Early Detection of LDoS Attack using SNMP MIBs

Gayathri Rajakumaran[1], Neelanarayanan Venkataraman[1], Abdul Quadir MD[1]*

[1] School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India
[1*] Corresponding author: gayathri.r@vit.ac.in

Abstract. Early detection of Denial of Service (DoS) attacks are given more emphasizing due to its adverse effects on disrupting the services of legitimate users. LDoS attack is one among the DoS category which floods the target at ideal rate to keep the connections open for longer duration. Traditional defense measures are inadequate to filter due to its less traffic volume. The current works focus on either empirical studies or signal processing models to capture the behavioural characteristics of LDoS based on TCP's congestion control and timeout mechanism but none carries out detection at a faster timestamp. Early detection solutions are the main focus as it could scale up the revenue losses in today's online application issues. Hence our model is based on Simple Network Management Protocol (SNMP), through which the early detection of LDoS attacks is carried out. The relevant detection metrics are identified through theoretical validation of SNMP MIBs and existing dataset analysis. Experimental simulations illustrate the LDoS detection efficiency and the same has been validated for theoretically.

1 Introduction

Internet plays the vital role due to advanced computing technologies and digitized environment. It acts as the backbone without which the day-to-day activities turn out to be zero. The growth of technologies goes hand-by-hand with the security disruptions. Distributed Denial of Service (DDoS) attack is a critical threat as it makes complete disruptions to the internet community by keeping its traces in the availability feature. During DDoS, the target is flooded with continuous bogus requests which occupy victim's memory. The exhausted victim is unable to accept or respond to any kind of requests from legitimate users. Resources exhausted during such attacks include bandwidth of network, CPU cycles, and Server's memory; interrupt processing capability and protocol structures. The current applications also face low spike attacks which produce the effect similar to DDoS high spike. LDoS attack is one among the category of DDoS family as it makes the TCP sessions engaged for longer duration by sending low spikes of traffic. A large traffic spike originating from attacker reaches the target at a slower rate meanwhile very few connections are established to escape from the time out mechanism and traditional defense strategies.

LDoS attack exploits the vulnerability in the congestion control mechanism of TCP by either periodically or continuously sending attack requests in short term or at constant rate. The time out mechanism of TCP congestion control is based on the time taken for receiving a complete request from the source. In general the Round Trip Time (RTT) is constant and ranges from 10 to 100s of milliseconds. In case of delayed request from the source, the Retransmission Time Out (RTO) operates on a longer time-scale.

Since the LDoS attacks poses very less volume of incoming traffic which mostly goes undetected by the traditional security defenses. Due to large incubation periods, the attack traffic mixes with the normal ones which make the traffic segregation and analysis part most difficult. If an online service gets disrupted either due to high spike or low spike DDoS, the trust among legitimate users and regular customers will be vanished. Uninterrupted service is the success behind big online giants like Amazon, Flipkart, Snapdeal, etc. According to the latest Amazon report [1], even 100 millisecond disruptions of its online services causes 1% drop in the overall sales. Hence early detection is the expected and needy solution to better address the issues faced in the current scenario. We aim to offer such solution by employing the features of Simple Network Management Protocol.

Numerous researches are ongoing to address the DDoS issues and to provide better solutions. The existing solutions are categorized under detection measures in general and detection measures based on hypothesis testing.

2 Technical Backgrounds

Low rate attack detection through information metrics [8] helps in measuring the difference in distance between the normal and attack traffic cases. Information metrics can quantify the differences in network traffic concerning various probability distributions. The generalized entropy metric and information distance metric are utilized in the process

of detecting low rate DoS attacks. The entropy metric can detect the attack seven hops earlier than the traditional Shannon metric. This approach outperforms the famous Kullback-Leibler divergence approach as it enlarges the adjudication distance and yields the optimal detection sensitivity. The information metric can effectively reduce the low rate DoS attacks with a clear reduction in the false-positive rate. The IP traceback algorithm can find all attacks as well as attackers within the own Local Area Network (LAN) and discards the incoming traffic. It also considers the attacks based on the category of insiders.

Low rate shrew based DoS attacks [9] are detected through the TCP congestion control window behavior. The shrew based DoS attacks are threatening for real-time applications as it can easily throttle TCP flows through a very low attack cost. By capturing the adjustment behaviors of the TCP's congestion control window, the combined effect of the attack pattern concerning the network environment is realized.

Empirical evaluation of the information metrics [10] attempts to detect the low and high rate DoS attacks in the networked environment. The empirical evaluation is carried out for the metrics namely Hartley entropy, Shannon entropy, Renyi's entropy, generalized entropy, kullback-Leibler divergence and generalized information measure in the process of detecting both low and high rate DoS attacks. These metrics help greatly in the differentiation of network traffic data and facilitates the process of building an optimal model. For illustrating the efficiency and effectiveness of the metrics related to DoS through the data sets MIT Lincoln Laboratory, CAIDA, and TUIDS.

