A Novel Method for Early Detection of SYN Flooding based DoS attack in Mobile Ad Hoc Network

Dr. Sandip Nemade¹, Prof. Manish Kumar Gurjar², Zareena Jamaluddin³

¹HOD, E&C Department, TIT College, Bhopal. RGTU University, Bhopal, India
²Assistant Professor, E&C Department, TIT College, Bhopal. RGTU University, Bhopal, India
³Student M.Tech, E&C Department, TIT College, Bhopal. RGTU University, Bhopal, India

Abstract—Today Denial of Service (DoS) is the most common method of attack performed by intruders in a network. In areas where resources are constrained, these attacks can have catastrophic effects. Such is the case with Mobile AdHoc Networks (MANET). MANETs are characterized by their limited amount of computing power and memory. SYN flooding is a kind of denial of service (DoS) attack found in MANETs at the transport layer level. In this attack, the attacker tries to overflow the target buffer by sending a large number of SYN packets with spoofed addresses. An adaptive threshold algorithm is commonly used to detect SYN flooding attack in which an alarm is raised whenever the number of SYN packets increases abnormally. Optimization of the algorithm for better results is the major area in adaptive thresholding. This paper aims to develop an optimized adaptive threshold algorithm by optimizing the tuning parameters available.

Keywords—Mobile AdHoc Network, Denial of Service (DoS) attack, spoofing, SYN flooding, Adaptive threshold.

I. INTRODUCTION

The vision of Ubiquitous computing has stimulated much interest in mobile ad hoc networking (MANET) technology. It can turn the dream of getting connected “anywhere at anytime” into reality. In comparison with fixed wireless network, there is no master slave relationship that exists in the MANET. All network activities, such as discovering the topology and delivering data packets, have to be executed by the nodes themselves, either individually or collectively. MANETs are widely deployed in military battlefield, emergency services like search and rescue mission, cooperative mobile communication etc. Now a days they are also widely used in hotels, superstore, offices and airport because they allow easy collaboration and efficient communication on the fly without need for costly infrastructure. In summary, the unique characteristics of MANETs present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. Nodes roaming freely in a hostile environment with relatively poor physical protection pose vulnerability for MANET [1].

II. ATTACKS IN MANET

The security attacks in MANET can be classified in different ways

A. Passive attacks

In a passive attack an unauthorized node monitors and aims to find out information about the network. The attackers do not otherwise need to communicate with the network. Hence they do not disrupt communications or cause any direct damage to the network. However, they can be used to get information for future harmful attacks. Examples of passive attacks are eavesdropping and traffic analysis.

B. Active attacks

These attacks cause unauthorised state changes in the network such as denial of service, modification of packets, and the like. These attacks are generally launched by users or nodes with authorisation to operate within the network. We can classify active attacks into four groups: dropping, modification, fabrication, and timing attacks.

C. Transport layer attacks

The security issues related to transport layer are authentication, securing end-to-end communications through data encryption, handling delays, packet loss and so on. The transport layer protocols in MANET provides end-to-end
connection, reliable packet delivery, flow control, congestion control and clearing of end-to-end connection. Various attacks possible in transport layer are SYN Flooding based DoS attack, Distributed DoS attack, Session Hijacking and TCP ACK storm [2].

1) SYN flooding based DoS attack
It exploits the weakness in TCP specifications. In TCP, a node communicates with a remote node (i.e., a server) by way of a virtual connection established through a process called a 3-way handshake which is illustrated in figure 1(a). When a server receives a SYN packet from a client, the connection is considered to be half-open state for a period of up to the TCP connection timeout, which is typically set to 75 seconds. The server has built in its system memory a backlog queue to maintain all half-open connections. In SYN flooding based DoS attack, an attacker will send a large number of spoofed SYN packets to the victim server. Since the SYN request is spoofed, the victim server will never receive the final ACK packet from the client to complete the 3-way handshake as shown in figure 1(b). Since the backlog queue of victim server is of finite size, flooding of spoofed SYN requests can easily exhaust the victim server’s backlog queue, causing all of new incoming legitimate SYN request to be dropped. In addition to SYN flooding attack, UDP flooding, Smurf attack and ICMP flooding (Ping flooding) also pose a major threat in MANET.

D. Organisation of paper
In Section III, we provide some related works on attack detection and attacker traceback. In section IV, we explain our proposed work early detection of SYN flooding based DoS attack. Experimental result is provided in section V. Section VI summarizes the paper.

III. RELATED WORKS ON ATTACK DETECTION AND Attacker Traceback
During SYN flooding based DoS attack, the normal behaviour of the network is affected seriously. Thus, during the attack, traffic volume increases abnormally, network status like packet delay, dropping rate, etc also increases due to congestion in the network. Rajesh et al. [3] proposes a method to detect the attack based on network status such as packet delay, dropping rate etc. Shin et al. [4] proposes a method which monitors the number of SYN packets and the change in the ratio of SYN packets to other type TCP packets. Through their experiments, Ohista et al. [5] claims that the distribution of SYN packet rate of normal traffic can be modelled by the normal distribution. But the SYN packet rate distribution of DoS attack traffic deviates far from a normal distribution.

