Volume 7, Issue 4, April 2017 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

MANET: Simulation Analysis of Security Attacks and Preventions on AODV Protocol using NS-3

[1]Sakshi, [2]Neha Goyal

[1] M.tech CSE, [2] Assistant Professor

Department of Computer Science & Engineering, Shri Ram College of Engineering, and Management, Palwal, Affiliated to M.D.U Rohtak, (Haryana), India

Abstract: MANETs are open and cooperative networks and can be formed quickly and without any complex infrastructure. These are very useful characteristics for fast and easy connectivity, however this poses severe security threats. In this paper, we only focus on the security threats posed to most popular MANET routing protocol AODV by black hole and flooding attacks. A Simulation study has been conducted in ns-3 to compare the performance of preventive schemes FAP and AMTT in case of flooding and black hole attacks on MANET's. The performance is analyzed based on throughput, message delay and routing overhead. In trust management security scheme, the trust model has two components: direct observation and indirect observation. In direct observation, trust value is calculated from an observer node to observed node. On the other hand, indirect observation is also referred as secondhand information which is obtained from neighbor nodes of the observer node; the trust value is calculated between them. By combining these two components in the trust model, a more accurate trust value is obtained. This will help to improve throughput and packet delivery ratio in the network.

Keywords**: MANET, Security, AODV, DOS, Black Hole, AMTT, FAP, NS-3***

I. INTRODUCTION

MANETs (Mobile Ad Hoc Networks) are self-organized networks and have applications in industrial, academic and military domains. Routing in MANETs is complex and varies as compared to fixed-wire and infrastructure based Wireless networks. MANET routing have to cope up with constrained resources and infrastructure-less topologies. AODV (Ad hoc On-Demand Distance Vector) routing protocol is one such protocol which is very popular in MANETs because of its lightweight stack and support for low overhead routing. MANETs routing protocols are vulnerable to security attacks, as they are easily interceptable , this can severely deteriorate the performance and effective throughput of the network. In this research, AODV routing protocol performance is studied in the presence of two severe security attacks (flooding attack and black hole attack). NS-3 (Network Simulator 3) is used to simulate a MANET environment with wireless nodes running AODV protocol. Flooding and black hole attacks are simulated to show the effects of these attacks on the network in terms of packet drop ratio, transmission delays and routing overheads. Then, we have implemented the widely used prevention schemes in order to improve the vulnerabilities observed in the existing protocol AODV. The proposed future work is to combine the existing protocols with some medium access schemes to improve the security vulnerability of MANET routing protocols.

II. TYPES OF SECURITY ATTACKS FACED IN AODV PROTOCOL

AODV has very limited capability to prevent against security threats. An attacker can exploit several vulnerabilities of AODV, such as absorbing routing packets, modifying and forwarding, false reply or sending false route request messages. In this paper, we are limited to only two types of attack flooding and black hole attack. We will present a comparison on the impact of these attack on the AODV based MANETs. Flooding The goal of a flooding attack is to degrade the MANETs performance by flooding it with large amounts of traffic to disrupt the routing discovery or the maintenance phase within a MANET . This attack is launched in AODV by sending multiple RREQs to non-existing destination nodes in a short time through RREQ flooding or routing table overflow the malicious node represents false routes to all authentic nodes within this network. The role of this malicious node is to prevent the creation of new actual ones; consequently, it causes routing table overflow by the authentic users. The avalanche of RREQs all over the network leads to the consumption of battery power and network bandwidth, causing DoS (Denial of Service).

A Passive Attack does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic. Passive attacks basically involve obtaining vital routing information by sniffing about the network. Such attacks are usually difficult to detect and hence, defending against such attacks is complicated. Even if it is not possible to identify the exact location of a node, one may be able to discover information about the network topology, using these attacks.