Robust RED algorithm [11] is applied for detecting low rate DoS attacks. The RED algorithm maximizes the TCP throughput and attempts to filter, detect attack packets before the adoption of a normal RED algorithm for attack flows. The RRED algorithm claims the incoming flow as an attack only if the majority packets in the flow are sent within the short duration after a packet drop. RRED is efficient in suspecting both TCP and UDP based flow in the case of detecting low rate DoS attacks.

CPR based approach is used for the detection and filtering of the LDoS attack as they intend to cause network congestion. An incoming flow with Congestion Participation Rate (CPR) higher than the expected threshold is declared as suspicious and all the subsequent packets are dropped. The effectiveness of CPR is quantified through the average CPR distance for the normal and attack flows. This approach is more effective in terms of comparison with the existing Discrete Fourier Transform (DCT) technique in the process of detecting the LDoS attacks. A major difference in differentiating the TCP flows is that the normal TCP flows usually avoid the network congestion as it poses the TCP congestion control mechanism whereas the LDoS attack traffic introduces network congestion to degrade the network performance. In extreme cases, the LDoS attack throttles all normal TCP incoming flows and the aggregate value of the attack is very closer to the bandwidth of the network. CPR approach works well as it doesn't drop any packet and no network congestion is observed.

Low rate DoS detection based on network multifractal [12] considers the characteristics of network traffic in the process of detecting DoS attack. LDoS sends periodic pulse sequences with a low-frequency relative to form aggregation flows at the victim side. LDoS attacks, in general, are harder to detect as it poses the low rate property. For characterizing and analysing the network traffic, mathematical models are used for exploring the complex multifractal structure. Even though the LDoS attacks are slow, it contributes to the multifractal characteristics of network traffic.

The Multifractal Detrended Fluctuation Analysis Algorithm (MF-DFA) identifies the changes in the multifractal characteristics in small quantity for detecting the LDoS. Through the wavelet analysis process, the singularity, bursty nature of network traffic is captured and estimated using the Holder exponent. The difference values of Holder exponent between the normal and LDoS attack traffic are distinguished. The difference value is used as the basis for differentiating normal flow with the attack ones.

The dynamic time warping approach is used for robust and accurate identification of DDoS attacks. When the affected TCP flow enters into timeout and starts to retransmit the packets, the LDoS attack will send a small burst to force the TCP flows to enter into the RTO again. This results in very low transmission bandwidth for the TCP flows. When an attack is identified through the dynamic warping approach, the count of affected TCP flow is minimized, sufficient resource protection is done for the affected flows and behavioural analysis based prediction is carried out. This method has very low false positives and false negatives and efficient in the process of isolating legitimate users with the attacker.

3 Characterization of LDoS Attack

In LDoS, the attacker sends low traffic spikes at a very low frequency in order to hide its presence in the network. Complete analysis of attack pattern and characteristics plays a vital role for yielding a prominent and proactive solution. Representation of LDoS is depicted as in below Fig 1. LLDoS indicates the duration of attack pulse, SLDoS is the beginning of attack, RLDoS is the rate of requests received during attack and FLDoS represents the frequency of attack. The attack strength ASLDoS is represented as below.

$$ASLDoS = RLDoS \times LLDoS/FLDoS \quad (1)$$

The range of ASLDoS is very small in the case of normal traffic whereas it varies significanlty during attack traffic. The general behvarioural inhibitence of DDoS least helps in the LDoS detection procedure.

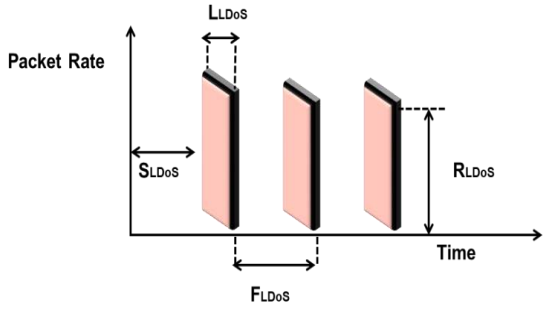

Fig. 1. Representation of LDoS

On receiving the low traffic spikes, the TCP's timeout delay gets increased from its initial value. In general, the delay is increased to facilitate proper connectivity and to prevent connection breakdown for the requesting client.

