ISSN:0975-9646

SYN Flooding Attacks in Mobile Adhoc Networks

K.Geetha
Department of Computer Science
Periyar Arts College, Cuddalore, India

Abstract**—*****Mobile Adhoc Networks (MANET) are special because of their self configuring and self maintenance capabilities. The highly dynamic network topology and the shared wireless medium are the main attractions and at the same time the main challenges of the MANET. These characters make MANET vulnerable to various attacks. There are several attacks on each layer of the protocol stack. Providing the security solution to these attacks is a challenging task due to the dynamically changing topology of the network. The main parameters of network are being affected by these attacks. In this paper we study the performance of the network with one type of the attack called SYN flooding attack and its effect on the specific Quality of Service (QOS) parameters. Two well known routing protocols are taken for analysis***

Keywords— ***MANET, SYN Flooding attacks, QOS parameters***

I. INTRODUCTION

MANET, the emergency network is organizing itself, and this dynamic network topology makes MANET, a victim of various security threats and attacks. Security attacks are common in every layer. A lot of solutions are being suggested to these attacks. Multi layer attacks get more attention by the researchers. One of the multilayer attacks is SYN flooding attack. This attack mainly considers the transport layer of the attack. In this paper the TCP SYN Flooding attacks is analyzed. This paper is organized as follows. The section 2 analyses the various attacks. In section 3 the TCP communication is discussed. The section 4 describes the SYN flooding attacks and its impact on the MANET. Section 5 discusses the routing protocols taken for our study. In Section 6 the implementation of the attack is carried out and a study is performed on various parameters. The section 6 provides conclusion.

II. ATTACKS

There are a lot of security attacks in each layers of network. In wired networks, well defined routers are available, In MANETS the intermediate nodes act as routers, because of this, the network user and the malicious attacker can access each and every node unlike wired network. The table 1 gives a clear picture of the functions and security issues on the major layers of the network

The SYN Flooding attack is a multilayer attack which may occur in any layer. We describe the TCP SYN Flooding attack which occurs by exploiting the TCP's three way handshake in the transport layer

TABLE 1. SECURITY ISSUES OF LAYERS

Layer	**Functions and Security Issues**
Application layer	Functions: Commonly needed functions by the user like e-mail, remote access, Inter process communications etc. Security issues: Security should be provided to handle attacks using viruses, malicious codes
Transport layer	Functions: End to End communication, message segmentation, message acknowledgement etc. Security issues: Protection against attacks on the authentication and end-end communication
Network layer	Functions: The functions include controlling the operations of the network, routing etc. Security issues: Protection for attacks against the Routing and forwarding protocols
Data link layer	Functions: Error free transmission. Security issues: Providing security against attacking over the MAC protocol
Physical layer	Functions: Transmission and reception of raw bit stream, Describing the transmission medium etc. Security issues: against Signal jamming attacks

III. TCP THREE WAY HANDSHAKE

Initially the server will be in the listen state. The client will send a SYN to the server. The server will acknowledge the client by sending the SYN ACK. This state is half open state. The server maintains the information regarding the client communicated in a buffer along with other information

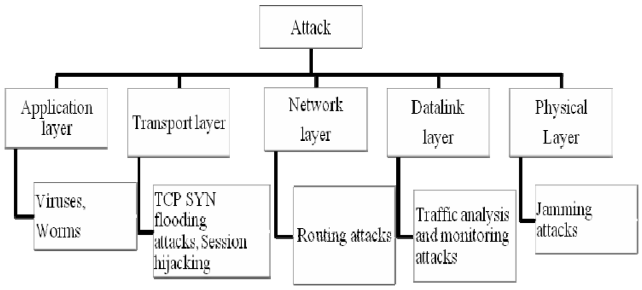


Figure 1 Different types of attack

This SYN ACK is acknowledged by a final acknowledgement from the client by means of sending an ACK back to the server. The connection is established now. This is called a three way handshake of Transmission control protocol as explained in the figure 2. Connection is established only after receiving the final acknowledgement from the client