To perform efficient DoS/DDoS attacker traceback in highly constrained MANET environment, several traceback schemes are developed. Zone Sampling Based attacker Traceback (ZSBT) [6] proposed by Xin Jin et al. is an extended version of probabilistic packet marking (PPM) [7] approach particularly deployed in the MANET environment. In this method, when a node forwards a packet, the node writes its zone ID into the packet with a probability. After receiving these packets, the victim can reconstruct the path between the attacker and itself. Kim and Helmy have proposed a small world-based attacker traceback (SWAT) [8] approach to trace DoS attacker in MANET. They use traffic pattern matching (TPM) and traffic volume matching (TVM) as matching-in-depth techniques to traceback DoS attackers. Later, an improved traceback protocol developed by the same team called ATTENTION [9] which uses MAC layer abnormality for tracing the attacker.
IV. Optimised Algorithm for Early Detection of SYN Flooding Based DOS Attack

DoS attack detection applications are commonly based on anomaly detection models, where the behaviour of a measurable network characteristic is compared to its normal behaviour, and an alarm is raised when a significant deviation from normal behaviour is detected. We are using an optimised version of the adaptive threshold algorithm. If the number of packets increases the threshold level, then an alarm is raised. We used SYN Arrival Rate (SAR) as the measuring parameter for the early detection of SYN flooding attack. In order to account for seasonal (daily and weekly) variations and trends, the value of the threshold is set adaptively based on an estimate of the mean number of SAR, which is computed from recent traffic measurements. If $x_n$ is the SAR in the $n$th time interval, and $\mu_{n-1}$ is the mean SAR estimated from measurements prior to $n$, then the alarm condition is given by:

$$x_n \geq (\alpha+1) \mu_{n-1}$$

Then alarm is signalled at time $n$. Here, $\alpha \geq 0$ is a parameter, this indicates the percentage above the mean value that we consider to be an indication of an anomalous behaviour. The mean SAR $\mu_n$, can be computed over some past time window or by using an exponentially weighted moving average (EWMA) of previous measurements.

Mean SAR, $\mu_n = \beta \mu_{n-1} + (1-\beta) x_n$, where $\beta$ is the EWMA factor.

Direct application of the above algorithm would yield a high number of false alarms (false positives). A simple modification that can improve its performance is to signal an alarm after a minimum number of consecutive violations of the threshold, say $k$. The changeable parameter of the above algorithm are the threshold factor for calculating the successive threshold, the number of successive threshold violations $k$ before signalling an alarm, the EWMA factor $\beta$, and the length of the time interval over which SYN packets are diagnosed. Since the exponential weighted moving average plays an important role in setting the adaptive threshold, tuning of the EWMA factor is very much important. Experimentally, we got $\alpha = 0.2$ and $\beta = 0.88$ which reduces the number of false alarms. The pseudo code for the detection of SYN flooding based DoS attack is illustrated in Algorithm 1.

V. Experimental Results

For detecting SYN flooding based DoS attack, we will classify the incoming packets as TCP, UDP and ICMP packets based on the protocol field in IP header (For ICMP packets protocol field is 1, for TCP packets protocol field is 6 and for UDP packets protocol field is 11 (hex)). Since we are interested in detecting SYN flooding based DoS attack, we will deal with TCP packets only. So incoming TCP packets are classified into TCP control segments and TCP data segments using offset field and total length field in IP header. TCP
control segments are again classified into TCP SYN, FIN and RST packets based on TCP flag bits in TCP header. Then, we will calculate the SYN Arrival Rate (SAR) which is defined as the ratio of incoming SYN segment to total number of incoming TCP segments. We verified the above attack detection algorithm by conducting experiments in the lab. The experiment is conducted for studying the SYN Arrival Rate (SAR) for the normal traffic in our lab. For finding SAR for the normal traffic, we conducted the experiment for 20 days capturing around 5000 packets per day. That is, 10 samples are taken per day capturing 500 packets per sample. Typical arrangement for conducting the experiments is shown in figure 2.

Even though tcpdump can be used for the analysis of TCP traffic in the network, we developed a packet capture program written in C language for our convenience. After studying the SYN Arrival Rate (SAR) for normal traffic, we injected attack traffic on day 21 using a tool called Hping3. We conducted SYN flooding attack as well as ICMP flooding attack using Hping3 tool. We took 200 samples of the attack traffic capturing 500 packets per sample for the convenience of comparison. SAR is compared for normal traffic and traffic in presence of flooding attack which is as shown in figure 3.

A typical screen shot of the experiment conducted in our lab is as shown in figure 4. The SAR for normal traffic was around 0.06.

SYN flooding attack is done using Hping3 at the rate 100 SYN packets per second. It is observed that, in the presence of attack, SAR is around 0.98. Now, mean SAR is computed using exponential weighted moving average (EWMA). By using Adaptive Threshold Algorithm, any anomaly in mean SAR is identified.

Observations
Mean SAR for normal traffic: 0.06
Mean SAR for normal traffic: 0.98
VI. CONCLUSION

In this paper, we proposed a novel method for early detection of SYN flooding based DoS attack using adaptive thresholding. SYN flooding based DoS is a major problem in MANET due to its limited resource constraints. Detection of flooding attack is to be made as early as possible in order to perform preventive measures to avoid more damage in the network. Adaptive thresholding enables us to consider the seasonal variations in SAR in the network. By tuning the parameters like $\alpha$ and $\beta$, early detection of SYN flooding attack can be made with lower false alarm. In our experiments, we got $\alpha = 0.2$ and $\beta = 0.88$.

REFERENCES


