A REVIEW ON SYN FLOODING ATTACK COUNTER MEASURES IN MOBILE AD-HOC NETWORK

Jasvir Markandy †, Manmohan Sharma ‡
† Research Scholar, Lovely Professional University, Phagwara, Punjab.
‡ Assistant Professor, Lovely Professional University, Phagwara, Punjab.
E-mail: † jasvirmarkandy@gmail.com, ‡ manmohan_er@yahoo.co.in

ABSTRACT: A mobile ad-hoc network (MANET) use less infrastructure and consist number of nodes for interfacing the wireless sensor network. In mobile ad-hoc network every node is transmitters which give data to routers. Routers work as a sink. MANET shows the dynamic topology because it depends on coverage area of nodes which one connected to other or not. If consider the security, MANET is also a soft target but effective attack on MANET is SYN flooding .This paper presents review of several security methods used for diminishing SYN Flooding attacks in MANET.

Keywords: MANET, Dynamic topology, Adhoc security, Attack, SYN flooding

I. INTRODUCTION

Mobile ad-hoc network is a dynamic network with a collection of mobile nodes. In MANET, all the nodes behave like router because of dynamic nature of the mobile nodes. It works on the shared medium called as radio communication. MANET supports the feature of mobility in the network. Every node in MANET is behave like a Relay and cooperates with other nodes. Autonomous feature of MANET give the right to every node to act like a router of a node [1].

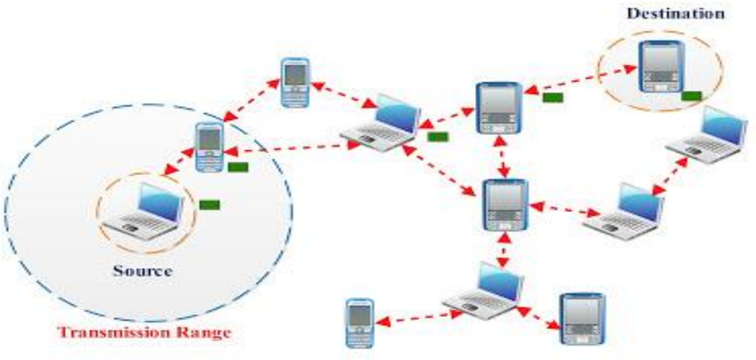


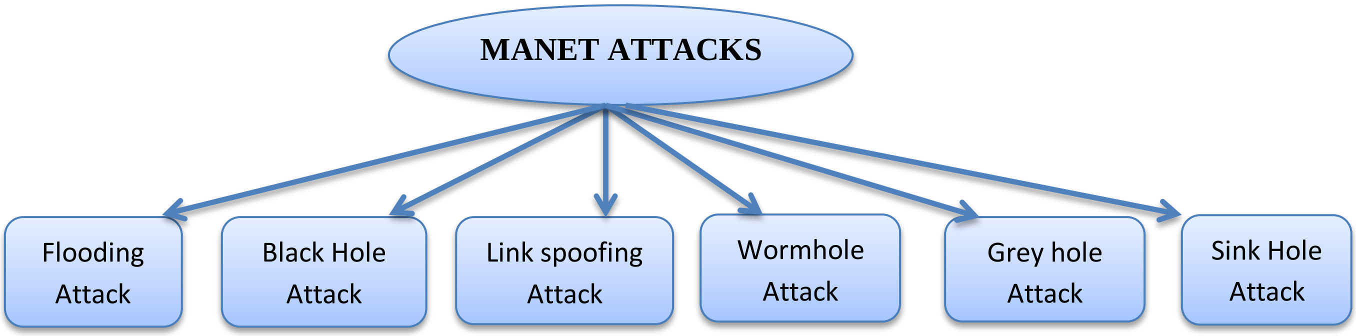
Figure 1.1 Architecture of MANET

Figure 1.1 shows the Architecture of MANET in which mobile devices are connected to each other by wireless links. In this figure range of the node is define its wireless network area. It shows the data transfer between the sources nodes to the destination node using mobile ad-hoc network.

II. ATTACKS IN MANET

MANET is used in various fields for the effective communication process in which user send their information from one node to another node. Sometimes user sends the secret information data on the wireless network, it is very important to send this information very safely. In this network sensor nodes used wireless communication and it is easy to eavesdrop. Attacker can easily inject malicious message into the network.