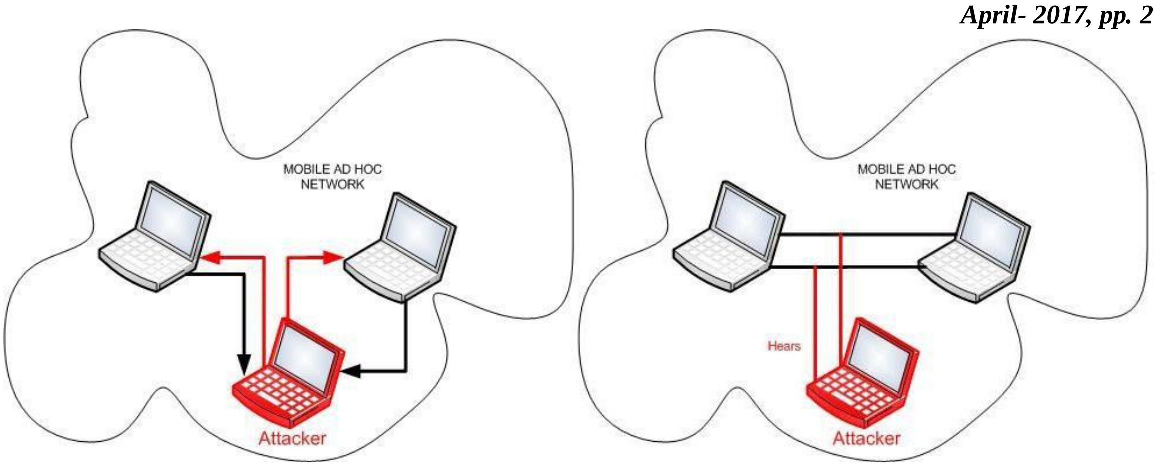


Fig. 2.1 Active and Passive Attack in MANETs

An Active Attack, however, injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes. The goal is basically to attract all packets to the attacker for analysis or to disable the network. Such attacks can be detected and the nodes can be identified.

On the basis on network protocol stack, attacks can be classified into following categories (below is a classification of security attacks based on protocol stack; some attacks could be launched at multiple layers):

a.	Application layer	:Repudiation, Data Corruption Attacks
b.	Transport layer	:Session Hijacking, SYN Flooding Attacks
c.	Network layer	:Wormhole, Blackhole, Byzantine, Flooding Attacks
d.	Data link layer	:Resource Consumption, Location Disclosure Attacks
e.	Physical layer	:Traffic Analysis, Monitoring, Disruption MAC (802.11)

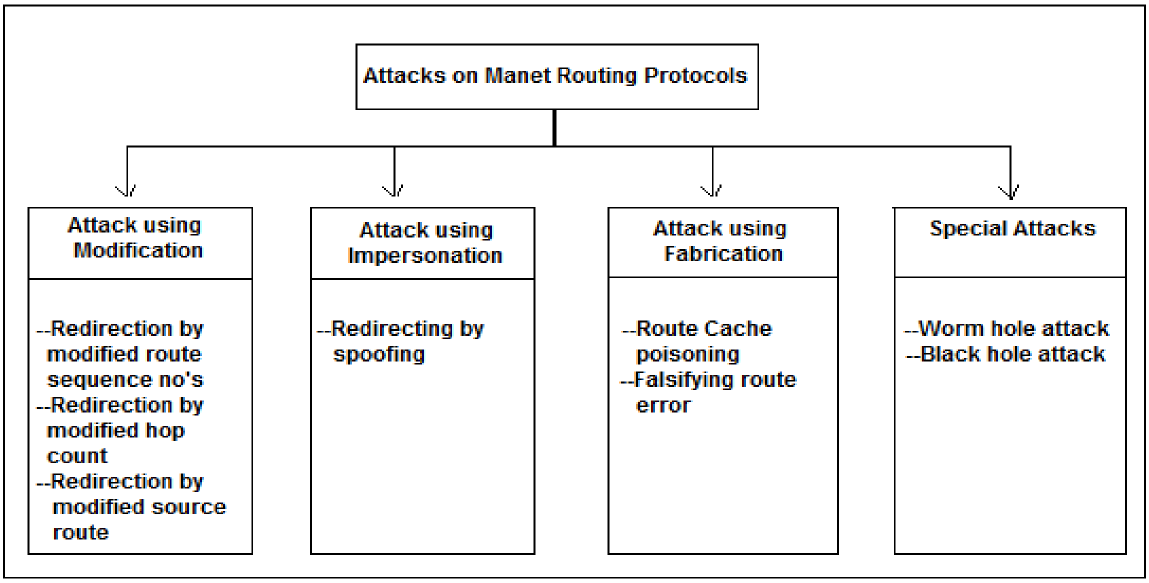

Attacks on Manet Routing Protocols
Attack using Modification
--Redirection by modified route sequence no's
--Redirection by modified hop count
--Redirection by modified source route
Attack using Impersonation
--Redirecting by spoofing
Attack using Fabrication
--Route Cache poisoning
--Falsifying route error
Special Attacks
--Worm hole attack
--Black hole attack

Fig 2.2 Attacks on MANET routing protocols

(i) Attacks using Modification: In case of modification type of attacks some of the messages in the protocol fields are modified and then these messages passed among the nodes, due to this way it become the cause of traffic subversion, as well as traffic redirection and also act as a Denial of Service (DoS) attacks. There are some of these types of attacks are given below:

A. Route sequence numbers modification: In this type of attack which is mainly possible against the AODV protocol. In this case an attacker (i.e. malicious node) used to modify the sequence number in the route request packets.

