Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 626 – 633

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

CPU Load Analysis & Minimization for TCP SYN Flood Detection

Deepak Kshirsagar[a,*], Suraj Sawant[a], Amit Rathod[b], Sachin Wathore[c]

[a]*Assistant Professor, College of Engineering Pune(COEP),Pune-411005,India*
[b]*PGP Participant, Indian Institute of Management Indore, Indore-453556, India*
[c]*Member of Technical staff, Vmware Software India Pvt. Ltd, Bangalore-560076, India*

Abstract

Denials of service attacks are well-known as one of the major threats in today's Internet services. Majority VOIP services, DNS servers, online gaming and e-commerce applications are suffering and targeted by hackers using the execution of denial of service attack. Web application attacks and denial of service attacks in distributed architecture is significantly increases day by day. The denial of service attack hampers the load on CPU of web servers during the attack. Therefore, there is a need to minimize the load of CPU after effective attack detection.
This paper proposes and implemented denial of service detection framework which consists of packet sniffer, feature extraction, attack detection and output module. The proposed framework detects denial of service attack such as TCP SYN Flood based on threshold and misuse detection. The system is analyzed with the help of CPU load and the load of CPU is minimized after TCP SYN flood attack detection.

Peer-review under responsibility of the Organizing Committee of CMS 2016

Keywords: Denial of Service (DoS) Attack; CPU Load; Threshold; Misuse Detection; Feature Extraction

1. Introduction

The Internet is suffering from one of the common threat and most traditional Denial of Service (DoS) attack. The volatile growth in the size of internet traffic and complexity of denial of service attacks has posed serious challenges on how to efficiently detect these attacks with appropriate analysis in accurate and scalable manner.

1.1. Current status of DoS attack

Second quarter of 2015, Global Denial of Service Attack Data Report[1] by Arbor Networks Inc. shows that denial of service attack has tremendously increased from both packets per second and bits per second viewpoints. Denial

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.230

of service attack is increased by 21% of attacks and also in average size of attacks. SYN flood is increased by 100GB/sec space which is targeted in the Canada and US during June 2015.

Corresponding author *E-mail address:kdeepak83@gmail.com;ddk.comp@coep.ac.in*

The hackers are changing the strategy, looking for new vulnerabilities and using old, outdated techniques to exploit attacks. Akamai Technologies[2], which provides cloud based application services, shows that denial of service attacks increased by 132% as compared to second quarter of 2014 and in the second quarter of 2015.

The service provider websites are suffered by 45.8% of the denial of service attacks. Hackers uses automated denial of service and bot technology to execute DoS attacks. Denial of service bot related traffic contributed from china is 37.5% out of total 100% taken collectively from other countries[3].

1.2. Denial of Service (DoS) Attack

Intruder, who makes the system unavailable to genuine users, uses these attacks. These attacks result into unavailability of network resources and services to valid end users. These attacks, flood's resources of the network with increased malicious network traffic. The malicious network traffic comprises network packets that consume the bandwidth, CPU load and network buffers. Denial of service attacks are classified[4] into vulnerability and flood attacks based on exploiting weakness as shown in figure 1.

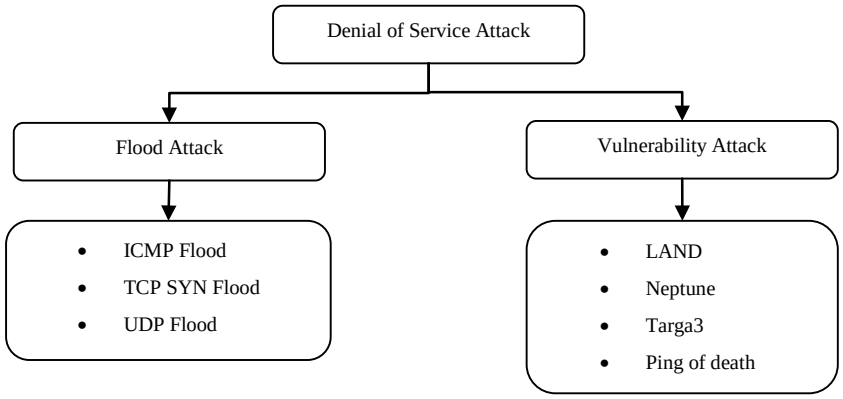

Fig. 1. Classification of DoS Attack[4]