As per RFC 6298 standard [2], the RTO calculation for TCP is achieved through its two states SRTT (Smoothed Round-Trip Time) and RTTVAR (Round Trip Time Variation). The clock granuarity is assumed as G seconds. Initially the RTO is updated as 1 second till the RTO measurement is estimated.

$$RTO = SRTT + \max(G, K * RTTVAR) \quad (2)$$

For the first measurement of RTO value, RTTVAR=R and SRTT=R/2. For the subsequent RTO measurements the values :$(1-\beta)*RTTVAR+\beta*|SRTT-R|$. In case of abnormal behaviour, where the ACK is not received from the sender within the depicted RTO value, then the RT gradual increase in RTO is depicted in Fig 2.

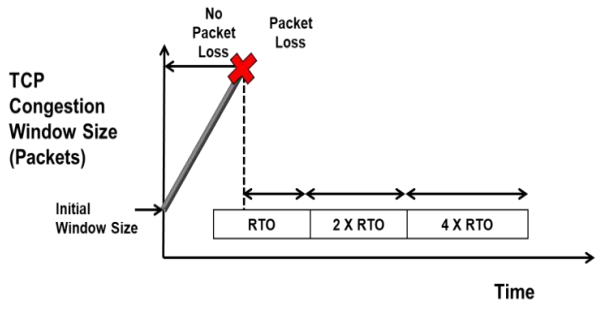

Fig. 2. TCP Retransmission Strategy

For better understanding, TCP's deterministic re-transmission strategy is exhibited. The RTO will be set for each and every incoming request.

$$\text{Total}(t) = \begin{cases} \text{RTOmin where LDoS} = 0 \\ 2 * \text{RTOmin where LDoS} = 1 \end{cases} \quad (3)$$

In general, the requests arises in a network is modeled as a Poisson distribution where the events are random [3]. 'n' number of arrivals in a time interval 't' is considered. The arrival rate is represented as 'ƛ'.

$$P(n\_t) = (ƛt)^n e^{(-ƛt)}/n! \quad (4)$$

A modulation of the above assumption could be done from the little's formula as few days network will be congested where it will not be the case for all times. In such cases, a network system could be modelled as (R_a,R_t). 'Ra' is the average number of reqeusts in the system and 'Rt' is the amount of time spent by each request in the system and 'ƛ' is the arrival rate.

$$R\_a = ƛ\, R\_t \quad (5)$$

The little's theorem [4] could be applied to either a whole system or part of a system as both serves the purpose. In the case of LDoS attack, the parameters affected network metrics could be packet transmission time, propagation delay, average queueing delay and average number of packets received. Estimating all these metrics values helps in faster attack detection as well helps to analyse the performance issues raised during LDoS. All the packets are considered as requests as we are employing the SNMP for anlaysing the incoming traffic. SNMP captures all incoming requests which are further considered for a detailed analysis. The various system parts considered for a bried analysis are listed as below

- Transmitter / Sender
- Transmission Line
- Buffer/ Memory
- Transmitter / Sender + Buffer/ Memory

'D_tr' is the request transmision time. The average number of requests at transmitter is depicted as 'D_tr' or þ for link utilization. 'D_r' is the propagation delay. The average number of requests on the fly is ƛ D_r. 'Dq' is the average queuing delay. The average number of requests in memory is ƛ Dq. Finally the average number of requests is illustrated by the equation þ + ƛ Dq.

4 Attack Modelling of TCP Variants

Detection solution for LDoS is achieved by considering the current variant of TCP adopted in today's Internet scenario and majority of websites. Among the other prevalent TCP variants, BBR [4],[5], [6], [7] is the dominant as it is adopted in most of the websites inclusive of Google cloud and Amazon Web Services (AWS). Our solution is modelled by assuming the constraints specific to behav-ioural characteristics of BBR. It attempts to provide solu-tions on the basis of traffic delivery and latency of roundtrips. BBR adopted in Amazon CloudFront effectively increased the performance gain upto 22% on aggregate throughput across various networks and regions. The performance gains rely on quality, capacity and distance of the connectivity. The congestion indicators of TCP BBR are Current Bandwidth Estimate (BWE) and RTTmin which is depicted in below cases. Rrate indicates the response rate of BBR TCP connections,

B_{qu} is the bottleneck queue utilization, tcp is the transit capacity, B_{asr} is the base sending rate, B_a is available bandwidth.

