ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 9, September 2015*

# Survey on Low Rate Denial of Service Attacks

**Veeradanya. K.S[1], Dr.Thilagavathi. D[2]**

P.G Scholar, Dept of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India[1]

Professor and Head, Dept of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India[2]

**Abstract:** Low-rate denial of service attacks sends the sequence of periodic pulse which are low rate, when it is aggregated there will be a huge loss at the victim end. LDoS attack flows low rate of scaling function and hiding information for long duration. LDoS attacks severely degrade the availability of a victim, which can be a host, a router, or an entire network. The occurrence discovering is takes place based on the network traffic features. It will detect both the known and unknown LDOS attack in the considered network traffic features. The traffic records can be analyzed by different algorithm. This paper is concentrated on the survey of LDoS attacks and it is detected by the mechanism using holder exponent of difference value (D-value) between normal and LDoS attack under network traffic.

**Keywords:** LDoS, Holder exponent, D-value.

## I. INTRODUCTION

There are many network security threats are available over the web. The most common threats are viruses, worms and Trojan horses, spyware, denial of service attack, hacker attacks, and identity theft. It may be accomplished through hardware and software. That software will update and managed to protect from the threats. The security can be manages in different kind of situations like home or small office may require the basic security, in large business it requires the high maintenance. The traffic based anomaly detector, whose normal profiles are generated using different algorithm to produce the traffic records.

LDOS attacks severely degrade the availability of a victim, which can be a host, a router, or an entire network. Threat modeling is based on the notion that any system or organization has assets of value worth protecting, these assets have certain vulnerabilities, internal or external threats exploit these vulnerabilities in order to cause damage to the assets, and appropriate security countermeasures exist that mitigate the threats.

The normal profiles and thresholds have direct influence on the performance of a threshold-based detector [1].A low-quality normal profile causes an inaccurate characterization to legitimate network traffic. From the network traffic records the LDOS attack is detected by comparing the threshold value and the normalized value. Normalized value is estimated by holder exponent.

In this paper, we focus on research in the area of LDoS Attacks detection. Specifically, the work published during the period of 2007-2014. We analyze major components in each study for the evaluation and comparison of the LDoS attack detection techniques. These components include the characteristics of the performed experiments and the methods used for performance evaluation.

The paper is organized as follows: Section II presents the overview of the related work. In Section III, we present our evaluation methodology. Finally, Section IV concludes the survey and provides some future directions.

## II. RELATED WORK

In the literature, the detection of anomalies has be survived widely in the context distributed system. With some significant reported works related to this problem identification based on the detecting network traffic behavior and characteristics are as follows.

Garca-Teodaro , J. Daz-Verdejo, G. Maci-Fernndez, E. Vzquez.In this paper, they proposes the anomaly based network intrusion detection technique, system and challenges[3] along with their operational architecture and also presents a classification based on the type of processing that is related to the “behavioral” model for the target system. This detects only the path of network but it doesn’t find out the specific attacker detail. Intrusion detection is not identified the optimal set of indicator for known and potential abnormalities. An advantage of assessment in real environment is that the traffic is sufficiently realistic. The main drawback is that the development of high quality knowledge is often difficult and time consuming.

C.Yu, H.Kai, and K. Wei-Shinn,Collaborative Detection of LDoS Attacks over Multiple Network Domains (2007).[4]in this paper, they proposed that it was crucial to detect the LDOS flooding before widespread damages done to legitimate application on the victims system. They developed a distributed change point (DCP) detection architecture system based on change aggregation trees (CAT) mechanism. The detection of LDoS attacks minimize the flooding damages to the victim systems serviced by the provider. Advantage of collaborative detection is its enlarged area of protection coverage. Majority of ISPs do not share their Autonomous system (AS) domains with competitors so those AS are not detected the attacks.