Following are the types of Attacks in MANET



(a) Black Hole Attack: In this type of attack, attacker supposed to communicate packets in the network rather than discard the packets. The reason behind this attack is that a node is compromised from different number of causes. In this attack, packets are dropped from the loss network. It is not easy to detect this type of attacks [3].

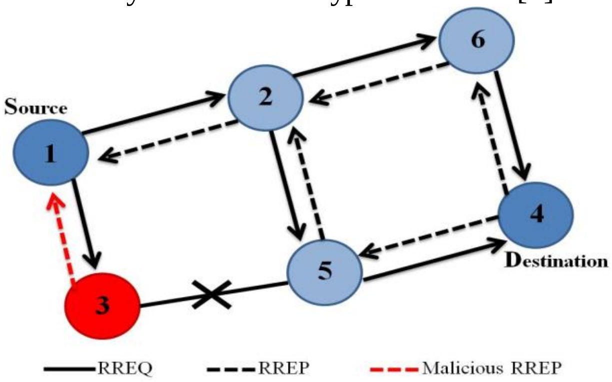


Figure 1.2 Black Hole Attack

(b) Link Spoofing Attack: In this attack a fake link is displayed with the neighboring node which disturbs the routing process with the other nodes. Malicious code is sent over this link and it drops the data packets. This type of attack can be detected by OLSR protocol because it determined the node which sends the malicious code. In this types of attack message is completely lost [3].

(c) Wormhole Attack: In wormhole attack, the attacker can record the data packets at one location in the network and retransmit the data from another route of the data. Wormhole attack is a serious issue that occurred into the wireless sensor network. In the figure [1.3] the tunnel may be a wired link or wireless link between two nodes, this creates an illusion that the end point are very close to each other [2].

A wormhole attack has two modes.

1. Hidden mode
2. Participation mode

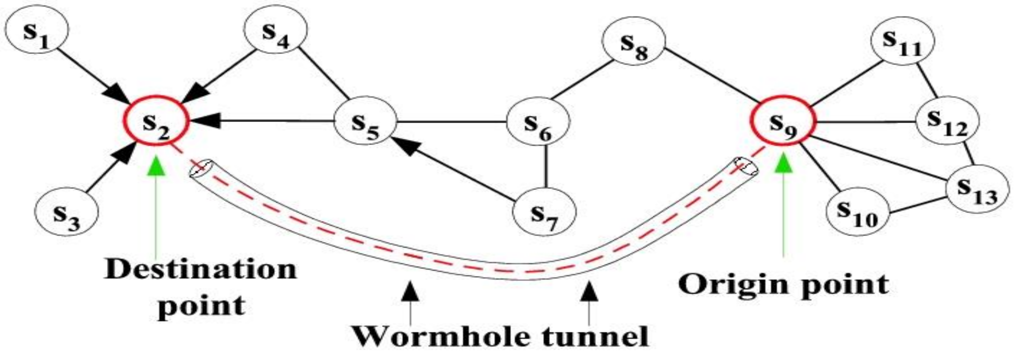


Figure 1.3 Wormhole Attack

(d) Grey Hole Attack: This attack is modification of black hole attack. In this attack attacker node behaves like a normal node for discovering route in the network. After it discovers the route then it drop the infected packets in network. This attack is difficult to detect because packet is dropped with certainty [4].

(e) Sink Hole Attack: In this attack incorrect information of the routing is send to the nodes as it is low cost and it provides proper destination node. Due to incorrect routing information it leads to packet loss and manipulation in original data packets. This attack

disturbs all the network process because nodes are sometime dependent on each other for information [4].

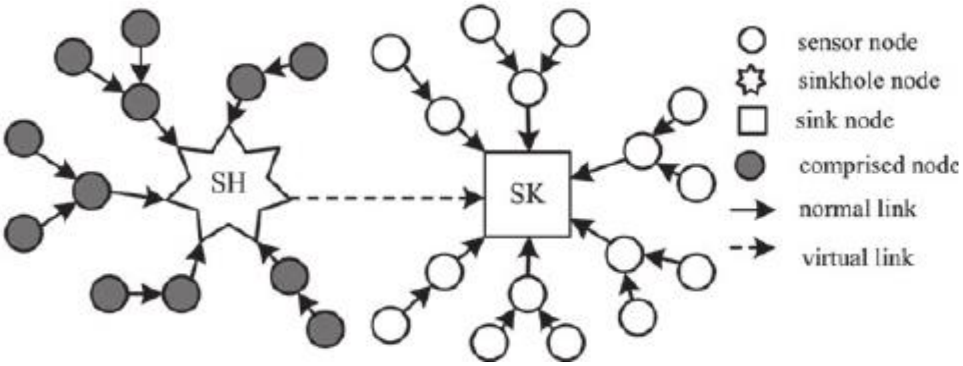


Figure 1.4 Sinkhole Attack

III. SYN FLOODING ATTACK IN MANET

In SYN Flooding attack, attacker sends a large amount of synchronization packet to the destination nodes and these nodes consumes a lot of memory. After getting the IP of the spoofed client the attacker behaves like original client node and starts sending SYN message to the server and server send SYN ACK in reply to the malicious node. By doing this again and again server makes a half open connection with the malicious node. Server sends continuous SYN ACK to the malicious client and updated the repeated information in its buffer. When the buffer is full server is not able to send the reply to other clients and it deny the entire session [11].

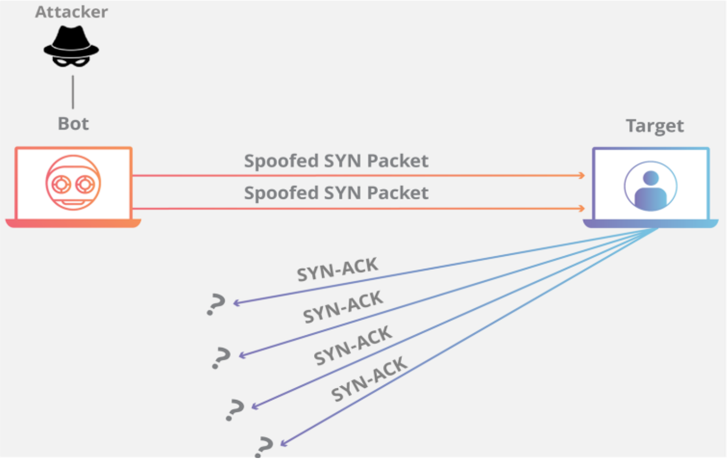


Figure 1.4 SYN- Flooding Attack

IV. COUNTER MEASURES FOR SYN FLOODING ATTACK

A. Ad-Hoc On Demand Distance Vector

Moudni, Houda, et al. worked on the flooding attack, black hole attack and rushing attack in MANET. In this paper, the author used AODV routing protocol to analyze the impact on the network. In previous research only one or two parameters are used but in this paper author analyze packet delivery ratio, throughput and end to end delay for evaluation. The results show that black hole attack effects more than flooding attack [5].

Geetha, K., et al. proposed a method of SYN attack detection and prevention in their work. This attack is not easy to detect in early stage due to the dynamic nature of the MANET. The proposed algorithm is used to detect this type of attacks in early stages. In this attack malicious node affects the communication process in attack. This method identifies the nodes which affects the communication by unwanted delays. Game theory is used between the multimedia server node and malicious node. Performance evaluation is done by checking quality of service of the network [6].

B. Trust Based Routing Mechanism

Tan, Shuaishuai et al proposed optimized link state routing mechanism to solve the issues of attacks in the wireless sensor networks. In this protocol trust based mechanism is used with fuzzy rules to evaluate the trust values of the mobile nodes. This algorithm selects the route on the basis of maximum path trust value between the nodes. To evaluate the trust of nodes trust factor collection method is used. It generates only relevant information and do not generate extra control messages. In results it enhances the packet delivery ratio and latency and reduced the network overhead [7].

C. Behavioral Approach

Patel, Meenakshi et al. proposed a method of attack detection by using the behavioral approach. In this work author identifies flooding attack by detect the behavior of nodes. In this attacker sends the fake RREQ request and block the whole network by using the resources. In this APDV protocol is used to detect the malicious code and support vector machine is used to identify the input classes' feasibility. In this method performance evaluation metrics are packet delivery ratio, Modification rate and packet misroute rate [8].

Choudhury, Prasenjit, et al. proposed an approach of SYN attack detection in MANET by using behavior detection method. In this they observe behavior of the node time to time and limits the request sending rate if any node sending multiple requests at the same time [9].

D. Adaptive Response Mechanism

Nadeem et al. introduced intrusion detection and adaptive resource response mechanism for wireless sensor network. This method detects the range of the attack and gives the protection mechanism at low cost. Intrusion deficiencies overcome by using flexible response method. This method improves the network performance low network overhead [10].

E. SYN-Flood Detection Mechanism

Neethu Raj, et al. proposed a method of detecting SYN-Flooding and uses transport layer parameters like increased in packet and enhancement in FIN Rate. AR method is used for preprocessing and prediction of the traffic on the network. Attack is detected by using threshold value and matches at least two values for final decision. This attack is performed on NS2 simulator and found that false alarm rate is very less [14].

F. LPTR-PSO Method

Ahmed, Zonayed et al. [15] in this paper, the author proposed an algorithm for SYN-Flood detection called as LPTR-PSO. Largest processing Time rejection- Particle Swarm Optimization algorithm used to detect the SYN flood attack. It is a three phased algorithm and considers the half open connections in server buffer and then select the phase accordingly. This algorithm detects the job by matching the time with the threshold value in the half open connection. PSO is used for the optimization of the results in the third phase. The proposed method enhanced the detection rate of the attack on the network.

V. CONCLUSION

This paper highlights security issues of mobile ad-hoc network. Security is a big challenge for wireless network. Security issue arises more due to dynamic behavior of the network. This paper gives a brief introduction on the attacks in the MANET and review the SYN flooding attack along with analysis the effect of SYN flooding attack by different parameters. It gives the review over the methods and algorithms used to resolve the attack problem in MANET.

REFERENCES

[1] Rmayti, M., et al. "Flooding attacks detection in MANETs." *Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on*. IEEE, 2015.

[2] Prabha, Jyoti, et al. "Prevention of Conjunct Black Hole MANET on DSR Protocol by Cryptographic Method." *Smart Trends in Systems, Security and Sustainability*. Springer, Singapore, 2018. 233-240.

[3] Dharini, N., Ranjith Balakrishnan, and A. Pravin Renold. "Distributed detection of flooding and gray hole attacks in Wireless Sensor Network." *Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015 International Conference on*. IEEE, 2015.

[4] Ma, Rui, et al. "Defenses Against Wormhole Attacks in Wireless Sensor Networks." *International Conference on Network and System Security*. Springer, Cham, 2017.

[5] Moudni, Houda, et al. "Performance analysis of AODV routing protocol in MANET under the influence of routing attacks." *Electrical and Information Technologies (ICEIT), 2016 International Conference on*. IEEE, 2016.

[6] Geetha, K., and N. Sreenath. "Detection of SYN Flooding Attack in Mobile Ad hoc Networks with AODV Protocol." *Arabian Journal for Science and Engineering* 41.3 (2016): 1161-1172.

[7] Tan, Shuaishuai, Xiaoping Li, and Qingkuan Dong. "Trust based routing mechanism for securing OSLR-based MANET." *Ad Hoc Networks* 30 (2015): 84-98.

[8] Patel, Meenakshi, and Sanjay Sharma. "Detection of malicious attack in manet a behavioral approach." *Advance Computing Conference (IACC), 2013 IEEE 3rd International*. IEEE, 2013.

[9] Choudhury, Prasenjit, et al. "Mitigating route request flooding attack in MANET using node reputation." *Industrial informatics (INDIN), 2012 10th IEEE international conference on*. IEEE, 2012.

[10] Nadeem, Adnan, and Michael P. Howarth. "An intrusion detection & adaptive response mechanism for MANETs." *Ad Hoc Networks* 13 (2014): 368-380.

[11] Nemade, Sandip, Manish Kumar Gurjar, and Zareena Jamaluddin. "A Novel Method for Early Detection of SYN Flooding based DoS attack in Mobile Ad Hoc Network."

[12] Geetha, K., and N. Sreenath. "SYN flooding attack—Identification and analysis." *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*. IEEE, 2014.

[13] Geetha, K. "SYN Flooding Attacks in Mobile Adhoc Networks." *(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5033-5037*

[14] Neethu Raj, P., S. Suresh Babu, and N. Nishanth. "A Novel Syn Flood Detection Mechanism for Wireless Network."

[15] Ahmed, Zonayed, Maliha Mahbub, and Sultana Jahan Soheli. "Defense against SYN Flood Attack using LPTR-PSO: A Three Phased Scheduling Approach." *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS* 8.9 (2017): 433-441.