International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 29, 2017 ISSN: 2348-6600
Reference ID: IJCS-296 PAGE NO: 1953-1961

PERFORMANCE EVALUATION OF LDOS ATTACK BY USING ABE ALGORITHM

Ms. Ranjitha R *PG Scholar, Dept. of.CSE(with specialization in networks)., Dhanalakshmi Srinivasan Engineering College,*
Mr. Britto Dennis J *Professor, Dept. of Information Technology, Dhanalakshmi Srinivasan Engineering College,Tamilnadu,India,*
Mrs. Suganya K *PG Scholar, Dept. of.CSE (with specialization in networks)., Dhanalakshmi Srinivasan Engineering College, Tamilnadu,India.*

Email ID- ranjitha.yadev@gmail.com

Abstract - Denial of service (DoS) attack and distributed denial of service (DDoS) attack on the internet aim to prevent legitimate clients from accessing a service and are considered a serious threat to the availability and reliability of the internet services. Client puzzle is a well known countermeasure, which demands a client to perform computationally expensive operations before being granted services from a server. However, an attacker can inflate its capability of DoS/DDoS attacks with the fast puzzle-solving software and/or built-in graphics processing unit (GPU) hardware to significantly weaken the effective of client puzzle. 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, TCP's retransmission timeout mechanism can be exploited by using maliciously chosen low-rate attack flow to make TCP throughput fall to a very low rate. LDoS attacks will degrade the performance of web traffic, TCP services and reduce TCP throughput to zero. Based on LDoS, bots multiplexing in multi-targets attack scenario is proposed, and then present the LDoS attack ability enhancing method. In simulation, the method shows good performance and adaptability, it can enhance attack ability effectively under variety of correlated parameters.

Keywords: DDoS, client puzzle, software puzzle, LDoS, multi-targets attack.

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

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) and
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 29, 2017 ISSN: 2348-6600
Reference ID: IJCS-296 PAGE NO: 1953-1961

execution to launch the attack. DDoS attacks have not been addressed properly yet .

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].

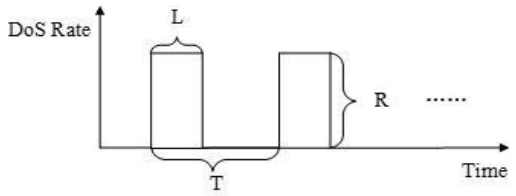


Fig-1: Notation for LDoS

Hash-reversal is an important client puzzle scheme which increases a client cost by focusing the client to crack a onwe way hash instance. technically, in the puzzle generation step,given a public puzzle function p derived from one way functions such as SHA-1 or block cipher AES, a server randomly choose a puzzle challenge x, and sends x to the client. an attacker can easily utilize the “free” GPUs or integrated CPU-GPU to inflate his computational capacity. This renders the existing client puzzle schemes ineffective due to the significantly decreased computational cost ratio. For example, an attacker may amortize one puzzle-solving task to hundreds of GPU cores if the client puzzle function is parallelizable or the attacker may simultaneously send to the server many requests and ask every GPU core to solve one received puzzle challenge independently if the puzzle function is non-parallelizable. , this scheme is vulnerable to DoS attackers who can implement the puzzle function in real-time.

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.

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

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) and
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 29, 2017 ISSN: 2348-6600
Reference ID: IJCS-296 PAGE NO: 1953-1961

non-attack situations is the basis of detecting LDoS attacks [11].

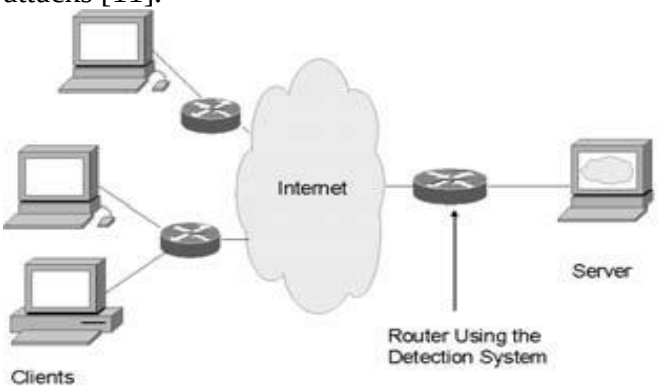


Fig -2: Proposed detection mechanism deployed in an edge router.