Case 1: Primary Congestion Response

$$\downarrow BWE \rightarrow \downarrow R_{rate} \quad (6)$$

Case 2: Recovery Mode

$$Count\ (R_{data}) = Count\ (REQ_{ack}) \quad (7)$$

Case 3: Core State (PROBE_BW) B_{qu} = tcp

$$BWE = B_{asr} \quad (8)$$

$$C_{wnd} = 2X\ BWE\ X\ RTT_{min} \quad (9)$$

Case 4: Exhausted Bandwidth

$$\downarrow Ba \rightarrow \downarrow Rrate\ |\uparrow Bqu\ |\ \downarrow BWE \quad (10)$$

$$\uparrow Ba \rightarrow \downarrow Bqu \quad (11)$$

TCP BBR addresses the bottleneck adopting the solutions based on the above computations. If the Ba falls, BWE will not represent it in the first 10 RTT's. The increased sending rate of BBR raises the B_{qu} and fall in BWE to match the returning ACK's rate. Similarly, the B_{qu} falls with the rise in Ba. Adopting SNMP in the above context, attempts to eliminate the congestion at primary level. The Rrate, REQ_{ack} could be obtained based on the TCP specific SNMP MIB's tcpPassiveOpens, tcpCurrEstab and tcpActiveOpens respectively. Through SNMP, by comparing the incoming and response counter values, LDoS attack traffic could be detected. To enhance the detection accuracy and minimize time constraint, the additional required parameters could be better validated based on outcomes of real time data set analysis.

5 Detection metrics based on Dataset Analysis

To understand the behavioural characteristics and traffic pattern of Denial of Service attacks, a complete analysis of the existing data set is important. To carry out the same, the KDD-99, NSL-KDD data set are chosen as it is one of the standard bench-marked data set. Out of the overall 41 features, the incoming frequency count is a derived one which plays a vital role in DoS detection. In order to achieve a complete traffic distinction between attack and normal traffic, additional parameters need to be explored. Hence the EDGAR (Electronic Data Gathering, Analysis, and Retrieval) data set is considered. Differentiation of normal traffic with Denial of Service is the expected outcome of the analysis, based on which the mitigation measures could be tested by generating the synthetic data set.

The Division of Economic and Risk Analysis (DERA) has assembled information on internet search traffic for EDGAR filings through SEC.gov generally covering the period February 14, 2003 through June 30, 2017.The data is intended to provide insight into the usage of publicly accessible EDGAR company filings in a simple but extensive manner.

The attack features are exactly understandable through the traffic patterns of the KDD data set but the normal requests which could be received per second from vari-ous IP addresses could not be retrieved from it as the data set does not contain the IP address column. The data set utilized for analysis is the most the recent year 2017 log record data set where it contains numerous factors particularly IP address, data and incoming time of request entry in seconds. These properties are utilized for further detailed analysis. Hence the U.S government data set EDGAR is used for observing the patterns of normal traffic. The detailed steps in the process of extracting requests based on the IP address and mapping it to the time scale are illustrated as below steps:

- The dataset is isolated with the factors IP address, date and time in seconds
- Normalize the obtained data set for removing duplicates
- Plot the incoming frequency of incoming IP address Vs Time to identify the number of requests which arrives from the same IP address per second
- Plot the distribution pattern based on the IP address which in turn helps to distinguish the normal traffic with the attack one

EDGAR dataset collection is achieved through 11 variables which provides complete picture about the IP ad-dress and status code of incoming requests and few other important metrics which are chosen through the feature selection process. The frequency of incoming requests from the same IP address is calculated by observing the IP address of incoming requests concerning time. The various variables of EDGAR dataset are illustrated as below:

- IP address of the incoming request
- Date
- Time
- Zone
- cik - index key associated with the requested document
- Accession number of the document
- Document file size
- Apache status code for the incoming request
- Referrer header
- Crawler information
- Browser information

The identified detection metrics are mapped with the TCP BBR modes for estimating the current state of incoming connection requests**.**

6 Experimental Testbed for LDoS

In order to validate the finding from the real time EDGAR data set analysis, experimental test bed set up is done to generate the synthetic data set based on the input metrics Arrival Rate and Request Size. To carry out the validation procedure, TCP specific SNMP MIBs are monitored by performing the experimental

set up of SNMP in a controlled environment as per the study. The set up involved 1 PC as Attacker, 1 PC as Normal user, 1 L2 switch and 1 PC as SNMP manager. SNMP agent is installed in both the attacker PC and Normal user PC for collecting the statistics. A test bed is set up for simulating the TCP-SYN attack and normal traffic requests. Any Web servers such as either Apache or XAMPP server will be handling requests in the victim system.

The test bed setup is connected to the D-Link DES-3528 switch. The switch could be managed through the serial port, telnet or web based management agent. The Com-mand Line Interface (CLI) is utilized for configuring and managing the switches through the serial port or telnet interfaces. This type is designed to provide the features fault tolerance, flexibility, port density, robust security and maximum throughput by providing the user-friendly management interface for the users. The test bed consists of one web server, an attacker, legitimate user, SNMP agent and SNMP manager system is depicted in Fig 3.

