“SURVEY ON DEFEATING DOS ATTACKS IN LOW RATE NETWORKS USING NETWORK MULTIFRACTAL”

1SHRADDHA C. BELSARE
CSIT, HVPM, College of Engineering & Technology, Amravati, India.
shraddhabelsare@gmail.com

2DR. ANJALI B. RAUT
Head, Computer Science & Engineering, HVPM, College of Engineering & Technology, Amravati, India.
anjali_dahake@rediffmail.com

ABSTRACT: Low-rate denial of service (LDoS) attacks send periodic pulse sequences with relative low rate to form aggregation flows at the victim end. LDoS attack flows have the characteristics of low average rate and great concealment. It is hard to detect LDoS attack flows from normal traffic due to low rate property. Network traffic measurement shows that aggregate network traffic is multifractal. In order to characterize and analyze network traffic, researchers have developed concise mathematical models to explore complex multifractal structure. Although the LDoS attack flows are very small, it will inevitably lead to the change of multifractal characteristics of network traffic. The algorithm of multifractal detrended fluctuation analysis (MF-DFA) is used to explore the change in terms of multifractal characteristics over a small scale of network traffic due to LDoS attacks. Through wavelet analysis, the singularity and bursty of network traffic under LDoS attacks are estimated by using Holder exponent. The difference values (D-value) of Holder exponent of network traffic between normal and under LDoS attack situations are calculated. The D-value is used as the basis to determine LDoS attacks. A detection threshold is set based on the statistical results. The presence of LDoS attacks can be confirmed through comparing D-value with detection threshold. Experiments on detection performance have been performed in simulation platform. The extensive experimental results are congruent with the theoretical analysis.

Keywords: Low-rate denial of service (LDoS), multifractal detrended fluctuation analysis (MF-DFA), simulation.

1. INTRODUCTION

The growing popularity of mobile devices has led to the rise of mobile malware. It is also one of the reason why amount of new mobile malware families, which are secretly connected over the internet to a remote command and control server. Through mobile device an attacker can spread classic DENIAL OF SERVICE attacks that are distributed through pcs. Universal Mobile Telecommunications System (UMTS) is a major update to GSM standard which worth it the third generation (3G) epithet. Instead of other GSM updates like GPRS and EDGE, UMTS requires new base station equipments and new frequency band for its operation. In respect to 2G technologies it is characterized by greater spectral efficiency and higher throughput bandwidth ranging from 348kbps of first UMTS release, called R99, to actual 42Mbps of HSPA+. Bandwidth increment is also what drives marketing during early stages of this new technology; great emphasis has been posed by MNOs on services like mobile TV and video calling but their effort has not really been appreciated by end user: in fact, nowadays the main utilization of 3G networks is for plain internet access. UMTS introduction highly affects the radio access portion of the network, the core part.

Users of mobile devices also suffer from various DOS attack. DOS attack which are targeting mobile devices are jamming attack, flooding attack, and blocking attack. Here in our paper the DDOS attack works on single node. In network the DDos attackers are placed are installed in the computers as name zombies. They attack on single node in the network. This single Node provides service to the other node in the network.

The attacker attack on the nodes which provide services and Make the node overload with the message packet. Due to heavy load the node fails to give response to other nodes in the network which sends request. The attacker delays the request of client node in the network. To resist the DDos attack we scan the nodes one by one. But scanning one by one is very time consuming, so we switched toward the DDos attack. In DDOS attack scanning starts with group of node and extra packet is drop and congestion is control. Distributed denial of service (DDoS) attack aimed to remove malicious activity or a typical behavior, which cooperate the availability of the server’s resources and prevents the legitimate users from using the service. DDOS attacks are not meant to alter data contents or achieve illegal access, but in that place they target to crash the servers, generally by temporarily interrupting or suspending the services of a host connected to the Internet. DOS attacks can occur from either a single source or multiple sources. Multiple source DOS attacks are called distributed denial-of-service (DDOS) attacks.
2. SURVEY RELATED DETAILS

Low Denial of Service (LDoS) [1] attack has become a major problem in network services. LDoS attack is a kind of DoS attack, in which more number of packets are sent in a short period of time and it is repeated for several intervals. 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. To prevent LDoS attack, there are two methods exist. One is to maintain throughput of TCP and another is to identify the characteristics of LDoS attacks. Randomizing retransmission Time Out (RTO) of TCP is one method discussed in LDoS.