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

The low-rate TCP-targeted DDoS attack (LDoS) is a very low detectable attack, which benefits from low average rate. In order to detect an LDoS attack, it is necessary to sample and analyze network flows. An individual botnet device can be simultaneously compromised by several perpetrators, each using it for a different type of attack and often at the same time. For instance, a malware-infected personal computer could be ordered to rapidly access a website as part of a larger DDoS attack. At the same time it could also be performing vulnerability scans, with its owner browsing the web unaware of both occurrences. The packet sending rate is so high, so that it crosses the link capacity and hence congestion will occur in network. It is very difficult to identify LDoS attack, because of low average rate is maintained during network congestion.

Randomizing retransmission Time Out (RTO) of TCP is one method discussed in LDoS. The LDoS attack reduces TCP throughput to zero by exploiting TCP's slow-time-scale dynamics of RTO. A flow will be timed out frequently because of high rate of pushing LDoS attacking packets.
A DoS attack involves a single machine used to either target a software vulnerability or flood a targeted resource with packets, requests or queries. A DDoS attack, however, uses multiple connected devices often executed by botnets or, on occasion, by individuals who have coordinated their activity.

DDoS attacks can be divided into two general categories:

1. Application layer DDoS attack types include HTTP floods, slow attacks zero-day assaults, and those targeting vulnerabilities in operation systems, web applications and communication protocols.

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) and
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 29, 2017 ISSN: 2348-6600
Reference ID: IJCS-296 PAGE NO: 1953-1961

Comprised of seemingly legitimate and innocent requests, their magnitude usually being measured in requests per second (RPS), the goal of the attacks is to overwhelm a target application with requests. This causes high CPU and memory usage that eventually hangs or crashes the application.

2. Network layer DDoS attack types include UDP floods, SYN floods, NTP amplification, DNS amplification, SSDP amplification, IP fragmentation and more.

DRAWBACKS

- Effectiveness depends on network scale and bandwidth.
- Computational overhead.
- Accurate for only smaller attack signals.

Not scalable

Client puzzle schemes which publish a puzzle function in advance, the software puzzle scheme dynamically generates the puzzle function P(·) in the form of a software core C upon receiving a client's request. Specifically, by extending DCG technology which produces machine instructions at runtime [10], the proposed scheme randomly chooses a set of basic functions, assembles them together into the puzzle core C, constructs a software puzzle C0x with the puzzle core C and a random challenge x. If the server aims to defeat high-level attackers who are able to reverse-engineer software.

An attacker may amortize one puzzle-solving task to hundreds of GPU cores if the client puzzle function is parallelizable (e.g., the hash reversal puzzle), or the attacker may simultaneously send to the server many requests and ask every GPU core to solve one received puzzle challenge independently if the puzzle function is non-parallelizable (e.g. modular square root puzzle [7] and Time-lock puzzle [8]). This parallelism strategy can dramatically reduce the total puzzle-solving time, and hence increase the attack efficiency. 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.

Problems Identified:

- A client has to spend a certain amount of time tc in solving the puzzle (i.e., finding the puzzle solution y)
- The server has to spend time ts in generating the puzzle challenge x and verifying the puzzle solution y.
- The existing client puzzle schemes assume that the malicious client solves the puzzle using legacy CPU resource only.

2.2 Proposed System

The proposed scheme randomly chooses a set of basic functions, assembles them together into the puzzle core C, constructs a software puzzle C0x with the puzzle core C and a random challenge x. LDoS is an active type of attack which targets the buffer capacity of the server thus bogging down the network considerably. During an LDoS attack the attacker fills the buffer of the server instantaneously and remains latent for a certain amount of time till the buffer inputs are processed by the server, and this Mechanism is carried out in a loop till the attacker wishes to keep the server engaged. Following steps were carried out in given sequence:

Server was implemented which provides files to client when requested

Legitimate application was implemented which genuinely asks the server for a file.