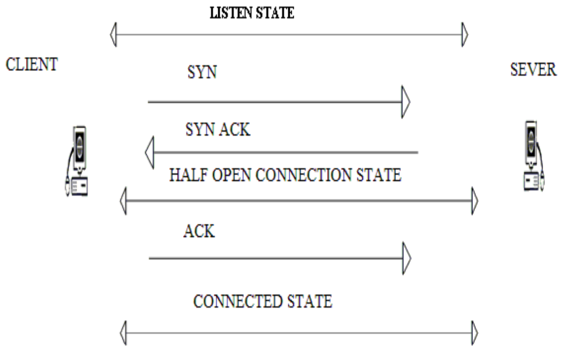


Figure 2 TCP Three way Handshake

IV. SYN FLOODING ATTACKS

When the malicious node sends SYN by spoofing the ip address of the client, the server responds to it by a SYN ACK. The malicious node will not respond to it by the final acknowledgement. As the client's address is spoofed the client also does not respond by a final ACK. The connection remains half open. The malicious node sends a lot of SYNs and the server acknowledges to it .The server starts maintaining information in the buffer. At one point the buffer becomes full; all the resources of the client are occupied. The server cannot consider the further legitimate requests. This type of attacks is also known as Denial of Service (DOS) attacks. The SYN Flood attack scenario is as shown in the figure 3.

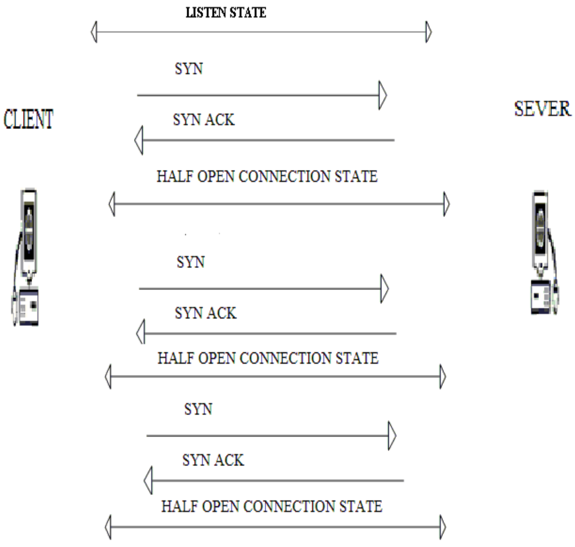

LISTEN STATE
SYN
CLIENT
SYN ACK
SEVER
HALF OPEN CONNECTION STATE
SYN
SYN ACK
HALF OPEN CONNECTION STATE
SYN
SYN ACK
HALF OPEN CONNECTION STATE

Figure 3 SYN Flooding Attack Scenario

The following conditions hold in a SYN Flood attack situation as shown in the figure 4.

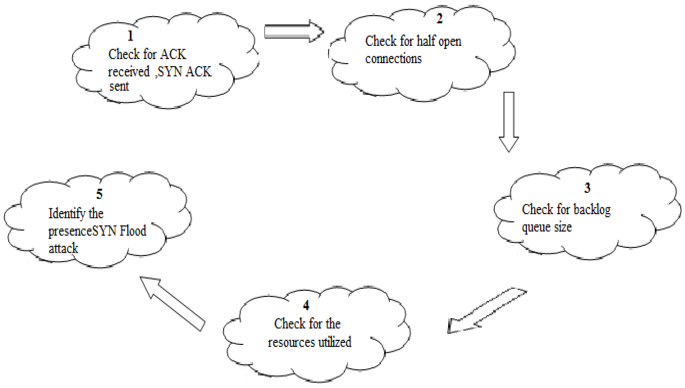

1
Check for ACK received ,SYN ACK sent
2
Check for half open connections
3
Check for backlog queue size
4
Check for the resources utilized
5
Identify the presenceSYN Flood attack

Figure 4 identifying the presence of SYN Flood attack

V. PROTOCOLS USED FOR THE STUDY

In MANETs two types of protocols predominantly exist from the beginning. One is Proactive Routing protocols or otherwise known as table driven routing protocols. The information regarding the routes is maintained in a table. These protocols are not suited to highly dynamic environment as they require periodic updating and increased control overhead. The second one is Reactive routing protocols or source initiated protocols where the route is created only when the source requests for a route to destination. Packets are flooded from the source to destination by flooding the packets to the next neighbour. Two phases are there while forming the route: route discovery phase and route maintenance phase.Another type of protocol existing is a hybrid protocol; It combines the aspects of table driven and reactive routing protocols. The general concept is that hybrid protocols behave as proactive protocol where the changes are not frequent. The behaviour of reactive routing protocol is adapted during high mobility..

