International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

Low Rate DDoS Attack Detection and Traceback using Wavelet Analysis

Ms. Hamna Farhan P C, Mr. Britto Dennis J, Mrs. Suganya K

PG Scholar, Dept. of.CSE(with specialization in networks)., Dhanalakshmi Srinivasan Engineering College, Professor, Dept. of Information Technology, Dhanalakshmi Srinivasan Engineering College,Tamilnadu,India, PG Scholar, Dept. of.CSE (with specialization in networks)., Dhanalakshmi Srinivasan Engineering College, Tamilnadu,India.

Abstract - *LDoS (Low-rate Denial-of-Service) attacks are stealthier than the traditional DDoS attacks. According to the characteristic of periodicity and short burst in LDoS flows, a detection system, MultiFractal Detrended Fluctuation Analysis (MF-DFA) against LDoS attacks has been developed based on the change in terms of multifractal characteristics of network traffic due to LDoS attacks. The difference in the Holder exponent value (using wavelet analysis) before and after LDoS attack is estimated and recorded as difference value or D-value. A threshold is set based on normal network traffic analysis. Comparing D-value with detection threshold confirms the presence of LDoS attacks. Experimenting in simulation platforms shows that MF-DFA yields higher detection probability with lesser false positive and false negative rates.*

Key Words: LDoS, MF-DFA, Multifractal characteristic, Holder exponent, D-value.

1.INTRODUCTION

Denial of service (DoS) attack on the Internet aims to make resource unavailable to the valid users by sending a spurious request. Distributed Denial of service attack is a large-scale and coordinated attack on availability of a network resource or a victim system, floated diffusely through many compromised computers on the Internet. "Primary victim" are those services that are under the attack, while "secondary victim" are compromised system that are used to launch the attack. An Attacker controls the primary victims, which in turn control the secondary victims (Zombies). The attackers require a few resources and bandwidth for execution to launch the attack. DDoS attacks have not been addressed properly yet [1].

Low-rate Denial of service (LDoS) is different from flood denial of service attacks. The most important feature of LDoS is that it does not have to send a high rate of continuing attack traffic streams, instead of that, it periodically sends a short time high-rate pulse. LDoS attack mainly through the self-adaptive mechanisms of network to reduce the service quality. Compared with flooding attacks, LDoS attack is a low-rate attack, making the attack stream more subtle, which makes the DoS attacks difficult to detect by traditional DoS detection methods.

LDoS attacks exhibit a periodic pulse sequence, which can be expressed in a triple of attack period T, attack duration L, and attack rate R, i.e.. $LDoS(T,L,R)$. Here, T is the interval between two successive attack pulses, and T can be obtained by estimating the execution duration of trusted source. The duration of the timer refers to RTO (retransmission timeout). L is the width of attack pulse. R is the intensity of attack pulse[2][3].

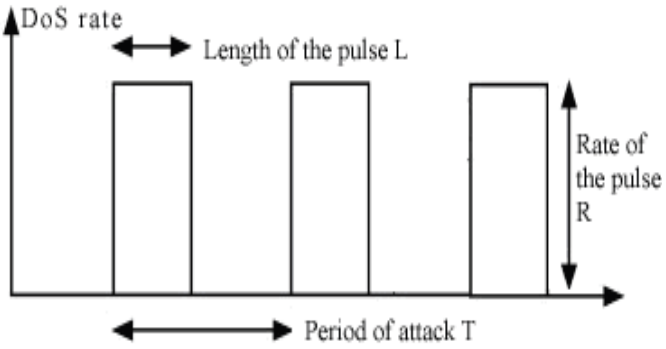

Fig-1: Simple model of pulse Attack signal

LDoS attacks attempt to deny bandwidth to TCP flows while sending at sufficiently low average rate and keeps damaging the victim for a long time without being detected. LDoS attacks send attack packets periodically in a short time interval. The network traffic exhibits self-similarity over a large time scale while presenting multifractal characteristics over a small time scale. The parameter α in multifractal characteristics known as Lipschitz-Hölder exponent (singularity exponent) presents the local singularity of a function. The network multifractal must be disrupted when LDoS attacks are launched suddenly. As a result, the Holder exponent is abnormal.

Barford Paul et. al. [4], and HE Yanxiang et. al. [5] introduced the wavelet processing idea in detecting LDoS attacks by using the discrete wavelet transform (DWT)

technology. This method transforms network traffic into high, middle, and low frequency components for the purpose of finding the attack traffic. *Chen Yu et. al*. [6] proposed a collaborative approach of defense against periodic shrew DDoS attacks in the frequency domain. This approach detected shrew DDoS attacks using the frequency-domain characteristics from the
Auto correlation sequence of Internet traffic streams. A study based on the fact that LDoS attacks can lead to abnormal flows which will change the multifractal characteristics of the network traffic was made[10]. Hence, the difference in Hölder exponents between attack and non-attack situations is the basis of detecting LDoS attacks [11].