Data mining is a process of analyzing data from different sources and summarizing it into useful information. It is a process of converting data into

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) and
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 29, 2017 ISSN: 2348-6600
Reference ID: IJCS-296 PAGE NO: 1953-1961

information. Data are facts and information is processed data. Data mining is process of finding correlations or patterns among a large dataset. The proposed mechanism uses data mining algorithms for classification of dataset.

Advantages

- Low-rate DoS attacks degrade the performance of both short and long lived TCP traffic.
- IF RTT (Round Trip Delay Time) of packets are low then effect of attack is more.
- Low-rate periodic packets can be very harmful to short-RTT TCP traffic. **Fig-3:**

3. MODULES

3.1 Network Formation

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. When a route to destination is needed, the node broadcasts a route request (RREQ) packet to its neighbors to find the optimal path.

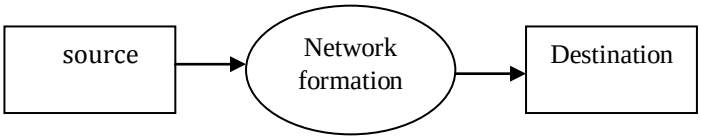


Fig-4: Network Formation

3.2 Ad-Hoc On-Demand Distance Vector Routing (Aodv) Protocol

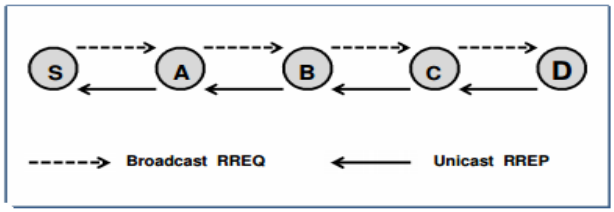
AODV is an on-demand routing protocol designed for operation of mobile ad hoc network. Protocol provides self starting, dynamic, loops free, multi-hop routing. Protocol allows mobile nodes to establish routes quickly for new destinations as well as to respond to changes in network topology and link failures as only affected set of nodes are notified. Nodes do not maintain routes to the destinations that are not in active communication.
AODV protocol works in two phases

- Route discovery process and
- Route maintenance process.

Route discovery process uses Route Request (RREQs) and Route Reply (RREPs) messages. RREQ message contains route request broadcast ID, Destination IP Address, Destination Sequence Number, Source IP Address, Source Sequence Number and Hop Count.
So that RREP message can be unicast to that sender node from the destination or any intermediate node that satisfy the request conditions. Upon receiving the route request message, the intermediate node forwards the RREQ message until a node is found that is the destination itself or it has an active route to the destination with destination sequence number greater than or equal to that of RREQ. Route maintenance is performed with two additional messages: Hello and RRER messages. Each node broadcast Hello messages periodically to inform neighbors about its connectivity. The receiving of Hello message proves that there is an active route towards the originator.

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) and
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 29, 2017 ISSN: 2348-6600
Reference ID: IJCS-296 PAGE NO: 1953-1961



The routing message exchange in AODV

Fig-5: Ad-Hoc On-Demand Distance Vector Routing (Aodv) Protocol

3.3. Intrusion Detection

Consider a network of wireless nodes, each having an intrusion detection system (IDS) that is responsible for detecting malicious activities within its neighborhood. More importantly, the neighbors spend their valuable computational resources and energy while monitoring node a all the time. However, it may not be required to keep the IDS running on each node all the time. The proposed system attempt to reduce this redundancy, thereby saving the afore-mentioned resources. The assumptions that are made are summarized as follows:

1. Each node is equipped with an IDS component.
2. The IDS monitors the traffic of its neighbors all the time.

ABE: Attribute Based Encryption –algorithm Least Degree for k

Attribute based encryption (ABE) is a relatively new perception of public key encryption for data-centric security solutions. Traditionally, we view encryption as a way for a user to cipher data to a specific target recipient.