A) Optimum Link State Routing (OLSR)

The OLSR protocol is designed by clause et.al (3), it uses the a Multi Point Relay technique (MPR) which is shown in the figure 5. MPRs forward messages and link state information is maintained by MPRs only. The multipoint relay tries to reduce retransmissions within the same area. Each node selects a set of multipoint relays (MPR) for the node. The neighbours of the node can only process the packets and they cannot forward them. The multipoint relay set must be chosen such that its range covers all the two-hop neighbours. A route is a sequence of hops from a source to a destination through multipoint relays within the network. The source does not know the complete routes. They have the information of next hop to forward the messages

B) Fish eye state protocol(FSR)

Pei et.al (2) proposed the FSR protocol. It behaves like a Fish eye. This technique means that, the node maintains accurate distance and the quality of the path about its immediate neighbors. But the information decreases with distance. Higher level updates are provided for neighbors with 1 to 2 hops whereas the updates are fewer for faraway nodes.

When the size of the network grows, the updation of the messages consumes considerable bandwidth. As in the figure 6 the scope defines the set of nodes that can be reached with in a given number of hop, Nodes corresponding to the small scope are receiving messages with high frequency. In the figure 6, three scopes are maintained as scope 1 with one hop neighbours, scope 2 with two hop neighbours and scope greater than 2 for the other nodes.

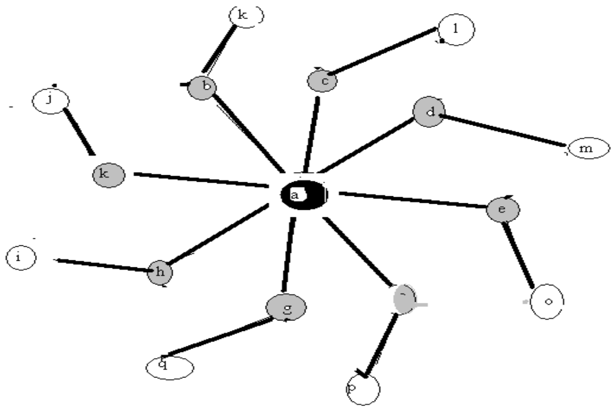


Fig 5 Multipoint Relay Technique of OLSR

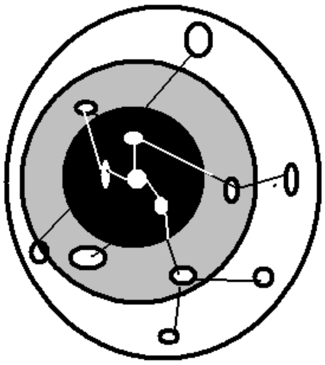


Fig 6 Fish Eye State Routing Protocol - Scope of Fish eye

VI Simulation And Analysis

A simulation is carried out using NS-2, with the following parameters. Multimedia message is taken for analyzing the various parameters. The parameters taken for analysis are Packet delivery Ratio, Delay, Jitter, Control Over head, and throughput. The SYN packets received, the SYN acknowledgements sent and the acknowledgements received in turn are analyzed to confirm the presence of SYN Flood attack.

Table 2 Simulation Parameters

Number of Nodes	150
Simulation Area	1000mX1000m
Buffer Size (Queue Length)	50 Pkts
Packet size	1024 Bytes
Application Traffic	Video traffic
Simulation Time	200 Sec
Number of Connections	150
Routing Protocols	OLSR,FSR

The number of SYN Packets received is normal and very less if the network is without attacker. With SYN Flood attacks the SYN packets increases as the malicious node sends a lot of SYNs. The following figure 7 and figure 8 show the graph.

The Number of SYN ACK packets sent by the server for the SYN packets received as per the fig 7 and figure 8 is given figure 9 and figure 10. 100% of SYN ACKs are sent from the server for the SYN messages received.