G.Thatte, U.Mitra, J.Heidemann.Parametric Methods for Anomaly Detection in Aggregate Traffic (2011). In this paper, they have developed the bivariate parametric detection mechanism (bPDM) [5], which can detect anomalies and low rate attacks in a few seconds. This

DOI 10.17148/IJARCCE.2015.4921

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

approach allows the real time estimation of model parameter and only requires 2-3 seconds of background traffic for training. Incorporating the packet rate and packet size features enables us to detect anomalies in encrypted traffic and avoid state intensive flow tracking. They did not use the flow separated traffic .so that the source and destination IP addresses of the each packet at the router ,port number are not available. They use only one link in the LOS line.

W.Wang, X.Zhang, S.Gombault, and S.J.Knapskofg. (2009) have proposed Attribute Normalization [6] in Network Intrusion Detection with different scheme of attribute normalization on the detection performance with three anomaly detection algorithm. PCA(Principal component analysis), k-NN (K-Nearest Neighbor) and SVM (support vector machine).the schemes of attribute normalization, statistical normalization, frequency normalization and ordinal value normalization. The schemes of attribute normalization to preprocess the data for the anomaly intrusion detection. The original data and employed normalized data are compared to form the detection results. They doesn't normalized the streaming data.

K. Lee, J. Kim, K.H. Kwon, Y. Han, and S. Kim (2009), they proposed LDoS Attack Detection Method Using Cluster Analysis [7] and proposed the solution to detect the pattern behavior of traffic sources by observing packet arrival. This technique is an efficient method to discriminate the packets among LDoS attack sources and real user including proxies.

Sahar Namvarasl, Marzieh Ahmadzadeh (2014),This paper introduces flooding attack detection system based on SNMP MIB data[8], which selects effective MIB variables and compares some different classification algorithms based on chosen variables.The advantage of this system is its ability to learn the system's detection model will be optimized after receiving the new data.It stated that KST is able to detect more attacks in all situations even at low traffic intensities.

Monowar H. Bhuyan, H . J . Kash yap, D . K. Bhattacharyya and J . K. K alita (2011)They present aComprehensive survey of LDOS attacks, detection methods and tools[9] used in wired networks. The paper also highlights open issues, research challenge s and possible solutions in this area.Instances of the agents of tware are placedin the compromised systems that finally carry out the attack.D-WARD not only detecting slowly, ratebutals are reduces DDoS attack traffic significantly.

Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, Ren Ping Liu(2011)The effectiveness of the proposed multivariate correlation analysis[10] approach is evaluated on the KDD CUP 99 dataset. A multivariate correlation analysis approach to investigate and extract second-order statistics from the observed network traffic records. The advantage in detecting unknown attacks, anomaly intrusion detection mechanism has captured the major attention from research community. This comparative high false positive rates and do not work under the situation where an attack linearly changes all monitored features

## III. EVALUATION METHODOLOGY

### Estimating Holder Exponent:

Based on the analysis of network traffic records, the robust approach for estimating point wise Holder Exponent in this paper, [1]
Let consider positive process X(t),burst strength of X at the time t can be characterized by[2]

$$\alpha(t) = \lim_{k_n 2^{-n} \to t} \alpha_{k_n}{}^{n} \qquad \rightarrow (1) \text{ Where,}$$

$$\alpha_{k_n}{}^{n} = -\frac{1}{n}\log_2\left|X\left((k_n + 1)2^{-n}\right) - X(k_n 2^{-n})\right| \qquad \rightarrow (2)$$

And $k_n = 0,1 \ldots .\, 2^n - 1$

Let $\alpha(t)$is said to be Local Holder Exponent which points out the network characteristics traffic due to LDoS attack.
$\alpha(t)$ is the key step of LDoS attack detection
$n = 2^m$ is packets which given as discrete time signals with samples. Holder exponent at the point $k_0$is estimated by the algorithm as given below:

Step 1: Plotting the parametric curve

$$j(0 < j \leq m),$$

$$x_j(k) = \log_2( 2^{-j} + |k - k_0|2^m = x\,(j, k) \qquad \rightarrow (3)$$

$$y_j(k) = \log_2\left(\left|d_{j,k}\right|\right) \qquad \rightarrow (4)$$

Step 2: Finding each straight line
$D: y = \alpha x + C$ Such that,
D is an upper – bound for all plotted points$\left(x_j(k), y_j(k)\right)$, i.e.,

$$\forall j, \forall k$$

$$y_j(k) \leq \alpha x_j(k) + C \qquad \rightarrow (5)$$

There exists a sequence of pairs $(j_i, k_i)$ such that,

$$\lim_{i\to\infty} y_{j_i}(k_i) - \left(\alpha x_{j_i}(k_i) + C\right) = 0 \rightarrow (6)$$

Step 3: Finding the maximum of slops $\alpha_{max}$ over all lines D satisfying both the formulas (5) and (6).The slope $\alpha_{max}$ is the Holder Exponent of the signal at the point$k_0$.

**LDOS attacks detection:**
Sampled network packets are estimated by holder exponent. The difference of holder exponent is indicated as$|\Delta \text{Hölder}|$and calculated as normalized.
Normalized $|\Delta \text{Hölder}|$ occurred at beginning and end of LDoS attack. The threshold value is set as σ and it is compared with LDoS attack.
Normalized $|\Delta \text{Hölder}| > \sigma$,then LDoS attack exists.
Normalized $|\Delta \text{Hölder}| < \sigma$,then LDoS attack doesn't exist.

## IV. CONCLUSION

In this paper, different approach are surveyed in the analysis of network traffic and the estimation of LDoS attack detection using holder exponent mechanism. Comparing the holder exponent with the threshold for

DOI 10.17148/IJARCCE.2015.4921

LDoS attack detection probability performance. The future research can be based on Markov Chain Monte Carlo (MCMC) method for analyzing the traffic records and attack detection are proposed to compare the performance.

## V. REFERENCES

[1] WU Zhi-jun, Zhang Liyuan, Yue Meng," Low-Rate DoS Attacks Detection based on network multifractal" ieee transactions on dependable and secure computing, tdsc-2014-06-0130.

[2] António Nogueira, Paulo Salvador, Rui Valadas, and António Pacheco, "Modeling Network Traffic with Multi fractal Behavior,"Telecommunication Systems, vol. 24(2-4), pp 339-362, October2003, doi: 10.1023/A: 1026183318200.

[3] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E.Vzquez, "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges," Computers and Security, vol. 28, pp. 18-28, 2009.

[4] Yu Chen, Member IEEE, Kai Hwang, Fellow IEEE, and Wei-Shinn Ku, Member, IEEE," Collaborative Detection of DDoS attacks over multiple network domains," IEEE transactions on parallel and distributed systems, TPDS-0228-0806.

[5] Gautam Thatte, Urbashi Mitra, and John Heidemann,"Parametric Methods for Anomaly Detection in Aggregate Traffic (Extended Version) 0,"Usc/Isi Technical Report ISI-TR-663b, August 2010.

[6] W. Wang, X. Zhang, S. Gombault, and S.J. Knapskog, "Attribute Normalization in Network Intrusion Detection,"Proc. 10th Int'lSymp. Pervasive Systems, Algorithms, and Networks (ISPAN), pp. 448-453, 2009.

[7] K. Lee, J. Kim, K.H. Kwon, Y. Han, and S. Kim, "LDoS Attack Detection Method Using Cluster Analysis, "Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.

[8] Sahar Namvarasl, Marzieh Ahmadzadeh,"A dynamic flooding attack detection system based on SNMP MIB Data "International journal of computer networks and communication security, VOL.2, NO.9, SEP 2014, 279-284.

[9] Monowar H. Bhuyan, H . J . Kash yap, D . K. Bhattacharyya and J . K. K alita,"Detecting distributed denial of service attacks: methods , tools, and future direction" TheComputerJournal.March 28,2013.doi:10.1093/comjnl/bxt031.

[10] Zhiyuan Tan ,Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, Ren Ping Liu,"A system for Denial of service attack detection based on multivariate correlation analysis" IEEE Computer Society. Issue No.02-Feb (2014 vol.25) pp: 447-456.

DOI 10.17148/IJARCCE.2015.4921