B. Hop count modification attack: In this type of attacks where it is also mainly possible against the routing protocol AODV, here attacker mostly change hope count value and due to this way it will become the cause of attract traffic. They are mainly used to include new routes in order to reset the value of hop count field to a lower value of a RREQ packet or sometime even it is used to set to zero.

C. Source route modification attack: In this type of attack which is possible against DSR routing protocol where attacker (malicious node) modify source address and move traffic towards its own destination. In Fig. 2.6 the mechanism is defined, where the shortest path between source S and destination X is defined (S-A-B-C-D-X). Which shows that node S and the node X cannot communicate each other directly, and in the scenario where the node M which act as a malicious node which are going to attempt a denial-of-service attack. Let suppose that the node S which act as a source try to send a data packet towards the node X but if the node M intercept the packet and remove the node D from the list and the packet forward towards node C, where the node C will try tosend the picket towards the distention X which is not possible because the node C can't communicate with X directly, Due to this way the M node has successfully established a DoS attack on X.

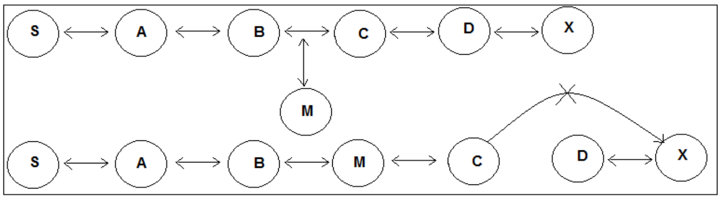


Fig. 2.3 an example of route modification attack

(ii) Attacks using Impersonation: In this type of attacks where attacker is used to violates authenticity and confidentiality of a network. In this attack an attacker (i.e. malicious node) uses to impersonate the address of other user node in order to change the network topology. This type of attack can be described in the Figure 2.7 given below:

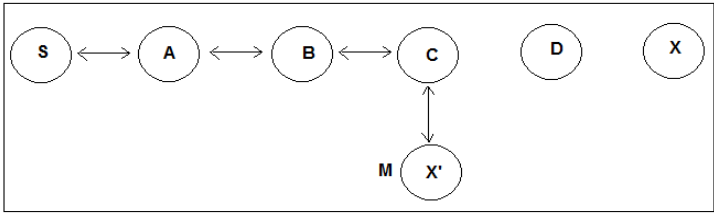


Fig. 2.4 Type of impersonation attack

In the above figure where the S node wants to send data towards the node X and before sending data to node X it starts a Route Discovery process. During route discovery process there is a malicious node M, when it receive route discovery packet regarding the node X then it modify its address and change to node X, like impersonates node X as X'. After that it send packet back to source node S that I am the destination node by RREP packet request. When the source node receives RREP packet information it doesn't authenticate node and accept the route and send data to the malicious node. This type of attacks also called routing loop attack which will become the cause of loops within the network.

(iii) Attacks using Fabrication: In this type of attacks, where an attacker as a malicious node try to inject wrong messages or fake routing packets in order to disrupt the routing process. The fabrication attacks are very much difficult to detect in the mobile ad hoc network. Attacks using fabrication process are discussed very well in [20] and [21]. In Figure 2.8 where fabrication attacks is explained by an example. In the example where the source node S wants to send data towards the destination node X, so therefore at start it sends broadcast message and request for route towards the destination node X. An attacker as a malicious node M try to pretends and modify route and returns route reply to the node (S). Furthermore, an attacker's nodes use to fabricate RERR requests and advertise a link break nodes in a mobile ad hoc network by using AODV or DSR routing protocols.

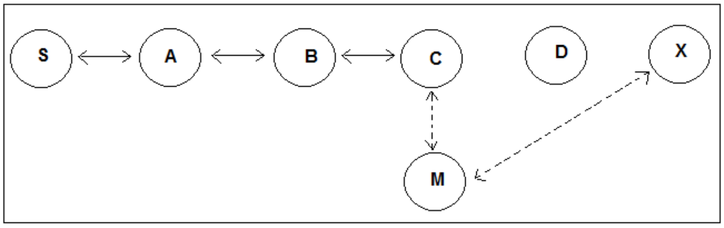


Fig.2.5 Fabrication attack example

(iv) Special Attacks: There are also some other severe attacks in MANET network which are possible against routing protocols such as AODV and DSR.