Network based Denial of service attacks are based on exploited weakness classified[4] into Flood and Vulnerability attack. Malicious packets with some network layer protocol create vulnerability attack. Malicious traffic is repeatedly processed by the system and after some time this vulnerable system crashes. Local Area Network Denial (LAND), Neptune, ping of death and targa3 are well unknown vulnerability attacks. Flooding attacks are generated by sending continuous malicious traffic to the servers. This malicious traffic consumes the bandwidth and makes network resources and services unavailable to end users. ICMP, UDP and TCP SYN flood are well-known flooding attacks. This paper mainly focuses on TCP SYN Flood attack.

1.3. TCP SYN Flood Attack

TCP SYN flood attack is well-known for a decade and one of the most common denial of service attacks. Denial of service attack exploits TCP three-way handshake resulting into network resources unavailable to the end users.TCP three-way handshake[5] for normal connection between client and server is as shown in figure 2.

The client send request, SYN message to the server for connection. The sever sends SYN-ACK message to the client for acknowledgement of the request. The client responds with ACK message to the server and establishes the connection.

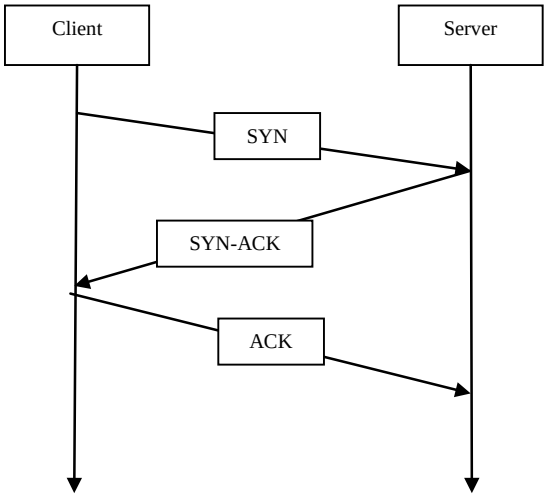

Fig. 2. TCP Three-way Handshake.

The attacker sends continuous flow of TCP SYN packets to the server, but does not ACK message back to the server. Therefore, half open connection is established between client and server. This flood of TCP SYN packets consumes the bandwidth of the server and makes the network resources unavailable to legitimate user. In this way denial of service attack such as TCP SYN flood is executed by exploiting TCP three-way handshake which is as shown in figure 3.

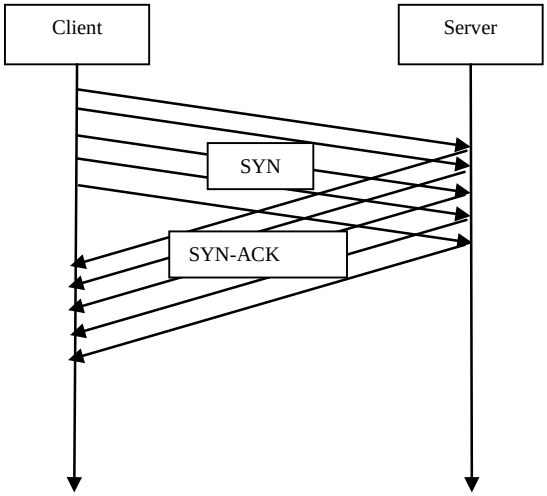

Fig. 3. TCP Three-way Handshake Exploited by Attacker.

1.4. DoS Defense System (DDS) Techniques

Firewall, DDS based defense and application front end hardware defense techniques are used for detection of denial of service attacks. Intrusion Detection Systems and Intrusion Prevention Systems are also used for detection and mitigation of denial of service attacks.

- Intrusion Prevention Systems (IPS)

Intrusion prevention systems are used for prevention for DoS attack before it happens. These systems are also used

to reduce attack attempts and preventing user to avail network services and resources.

