exposure (behavior/disease) on an outcome (disease/ death) through comparing a group of cases and controls, thus confirm if that exposure is a risk factor or not. Accordingly, some necessary medical proceedings are taken. Depending on the former population divided groups the two-by-two frequency table is formed as presented at Table. I [34], which in turn is used to calculate the odds ratio relation. The OR represents the odds that an outcome will occur given a particular exposure, compared

*TABLE I: Odds Ratio Table*

| | | Outcome Status | |
|---|---|---|---|
| | | Case | Control |
| Exposure Status | Exposed | a | b |
| | Unexposed | c | d |

to the odds of the outcome occurring in the absence of that exposure thus the odds ratio can be determined depending on this relation [34],

$$OR = \frac{\text{Odds of exposure in the case group}}{\text{Odds of exposure in the control group}}$$

and its value can be calculated as in Eq. (1) [34].

$$OR = (\frac{a}{c})/(\frac{b}{d}) = \frac{ad}{bc} \qquad (1)$$

where it is noticed clearly from the frequency table that,
$a$ is the number of exposed cases
$b$ is the number of exposed control
$c$ is the number of unexposed cases
$d$ is the number of unexposed control

The odds ratio measure ranges between three values as follows.

$$\begin{cases} OR & < 1 \text{ or,} \\ OR & = 1 \text{ or,} \\ OR & > 1 \end{cases}$$

If the odds ratio value equal to one it means that the exposure (behavior/disease) is not associated with the outcome (disease/ death). If the former value is less than one it means that the exposure (behavior/disease) may be protective against the outcome (disease/ death). In the event that the value of odds ratio is greater than one it means that The exposure (behavior/disease) may be a risk factor for the outcome (disease/ death) [34]. Here we introduce the odds ratio measure for quantifying the strength of the association between the DDoS flooding attack packets and the server response.

### B. DDoS Flooding Attack

The DDoS flooding attack includes several types, as UDP, ICMP, HTTP, and SYN flooding attack. Here we will focus on the SYN flooding type as our case study. In the SYN flooding attack, the attacker send a high rate of half-open connection requests(SYN packets). These packets consume the server resources [35], [36], thus the services are denied which lead to failure of the server's main mission towards the legitimate users.

At the normal case of the TCP connection establishment, the client and server start their connection by exchange a series of packets. The first packet is from the client which is a request for the connection or a SYN packet to the server. Sequentially the server acknowledges this request by sending SYN-ACK packet back to the client. Finally, the connection is established by a respond with an ACK packet from the client as shown in Fig. 2.

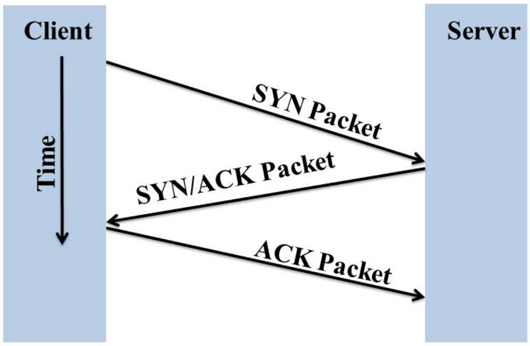

*Fig. 2: The TCP connection establishment*

On the other side in the SYN flooding attack scenario, the client floods the victim server by multiple SYN packets with spoofed IP addresses without responding to the server's SYN-ACK packets. The victim server in turn bind the resources while waiting for the ACK packets, however it will never receive the final ACK packets to complete the three-way handshake. Thus ultimately resulting in denial of service through exhausting the server's resources.

By comparing the influence of the SYN flooding attack on the server with the influence of the biological viruses during the infection process on the host cell, we note that there is a similarity between both the SYN flooding attack and the biological viruses. The both former influences lead to the same result, where the viruses disrupt the biological cell main function, also the SYN flooding attack disrupt the server through dominance on its resources. As the SYN attack influence is similar to the biological viruses influence, so the attack can be considered as a particular illness (i.e., virus infection) that affects the server and leads to some outcome. Therefore we can classify the server status into cases and controls depending on if that server is exposed to the attack or not.