A. Wormhole Attack: The wormhole attack [15] is one of the severe types of attack in which an attacker introduces two malicious nodes in the network where an attacker used to forward packets through a private "tunnel". This complete scenario described in Figure 2.9 which is given below:

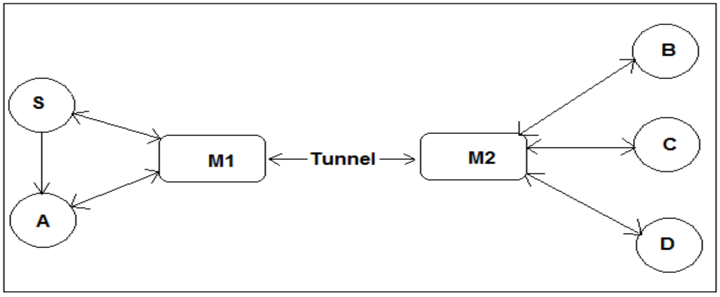


Fig. 2.6 Wormhole attack example

B. Black hole attack: This kind of attack is described very well in detail in [21]. In this type of attack, node is used to advertise a zero metric to all destinations, which become cause to all nodes around it in order to route data packets towards it. The AODV protocol is vulnerable to such kind of attack because of having network centric property, where each node of the network has to shares their routing tables among each other.

In the above example where there are two malicious nodes M1 and M2 which link through a private connection. In this type of attack every packet which an attacker receive from network 1 forward to other network where another malicious node exist, simple speaking these two nodes use to exchange network information and fabricate traffic among each other. The traffic between the two nodes passes through "wormhole" among each other. Due to this way it will become the cause of disrupts routing protocols and violating normal flow of routing packets. These types of attacks are very difficult to detect in a network, and become the cause of severe damages to the nodes. These types of attacks can be prevented by using mechanism packet leashes [15], which are used to authenticate nodes among each other by timing information process.

C. Flooding: The goal of a flooding attack is to degrade the MANETs performance by flooding it with large amounts of traffic to disrupt the routing discovery or the maintenance phase within a MANET [12]. This attack is launched in AODV by sending multiple RREQs to non-existing destination nodes in a short time through RREQ flooding or routing table overflow as shown in Figure 2. This means that the malicious node represents false routes to all authentic nodes within this network. The role of this malicious node is to prevent the creation of new actual ones; consequently, it causes routing table overflow by the authentic users. The avalanche of RREQs all over the network leads to the consumption of battery power and network bandwidth, causing DoS (Denial of Service) [13]. This can severely degrade the network throughput and performance.

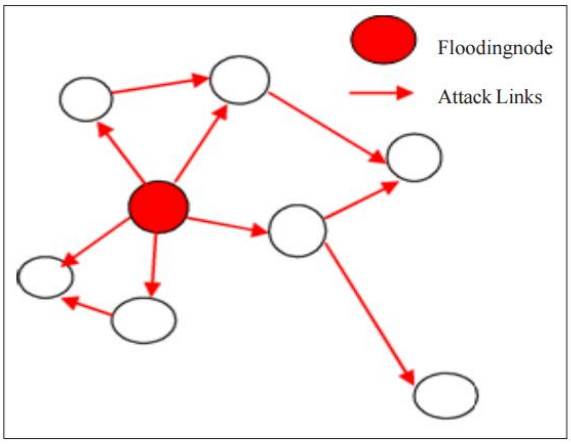


Figure 2. Flooding Attack Scenario

III. PREVENTIVE SCHEMES

1) AMTT (Avoiding Message Transmissionables): AMTT is a technique that uses AODV FIFO rule to transmit route requests to neighbors. AMTT use the rule of priority instead of FIFO; the priority is inversely