- Intrusion Detection Systems (IDS)

Intrusion Detection Systems are used during the attacks, to detect denial of service attack. These systems are used to minimize the impact of attacks. The intrusion detection is done based on misuse or anomaly.

This paper deals with effective detection of DoS attacks based on both threshold mechanism and misuse detection. The proposed system captures network raw traffic with the help of open source tool and necessary features are extracted for rule generation. The main objective of this paper is to reduce the load of CPU after SYN Flood attack.

This work makes the following contributions
1. Minimizes the load of CPU after detection denial of service attack such as TCP SYN Flood and avail the services and resources to the genuine users.
2. The solution provides efficient detection of denial of service attacks based on misuse detection and threshold mechanism.

The reset of the paper is organized in sections as follows. Section 2 presents survey of detection approaches for denial of service attacks. Section 3 provides proposed system architecture for efficient DoS attack detection. Section 4 deals with system implementation. Section 5 describes result analysis and section 6 concludes followed by future scope.

2. Survey of Detection Approaches

This section covers literature survey on detection of denial of service attacks. Three categories of IDS's are identified as follows;

2.1. Host based IDS

A mitigation model[6] is designed and developed for prevention and detection of bandwidth attack such as TCP SYN Flood with spoofed IP addresses. TCP probing is used for prevention of TCP SYN Flood in this model. Initially, packet data recording and learning is done with the help of network monitoring software. This software monitors the captured packets with SYN field and threshold limit is used to detect malicious packet. This host based intrusion detection architecture uses TCP Probing Reply Acknowledgement Packet method for the detection of TCP SYN Flood attacks. The detector detects malicious packet based on TCP probe and recording and learning packet analyzer. TCP probing has computational cost and overhead. This mitigation method is useful only for detection of TCP SYN Flood and unable to detect UDP Flood.

2.2. Network based IDS

Three Counter Algorithm[5] is proposed for detection and mitigation against TCP SYN flooding attacks. This algorithm uses valid SYN-FIN pair behaviour to detect these attacks. This algorithm uses three counting filters to record SYN packets of each connection, other SYN packets and SYN packets, whose three way handshake is completed. The TCP SYN flood attack is mitigated based on 4-tuples as source port, destination port, source IP, and destination IP. The algorithm is evaluated with the help of performance of the detection scheme for TCP SYN flood attacks.
Data mining tool[7] is developed for detection of DoS and brute force password cracking attacks in Ubuntu platform. This tool detects these attacks based on both signature database and anomaly detection using data mining techniques. This tool runs data mining techniques on log file to detect malicious patterns. This tool detects attacks based on the concept of clustering log entries that appears multiple times. This tool initially analyzes and parses the network log files and extracted information added to the body of the file. Clustering algorithm is used to detect denial of service and brute force password cracking attacks with the help of connections appears multiple times. DoS attack is simulated with the help of Ping Flood and also focused on brute force password attacks.

Layered framework approach[8] is used for denial of service attack such as ping floods, UDP flood and SYN flood detection. This system initially trained with Knowledge Discovery and Data Mining (KDD) 1999 dataset and then creates own data set by analyzing real time incoming packets. Real time captured packet data set is compared with previous KDD 1999 dataset trained system and detects DoS attacks. Training set generation and real time layered intrusion detection system are basic modules in proposed system architecture. Again, each module is divided into packet sniffer, packet analyzer, feature extraction and section. Real time layered intrusion detection system module detects denial of service attacks by combining the use of improved k-means clustering algorithm and naive Bayes classification algorithm. Classical evaluation metrics Precision and Recall are used for performance measurement.