3. FUNDAMENTALS OF DDOS ATTACK

A Distributed Denial of Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the Denial of Service significantly by harnessing the resources of multiple unwitting accomplice computers which serve as attack platforms. Typically a DDoS master program is installed on one computer using a stolen account. The master program, at a designated time, then communicates to any number of "agent" programs, installed on computers anywhere on the internet. The agents, when they receive the command, initiate the attack. Using client/server technology, the master program can initiate hundreds or even thousands of agent programs within seconds.

4. ARCHITECTURE OF DDOS ATTACK

The Architecture consists of main attacker’s host and three compromised hosts to launch the coordinate attack through the internet by sending a large number of requests through the network. The network of the target server gets busy and then it will not respond to its legitimate users and will not able to provide services to the other actual hosts.

5. PROPOSED WORK

In this approach propose a method by which DDOS attacks can be detected and removed in simless device environments. This approach will be based on a time frame based tracking system, which will check the number of packets arriving in a particular time frame, and then take an action based on the packets and their signature from all the nodes. If the nodes are sending packets in a particular signature, then decide that the particular set of nodes is performing DDOS attack and can remove them from the network. This will help to improve the efficiency of the network, by reducing the overall delay and energy consumption needed to transfer a packet successfully from source to destination.

UMTS security is built on the success of GSM by retaining its strong security features and advantages. Although GSM security has been very successful compared to 1G, one of the purposes of the UMTS security design was to address its original and noticed GSM weaknesses. The following are some of these weaknesses and threat Unidirectional Authentication and Key Agreement (AKA) protocol. Possibility of replay attacks.

- Cipher keys and authentication data are transmitted in clear between and within networks.
- Encryption does not extend far adequate towards the core network and data is transmitted in Clear on the microwave links.
- 2G systems do not have the flexibility to upgrade and enhance security functionality overtime. Therefore, 3G defined the UMTS system to improve security of communication systems. It provides a high level of security in comparison with GSM. It also prepares significant improvements to overcome the vulnerabilities in the 1G and 2G systems. These improvements include mutual authentication, freshness and liveliness assurance of AKA, sufficient and suitable Integrity
Key (IK) and Cipher Key (CK) sizes (128 bits) and data integrity of signaling messages in radio interface.

6. AIMS AND OBJECTIVES

The following are the major aims of carrying out this work.  
1. the most important security mechanisms of the UMTS system are presented.  
2. Most efficient attacks on UMTS system are studied and analyzed.  
3. UMTS attacks are classified based on three major factors and demonstrate authentication is more attractive than others for attack.  
And Objective of this work is as follows:

- To reduced Delay  
- To reduced energy  
- To improved Throughput

7. CONCLUSION

There are number of LDoS detection and prevention algorithms exist to tackle LDoS problem and their performance vary from one algorithm to another. Some methods use per flow analysis and some other methods use partial flow analysis. Some methods can only detect Denial of Service (DoS) attacks based on high bandwidth flows. We believe that all of the algorithms surveyed in this paper are effective, but the advantages favors more time frames based tracking system which is help to improve the efficiency of the network, by reducing the overall delay and energy consumption and get efficient result.

8. REFERENCES


9. AUTHOR PROFILE

Shraddha C. Belsare received the B.E. degree from Sant gadge baba Amravati university in computer engineering. She is currently pursuing M.E. in computer science and information technology from HVPM COET Amravati.

Prof. Anjali B. Raut received the B.E., M.E degree in Computer Science and PHD. Her field of specialization is data Mining. She is currently working as HOD of CSE at H.V.P.M’s college of Engineering and Technology, Amravati.