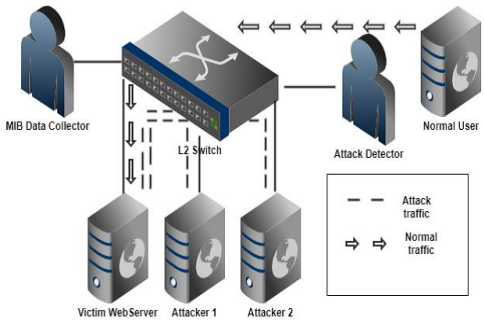

Fig 3: LDoS Testbed

6.1 Traffic Differentiation Based EDGAR Metrics on IP Frequency

The frequency of incoming requests from the same host is an important metric for differentiating the DoS traffic with the normal one which is derived from the EDGAR data set. During the first observation of per second arrival rate, the incoming requests from the same IP address are not exceeding the maximum threshold of 10. The observations are repeated for 30 days of the data set and the arrival rate of incoming IP addresses is monitored randomly to estimate the rough arrival rate of requests from the same IP address per second. All the 30 days results illustrate that the maximum requests which arise from the same IP address per second range between 10 to 40.

Graphs are constructed for a peak day of traffic from 9 AM to 5 PM in order to analyse the maximum requests which arise from the same IP addresses in the interval of 1 hour from the time period of 9 AM to 5 PM in a randomly chosen day of data. The obtained results are plotted with respect to the IP address and number of incoming requests depicted in Fig 4.

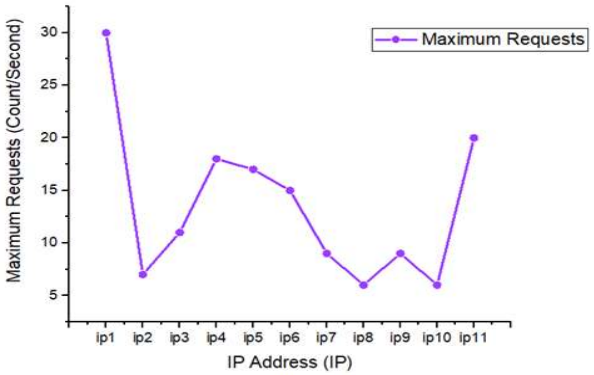

Fig 4: Request frequency 9 AM to 10 AM

Based on the incoming frequency analysis of the graphs based on the data collected from 9 AM to 5 PM, it is inferred that the count of requests which arrive from the same IP address reaches the maximum point of 34 in all the graphs. The analysis is done for the random 1-hour traffic data chosen for the 30 days statistics of the EDGAR data set and all the graphs are showing the same variation. Another interesting feature that has to be observed in the EDGAR analysis is that, even if the repeated requests arise from the same IP address, the request size is different for every individual request which is evident from the below graph. The overall incoming requests from the same IP address from 9 AM to 5 PM are represented in Fig 5.

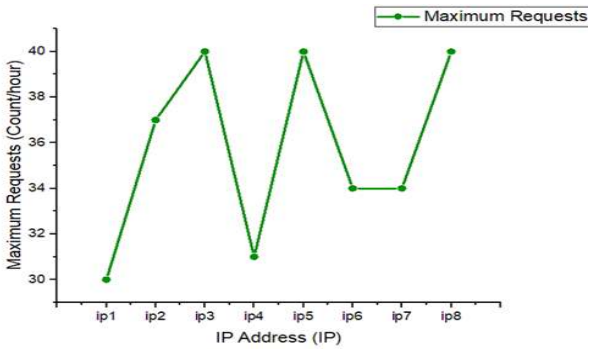

Fig 5: Request frequency from 9 AM to 5 PM

From the above graphs, it can be concluded that if the incoming request is normal, as per human behavioural and EDGAR analysis, a request of same size cannot be executed more than 5 by a normal user even if he tries to access the same file, for any scenario the request size will vary and it doesn't remains the same. This contradicts the attack scenario, as the incoming attack request sizes follows the same size and the arrival rates of attack varies from the range of 100 to 1 million as it merely depends on the capacity of the attacker system.

On observing the arrival rates of normal pattern of EDGAR, it ranges between 1 to maximum of 40 requests and not exceeding the mentioned range. From this analysis, conclusion is drawn for differentiating the normal traffic with the attack one. The analysis of each 1 hour traffic on every day is captured and analysis for a day is illustrated in the below Fig 6. It illustrates the

number of IP's with the same number of request count for the randomly chosen 1 hour time period in a day of EDGAR data set.