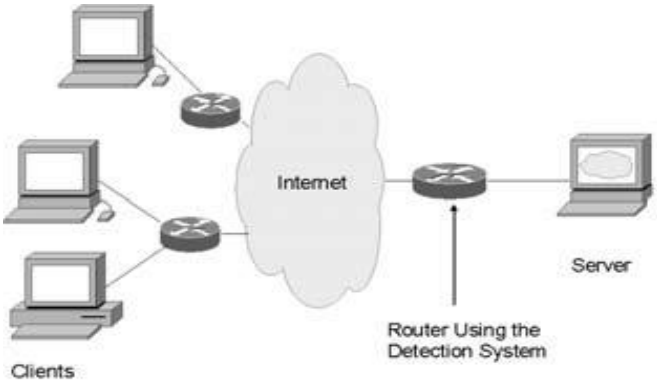

Fig -2: Proposed detection mechanism deployed in an edge router.

The network traffic exhibits self-similarity over a large time scale while presenting multifractal characteristics over a small time scale [7]. The parameter α in multifractal characteristics is defined as Lipschitz-Hölder exponent (hereafter referred to as Hölder exponent), it is also known as the singularity exponent [8], which presents the local singularity of a function. LDoS attacks send attack packets periodically in a short time interval. The network multifractal must be disrupted when LDoS attacks are launched suddenly. Hence, the Hölder exponent is abnormal. According to the above analysis, the approach of LDoS attacks detection based on network multifractal is proposed in this paper. Based on the essential attributes and features of network traffic, this approach calculates the value of Hölder exponent at all points, and the abnormal difference between the values of Hölder exponent is the basis of the LDoS attack detection.

2. SYSTEM MODEL

In this section we consider the existing system design and the proposed system.

2.2 Existing System

In order to detect an LDoS attack, it is necessary to sample and analyze network flows. Multiple Sampling Averaging Based on Missing Sampling (MSABMS) is used to detect LDoS attacks and to determine the attack's period [9]. MSABMS is a method of detecting small period signal. MSABMS has two functions in detection of small signals. An m × n matrix M is built by the sampling of network flows. The matrix M is transformed into an n-dimension vectors to calculate the average value of m on each column. The maximum and minimum average values of each column are obtained. Then the difference between the maximum and minimum value VJG is computed by iteration algorithm. Here VJG is called judging eigenvalue, which is used to estimate the attack's period.

An LDoS attack is taken as a signal Atk(t) with a period of T (unknown) with maximum and minimum value as Atkmax and Atkmin respectively. In an LDoS attack, Atkmax and Atkmin are obtained by counting the number of LDoS attack packets. If the difference of peak-to-bottom is defined as D, then

D = Atkmax - Atkmin

The judging eigenvalue VJG is obtained in a hunting interval Th by calculating the difference between the average of maximum and minimum signals.

VJG = Atkmax _ Atkmin (1)

If periodic signal Atk(t) doesn't exist, or the iteration operation is asynchronous with hunting interval Th, then VJG << D. A threshold thr is settled to determine whether LDoS attack is detected or not. If VJG ≥ thr, this value is recorded in an array P. The average of elements in array P is used as the prediction of the period after the periodic attack signal is detected. If P doesn't exist, there will not be any periodic small signals.

DRAWBACKS

- Effectiveness depends on network scale and bandwidth.
- Computational overhead.
- Accurate for only smaller attack signals.
- Not scalable.

2.2 Proposed System

Existing system possess some defects, such as, (i) the accuracy and the efficiency of entropy calculation will be greatly reduced with the expansion of network scale and the increase of network bandwidth. (ii) Lower detection rate, and higher false positive rate and higher false negative rate. (iii) Higher computational complexity.
The Hölder exponent, a fractal parameter of the network traffic, is used to characterize the bursty of network traffic at a certain point. The smaller the Hölder exponent is, the "burstier" the network traffic at the point is. Hence, when LDoS attacks have been launched, the multifractal characteristics of network traffic are changed, which indicates the bursty of network traffic. Through the estimation of Hölder exponent, the bursty of network traffic

is measured. Therefore, the LDoS attacks can be detected by Hölder exponent.

