IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# DIMINISH THE FLOODING ATTACK USING MUTUAL AUTHENTICATION IN MOBILE AD-HOC NETWORK

**Jasvir Markandy[1], Manmohan Sharma[2]**
M.Tech Scholar[1],Assistant Professor[2]
[1]Departmentof Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab
[2] Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab

**DOI**: 10.5281/zenodo.1241365

## ABSTRACT

Mobile ad-hoc network (MANET) is a group of wireless mobile nodes and dedicated routers used by base station. MANET application in mobility management, broad casting, and bandwidth management are important issue in routing and information gathering. In MANET, Different types of attack has been developed today which degrade the performance of network and makes it less efficient like SYN flooding, Black hole attack,Worm hole attack, Grey hole attack etc.In this paper, we are representing flooding attack proposed by various author inmobile ad-hoc network.

**Keywords:** Mobile Ad-Hoc Network (MANET), Flooding Attacks, Wireless Security, Quality of services, Attack Detection, Network lifespan.

## I. INTRODUCTION

Mobile ad-hoc network is combination of mobile devices which communicate with each other without any predefine infrastructure or any centralized administration. MANET supports dynamic structure of network. MANET applications are mainly used in disaster relief, vehicle network, military, and robot networks and so on. MANET is used in various fields for the effective communication process in which user send their information from one node to another node [1]. Sometimes, User sends the secret information on the wireless network, it is important to send this information very safely. In such network sensor nodes use wireless communication and it is easy to eavesdrop. Attacker can easily inject malicious message into the network.

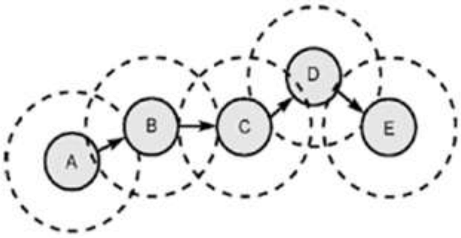

*Figure 1.1 MANET architecture*

## II. PROPERTIES

Following are the properties that are supported by the MANET.

- Limited Power: In MANET, all the nodes rely on the exhaustible sources of energy like battery powers.
- Mobility: Nodes in the network move freely due to flexibility and it accommodate all types of links.
- No Centralized router: In MANET, Every node is independent and selects their route according to the receiver node location and this feature also supports the dynamic topology [2].

## III. ATTACKS

In MANET, Attacks are mainly affecting the functionality of network layer which is responsible for routing in MANET. There are mainly three types of attack which are occurred in mobile ad-hoc network.

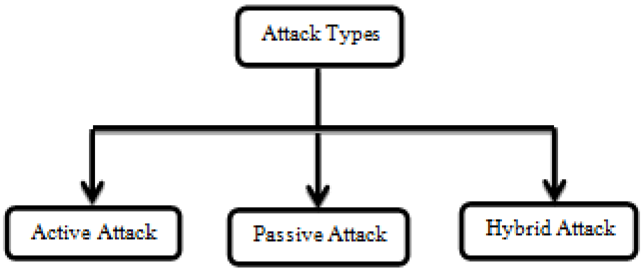

Figure 3.1 Attacks in MANET

### A. Active Attack

In active attack, attacker modifies the content of data that is to be exchanged in the network. In this process, attacker can inject new packets, drop the packets and modify the existing data packets. This type of attack is very harmful for the network as well as sender. It is further divided into two parts; attack done by the node which is already present in network is called internal attack and a node which attacks from outside is called external attack.

### B. Passive Attack

In passive attack, attacker captures the data without altering or modifying it. This attack does not affect the normal working ofnetwork. The main difficulty is detection. This attack is done mainly to gather the information about communication between sender and receiver.

### C. Hybrid Attack

It is basically, a combination of two attack that are dictionary attack and Brute-Force attack. Dictionary attack includes the wordlist of passwords and Brute force attack would be applied to each possible password in that list.

## IV. FLOODING ATTACK

It is a type of active attack in which RREQ and data packets sent to the nodes in a large number which leads to congestion on the network as well as network failure due to unwanted traffic. This type of attack is not easy to detect. In this section different types of flooding attacks are defined [3].

### A. Hello Flooding:

Hello packets are used in this type of attack. Attacker sends hello packet and try to connect with neighbor nodes like a normal node. In this attack, Hello packets are transmitted by attacker with high transmission range which assure other nodes that it is the base station and begins sending packet towards attacker node by trusting that it will have best path to the destination. This will prompt increment delay in the network as well as assure other nodes that base station (attacker node) is it’s neighboring node. In order that various nodes will react to the Hello packet and waste their energy.

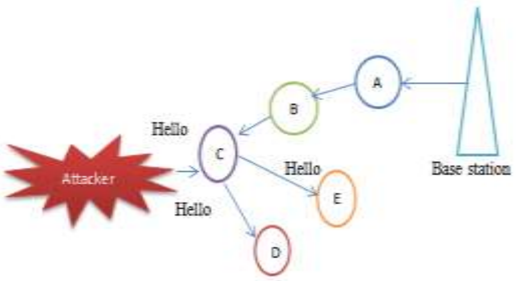

*Figure 4.1 Hello Flooding Attack*

**B. RREQ Flooding:**

In RREQ flooding attack, Attacker generates many RREQ packets for that destination which does not present in the network. This attack affects the network and consumes more network bandwidth along with battery power of nodes.

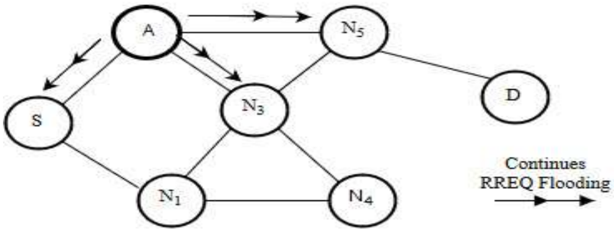

***Figure 4.2 RREQ Flooding attack***

**C. Data Flooding:**

In data flooding attack the malicious node first construct the path to all the nodes and sends large amount of useless data to the node which exhaust the bandwidth. This attack is difficult to detect because attacker use spoof identification as well as choose wrong destination id which does not exist in the network thus it is not easy to identify the data packets.

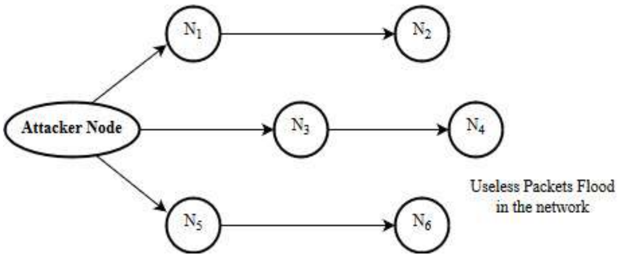

***Figure 4.3 Data Flooding attack***

**D. ICMP (Internet Control Message Protocol) Flooding:**

In ICMP attack, Attacker sends ICMP echo messages to the nodes and all the nodes are replying to ICMP request by sending ICMP reply packet. It leads to wastage of resources and battery power of the nodes on the network.

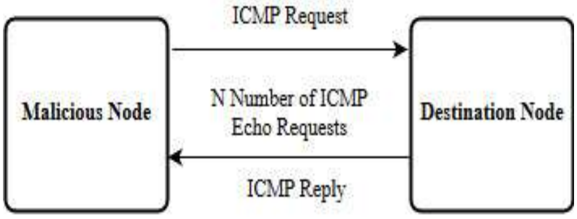

***Figure 4.4 ICMP Flooding attack***

**E. UDP Flooding:**

In this attack UDP data packets are sends to the nodes to consume the bandwidth of the nodes. Protection from this attack is done by using the firewall on the network layers.

**F. SYN Flooding:**

In SYN Flooding attack, attacker sends a large number of synchronization packet to the destination nodes and these nodes consumes a lot of memory. After getting the identity of the spoofed client, attacker behaves like original client node and start sending SYN message to the server and server send SYN ACK in reply to malicious node. By doing this again and again, server makes a half open connection with malicious node. Server sends continuous SYN ACK to the malicious client and updated the repeated information in its buffer. After the buffer is full, server is not able to reply to other clients and it deny the entire session [4].

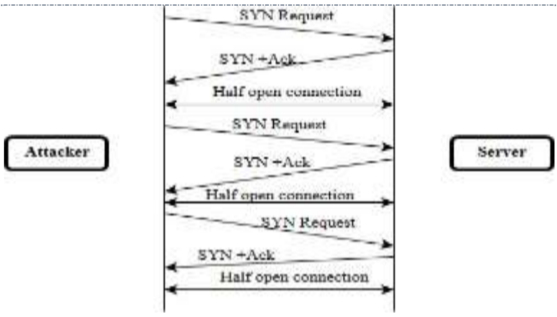

***Figure 4.5 ICMP Flooding attack***

## V. RELATED WORK

Singh, Kuldeep et al. [2] Intrusion detection in mobile ad-hoc network depends upon the parameters of nodes. By using the threshold values of the parameters ant colony optimization algorithm is used for intrusion detection. After the detection of intrusion, recovery is done by using genetic algorithm.

Nemade, Sandip et al.[4]In SYN Flooding attack, attacker sends a large number of synchronization packet to destination nodes and these nodes consumes a lot of memory. After getting the Identity of the spoofed client, attacker behaves like original client node and start sending SYN message to server and server send SYN ACK in reply to the malicious node. In this paper, author proposed an adaptive threshold algorithm that raised alarm when it detects the SYN packets abnormally.

Song, et al.[5]In this paper, a filtering method against the RREQ flooding attacks in MANET is proposed. In these types of attack infected nodes behaving like normal nodes and leads to congestion of network. These nodes send RREQ packets with high data rate towards the destination than other nodes. In proposed method, nodes are filtered by their behavior and prevent from this type of attack.

K. Geetha et.al [6] Introduce, An intrusion detection system (IDS). The NASH balance is calculated, and the possibilities of the attacker to attack and the safeguard to protect are additionally calculated. This gives full affirmation that the node chose for the exchange of information is not malignant and furthermore this node can furnish exchange with least delay and jitter.

Patel, Meenakshi et al. [7]In this paper, the author proposed a method of attack detection by using behavioral approach. Author identifies flooding attack by detecting behavior of nodes. Attacker sends fake RREQ nd block the whole network by using resources. AODV protocol is used to detect the malicious node and support vector machine is used to identify input classes feasibility. In this method, performance evaluation metrics are Packet Delivery Ratio, Modification Rate and Packet Misroute Rate.

Choudhury, Prasenjit, et al. [8]In this paper, author 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.

Neethu Raj, et al. [9] In this paper, the authorproposed 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.

## VI. RESEARCH METHODOLOGY

Since flooding attack is one of the biggest and dangerous attack in mobile ad-hoc network, it flood the victim node with number of packets due to this network performance degrade. The main goal is to migrate the flooding attack from mobile ad-hoc network. Furthermore, its security is detracting challenge due to its nature, much of the time topology changes. That is the reason MANET is survival from physical to application layer unsecured. In any case, security is measure issue for the communication so we contemplate number of detection-prevention techniques and ensure mobile ad-hoc network through various attacks.In this research, our basic goal is to isolate the flooding attack from MANET. Following is the steps that we follow to implement our proposed methodology technique:

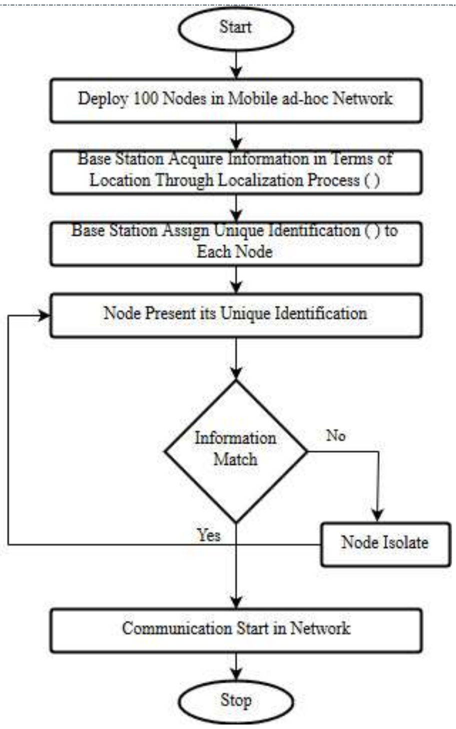
Start
Deploy 100 Nodes in Mobile ad-hoc Network
Base Station Acquire Information in Terms of Location Through Localization Process ( )
Base Station Assign Unique Identification ( ) to Each Node
Node Present its Unique Identification
Information Match
No
Node Isolate
Yes
Communication Start in Network
Stop

***Figure 4.6: Proposed flow chart***

## VII. RESULT AND DISCUSSION

This research is cut down the flooding issue on MANET and upgrade the results of routing protocol in terms of throughput, packet delivery Radio and overhead. The flooding attack is the dynamic kind of attack which is activated by the selfish nodes. In the flooding attack the selfish nodes flood the victim node with boundless number of packets because of it the victim node gets intensely stacked and the server or node couldn't answer for other node's request. Thus the whole session have denied.Following is the result screenshots that we predicate:

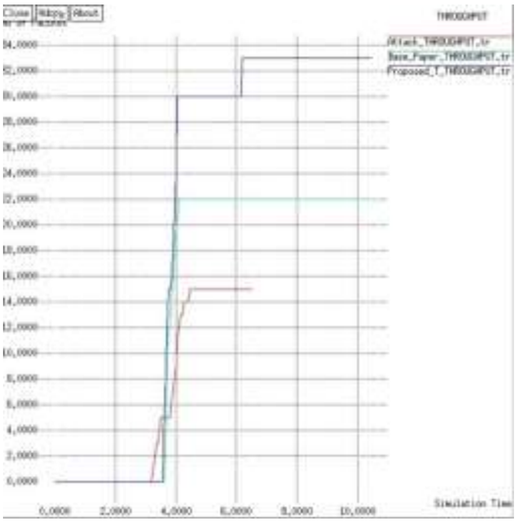

***Figure 4.7: Throughput Comparison***

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

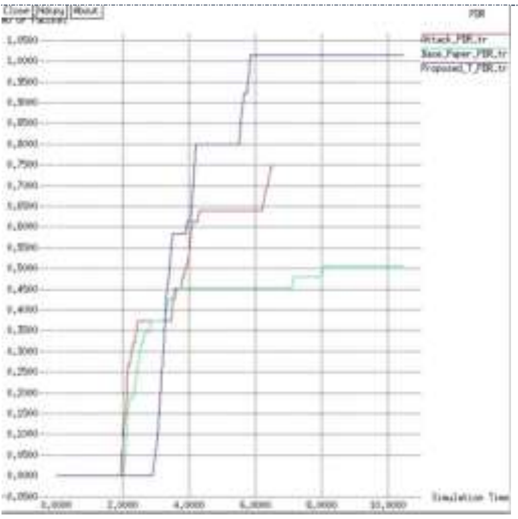

*Figure 4.8: PDR Comparison*

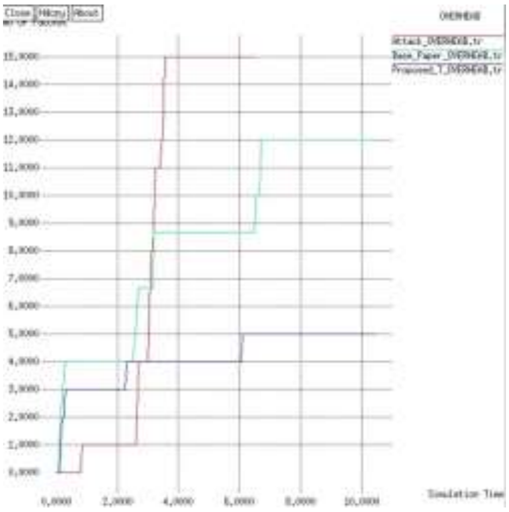

*Figure 4.9: Overhead Comparison*

## VIII. CONCLUSION

The Mobile Ad-hoc network (MANET) is a dynamic profitable network and furnishes communication with irregular movement of mobile nodes. The security is the significant issue in this sort of decentralized network. The absence of centralized control is admired to network from various attacks. In this research, we study the flooding attack, security and typical routing in the network and discover its effects.

MANETs are mainstream network utilized broadly because of their dynamic nature. These kinds of network are suffered from flooding attack as there is no consolidate security management. Here in this paper, we center on, to analyses and diminish flooding attack in MANET

## IX. REFERENCES

[1] Pham, Thi Ngoc Diep, et al. "Detecting Flooding Attack and Accommodating Burst Traffic in Delay-Tolerant Networks." IEEE Transactions on Vehicular Technology 67.1 (2018): 795-808.

[2] Singh, Kuldeep, and Karandeep Singh. "Intrusion Detection and Recovery of MANET by Using ACO Algorithm and Genetic Algorithm." Next-Generation Networks. Springer, Singapore, 2018. 97-109.

[3] Soni, Rajshree, Anil Kumar Dahiya, and Sourabh Singh Verma. "Limiting Route Request Flooding Using Velocity Constraint in Multipath Routing Protocol." Proceedings of First International Conference on Smart System, Innovations and Computing. Springer, Singapore, 2018.

[4] 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."International Journal of Engineering Trends and Technology (IJETT) Voulume -7 ,Number -4, 2014.

[5] Song, Jian-Hua, Fan Hong, and Yu Zhang. "Notice of violation of ieee publication principles effective filtering scheme against RREQ flooding attack in mobile ad hoc networks." Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT'06. Seventh International Conference on. IEEE, 2006.

[6] K. Geetha, N et.al,"Detection of SYN Flooding Attack in Mobile Ad hoc Networks with AODV Protocol "Arabian March 2016, Volume 41, Issue 3, pp 1161–1172.

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

[8] 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.

[9] Neethu Raj, P., S. Suresh Babu, and N. Nishanth. "A Novel Syn Flood Detection Mechanism for Wireless Network.".International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 22 - 27 (2015) Special Issue of ICEEC 2015 - Held on August 24, 2015 in The Dunes, Cochin, India

## CITE AN ARTICLE

Markandy, J., & Sharma, M. (2018). DIMINISH THE FLOODING ATTACK USING MUTUAL AUTHENTICATION IN MOBILE AD-HOC NETWORK. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *7*(5), 24-30.