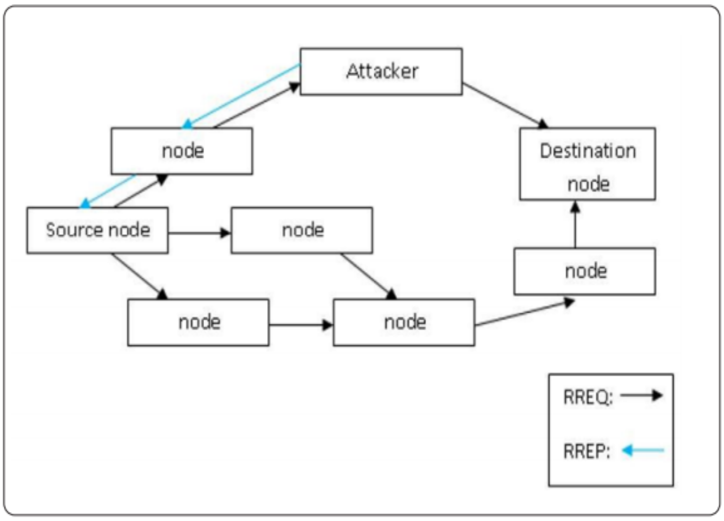


Figure 3. Black Hole Attack

Proportional to the frequency of RREQ originated by a neighbor and compared to a threshold (Threshold is the number of RREQ allowed in a given time). If the frequency of the RREQ generated by a neighbor exceeds the threshold the neighbor is blocked for any more RREQ's, this was firstly proposed in 2006. In this scheme "Legal nodes can distinguish illegal nodes and refuse to forward packages for them, so flooding attack can be defended".

2) FAP(Flooding attack Prevention): FAP is a technique that has two methods to resist the flooding attack in Ad Hoc network. Firstly, to suppress the neighbors, this method is used to prevent RREQ flooding attack. Since the MANETs are multi-hop wireless networks, the node can send and receive packets from its neighbor nodes. If these neighbor nodes around the node refuse to receive its packets, this node cannot communicate with the others in MANET. By this way, the node has been isolated from the other nodes in the network, this is known as neighbor suppression and shown in Figure 5.

NS-3

In this research, the simulation tool used for analysis is NS-3.14. This simulator is highly preferred for academic networking research since it demonstrated the best overall performance.

IV. RESEARCH OBJECTIVE

The research Objective is to Simulation of Security Attacks and Preventions on AODV Protocol in NS-3. This paper focuses on the two most important issues in mobile ad hoc networks – Security Attacks and Preventions. Each mobile node in a MANET acts as a router by forwarding the packets in the network. Hence, one of the challenges in the design of routing protocols is that it must be tailored to suit the dynamic nature of the nodes. This chapter discusses some of the other challenges faced by the designers of routing protocols for MANETs. A complete understanding of these issues will help in designing efficient and effective routing protocols. Some of the open challenges in designing a security solution are discussed, elucidating the practical implications with respect to confidentiality, integrity, availability and authenticity. The chapter then focuses on the network layer security and discusses secure routing in MANETs. It also classifies the attacks that are possible against the ordinary routing protocols and gives a threat assessment of the attacks. The second half of the chapter discusses another important aspect of security in MANETs – the key management issue. In particular, the chapter focuses on certificate-based authentication mechanisms. The requirements for an effective certificate-based authentication mechanism are identified, a survey of existing mechanisms is done and they are compared with respect to those requirements.

V. SIMULATION AND SCENARIOS

The experiments were setup to understand the severity of flooding and black hole attacks on MANET nodes running AODV protocol. The topology is explained in next section.

3.1 Topology:

The simulation environment uses Wireless ad hoc network, which consist of 50 nodes. The nodes are users of Wi-Fi physical and MAC layer and the nodes move in a random walk based on the Gaussian Markov Mobility Model [19]. In this model, the velocity of the mobile node is assumed to be correlated over time and modeled as a Gauss-Markov stochastic process. The nodes are set to move with a mean velocity and direction based on a uniform distribution, this model best describes the real world MANETs.TCP is enabled at the wireless nodes to simulate the SYN Flooding attack. The wireless nodes use Wi-Fi physical and MAC layer, the Wi-Fi channel is modeled as a fading channel as implemented in NS-3. At the Internet layer (IP), routing in conjunction with AODV for wireless routing is used. The ns-3 has derived AODV as a sub- class of the Ipv4Routing main class, hence AODV inherits all the functions which are part of the Ipv4 routing and plus the extra methods and functions which are specific to the AODV protocol.

3.2 Performance Parameters:

We recorded three parameters to analyze the performance of AODV nodes under variable rate flooding and black hole attack.

1) Average Time Delay: The delay refers to the time it takes to transmit a packet from its source to its destination, and this time is expressed in seconds. This value is attained by total transmission time divided by the number of packets received. This value is attained by using Delay Jitter Estimation class in NS-3. A time tag is attached to each packet transmitted and when it reaches the destination this information is subtracted from the simulator::Now function which keeps track of the current time.