2.3. Distributed IDS

Hadoop Based Live DDoS Detection Framework (HADEC)[9] is proposed for detection of flooding attacks. This framework consists of network traffic capturing and log generation, log transfer, DDoS detection and result notification phases. Live network data is captured with the help of an open source library Tshark. Tshark extracts protocol, source IP, timestamps, destination IP and brief packet header information and generates a log file. The traffic handler shares the log file information with a detection server in log transfer phase. In DDoS detection phase, the Map Reduce detection algorithm is used for detection of ICMP, TCP SYN, UDP and HTTP GET flooding attacks. The map Reduce algorithm performs filtering and sorting operations. Detection of attacks done with the help of execution of mapper function and results stored in HDFS. The HADEC is evaluated based on Hadoop cluster size, log file size and threshold for counter based algorithm parameters. The overall performance of the system is measured in terms of total time required for capturing, processing, transferring and detection with various file sizes.
A new form of Distributed Self-Organizing Map (DSOM)[10] is used for effective denial of service attack detection. Each DOSM consist of flow collector, feature extractor and k-means clustering classifier. Flow collector collects packet information as input for SOM. Feature extractor extracts protocol, duration, number of flows, number of packets, number of bytes and growth of client ports features from packet information. K-means clustering algorithm is used for identification of traffic type. DSOM process is executed with the help of steps as initializing, separate operation and weighted sum of SOMs. The system is evaluated with the help of detection accuracy and detection performance is measured in terms of true positive, true negative, false positive and false negative.

3. Proposed System Architecture

The proposed system architecture is classified as follows:

3.1. Packet Sniffing

The network traffic data is captured with the help of open source protocol analyzer. This open source protocol analyzer tool captures the packet s coming from outbound traffic. This system mainly detects denial of service attack such as TCP SYN flood. Therefore, the open source protocol analyzer captures only TCP packets.

3.2. Features Extraction

The captured network traffic contains TCP packet information. The Packet information contains various fields with respect to TCP. The necessary features are extracted from TCP packets and stored in database. These extracted features are as Source port, Source address, Destination address, destination port, protocol. These featured are used for generating rules.

3.3. DoS Attack Detection

Threshold and misuse detection mechanism are combinedly used in the proposed system for the effective detection of DoS attacks. In threshold mechanism, initially count is ensured against the threshold. If the intruder sent numbers of data packets are greater than the threshold in a specified time interval, attack is identified. The features

are extracted from TCP packets which are stored in database. Signatures are developed with the help of the extracted features. These signatures are useful for the effective detection of DoS attacks.
Threshold mechanism and misuse detection is helpful for detection of TCP SYN Flood attacks, which produces high detection rate and minimizes the false alarm rate.

3.4. Output

The output module shows information regarding intruder and adds the information to the database.

4. System Implementation

This section describes experiments carried out for detection of denial of service attacks.

4.1. TCP SYN Flood Attack

TCP SYN flood attack is created with the help of hping tool in Linux. The numbers of malicious TCP packets are generated by hping tool for web server.

4.2. Packet Sniffing and Feature Extraction

The outbound network traffic is captured with the help of open source protocol analyzer Wireshark for UNIX. Open source protocol analyzer Wireshark captures the TCP packet in promiscuous mode over the network. The captured network traffic data contains information regarding TCP packets.

Ellipse in the Figure 4 highlighted with red colour shows TCP packets sent by the intruder which causes denial of service attack such as TCP SYN Flood. The information of packets contains various fields or features such as protocol, source address, source port, destination address, destination port etc