We can measure the odds of the influences of the different TCP requests types on the server status by using the odds ratio over each time interval, thus by the value of the odds ratio we can detect easily which time interval under attack.

## III. The Proposed Method (Odraddos)

In the case-control study, the odds ratio is a measure of association between an exposure and an outcome, where it tells us how much higher the odds of the exposure is among the cases compared with controls. Assuming that the server is the required study population, so we can classify its status to cases (death) and controls (Life) depending on its exposure to the different TCP requests (disease/attack). Therefore, we can classify the server state into four statuses, where these statuses represent the states of the four variables of the odds ratio equation ($a$, $b$, $c$, and $d$) as follows:

- $a$ is the number of exposed cases $\Rightarrow$ dead with disease
- $b$ is the number of exposed control $\Rightarrow$ live with disease
- $c$ is the number of unexposed cases $\Rightarrow$ dead without disease

- $d$ is the number of unexposed control ⇒ live without disease

By using the previous classification of the server statuses concurrently with the computing of the network traffic attributes from the server point of view, we can obtain the four cases of the SYN packets which corresponding to the four variables of the odds ratio equation sequentially as follows:

- Case 1:
  $a$ is the number of SYN requests at each time interval which is not associated with ACK packets by the client and at the same time the server can't respond to it with SYN/ACK packets. It is the inevitable death for the server with a disease.
- Case 2:
  $b$ is the number of SYN requests during time interval which the server can respond to it with SYN/ACK packets however the client doesn't respond to it with ACK packets. Where we can say that the server lives but with a disease.
- Case 3:
  $c$ is the number of SYN requests at each time interval which the server respond to it with SYN/ACK packets and at the same time client respond to it with ACK packets. It is a complete connection without any problem, which means death without disease.
- Case 4:
  $d$ is the number of SYN requests over time interval that the server terminate its connections without waiting the client responses. Which means that the server lives without disease.

After indicating the relation between the TCP dataset attributes and the odds ratio equation parameters, the overall architecture of the proposed method can be presented.

### A. The Overall Detection Architecture

As illustrated in Fig. 3, we can see the overall architecture of the proposed method. The proposed method starts by computing the desired attributes from the network traffic as mentioned at the former section to get the required parameters $a$, $b$, $c$, and $d$. Before computing the odds ratio (OR) for every time interval we should firstly test if any of the values $b$, $c$, or $d$ are equal to zero, we convert it to one because these values are denominators. Finally depending on the OR value we can make the decision if the time interval is an attack interval or not.

### B. Detection Model

Assuming that the influence of the SYN flooding attack on the server is similar to the biological viruses influence on the host cell, so we can deal with the network traffic by the case-control study estimators. One of the most important case-control study estimator is the odds ratio. Based on the calculation of the odds ratio, we can detect the attack intervals accurately and easily.

The proposed method begins with the attribute selection operation, where we calculate the number of SYN packets, SYN/ACK packets, ACK packets, and RST packets from the TCP SYN dataset over twenty second interval. Every interval we compute the number of the SYN packets under the four different cases to obtain the four parameters $a$, $b$, $c$, and $d$. Where $a$ equals the number of the SYN packets that is not responded by SYN/ACK or ACK from the server or the client respectively. whilst $b$ equals the number of the SYN packets that is responded by SYN/ACK from the server whereas the client doesn't respond to it by the required ACK packets. The parameter $c$ is the number of the normal connections where the server receives the ACK packets for the SYN requests in addition to sending its SYN/ACK packets without any problems. The last parameter $d$ is the number of the SYN packets that the server forced its connection to close by using the RST flag. Fig. 4, Fig. 5, Fig. 6, and Fig. 7 illustrate the four cases of $a$, $b$, $c$, and $d$ calculation respectively. Before computing the odds ratio value for every time interval we must make sure that not any of $b$, $c$, or $d$ values are equal zero since these values are denominators in Eq. (1).