2) Routing Over Head: This is calculated by Total no of routing bytes transferred over Total no of routing bytes +Total no of data bytes

Overhead = total routing bytes / (routing bytes + data bytes)

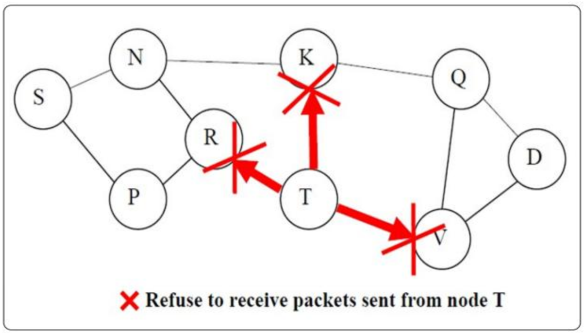


Figure 4. Neighbour Suppression

3) Packet Drop Ratio: This is the ratio of the total number of transmitted packets to the total number of received packets; this is expressed in terms of percentage so the resultant number is then multiplied by 100.

3.3 Node Types:

For the flooding attack, we set up three different scenarios to see the effects of flooding based on node positioning, the type of flooding and valid data packets. Four different types of nodes were used in the simulation. Nodes can have three different roles in these simulation studies:

1) Message Transmitting Node: Wireless nodes sending UDP packets on a user defined port; the transmission is either a unicast message to a particular host or broadcasting to all the nodes on the network.

2) Message Receiver Nodes: These nodes were only listening and receiving the messages on a well-known port, i.e. 80.

3) Flooding Nodes: These are similar to the AODV wireless nodes with a difference that they flood UDP packets on MANET and the destination port is unknown. The flooding nodes were either transmitting to a particular node (unicast) or broadcasting to all the nodes.

4) Black Hole Malicious Node: This node will work as a black hole node, which consumes information and generates fake RREP messages

3.4 Scenarios:

The values chosen for these parameters in running the experiments are the inter-packet interval of flooding messages varied between 1.2 to 0.1 seconds. The reason behind this variance (from the biggest to the lowest number) is to observe the impact of flooding increase on the network performance (the results shown in Figure 7-15)

The three scenarios are as follows:

1) Scenario 1: All the valid data packets and the flooding packets were broadcasted on the network, this was used to analyze the effect of flooding on nodes which work as central or relay nodes.

2) Scenario 2: All the flooding packets were broadcasted but the valid data messages were unicast. This was used as a measure to find the effect of the flooding on the one to one communication between nodes.

3) Scenario 3: The third scenario was setup with both the flooding node and the data transmission nodes sending the messages to a similar node. This was done to analyze the impact of flooding on the processing times of a receiver node which is receiving valid as well as malicious messages.

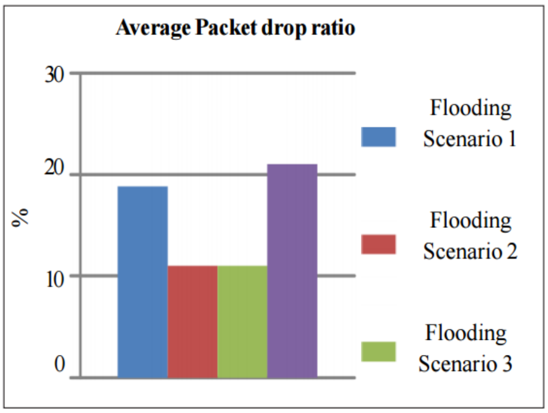


Figure 5. Comparison of Packet drop ratio

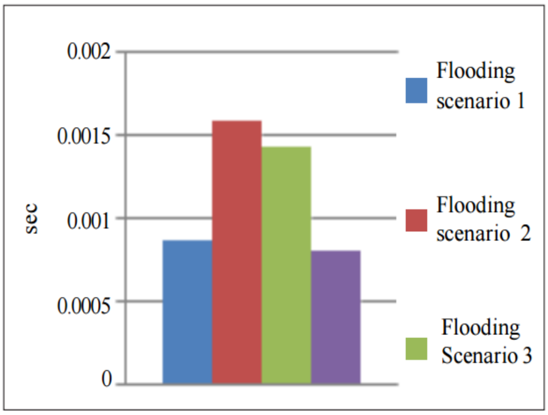
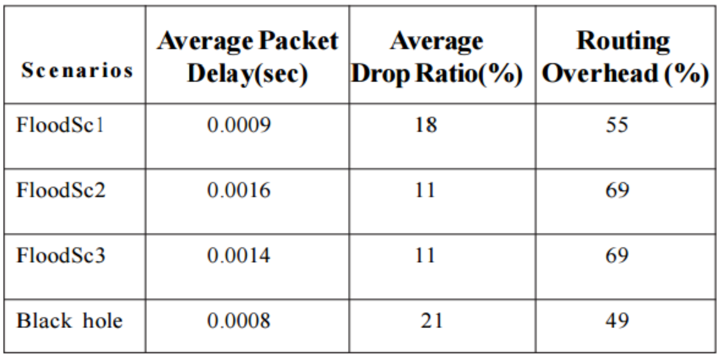