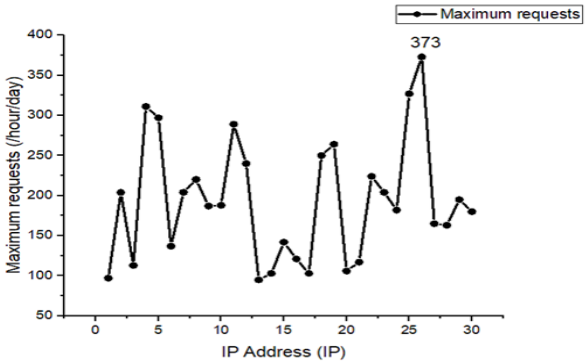

Fig 6: Maximum Request Count from various IP's

The maximum request value arriving from multiple IP addresses irrespective of the requested content are based on the 78 observation in the stipulated time period. Repeating this observation for all 30 days of the randomly chosen time period for each day, the maximum incoming request pattern and behaviour of normal IP's can be clearly understood. According to the observation, 96 are the maximum requests which arise from 107 IP addresses depicted in below figures. The graph is plotted by considering the IP address with respect to maximum request count for each day observed from the chosen time period.

It is concluded based on the observation of complete 30 days of EDGAR traffic, that if a request comes from a normal IP address, the maximum threshold from various IP addresses are not exceeding the range 373 and the number of requests per second from the same IP address is not exceeding the range of 40. In order to strongly conclude the incoming traffic as either attack or normal, additional parameter request size also needs to be considered as according to the EDGAR analysis, even maximum of 40 requests from the same IP address is handled as it belongs to different request sizes.

From the overall observation, only 2 requests originate from the same IP for the same request size which is termed as normal as it is within the threshold 5. Hence for traffic to be normal, the incoming request from the same IP should contain the various size of request else it will be distinguished as DoS attack traffic. The conclusions from the EDGAR dataset for attack distinction are carried out for the detection of LDoS attack.

6.2 Traffic Differentiation based on SNMP Metrics

We aim to address the above research gaps in the existing measures through the Simple Network Management Protocol (SNMP) [17][18]. The characterization of SNMP MIBs should be done initially which helps greatly to identify the purpose and importance of each. Based on the reference, the below SNMP MIBs are chosen.

The SNMP components, basic structure and the way of retrieving Management Information Base (MIB) variables are observed from the references. The MIBs relevant for LDoS detection are identified through the techniques theoretical validation and Linear Regression.

The metrics Request Size and Arrival Rate are fetched based on the real time data behaviour analysis of the KDD-99 dataset. To derive relation between the various attack distinction metrics for the LDoS attack traffic, the below ones are formulated. To have a detailed in depth analysis, the overall traffic, normal traffic, statistic traffic and attack traffic need to be represented which are denoted as ov(t), n(t), s(t) and a(t). The ov (t) could be expressed as

$$ov(t) = n(t)+a(t) \quad (12)$$

If the server is under normal traffic, then the representation is

$$a(t) = 0 \quad (13)$$

Therefore ov(t) = n(t)

If the server is under attack, then there is a rapid increase in the value of a(t) to larger levels. For easy attack identification, a(t) value needs to be captured. Our proposed method helps to capture the value of a(t) through the Management Information Base (MIB) variables of Simple Network Management Protocol (SNMP). The related MIB's are tcpActiveOpens, tcpPassiveOpens and tcpCurrEstab [14], [15], [16]. The attack detection algorithm is formulated as below.

Algorithm 1:Attack detection

```
Input: Analysis based on SNMP MIB's
        User requests: (R1, R2,..Rn)
        Sent user requests: IP_ tcpActiveOpensi
        Received user requests: IP_ tcpPassiveOpensi
        Failed user requests: IP_ tcpAttemptFailsi
        Established user requests: IP_ tcpCurrEstabi
    Threshold: T
        Sent user requests: IP_ ActiveOpensi
Output: Categorization of traffic 'LDoS' or 'Normal'
 begin
    if tcpActiveOpensi >= T
      "Differerentiate incoming Traffic"
    if tcpActiveOpensi != tcpPassiveOpensi &&
    tcpActiveOpensi != tcpCurrEstabi
Perform IP similarity comparison
    Compare consecutive IP's (IPi, IPj) at T
    if (IPi== IPj)
      "LDoS traffic"
    else
      "Normal traffic"
    endif
    endif
end
```

The captured results for SNMP MIB's from the experimental testbed are illustrated in the Fig 7, 8 and 9.