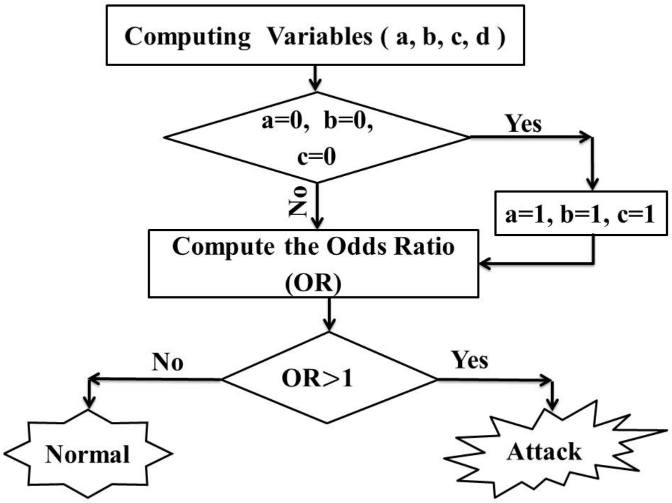
Computing Variables ( a, b, c, d )
a=0, b=0, c=0
Yes
No
a=1, b=1, c=1
Compute the Odds Ratio (OR)
OR>1
No
Yes
Normal
Attack

*Fig. 3: The diagram of the proposed method*

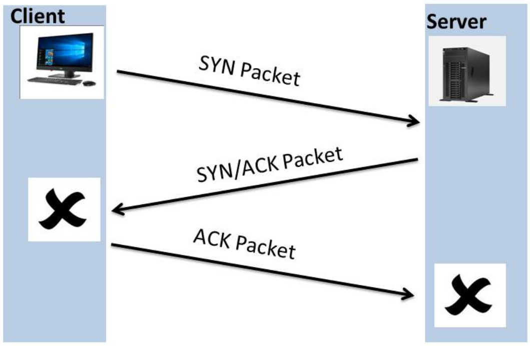

*Fig. 4: The first case of SYN packets selection*

Once we get the odds ratio values we can determine which interval is normal and which one is an attack depending on