The number of final acknowledgements received by the server at time unit t is given in the figures 11 and 12. Without the existence of attack the ACKs received at every interval is high whereas, with attacks the ACKs received are very low indicating the presence of half open connections.

A. QOS PARAMETERS

a) Packet Delivery Ratio: The Packet Delivery Ratio is the number of packets delivered successfully to the destination. In OLSR Protocol without attacks 100% of the packets are delivered successfully. In FSR protocol a maximum of 80% of packets are delivered. After the attack, the PDR reduces to 63% in case of OLSR and 57% in the case of FSR. Due to MPR technique the OLSR performs better than FSR. The packet Delivery Ratio are given in the Fig 13 and Fig 14 for OLSR and FSR protocol

b) Control Overhead: The Control Overhead is the number of control packets used for sending the messages to destination. It is measured in bits /sec. The lesser overhead involved increases the performance. As the control overhead increases the performance of the protocol decreases. Generally the hybrid protocols involve lesser overhead as in the case of FSR protocols which is given in the figure 15 and 16. The OLSR protocol involves higher control overhead with attack. Before the attack, both the protocols behave similarly

c) Delay: Delay is the time involved in sending the message from source to destination. Without attacks the delay for OLSR protocol is very less compared to the FSR protocol. At times when the node is at distance the delay increases in FSR. After attack, the delay in OLSR protocol increases which is given in the figure 17 and figure 18.

d) Throughput: Number of bits transmitted successfully per unit of time is called throuput. The throughput for OLSR and FSR protocols reaches maximum without attacks. After the attack the throughput decreases for both the protocols as shown in the figure 19 and figure 20 and even reaches zero at some time.

e) Jitter: Jitter is the delay between adjacent packets. For multimedia message transfer, the jitter must be very low to achieve quality. It is expressed in seconds. It is very low before attack in OLSR protocol. With FSR protocol, the delay is high compared to OLSR protocol before and after attack. So, the jitter is also increased after attack. These are shown in the figures 21 and 22.