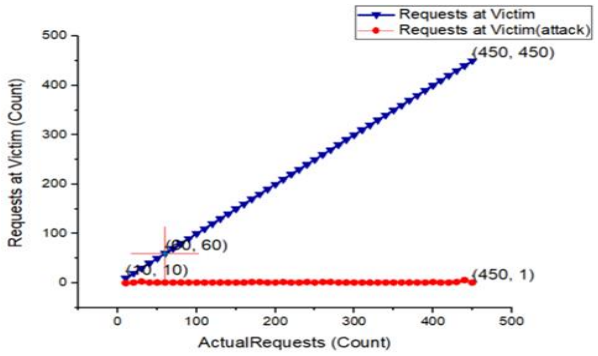

Fig 7: Variation of Actual Requests Vs tcpPassiveOpens

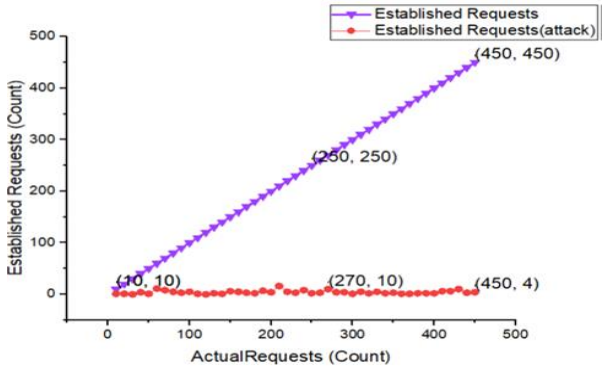

Fig 8: Variation of Actual Requests Vs tcpCurrEstab

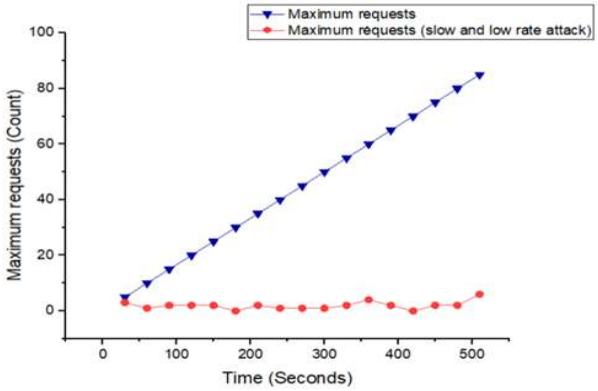

Fig 9: Variation of Time Vs Maximum requests

From the above, it is inferred that the during the nor-mal traffic, minimum variation exists between the SNMP MIB's tcpActiveOpens and tcpCurrEstab as 30 connections are established in 30 seconds. During attack traffic, there exists huge deviation between the chosen MIB's as only single connection is established in 30 seconds. Hence by combining the detection measures tcpActiveOpens, tcpCurrEstab, Time and maximum requests validation, 98.7 % detection accuracy is achieved. The general features and characteristics of DoS and LDoS [20], [21], [22], [23], [24] are analyzed based on the literature to arrive at a conclusion of the defensive measures.

7. Conclusion

The SNMP based detection measure is accompanied with the metrics based on the real time analysis of EDGAR dataset which helps in accurate detection of LDoS attacks and yields 98.7%. Early detection is another important criterion which is achieved in 6.9 seconds. The reseach gaps mentioned in the existing literature are examined carefully which paved way for the identification of an important metric tcpCurrEstab which helped to boost the accuracy. The chosen TCP specific SNMP MIB's are effective in distinguishing the LDoS attack from the normal one which is demonstrated through the simulation tools deployed in the experimental testbed. Theoretical validation is done is incorporated for the the aforementioned SNMP MIB's. The future work aims to analyse the real time log patterns to enhance the detection accuracy.

References

1. G. Linden, "Make Data Useful", Presentation, Amazon, November, 2006.
2. V. Paxson, M. Allman, J. Chu and M. Sargent, "Computing TCP's Retransmission Timer", https://tools.ietf.org/html/rfc6298, 2011.
3. Al-Haidari, F., Salah, K., Sqalli, M. et al. , "Performance Modeling and Analysis of the EDoS-Shield Mitigation", Arab J Sci Eng , Springer, 42, 793–804 (2017). https://doi.org/10.1007/s13369-016-2331-z.
4. Eytan Modiano , "Introduction to Queueing Theory ",http://web.mit.edu/modiano/www/6.263/lec5-6.pdf
5. Mishra, Ayush & Sun, Xiangpeng & Jain, Atishya & Pande, Sameer & Joshi, Raj & Leong, Ben. (2019). The Great Internet TCP Congestion Control Census. Proceedings of the ACM on Measurement and Analysis of Computing Systems. 3. 1-24. 10.1145/3366693.
6. AWS Admin, "TCP BBR Congestion Control With Amazon CloudFront", https://aws.amazon.com/blogs/networking-and-content-delivery/tcp-bbr-congestion-control-with-amazon-cloudfront/.
7. Colt McAnlis, "TCP BBR: Magic dust for network performance", https://medium.com/google-cloud/tcp-bbr-magic-dust-for-network-performance-57a5f1ccf437.
8. Xiang, Y., Li, K. and Zhou, W. (2011), 'Low-rate ddos attacks detection and traceback by using new information metrics', IEEE transactions on information forensics and security 6(2), 426–437.
9. Luo, J., Yang, X., Wang, J., Xu, J., Sun, J. and Long, K. (2014), 'On a mathematical model for low-rate shrew ddos', IEEE Transactions on Information Forensics and Security 9(7), 1069–1083.
10. Bhuyan, M. H., Bhattacharyya, D. and Kalita, J. K. (2015), 'An empirical evaluation of information