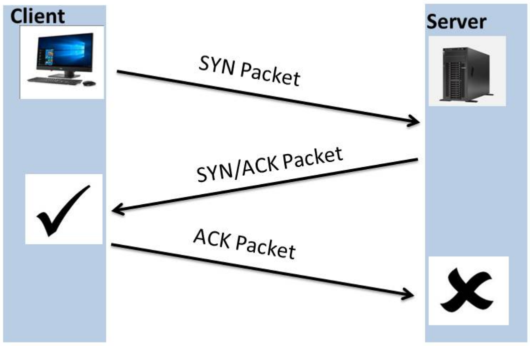

*Fig. 5: The second case of SYN packets selection*

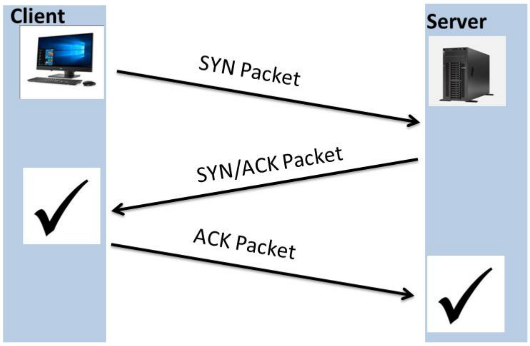

*Fig. 6: The third case of SYN packets selection*

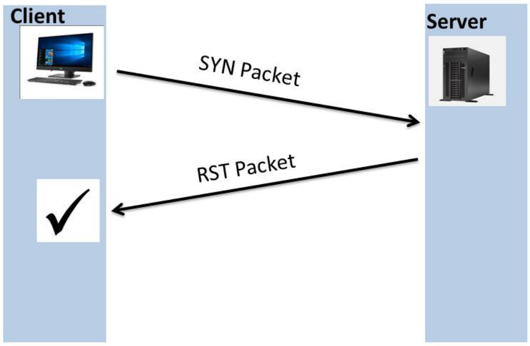

*Fig. 7: The fourth case of SYN packets selection*

the value of the flag as in Eq. (2). Where the attack interval is detected if the flag value equal one, whereas the interval is normal if the flag value is equal zero.

$$flag = \begin{cases} 0 & \text{if } OR \leq 1 \\ 1 & \text{if } OR > 1 \end{cases} \tag{2}$$

## IV. Performance Evaluation

To evaluate the performance of our method, we carry out the experimental analysis on two different datasets, ESynFlood dataset [37], and CICDDoS2019 dataset [38].

### A. Dataset

Our Experimental test is based on three traces namely ESynFlood trace, January CICDDoS2019 trace, and March CICDDoS2019 trace. A high rate of SYN flooding attack packets from 30 attacker nodes is comprised in ESynFlood trace, which sent on 25 may 2016 to port 80 of an internal web server node (smf). The access to smf's web site is blocked due to the distributed SYN flooding attack which start at time 11:25 and end at time 11:35. In another meaning a high volume rate of SYN flooding attack from second 1800 to second 2900. Fig. 8 shows the trace SYN packets distributions over time interval of twenty second. On January 12th, the January CICDDoS2019 trace was captured between time 10:30 and 17:15, while the period of SYN flooding attack was between time 13:29 and 13:34. While the captured period of March CICDDoS2019 trace was from time 09:40 to time 17:35, its SYN flooding attack intervals were between time 11:28 and 17:35. The distributions of CICDDoS2019 over time interval of twenty seconds are shown in Fig. 9 and Fig. 10 respectively.

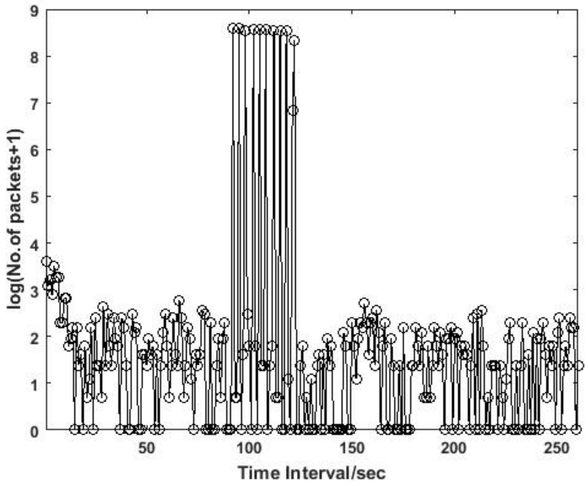

*Fig. 8: ESynFlood distribution*

### B. Normal Traffic Behavior

Before applying OR measure, we calculated the desired traces (SYN packets) from the former datasets over time intervals of twenty seconds. The normal traffic behavior for all traces is divided into two sections, before the attack occurrence and after it.