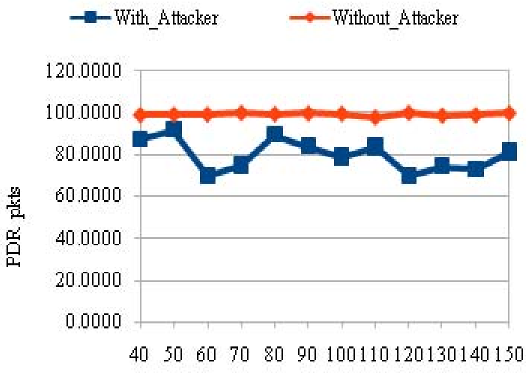


Figure 13 PDR with OLSR protocol

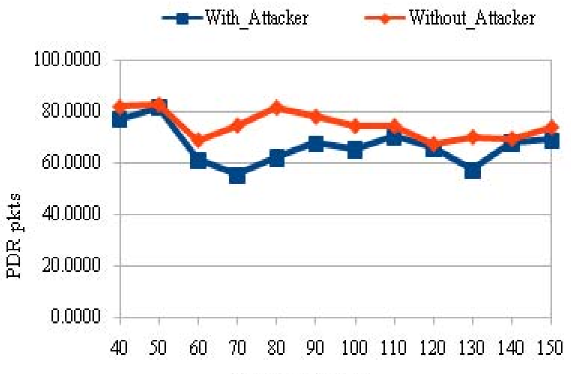


Figure 14 PDR with FSR protocol

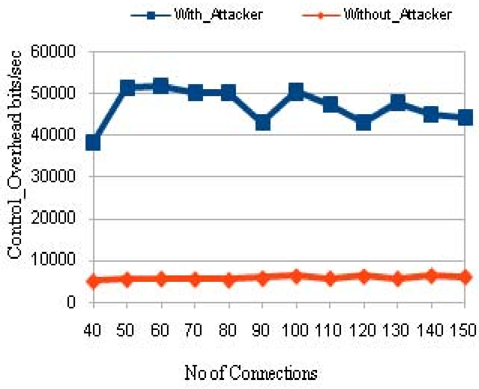


Figure 15 Control Overhead with OLSR Protocol

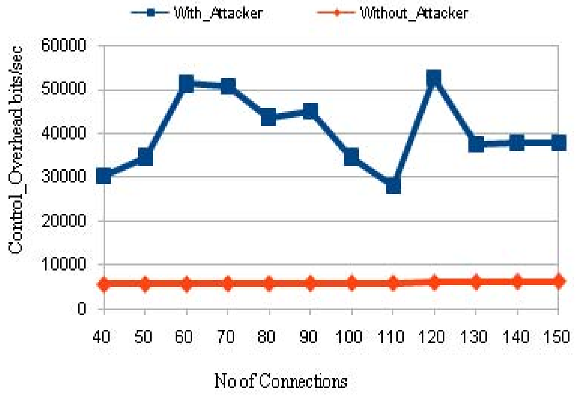


Figure 16 Control Overhead with FSR Protocol

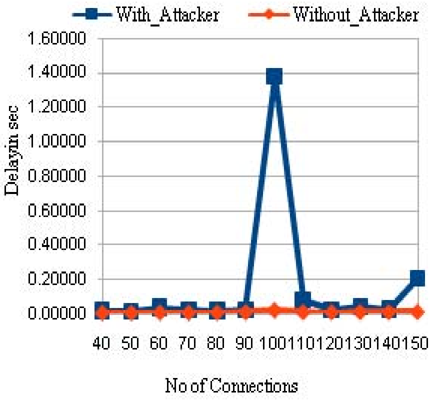


Figure 17 Delay with OLSR Protocol

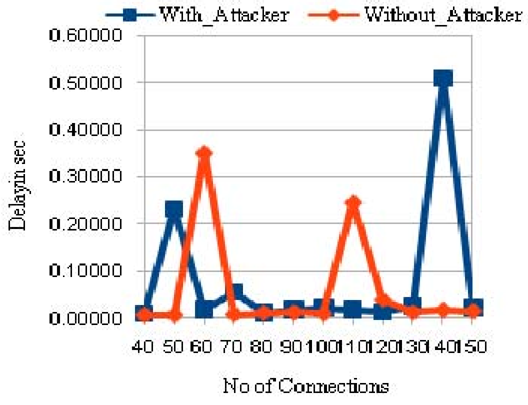


Figure 18 Delay with FSR Protocol

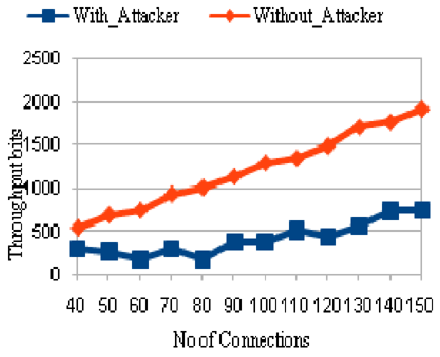


Figure 19 Throughput with OLSR Prtotocol

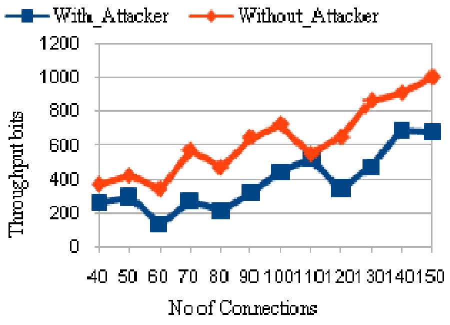


Figure 20 Throughput with FSR Protocol

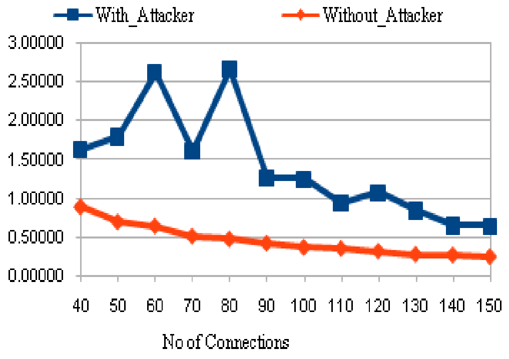
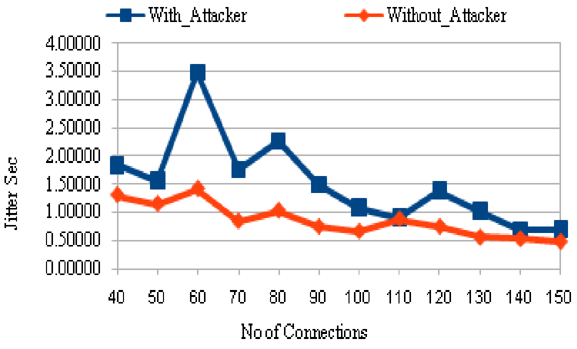