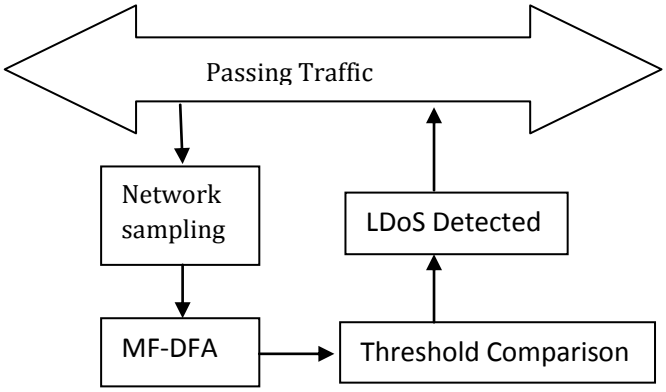

Fig -3: System Architecture.

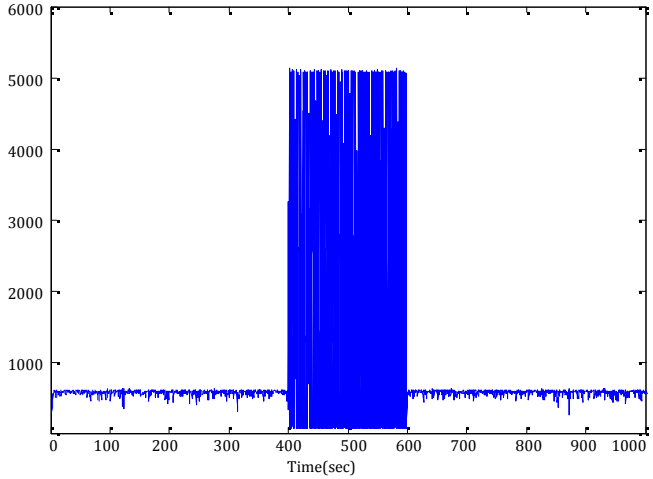

Fig -4: Packet number in the observed time interval

ADVANTAGES

- Improved detection probability.
- Reduced energy consumption.
- Additional stand-alone resources not required.

3. MULTIFRACTAL-BASED LDOS ATTACKS DETECTION

At present, more and more complex network traffic is described by using a traffic model in network traffic measurement. The discovery of self-similar feature of traffic gives an impulse to perform further intensive research. But researchers found that the self-similar model with its single scaling parameter is not enough as a multiple scaling on fine timescales. Therefore, multifractal model comes into being to illustrate the complex features of network traffic in detail. Available research result [18] reveals that the network traffic presents self-similarity on a large time scale and multifractal characteristic on a small time scale.

Network traffic measurement research [19] shows that most of the network traffic uses the TCP protocol. The primary reason is that the growing number of Internet users, the widespread availability of easy-to-use Web browsers, and the proliferation of Web sites with rich multimedia content combine to contribute to the exponential growth of Internet TCP traffic [15], while LDoS attack usually uses the UDP protocol. It is found that most of network services possess the multifractal characteristic, such as TCP, IP and HTTP, whereas UDP services have monofractal characteristic [16]. When LDoS attacks have been launched, a large number of UDP attack packets will appear in the network. This status will change the Hölder exponent which is used to measure local singularity of network traffic. A new approach of detecting LDoS attacks is proposed by monitoring the abrupt change of Hölder exponent through wavelet analysis.

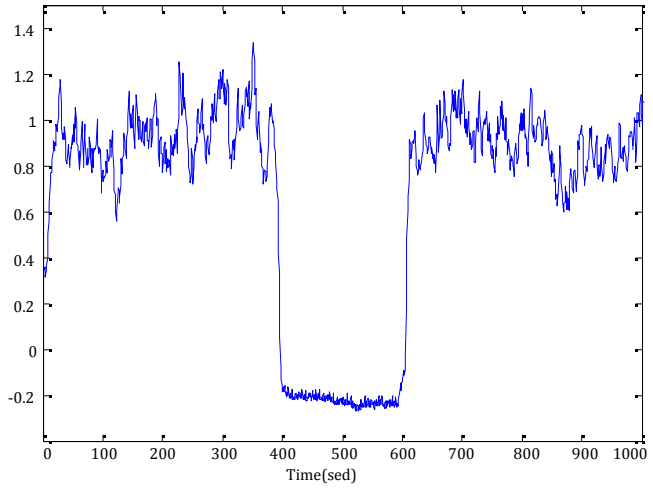

Fig- 5: Holder exponent.