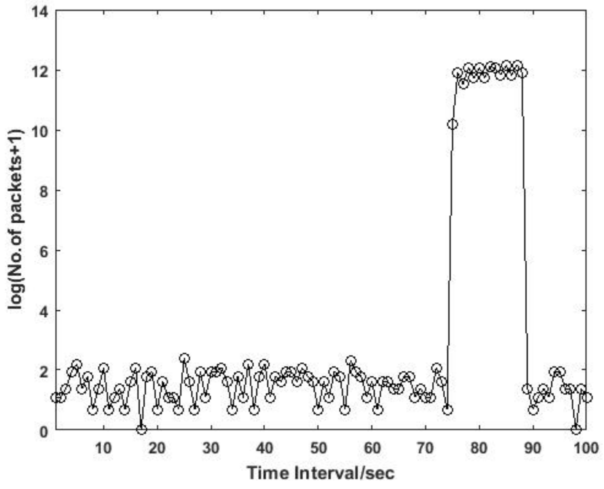

*Fig. 9: January CICDDoS2019 distribution*

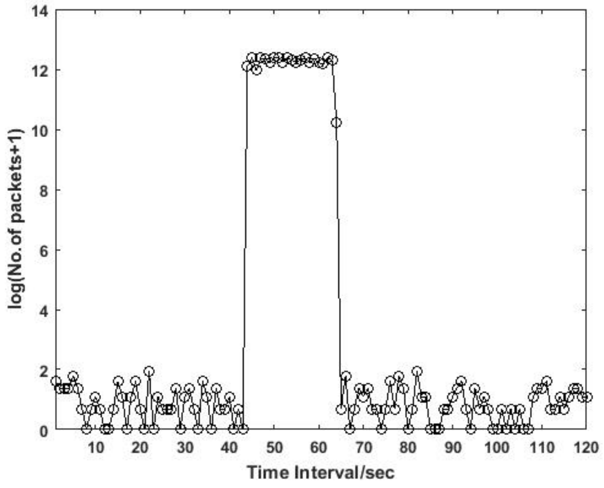

*Fig. 10: March CICDDoS2019 distribution*

The normal intervals of ESynFlood begin from time interval 1 to 91 before the attack and from time interval 123 to 260 after it, where the SYN packets number at these normal intervals not exceed 40 packets per second as shown in Fig. 8.

For January CICDDoS2019, the normal intervals range from 1 to 74 before the attack and from 89 to 102 after it, where its SYN packets number is nearly 10 packets per second . The same former SYN packets number is also repeated in the normal intervals of March CICDDoS2019, which begin from 1 to 43 before the attack and from 65 to the end of trace after it. Fig. 9 and Fig. 10 show SYN packets distribution at the normal intervals before and after the attack.

### C. Attack Traffic Behavior

The SYN flooding attack intervals of ESynFlood contain ten high rate pulses which begin from time interval 92 to time interval 122 as presented in Fig. 8. Where these pulses grade in its values upwards to 5500 packets per time interval.

A different manner of CICDDoS2019 trace from ESynFlood where its attack intervals are continues. For January CICDDoS2019, a very high rate SYN flooding attack begins from time interval 75 to time interval 88 where it reaches to 190000 packets per twenty seconds observation period as shown in Fig. 9. While for March CICDDoS2019 the SYN flooding attack begins from time interval 44 to time interval 64, where its number of packets reaches to 240000 per twenty seconds time interval shown in Fig. 10.

### D. Odds Ratio Values

To study the efficiency of odds ratio under the SYN flooding attack, we applied it to the previous traces. It is worth noting that the most important advantages of this method are the simple implementation and the high performance while using a small number of features. However, to obtain the best results, we must focus on the mapping process. If the network features are not mapped accurately with odds ratio parameters, this may lead to unacceptable results, while the accuracy mapping process gives high precision.

Fig. 11 shows the odds ratio (OR) that were computed over time intervals of twenty seconds for the ESynFlood trace. Depending on the values of OR we can efficiently identify the attack intervals, where by looking to Fig. 11 we notice that some of the OR values are very large at some intervals compared with its values at another intervals. We can see this clearly by focusing more on the OR values at the attack intervals.

Fig. 12 and Fig. 13 show the odds ratio values of the CICDDoS2019 traces respectively. We can see clearly that the OR values simulates the original traces behavior accurately, thus we can easily distinguish the attack periods and the normal periods depending on its values.