Figure 21 Jitter with OLSR Protocol



Figue 22 Jitter with FSR Protocol

VII CONCLUSION

The objective of this analysis was to provide a detailed study on the SYN Flooding attacks. This paper provides information on

- attacks of each layer
- TCP SYN Flooding attacks
- the scenario of the attack
- conditions for the attack occurrence
- OLSR,FSR protocols
- Impact of the attack on the selected QOS Parameter

The SYN Flooding attack is analyzed here with OLSR and FSR protocol. This paper gives a clear view on the SYN Flood attacks. The network performance is analyzed with OLSR and FSR protocols for the necessary conditions of the SYN Flood attack to occur like SYNs received by the server, SYN ACKs sent by the server and ACKs received by the server. The QOS parameters are analyzed before and after attack. The analysis is carried out before the attack occurrence and after implementing the attack statically. In future, detection may be carried out dynamically as the attack occurs in the MANET.

REFERENCES

[1] Monika Sachdeva, Gurvinder Singh, Krishan Kumar, and Kuldip Singh "DDoS Incidents and their Impact: A Review" The International Arab Journal of Information Technology,14-20, Vol. 7, No. 1, January 2010

[2] G. Pei, M. Gerla, T.-W. Chen, Fisheye state routing in mobile ad hoc networks, in: Proceedings of IEEE ICDCS Workshop on Wireless Networks and Mobile Computing, pp. D71–D78, April 2000.

[3] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum, L.Viennot, Optimized link state routing protocol for ad hoc networks, in Proceedings of IEEE INMIC, pp. 62–68 December 2001,

[4] Azzedine Boukerche, Begumhan Turgut, Nevin Aydin, Mohammad Z. Ahmad,,Ladislau Bölöni, Damla Turgut "Routing protocols in Adhoc Networks – A Survey" Computer Networks 2011

[5] Denial Of Service Attacks in Wireless sensor Networks" Journal of Information & Information Networking and Applications-Workshops, 2008. AINAW 2008. 22nd International Conference on. IEEE, 2008

[6] Chen, Wei, and Dit-Yan Yeung. "Defending against TCP SYN flooding attacks under different types of IP spoofing." Networking, International Conference on Mobile Communications and Learning Technologies, 2006. IEEE, 2006.

[7] Kim, Tae-Hyung, et al. "Annulling SYN flooding attacks with whitelist." Advanced Information Networking and Applications-Workshops, 2008. AINAW 2008. 22nd International Conference on. IEEE, 2008.

[8] Mehdi Ebady Manna and Angela Amphawan " Review of SYN Flooding attack detection mechanism" International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012

[9] C. Siva Ram Murthy & B.S. Manoj, Ad-hoc Wireless networks, Pearson Edition

[10] S. R. Das, C. E. Perkins, E. M. Royer and M. K. Marina," Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks," in IEEE Personal Communications magazine, special issue on Mobile Ad Hoc Networks, Vol. 8, No. 1, pp. 16-29, Feb 2001

[11] The Network Simulator, NS-2, from www.isi.edu/nsnam/ns, 2006

[12] Boukerche, Azzedine, et al. "Routing protocols in ad hoc networks: A survey."*Computer Networks* 55.13 (2011): 3032-3080."

[13] Wu, Bing, et al. "A survey of attacks and countermeasures in mobile ad hoc networks." *Wireless Network Security*. Springer US, 2007. 103-135.

[14] K.Geetha N.Sreenath "A general study on the multimedia message transfer"IJCA volume 81 number 9November 2013