3.1 Hölder Exponent Estimation

F.H.T. Vieira et. al. [15] have proved that local signals' singularity can be characterized by the wavelet transformation, and put forward Lipschitz exponent of signals' singularity, which can be estimated by tracking the crossscale change of wavelet transform modulus maxima(WTMM) in the cone of influence (COI). But the algorithm has some drawbacks. It can only be applied to isolated non-oscillating singularities, and the robustness and the accuracy of the algorithm are greatly reduced when WTMM curve fluctuates. Based on the analysis above, a robust approach of estimating the pointwise Hölder exponent is presented in this paper, whether the point is an oscillating singularity or not.

3.2 Detection of LDoS attack

Fig. 4 shows the network packet sequence. The packet number increases sharply at the start of LDoS attacks. For

the sequence, pointwise Hölder exponents are estimated by the algorithm introduced in section 3.2. Results are shown in Fig. 5.

The Hölder exponent changes abnormally by time with LDoS attacks. When the LDoS attacks start, the Hölder exponent falls quickly. When the LDoS attacks end, the Hölder exponent rises rapidly to the normal level. The abnormal change of singularity value of network traffic provides a new way to detect LDoS attacks. The procedure of LDoS attack detection is put forward, where the pointwise Hölder exponents of the sampled network packet sequence are estimated, and then the difference value of Hölder exponent is calculated as normalized.

From the results, there are two peaks in normalized *Holder* that occurred when LDoS attacks begin and end. Threshold is set based on the statistical analysis. If normalized Holder is larger than the detection threshold, LDoS attacks are considered to exist. Otherwise, there is no LDoS attack in the network.

4. CONCLUSIONS

In this paper, Network multifractal analysis based LDoS detection is presented. It aims at the distributed attack detection without extra memory requirements. The MF-DFA algorithm used in this approach is flexible, thereby making this model scalable for larger networks. It is proved that network traffic has the multifractal characteristic by using MF-DFA algorithm. Then, pointwise Hölder exponents are estimated based on wavelet analysis. And then, LDoS attacks are detected by comparing the Hölder exponent difference with the detection threshold, and the beginning or the ending of LDoS attacks are determined by t hypothesis test. This energy efficient approach enables devices to enter idle state when not in use, thereby enhancing performance of the network.

REFERENCES

[1] Zargar, S.T., Joshi, J., Tipper D, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046-2069, 2013.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] Yajuan Tang, Xiapu Luo, Qing Hui, Chang R.K.C, "Modeling the Vulnerability of Feedback-Control Based Internet Services to Low-Rate DoS Attacks," IEEE Trans. Information Forensics and Security, vol. 9, no. 3, pp. 339-353, March 2014, doi: 10.1109/TIFS.2013.2291970.

[3] Macia-Fernandez, G., Diaz-Verdejo, J.E., Garcia-Teodoro, P.,"Mathematical Model for Low-Rate DoS Attacks Against Application Servers," IEEE Trans. Information Forensics and Security, vol. 4, no. 3, pp. 519–529, Sept. 2009, doi: 10.1109/TIFS.2009.2024719.

[4] Barford P, Kline J, Plonka D, and Ron A, "A signal analysis of network traffic anomalies," Proc. ACM SIGCOMM Internet Measurement Workshop, Marseilles, France, 2002, pp. 71-82.

[5] HE Yan-Xiang, CAO Qiang, LIU Tao, HAN Yi, XIONG Qi, "A Low-Rate DoS Detection Method Based on Feature Extraction Using Wavelet Transform," Journal of Software, vol. 20, no. 4, pp. 930−941, April. 2009.

[6] Chen Y, HWang K, and Kwok Y-K, "Collaborative defense against periodic shrew DDoS attacks in frequency domain," Technical Report TR 2005-11. Submitted to ACM Trans. on Information and System Security (TISSEC), May. 2005.

[7] A. Feldmann, A. Gilbert, and W. Willinger, "Data Networks as Cascades: Explaining the MultiFractal Nature of Internet Traffic", Proc. ACM SIGCOMM, Vancouver, BC, pp. 42-55, September 1998.

[8] Xia, Zhengmin, Lu, Songnian, Li, JianHua, "DDoS Flood Attack Detection Based on Fractal Parameters," presented at 2012 8th International Conference on Wireless Communications, Networkingand Mobile Computing (WiCOM), pp.1 –5, 2012.

[9] Wu Zhi-jun, Zhang Hai-tao, Wang Ming-hua, Pei Bao-song, "MSABMS-based approach of detecting LDoS attack," vol. 31, pp. 402-417, 2012.

[10] Carey Williamson, "Internet Traffic Measurement," IEEE Internet Computing, pp.70-74, November-December 2001.

[11] Uday B. Desai, Krishna P.Murali, and Vikram M. Gadre, "Multifractal Based Network Traffic Modeling," Kluwer AcademicPublishers, December 12, 2003. ISBN-13: 9781402075667.