Figure 6. Comparison of Packet delay

4) Malicious Node Scenario: To analyze the behavior of a black hole attack. Malicious nodes are placed in vicinity of different participating nodes. In the black hole attack valid routing packets are dropped and malicious routing packets are generated hence the position of the node in the network is very important. This is why we chose differently located nodes with various mobility directions and analyzed the impact on the network performance.

Table 1. Statistics for security attacks



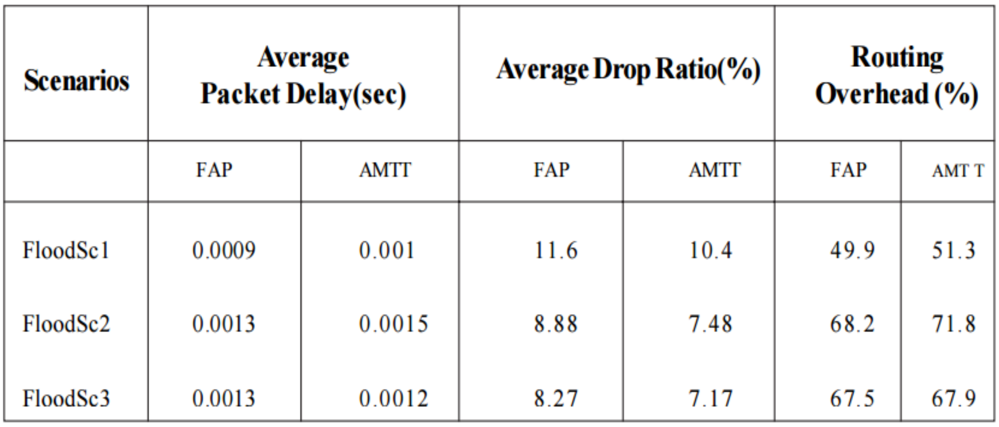
Scenarios	Average Packet Delay(sec)	Average Drop Ratio(%)	Routing Overhead (%)
FloodSc1	0.0009	18	55
FloodSc2	0.0016	11	69
FloodSc3	0.0014	11	69
Black hole	0.0008	21	49

VI. RESULTS

We compare three different set of experiments. Initially the packet drop ratio, average time delay and routing overhead was measured without any attacks for reference. The second set of experiments were conducted with the three different flooding and a black hole attack scenario. The last sets of experiments were with similar attack scenarios but using either FAP or AMTT protection. Figure 5-6 and Table 1 depicts the results in case of all three flooding and a black hole attack. All these change in averages of packet drop, time delay and routing overhead is compared to normal network operation. The results clearly indicate worsening of network performance in attack scenarios. The results for the flooding attacks show a higher average packet delayand routing overhead as compared to black hole attack. The packet drop ratio for flooding scenario 1 and black hole attack is worse than the other flooding scenarios. Figure 7-15 and Table 2 (prevention stats) shows the statistics for the no attack scenario, all the three different flooding scenarios, and with AMTT and FAP prevention implemented separately. AMTT increases the network throughput, compared with FAP, i.e. low packet drop ratio. However, AMTT has a higher routing overhead and prevention schemes have their pros and cons and the choice of each depends on the application scenario/s. In addition, we observed that flooding attack severely depreciates the network performance by dropping valid data packets ranging from 4% to 70% as proportional to the frequency of flooding packets.

A. Error-prone channel state: The characteristics of the links in a wireless network typically vary, and this calls for an interaction between the routing protocol, if necessary, find alternate routes.[4]

Table 2. Statistic with prevention scheme



Scenarios	Average Packet Delay(sec)		Average Drop Ratio(%)		Routing Overhead (%)	
	FAP	AMTT	FAP	AMTT	FAP	AMT T
FloodSc1	0.0009	0.001	11.6	10.4	49.9	51.3
FloodSc2	0.0013	0.0015	8.88	7.48	68.2	71.8
FloodSc3	0.0013	0.0012	8.27	7.17	67.5	67.9