metrics for low-rate and high-rate ddos attack detection', Pattern Recognition Letters 51, 1–7.

11. Zhang, C., Yin, J., Cai, Z. and Chen, W. (2010), 'Rred: robust red algorithm to counter low-rate denial-of-service attacks', IEEE Communications Letters 14(5), 489–491.
12. Wu, Z., Zhang, L. and Yue, M. (2015), 'Low-rate dos attacks detection based on network multifractal', IEEE Transactions on Dependable and Secure Computing 13(5), 559–567.
13. Yu, H. (2007), Dos-resilient secure aggregation queries in sensor networks, in 'Proceedings of the twenty-sixth annual ACM symposium on Principles of distributed computing', ACM, pp. 394–395.
14. Gayathri R and Neelanarayanan V, "Denial of Service Attack prediction using Gradient Descent Algorithm", Advances in Internet Research and Engineering (Springer Nature), Vol:1(45), pp.1-8,2020
15. Gayathri R and Neelanarayanan V, "Identification of Regression function and distribution model for Denial of Service attack in Second Life online community using Simple Network Management Protocol", International Journal of Web Based Online Communities , Inderscience, Vol:15(3), pp.225-237, August 2019
16. Gayathri R and Neelanarayanan V, "DoS detection solution for cloud platform using SNMP", International Journal of Pure and Applied Mathematics , vol.119 (11), pp.175-183, 2018.
17. Xiao, L., Wei, W., Yang, W., Shen, Y. and Wu, X. (2017), 'A protocol-free detection against cloud oriented reflection dos attacks', Soft Computing 21(13), 3713–3721.
18. Thapngam, T., Yu, S., Zhou, W. and Makki, S. K. (2014), 'Distributed denial of service (ddos) detection by traffic pattern analysis', Peer-to-peer networking and applications 7(4), 346–358.
19. Stavrou, A., Fleck, D. and Kolias, C. (2016), 'On the move: Evading distributed denialof- service attacks', Computer 49(3), 104–107.
20. Shevtekar, A., Anantharam, K. and Ansari, N. (2005), 'Low rate tcp denial-of-service attack detection at edge routers', IEEE Communications Letters 9(4), 363–365.
21. Luo, X., Chan, E.W. and Chang, R. K. (2006), Vanguard: a new detection scheme for a class of tcp-targeted denial-of-service attacks, in '2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006', IEEE, pp. 507–518.
22. Liu, Z. and Guan, L. (2010), Attack simulation and signature extraction of low-rate dos, in '2010 Third International Symposium on Intelligent Information Technology and Security Informatics', IEEE, pp. 544–548.
23. Kline, E., Afanasyev, A. and Reiher, P. (2011), Shield: Dos filtering using traffic deflecting, in '2011 19th IEEE International Conference on Network Protocols', IEEE, pp. 37–42.
24. Kiuchi, T., Hori, Y. and Sakurai, K. (2010), A design of history based traffic filtering with probabilistic packet marking against dos attacks, in '2010 10th IEEE/IPSJ International Symposium on Applications and the Internet', IEEE, pp. 261–264.
25. Jingle, I. D. J., Rajsingh, E. B. and Paul, P. M. (n.d.), 'Distributed detection of dos using clock values in wireless broadband networks', International Journal of Engineering and Advanced Technology (IJEAT) ISSN pp. 2249–8958.
26. Hoque, M. A. and Chakraborty, B. (2015), 'Anomaly based intrusion detection systems using snmp data', International Journal of Science, Engineering and Computer Technology 5(3), 44.
27. Habib, A., Hefeeda, M. and Bhargava, B. K. (2003), Detecting service violations and dos attacks., in 'NDSS'.
28. Gao, Z. and Ansari, N. (2005), 'Tracing cyber attacks from the practical perspective', IEEE Communications Magazine 43(5), 123–131.
29. Elleithy, K. M., Blagovic, D., Cheng, W. K. and Sideleau, P. (2005), 'Denial of service attack techniques: Analysis, implementation and comparison'.