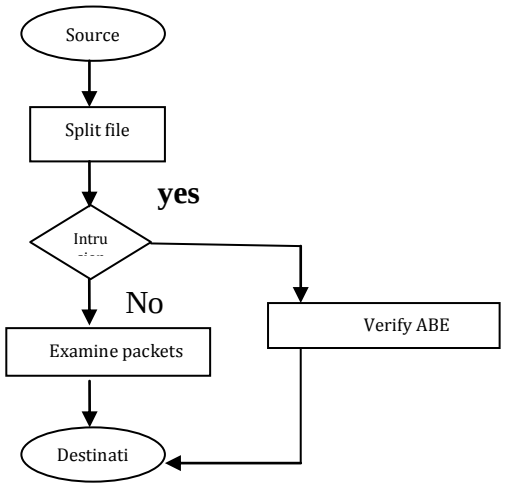


Fig-6: Intrusion Detection

3.4. LDoS Attack

Periodic square-wave of flow is the characteristic of LDoS. In this section, we will indicate that periodic square-wave can bring in more powerful attack ability in the case of multi-targets attack. Then, we will give LDoS attack ability enhance method, LAAEM, which can enhance the attack ability of LDoS significantly in the case of multi-targets attack. 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.

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) and
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 29, 2017 ISSN: 2348-6600
Reference ID: IJCS-296 PAGE NO: 1953-1961

3.4. Performance Evaluation

Throughput

It is defined as the total number of packets delivered over the total simulation time.

Mathematically, it can be defined as:

Throughput=N/1000

Where N is the number of bits received successfully by all destinations.

End to end delay

The average time it takes a data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination.

Mathematically, it can be defined as:

Avg. EED=S/N

Where S is the sum of the time spent to deliver packets for each destination, and N is the number of packets received by the all destination nodes.

Packet delivery ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources.

Mathematically, it can be defined as:

PDR= S1÷ S2

Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source.

3.PERFORMANCE BASED ON GRAPH

In this represents the software puzzle and the multifractal analysis and LDoS attack ability for enhancing method, how to identify the user and how to reduce the burst from the attacker for every (0.5)second. That performance level are following below.

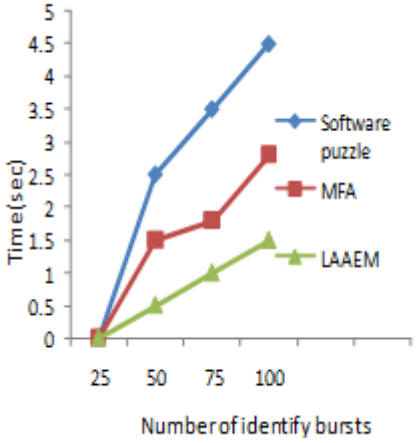


Fig-7: Performance Based On Graph

4. CONCLUSION

In this paper, performance evaluation of LDoS attack by using ABE algorithm based on (LAAEM) method is presented. It aims at the distributed attack detection reduce the time complexity. And also this represents the combination of software puzzle generation method and LDoS attack ability for enhancing method. In the software puzzle scheme is proposed for defeating GPU-inflated DoS attack. It adopts software protection technologies to ensure challenge data confidentiality and code security for an appropriate time period. Hence, it has different security requirement from the conventional cipher which demands long-term confidentiality only, and code protection which focuses on long-term robustness against reverse-engineering only. So much more chances may occur the attacker can easily get the files. So we propose this method LDoS with enhanced attack ability is a great threat

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) and
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 29, 2017 ISSN: 2348-6600
Reference ID: IJCS-296 PAGE NO: 1953-1961

to network security. LDoS has great potential of waveform transform and combination; in the future it may get stronger attack ability. Although there are already many researches on LDoS detection and prevention, in the long run, LDoS will still be a great threat, which still needs us to have deeper research.

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. 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.

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) and
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 29, 2017 ISSN: 2348-6600
Reference ID: IJCS-296 PAGE NO: 1953-1961

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.

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) and
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals