Defending Against RREQ Flooding Attack in AODV in MANETs

Suhail Mehraj[1] Er. Rupali Zakhmi[2]
[1,2]Department of Computer Science & Engineering
[1,2]SVIET College Banur, Patalia, India

Abstract— Mobile Ad Hoc Networks (MANETs) is an infrastructure less network, where each node provides a relay mechanism for data to reach the final destination. There is no centralised entity in MANETs to administer the nodes, this makes it challenging to make the network self-driven, and secure. MANETs have applications in communication in disaster and military where infrastructure for communications are unavailable. However, as MANETs use wireless transmission and the nodes are deployed in hostile conditions, the network is vulnerable to numerous attacks. Because of which security becomes one of the primary concerns for MANETs. Flooding attack is one of the many attacks that possess serious threat to performance of MANETs as it consumes bandwidths by flooding unnecessary data in the network. This paper proposed a detection and prevention mechanism for flooding attack in MANETs. Attack is simulated on NS2 simulator and the results are positive for detection and prevention of flooding of request packets in AODV routing protocol which is mostly used in MANETs.

Key words: RREQ, Flooding Attack, AODV, MANETs

I. INTRODUCTION

Today wireless networks [1] are very popular in our daily life network use and in providing communication during emergency situations. Wireless technology helps to transfer data without the need of infrastructure. The transmitted distance can be anywhere between a few meters (for example, a television's remote control) and thousands of kilometers (for example, radio communication). Some of the devices used for wireless communication are cordless telephones, mobiles, GPS units, wireless computer parts, and satellite television.

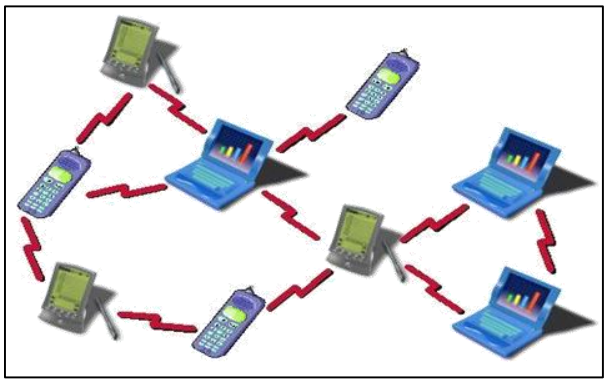


Fig. 1: Mobile Ad-Hoc Network [10]

Since the data in MANETs travels through an open medium, it is prone to many security threats. Security in MANETs is one of the major concerns for the researchers.

A. Routing Security in MANETs

Providing a secure system [2] [3] can be achieved by preventing attacks or by detecting them and providing a mechanism to recover for those attacks. Attacks on ad hoc wireless networks can be classified as active and passive attacks, depending on whether the normal operation of the network is disrupted or not.

1) Passive Attack

In passive attacks, an intruder snoops the data exchanged without altering it. The attacker does not actively initiate malicious actions to cheat other hosts. The goal of the attacker is to obtain information that is being transmitted, thus violating the message confidentiality. Since the activity of the network is not disrupted, these attackers are difficult to detect. Powerful encryption mechanism can alleviate these attackers by making difficult to read overheard packets.

2) Active Attack

In active attacks, an attacker actively participates in disrupting the normal operation of the network services. A malicious host can create an active attack by modifying packets or by introducing false information in the ad hoc network. It confuses routing procedures and degrades network performance. Active attacks can be divided into internal and external attacks:

Following are some of the attacks to which MANTEs are vulnerable:

3) Man-in-the-Middle Attack

In this attack, a malicious node reads and possibly modifies the messages between two parties. The attacker can impersonate the receiver with respect to the sender, and the sender with respect to the receiver, without having either of them realize that they have been attacked.

4) Routing Table Poisoning

In this attack, a malicious node sends false routing updates, resulting in sub-optimal routing, network congestion, or network partition. Rushing Attack A malicious node in rushing attack attempts to tamper Route Request packets, modifying the node list, and hurrying its packet to the next node. Since in on demand routing protocol only one Route Request packet is forwarded, if the route requests forwarded by the attacker are first to reach target (destination), then any route found by the route discovery mechanism will include a path through the attacker.

5) Black Hole

In this type of attack, a malicious node advertises itself as having the shortest path to all nodes in the network (e.g. the attacker claims that it is a level one node). The attacker can cause DoS by dropping all the received packets. Alternately, the attacker can monitor and analyze the traffic to find activity patterns of each node. Sometimes the black hole becomes the first step of a man-in-the-middle attack.

6) Wormhole Attack

In the wormhole attack, two compromised nodes can communicate with each other by a private network connection. The attacker can create a vertex cut of nodes in the network by recording a packet at one location in network, tunneling the packet to another location, and replaying it there. The attacker does not require key material as it only needs two transceivers and one high quality out- of-band channel. The wormhole can drop packets or it can selectively

forward packets to avoid detection. It is particularly dangerous against different network routing protocols in which the nodes consider themselves neighbor after hearing a packet transmission directly from some node.

7) Denial of Service (DoS):

In the DoS attack, an attacker explicitly attempts to prevent legitimate users from using system services. This type of attack impacts the availability of the system. An ad hoc wireless network is vulnerable to DoS attacks because of its dynamic changing topology and distributed protocols.

II. LITERATURE SURVEY

Yinghua et al.[4] presented a detailed investigation of the flooding attack in MANET. Further, they design two flow based detection features, and apply the cumulative sum algorithm on them to effectively and accurately detect such attack. The CUSUM monitors the mean variations of time series. It accumulates random variable values that are significantly higher than the mean level under normal operation or threshold, a change (or attack) is said to be detected. Flooding attack model is given, where by using different values of various parameters are attackers will launch the attack. Two different algorithms are presented to detect address spoofing which is based on the new RREQ flow and non-address spoofing attack deals with identical RREQ from the source node. Also through simulation the performance enhancement is compared with traditional technique.

Gunasekaran et al. [5] presented a DoSP-MAC prevent unfairness produced from the two mechanisms namely Fast Forward and Quick Exchange in sharing the channel among the nodes, a NAV Restriction Parameter is introduced. This Parameter cumulates number of metrics like traffic on the network, priority of data with other nodes, time for which the transmission has already taken place. Each time when a node tries to extend the NAV, this value is calculated for that node and only if the value of the RESTRICTION Parameter is above the defined threshold value, the extension of NAV is permitted, otherwise not allowed, thereby enhance its performance.

Azreen et al.[6] focused on the malicious behavior of the nodes. Sequence number and hop count are examined to check the vulnerabilities in the network. Destination sequence numbers maintained by different nodes are only updated when a newer control packet is received with a higher sequence number. Malicious nodes may increase this number to advertise fresher routes towards a particular destination. In case of hop count, a node prefers a control packet with a larger destination sequence and hops count over a control packet with a smaller destination sequence and hop count. However. Malicious nodes frequently exploit this mechanism in order to generate fallacious routes that portray minimal hop counts.

Mohamed et al.[7] proposed a Real-time Host Intrusion Detection for Ad hoc Networks (REHIDAN) algorithm to identify the flooding attacker nodes. It also takes the appropriate countermeasures to minimize the effectiveness of the attack and maintain the network performance within the accepted limits. The REHIDAN algorithm is based on the idea of the Neighbor Suppression algorithm. The REHIDAN algorithm is embedded in the routing layer with the AODV routing protocol without introducing any significant changes to the underlying routing protocol. The proposed algorithm follows the knowledge based methodology to detect network intrusions. It enables the system to detect malicious/attacker's activity in real-time rather than using statistical analysis of previously captured traffic. Operates locally in every participating node and depends on the network traffic observed by the node. REHIDAN algorithm reduces the effect of the attack by reducing the end-to-end delay and the routing overhead ratio.

Yinghua et al.[8] presented the work, focusing on the "analysis" part. They investigate and model the ASF attacks in MANET. In this model, they examine four attack parameters resulting in various attack patterns. They also propose an analytical model for looking for specific patterns of the ASF attack traffic. by the evaluation results, this analytical model can help network forensic investigators with (1) determine if there is an anomaly in the traffic and whether the anomaly is the ASF attack (2) Determine time when the ASF attack is launched. Additionally traffic analysis model can also be helpful to security enhancement, e.g. IDSs can detect DDoS attacks more effectively by traffic pattern identification proposed in this work.

Kashif et al.[9] proposed RFAP, a scheme for mitigating the RREQ flooding attack in MANET by utilizing AODV protocol. The RFAP is an amended form of AODV. The RFAP scheme totally disagrees with the idea that if a node misbehaves or find in malicious activities, just segregates it from the network. The scheme believes that a flooder node may be misused by some intruder and normalize thereafter or by extraordinary changing its position that may be in emergency condition. Keeping these facts in consideration, RFAP scheme is designed to provide enough time to blunderer to come to a dutiful life. RFAP scheme can easily single out the attacker node and protect the network resources from RREQ flooding attack. Indeed the actual AODV protocol can generate inoperative result at the time of flooding and its only execute the route requests again and again which result the network resources jam. In contrast the RFAP scheme works intelligently at the time of flooding. These results illustrate that RFAP has ability to separate the flooder node from the network with more reliable as compare to simple AODV.

III. PROPOSED ALGORITHM

The proposed scheme is based on the frequency of RREQ generation in an interval and broadcast id varies with that change. Here by launching the flooding attack, packet is dropped coming from malicious node. But if node is continuously doing it above a particular signature, then put the RREQ source of malicious node in the blacklist array buffer. Figure 2 shows the flow chart of the proposed algorithm

A. Algorithm

```
Recv_request()
{If(RREQ_source==blacklisted_node)
{Drop_request();} Else
{If(interval_timerexpired)
```



```
{
Update_Bidchange(); If(Bid_change>threshold)
{Blacklist(RREQ_source);}
Else
{proces_srequest();}
}
Else
{Process_request();}
}
}
//existing AODV Code
```

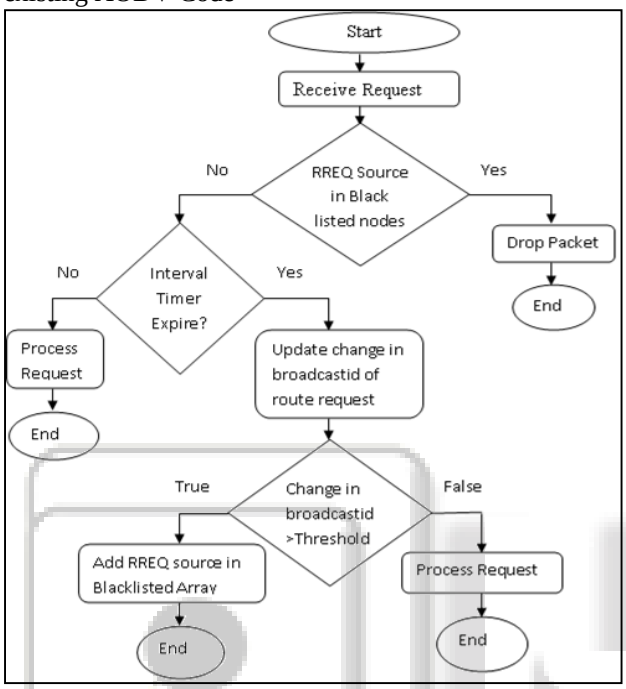


Fig. 2: Implementation Model for Defending from Flooding Attack

The proposed approach to detect the flooding attack uses the track of the signature of the request packet at the intermediate node. Two extra entries were made in the reverse route table of AODV, one store the destination address of the request packet and other stores the change in broadcast id of the source of the request packets on per second basis. If a certain threshold value of a particular source goes above the threshold the intermediate node makes a blacklist table entry of that source node, and when a new request is received at the node it first checks it's blacklisted node list, if the source of request is in the list then it drops the request, else it processes the request.

Round Trip Time (RTT) is the maximum time taken to receive the acknowledgement of a packet after travelling to the end node of the network. A normal node can issue RREQ only after the RTT is expired. Therefore, maximum RREQ issued by a normal node is 1000/RTT (1sec = 1000ms).Any node which issues RREQ with higher this value is consider as malicious.

IV. Simulation & Results

Parameter	Value
Dimension	1500x1500m^2
Number of Nodes	50
Simulation Time	300s
Traffic Type	CBR
Number of Connections	5-30(variable)
Packet Size	512 bytes
MAC Layer	IEEE 802.11b
Buffer Size	50
Propagation Radio Model	Two Ray Ground
Physical Layer	Bandwidth 2Mb/s
Pause Time	10

Table 1: Simulation Parameters

A detailed simulation model is used which is based on NS2. Table one describes the parameters used for the simulations in NS2. Distributed Coordination Function (DCF) on 802.11 is used as MAC layer Protocol. DCF of 802.11 uses Request to Send (RTS) and Clear to send (CTS) for unicast data transmission to the neighbor nodes. The RTS/CTS exchange precedes the data transmission and performs virtual sensing and medium reservation to reduce the problem of hidden terminal in wireless networks. CSMA/CA is used to transmit the data through medium. WaveLAN is modeled as shared media with nominal bit rate of 2Mb/sec with radio range of 250 meters. Pairs are spreaded randomly such as source and destination 512 bytes data packets are used. The mobility model used is random way point in a rectangular area of 1500X1500 with 50 Figure 3 shows the packet delivery ratio with respect to the number of mobile connections in the network. When the attack is launched in the network the packet delivery ratio drops because the bandwidth is consumed by the flood packets in the network. But as soon as the detection and prevention algorithm is implemented in the network, the packet delivery ratio is regained by the routing algorithm as the flooding is stopped in the whole network, because the malicious nodes are blacklisted and no node is forwarding the request packets issued by them.

V. Results & Discussions

Figure 3 shows the packet delivery ratio with respect to the number of mobile connections in the network. When the attack is launched in the network the packet delivery ratio drops because the bandwidth is consumed by the flood packets in the network. But as soon as the detection and prevention algorithm is implemented in the network, the packet delivery ratio is regained by the routing algorithm as the flooding is stopped in the whole network, because the malicious nodes are blacklisted and no node is forwarding the request packets issued by them.

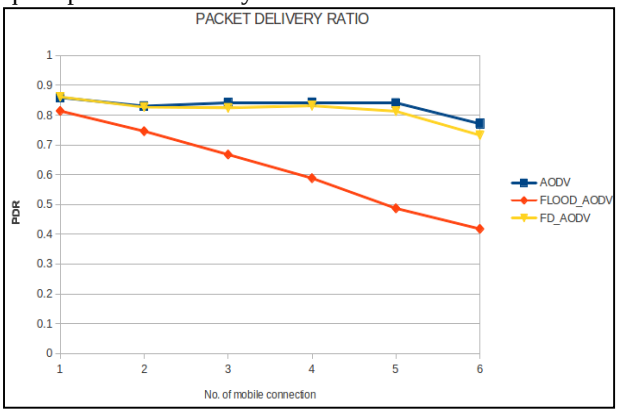


Fig. 3: Comparison of AODV, AODV with Attack and FD_AODV based on Packet Delivery Ratio

Figure 4 show the results of average end to end delay with respect to the number of mobile connections in the network. As the load in the network is increased, the delay of AODV increases because of the buffering of the packets at intermediate nodes. But in case of attack as the buffer is already filled with flood packets the end to end delay is exploited to a very high margin. As the detection and prevention scheme is launched the end to end delay comes under control and close to AODV routing protocols because the attack is been detected and the flooding has been restricted in the network.

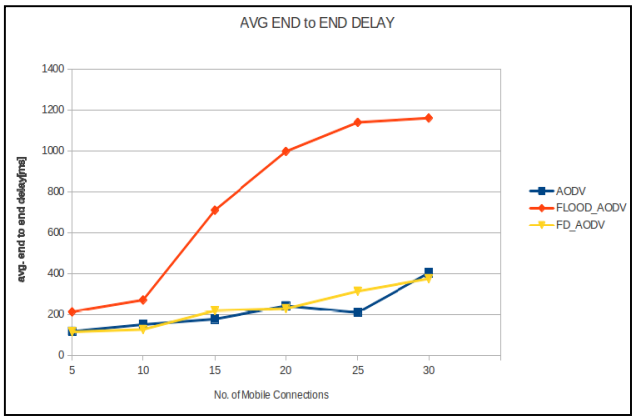


Fig. 4: Comparison of AODV, AODV with Attack and FD_AODV based on End to End Delay

Figure 5 shows the results of throughput with respect to the number of mobile connections in the network. When the attack is launched in the network the packet delivery ratio drops because the bandwidth is consumed by the flood packets in the network which degrades the number of packet received per second at the destination. But as soon as the detection and prevention algorithm is implemented in the network, the packet delivery ratio is regained by the routing algorithm as the flooding is stopped in the whole network so the packets received per second increased in the network, because the malicious nodes are blacklisted and no node is forwarding the request packets issued by them

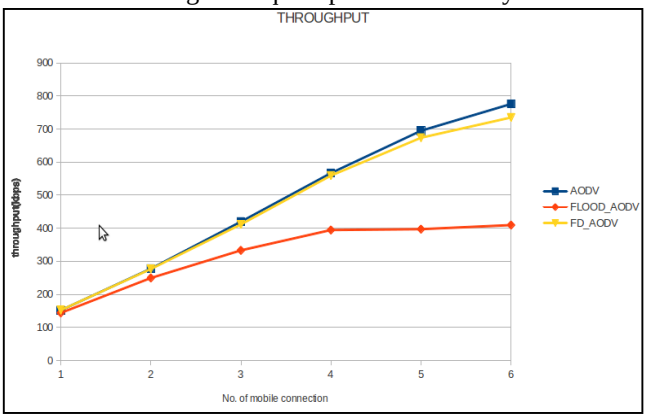
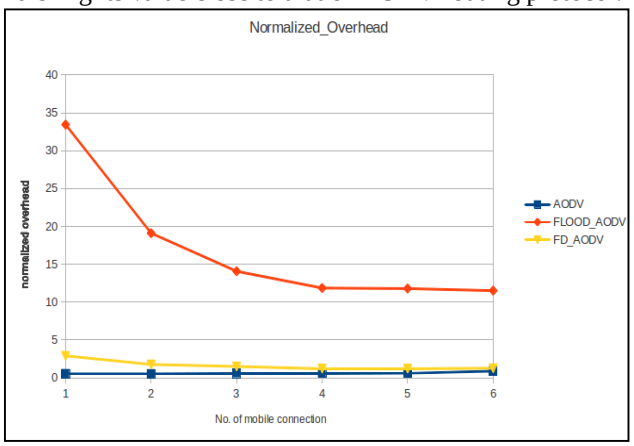


Fig. 5: Comparison of AODV, AODV with Attack and FD_AODV based on Throughput

A. Normalized Overhead Vs Number of Mobile Connections

The normalized overhead is the most effected metric of a routing packet when flooding attack is launched in a network. The results shows that normal AODV routing packet has very less overhead but as soon as the route request flooding is done, the number of routing packets in the networks increases and hence the overhead of the network is increased. The prevention mechanism is able to control the routing overhead of the network, by restricting the flood packets in the network and bring its value close to that of AODV routing protocol.



VI. CONCLUSION

Due to their unique characteristics, MANETs are suffering from a wide range of security threats and attacks. Among numerous possible routing attacks, the denial of service (DOS) attacks, especially the distributed denial of service (DDOS) attacks (e.g. route request flooding attack), acts as a major threat to ad hoc networks. In this thesis, a detection and prevention mechanism is proposed to identify the flooding malicious nodes in network. The proposed algorithm not only is able to detect multiple flooding nodes in the network but is also able to retain the performance of the routing protocol by blocking the flooding of the request packets in the network. The results shows, that the proposed mechanism can both detect and prevent the malicious node, and is also blacklisting the malicious node, so that in future the malicious node cannot harm the performance of the network.

VII. FUTURE SCOPE

The proposed technique is based on frequency Of RREQ generation in an interval broadcast Id varies with that change. Here by launching the flooding attack, packet is dropped coming from malicious node. But if node is continuous doing it above a particular signature, then put the RREQ SOURCE of malicious node in the blacklist array buffer.

REFERENCES

[1] Frikha, Mounir. "Routing in MANETs." Ad Hoc Networks: Routing, QoS and Optimization (2013): 23-47.

[2] Deng, Hongmei, Wei Li, and Dharma P. Agrawal. "Routing security in wireless ad hoc networks." Communications Magazine, IEEE 40, no. 10 (2002): 70-75.

[3] Pervaiz, Mohammad O., Mihaela Cardei, and Jie Wu. "Routing security in ad hoc wireless networks." In Network Security, pp. 117-142. Springer US, 2010.

[4] Guo, Yinghua, and Matthew Simon. "Network forensics in MANET: traffic analysis of source spoofed DoS attacks." In Network and System Security (NSS), 2010 4th

[5] Gunasekaran, R., and V. Rhymend Uthariaraj. "Prevention of denial of service attacks and performance enhancement in Mobile Adhoc networks." InCommunication Systems and Networks and Workshops, 2009. COMSNETS 2009. First International, pp. 1-6. IEEE, 2009.
[6] Azni, A. H., Azreen Azman, Madihah Mohd Saudi, A. H. Fauzi, and D. Iskandar. "Analysis of Packets Abnormalities in Wireless Sensor
[7] Network." InMEMS, NANO, and Smart Systems (ICMENS), 2009 Fifth International Conference on, pp. 259-264. IEEE, 2009.
[8] Ibrahim, Mohamed M., Nayera Sadek, and M. El- Banna. "Prevention of flooding attack in wireless ad- hoc AODV-based networks using Real-time Host Intrusion Detection." In Wireless and Optical Communications Networks, 2009. WOCN'09. IFIP International Conference on, pp. 1-5. IEEE, 2009.
[9] Guo, Yinghua, and Matthew Simon. "Network forensics in MANET: traffic analysis of source spoofed DoS attacks." In Network and System Security (NSS), 2010 4th International Conference on, pp. 128-135. IEEE, 2010.
[10] Laeeq, Kashif. "RFAP, a preventive measure against route request Flooding Attack in MANETS." Multitopic Conference (INMIC), 2012 15th International. IEEE, 2012.
[11] Tadeusz Wysocki, and Eryk Dutkiewicz. "A review of routing protocols for mobile ad hoc networks." Ad hoc networks 2, no. 1 (2004): 1-22.