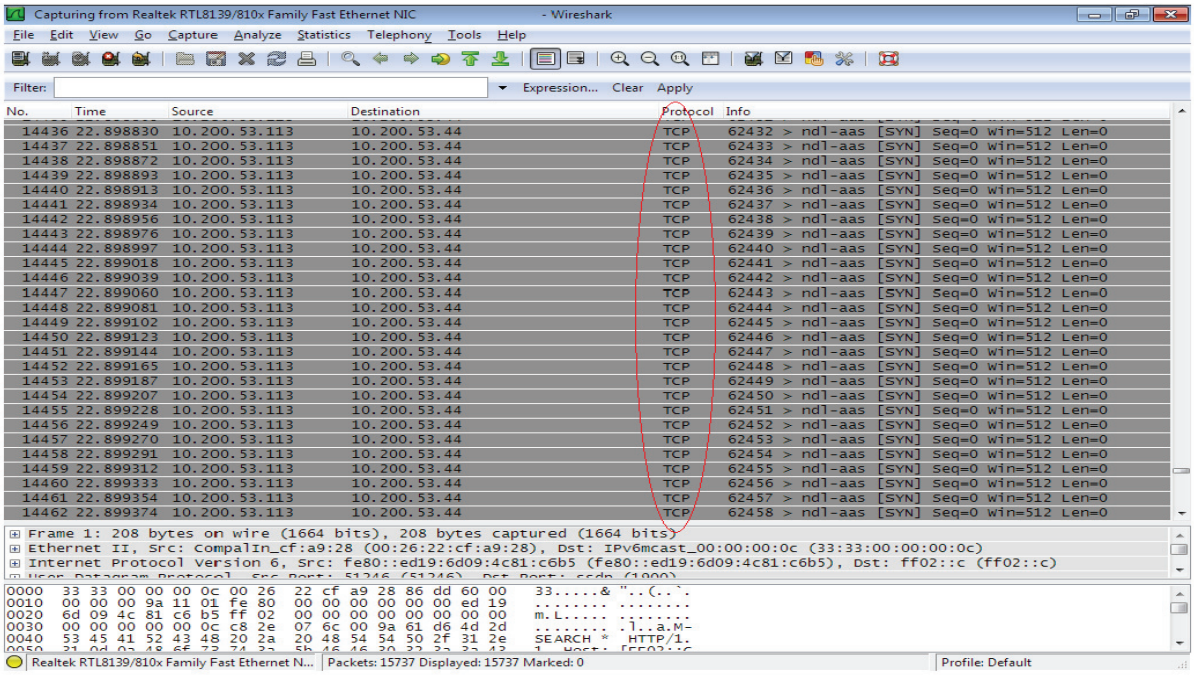

Fig. 4. TCP Packet Sniffing with Open Source Tool Wireshark.

4.3. DoS Attack: TCP SYN Flood Detection

The extracted features are stored in database oracle 10g and rules are developed based on these features. The denial of service attack such as TCP SYN Flood is detected based on threshold mechanism and rules developed from extracted features of TCP protocol.

5. Result Analysis

This section describes experimental results and analysis for the detection of denial of service attacks such as TCP SYN Flood attack.

Table 1 shows comparative study of existing IDS based on various types of IDS and performance of the system as a measurement metric for detection of denial of service attack.

Table 1. Analytical Comparison with State-of-art Existing IDS.

System	*Type of IDS*	*Performance*
A Mitigation Model[6]	*Host based IDS*	*Metric not considered*
Three Counter Algorithm[5]	*Network based IDS*	*Measured in terms of detection scheme*
Data Mining Tool[7]	*Network based IDS*	*Metric not considered*
Layered Architecture[8]	*Network based IDS*	*Precision and Recall metrics used*
DSOM[10]	*Distributed IDS*	*System is evaluated with true positive, true negative, false positive and false negative metrics*
HADEC[9]	*Distributed IDS*	*Performance is measured in terms of total time required for capturing, processing, transferring and detection with various file sizes*
Proposed DoS Attack Detection System	*Network IDS*	*Performance measured in terms of CPU load*

The systems performance is measured in terms of CPU load before attack, during attack and after attack detection. Figure 5 shows CPU load before attack, during attack and after denial of service attack such as TCP SYN flood detection. The observed values of CPU load in percentage ranges from 8-10 for before attack . Also it shows the CPU load during attack which ranges from 95-100%. The value ranges from 8-11% after detection of attacks. Figure 5 summarizes that this system is efficiently detecting TCP SYN Flood attack which minimizes the CPU load after attack detection and is approximately similar to the CPU load before attack.