VII. CONCLUSION

This work deals with monitoring the AODV protocol performance for use in MANETs. We showed different scenarios of flooding attack and black hole attack on a MANET with 10 nodes, which are connected on wireless network with random walk. The network performance was evaluated based on packet drop ratio, average packet delay and routing overhead with implementation of no attack and attack scenarios in ns-3. We chose three different flooding attacks with broadcast and unicast packets. The flooding attack severely deteriorates the network performance, packet drop ratio of between 70 to 100% in the unicast scenario. The black hole in comparison had a lower packet drop ratio. Also, average packet delay and routing overhead increased with flooding attack and had a severe effect on the network performance. This work looks into different prevention schemes, which can be effective for countering flooding attacks. We then choose two existing techniques, FAP and AMTT. The results from the FAP showed up to 30 to 35% improvement in packet drop ratio. The average packet delay in some scenarios increases with FAP prevention because of the extra processing time to segregate flooding packets from valid data packets. The routing overhead improves with FAP prevention because the scheme identifies the route from the flooding nodes as malicious and the routing packets, then at the neighboring nodes, are dropped. Similarly, with AMTT, the packet drop ratio has shown some improvement in comparison with FAP; an average decrease of 6 to 10% in the packet drop ratio is observed; however, this comes with a penalty. The timing delays increased to a level of 0.5 to 0.7 ms; also the complexity and the memory usage is quite high. On the other hand, the routing overhead is minimal, when compared to FAP. This is because a similar amount of routing updates and error messages are required as in FAP, but without any overheads.

ACKNOWLEDGMENT

It is a great pleasure for me to express my sincere gratitude to my supervisor, **Dr. Dinesh Kumar,** Professor /Assistant Professor, Department of Computer Science & engineering of Shri Ram College of Engineering & Management, for his valuable guidance, timely advice and constant encouragement during the project work.

REFERENCES

[1] "MANET: Empirical Analysis and Performance Evaluation of Routing Protocol Using NS-2" paper "" **by Raj Singh, Mtech, Dinesh Kumar Asst. Prof. Dept. of computer sci. & Engg., SRCEM,,** Palwal, affiliated to M.D.U Rohtak, Haryana. Published In **Volume 5,** Issue 4, 2015 ISSN: 2277 128X, **Link**: http://www.ijarcsse.com/docs/papers/Volume_5/4_April2015/V5I4-0131.pdf

[2] ”MANET: Security Issues and Behavior Analysis of Routing Protocol Using NS-2” **by Raj Singh, Mtech, Dinesh Kumar Asst. Prof. Dept. of computer sci. & Engg., SRCEM, Palwal, affiliated to M.D.U Rohtak**, Haryana. . Published In Volume 5, Issue 4, 2015 ISSN: 2277 128X, **Link**:http://www.ijarcsse.com/docs/papers/Volume_5/4_April2015/V5I4-0410.pdf

[3] By ‘Upneet Singh1, Mohinder Singh2 and Shanu Malhotra [Volume 3, Issue 5, May 2014] et al, In paper “Performance evaluation of routing protocols under different mobility models over MANETs”

[4] **Rakesh Kumar Jha** Shri Mata Vaishno Devi University In paper “ **A Comparative Performance Analysis of Routing Protocols in MANET using NS3 Simulator** “**Volume 3, March 2015** in MECS

[5] Sachin Dnyandeo Ubarhande, *Performance Evolution of AODV and DSR Routing Protocols in MANET Using NS2*, International Journal of Scientific & Engineering Research Volume 3, Issue 5, May-2012, ISSN 2229-5518

[6] **Mina Vajed Khiavi, Shahram Jamali, Sajjad Jahanbakhsh Gudakahriz,** ***Performance Comparison of AODV, DSDV, DSR and TORA Routing Protocols in MANETs***, International Research Journal of Applied and Basic Sciences. Vol., 3 (7), 1429-1436, 2012 ISSN 2251-838X ©2012 Victor Quest Publications.

[7] Dr.S.S.Dhenakaran1 [February 2013] et al, in paper ‘An Overview of Routing Protocols in Mobile Ad-Hoc Network’

[8] **Supriya Singla Thapar University Patiala, in Paper Performance Comparison of Routing Protocols of MANET in Real World Scenario using NS3 et India** ***Volume 99 – No.14, August 2014*** *International Journal of Computer Applications (0975 – 8887*

[9] S Johnson, D A. Maltz, and Y. Hu[April 2003] "The dynamic source routing protocol for mobile ad hoc network," Internet-Draft,. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt

[10] Samir R. Das, Charles E. Perkins, Elizabeth M. Royer and Mahesh K. Marina. "Performance Comparison of Two On-demand Routing Protocols for Ad hoc Networks." IEEE Personal Communications Magazine special issue on Ad hoc Networking, February 2001,p.16-28.