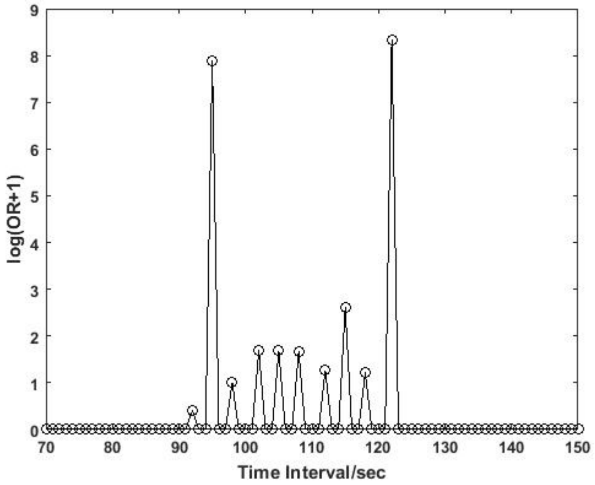

*Fig. 11: The Odds Ratio values of ESynFlood*

For ESynFlood trace we found that the OR measure could detect nine attack intervals out of ten, where the first interval is the missed one. This interval is considered as the incubation period of the server, where the value of $b$ is greater than the value of $a$ this means that the server suffers from the disease but is not dead yet. So the odds ratio measure does not consider it a risk interval.

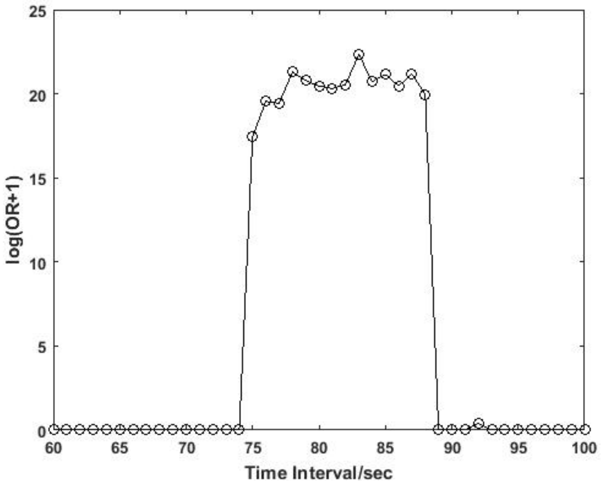

*Fig. 12: The Odds Ratio values of January CICDDoS2019*

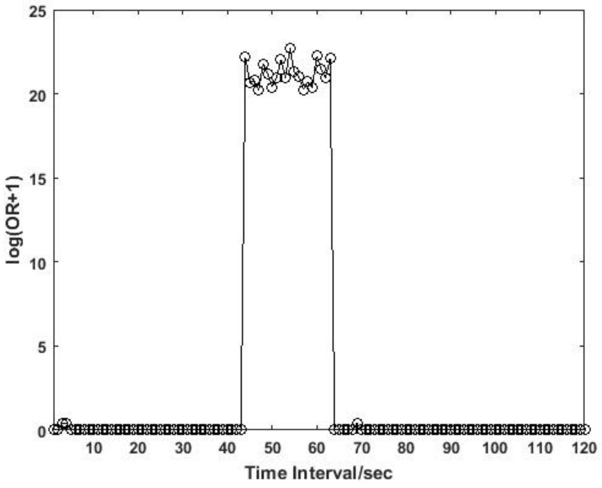

*Fig. 13: The Odds Ratio values of March CICDDoS2019*

Our method achieves a high detection rate of 90% in addition to zero false positive rate for ESynFlood trace, while it achieves a detection rate of 100% with zero false positive rate for both of CICDDoS2019 traces. The proposed method proved its efficiency as it outperforms the previous detection methods in [15], [16], [17], [18] whose detection rate ranged between 98% and 99.9% for CICDDoS2019 dataset although depending on training step Table. II shows that comparison.