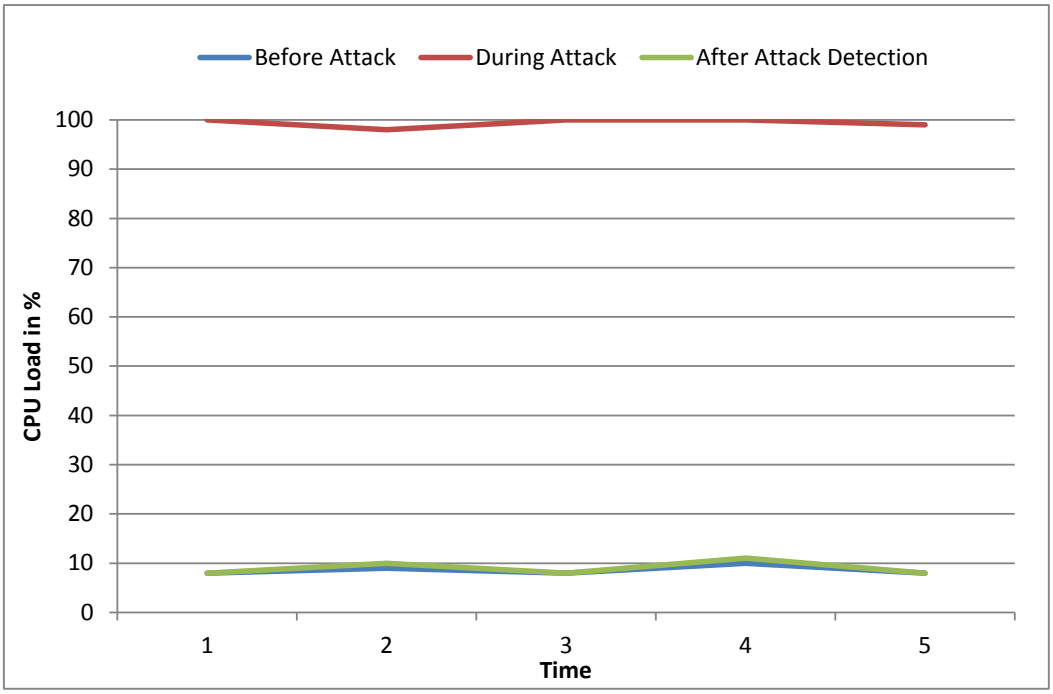

Fig. 5. CPU Load for TCP SYN Flood Attack

6. Conclusion and future work

This paper has proposed and implemented system architecture for efficient detection of denial of service attack such as TCP SYN Flood. The Proposed architecture consists of packet sniffing, feature extraction, DoS attack detection and an output module. The efficient detection of TCP SYN Flood attack is based on threshold and misuse detection. The results show that load of CPU is increased during occurrence of attack and the load of CPU is minimized efficiently after detection of TCP SYN Flood attack.
However, this detection system detects only denial of service attacks such as SYN flooding. The further task is to test the system for different denial of service attacks in distributed architectures.

References

1. Darren Anstee, Denial of service attack data, Arbor Networks Inc.,2015.
2. Andy Meek, DDoS attacks are getting much more powerful and the Pentagon is scrambling for solutions,2015.
3. Joseph Steinberg, Denial of Service Attacks Are Growing Increasingly Problematic: Here's What You Need To Know, 2015.
4. Carl G, Kesidis G, Brooks RR, Rai S. Denial-of-service attack-detection techniques. Internet Computing, IEEE. 2006 Jan;10(1):82-9.
5. Gavaskar S, Surendiran R, Ramaraj DE. Three Counter Defense Mechanism for TCP SYN Flooding Attacks. International Journal of Computer Applications. 2010 Sep;6(6):0975-8887.
6. Kavisankar L, Chellappan C. A Mitigation model for TCP SYN flooding with IP Spoofing. Proceeding of IEEE International Conference on Recent Trends in Information Technology (ICRTIT), 2011, pp. 251-256.
7. Ng J, Joshi D, Banik SM. Applying Data Mining Techniques to Intrusion Detection. Proceeding of IEEE 12th International Conference Information Technology-New Generations, 2015, pp. 800-801.
8. Salunke M, Kabra R, Kumar A. Layered architecture for DoS attack detection system by combine approach of Naive bayes and Improved K-means Clustering Algorithm. 2015.
9. Hameed S, Ali U. On the Efficacy of Live DDoS Detection with Hadoop. arXiv preprint arXiv:1506.08953. 2015.
10. Kim M, Jung S, Park M. A Distributed Self-Organizing Map for DoS attack detection. Proceeding of IEEE Seventh International Conference on Ubiquitous and Future Networks (ICUFN), 2015 2015, pp. 19-22.