*TABLE II: Comparison using CICDDoS2019 Dataset*

| Method | Technique | Features | Detection | False+ |
|---|---|---|---|---|
| [15] | Deep Learning technique | 77 | 99% | 0.01 |
| [16] | Lightweight DT model based on the C4.5 algorithm | 3 | 99.93% | 0.1 |
| [17] | Leverages an Autoencoder | 20 | 99% | Unkown |
| [18] | Tensor based framework and machine learning supervised classification | 64 | 99% | 0.01 |
| [21] | MFDFA | 3 | 100% | 0 |
| Our Method | Odds ratio | 4 | 100% | 0 |

## V. Conclusion and future work

In this paper, we proposed the biostatistics measurement odds ratio (OR) to detect DDoS flooding attacks. We treated the network traffic as an exposure that affects the server, which in turn is considered as the population study sample. By applying the odds ratio measure, we could determine the risk time of the traffic, therefore we could precisely detect the attack intervals. The proposed method revealed its simplicity, and the results confirmed its accuracy in addition to its low computational cost. As a first step in using the odds ratio for detecting the DDoS flooding attacks, we use the SYN flooding attack as a case study. We aim to apply the odds ratio to application layer flooding attacks in future work to prove the methods efficacy. It is notable, however, that the performance of the odds ratio is sensitive to the mapping process. Therefore, the difficulty of applying this method to other network security problems lies in the accuracy of mapping network features with odds ratio parameters.

## References

[1] Al-Hawawreh, Muna Sulieman. ”SYN flood attack detection in cloud environment based on TCP/IP header statistical features.” 2017 8th International Conference on Information Technology (ICIT). IEEE, 2017.

[2] Chakrabarti, Anirban, and Govindarasu Manimaran. ”Internet infrastructure security: A taxonomy.” IEEE network 16.6 (2002): 13-21.

[3] https://www.a10networks.com/resources/articles/5-most-famous-ddos-attacks

[4] https://www.thesslstore.com/blog/largest-ddos-attack-in-history/

[5] Moore, David, et al. ”Inferring internet denial-of-service activity.” ACM Transactions on Computer Systems (TOCS) 24.2 (2006): 115-139.

[6] Mao, Z. Morley, et al. ”Analyzing large DDoS attacks using multiple data sources.” Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense. 2006.

[7] Blenn, Norbert, Vincent Ghitte, and Christian Doerr. ”Quantifying the spectrum of denial-of-service attacks through internet backscatter.” Proceedings of the 12th International Conference on Availability, Reliability and Security. 2017.

[8] ”DDoS attacks in Q1 2020” https://securelist.com/ddos-attacks-in-q1-2020/96837/

[9] D. J. Bernstein and E. Schenk, ”Linux Kernal SYN Cookies Firewall Project.” [Online]. Available: http://cr.yp.to/syncookies.html

[10] Lemon, Jonathan. ”Resisting SYN Flood DoS Attacks with a SYN Cache.” BSDCon. Vol. 2002. 2002.

[11] Schuba, Christoph L., et al. ”Analysis of a denial of service attack on TCP.” Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097). IEEE, 1997.

[12] Netscreen 100 Firewall Appliance, http://www.netscreen.com/.

[13] Balyk, Anatolii, et al. ”A survey of modern IP traceback methodologies.” 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). Vol. 1. IEEE, 2015.

[14] Zhou, Yuyang, et al. ”Cost-effective moving target defense against DDoS attacks using trilateral game and multi-objective Markov decision processes.” Computers & Security 97 (2020): 101976.

[15] Elsayed, Mahmoud Said, et al. ”Ddosnet: A deep-learning model for detecting network attacks.” 2020 IEEE 21st International Symposium on” A World of Wireless, Mobile and Multimedia Networks”(WoWMoM). IEEE, 2020.

[16] Lucky, Godswill, Fred Jjunju, and Alan Marshall. ”A lightweight decision-tree algorithm for detecting DDoS flooding attacks.” 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE, 2020.

[17] Salahuddin, Mohammad A., et al. ”Time-based anomaly detection using autoencoder.” 2020 16th International Conference on Network and Service Management (CNSM). IEEE, 2020.

[18] Maranho, Joo Paulo A., et al. ”Tensor based framework for Distributed Denial of Service attack detection.” Journal of Network and Computer Applications 174 (2021): 102894.

[19] Limthong, Kriangkrai, Pirawat Watanapongse, and Fukuda Kensuke. ”A wavelet-based anomaly detection for outbound network traffic.” 8th Asia-Pacific Symposium on Information and Telecommunication Technologies. IEEE, 2010.

[20] Zhang, Daxiu, Xiaojuan Zhu, and Lu Wang. ”A SYN Flood Detection Method Based on Selfsimilarity in Network Traffic.” International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer, Cham, 2017.

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

[22] McHugh, Mary L. ”The odds ratio: calculation, usage, and interpretation.” Biochemia medica 19.2 (2009): 120-126.

[23] Kalra, Aakshi. ”The odds ratio: Principles and applications.” Journal of the Practice of Cardiovascular Sciences 2.1 (2016): 49-49.

[24] Friese, Christopher R., et al. ”Breast biopsy patterns and outcomes in surveillance, epidemiology, and end resultsMedicare data.” Cancer: Interdisciplinary International Journal of the American Cancer Society 115.4 (2009): 716-724.

[25] Levangie, Pamela K. ”Association of low back pain with self-reported risk factors among patients seeking physical therapy services.” Physical therapy 79.8 (1999): 757-766.

[26] Glas, Afina S., et al. ”The diagnostic odds ratio: a single indicator of test performance.” Journal of clinical epidemiology 56.11 (2003): 1129-1135.

[27] Levangie, Pamela K. ”Application and interpretation of simple odds ratios in physical therapy-related research.” Journal of Orthopaedic & Sports Physical Therapy 31.9 (2001): 496-503.

[28] Pesch, Beate, et al. ”Cigarette smoking and lung cancerrelative risk estimates for the major histological types from a pooled analysis of casecontrol studies.” International journal of cancer 131.5 (2012): 1210-1219.

[29] Gil, Santiago, Alexander Kott, and Albert-Lszl Barabsi. ”A genetic epidemiology approach to cyber-security.” Scientific reports 4.1 (2014): 1-7.

[30] Lvesque, Fanny Lalonde, et al. ”Technological and human factors of malware attacks: A computer security clinical trial approach.” ACM Transactions on Privacy and Security (TOPS) 21.4 (2018): 1-30.

[31] Santanna, Jos Jair, et al. ”Booter list generation: The basis for investigating DDoS-for-hire websites.” International journal of network management 28.1 (2018): e2008.

[32] Lewallen, Susan, and Paul Courtright. ”Epidemiology in practice: case-control studies.” Community eye health 11.28 (1998): 57.

[33] Mann, C. J. ”Observational research methods. Research design II: cohort, cross sectional, and case-control studies.” Emergency medicine journal 20.1 (2003): 54-60.

[34] Szumilas, Magdalena. ”Explaining odds ratios.” Journal of the Canadian academy of child and adolescent psychiatry 19.3 (2010): 227.

[35] Nashat, Dalia, Xiaohong Jiang, and Susumu Horiguchi. ”Router based detection for low-rate agents of DDoS attack.” 2008 International Conference on High Performance Switching and Routing. IEEE, 2008.

[36] Nashat, Dalia, Xiaohong Jiang, and Michitaka Kameyama. ”Group testing based detection of web service DDoS attackers.” IEICE transactions on communications 93.5 (2010): 1113-1121.

[37] Bowen, Tom, et al. ”Enabling reproducible cyber research-four labeled datasets.” MILCOM 2016-2016 IEEE Military Communications Conference. IEEE, 2016.

[38] Sharafaldin, Iman, et al. ”Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy.” 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, 2019.