Black hole Attack Prevention on AODV in MANET

Mrs. Preeti. A. Aware
ME (Comp.Engg) 2nd Year Student
Department of Computer Engineering,
L.R. Tiwari College of Engineering.
University of Mumbai, India.
awarepreeti11@gmail.com

Mrs. Amarja Adgaonkar
Assistant Professor
Department of Computer Engineering,
K.C. College of Engineering and Technology
University of Mumbai, India
amarja_lonikar@yahoo.co.in

***Abstract*—** Wireless networks have become very popular as they provide connectivity to people irrespective of their geographical position. An ad-hoc network is a infrastructure less network where all nodes cooperate to maintain network connectivity. In ad-hoc network when the nodes change their locations dynamically, then it is a mobile ad-hoc network (MANET). Due to Dynamic topology, large degree of freedom, MANET is open to various kinds of attacks like Gray hole, Black hole, Wormhole, Jamming, Sybil, Rushing one of the frequently used attack is the Black hole attack.

A Black hole attack is a most severe attack that can be easily used against routing in mobile ad hoc networks. It is a malicious node that falsely replies for any route requests claiming it has the shortest path to the destination without having active route to specified destination and drops the receiving packets.

***Keywords*—** Black hole attack, Collaborative Black hole attack, Gray hole attack, Sybil attack, Routing protocols, AODV, Ad hoc networks, MANET.

*****

I. INTRODUCTION

Wireless networks use radio frequencies in air to transmit and receive. The nodes in a wireless network consist of routers and host. Nodes in a mobile network move randomly, such a network is called mobile ad hoc networks (MANET). A mobile ad hoc network (MANET) is a group of mobile devices connected by wireless link without the requirement of fixed common infrastructure in place like wireless access point. Nodes in a MANET enter or vanish from the network rapidly. The biggest challenge faced by MANET is attacks on routing protocol. Nodes in MANET communicate with each other to deliver data. When the nodes are out the communication range of each other then the intermediate nodes act as routers to deliver the packet to the destined node. Each node in a MANET acts as host as well as router. In router mode, the node discovers the route and delivers the data with the help of the routing protocol. [5, 6]

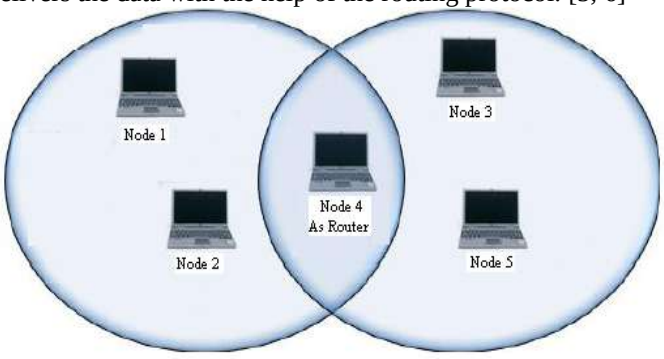

Figure 1: Mobile Ad-Hoc Network with Five Nodes

Figure 1 shows a simple mobile ad-hoc network with five nodes. The outermost nodes are out of the transmitter range of each other. However, the middle node i.e. node 4 can be used to forward packets between the outermost nodes. The middle node is acting as a router and the five nodes have formed a MANET [7].

Further paper is divided in to 7 sections, section II describe about Types of attack, section III Working of AODV routing protocol, section IV explains Black hole and cooperative black hole attack in detail, section V explain about related work, section VI explain the proposed method for prevention of black hole attack, section VII describes conclusion.

II. TYPES OF ATTACKS

There are many limitations of the MANETs like, lack of centralized administration, limited bandwidth, wireless links, dynamic topology, so MANETs are more susceptible to security attacks than existing conventional networks [8]. A network's objectives are confidentiality, availability, integrity. An attacker can break them by active or passive attacks on MANETs [9]. Table II. shows the characteristics and examples of active and passive attacks.

Type of Attack	Characteristics	Examples
Active Attack	• Attempts to change system or affect their operations. • Comparatively easy to detect as they involve modifications	Modifications, DOS, Replay, Masquerader.
Passive Attack	• Attempts to make use of information from the system. • Very difficult to detect.	Release of message content, Traffic Analysis, Traffic monitoring.

Table II Types of Attacks

III.AODV ROUTING PROTOCOL IN MANET

AODV stands for Ad-hoc On demand Distance Vector. AODV does not require nodes to maintain routes to destination. It uses different route messages like Route Request, Route Replies and Route Errors to discover and maintain links. AODV makes use of destination sequence number for each route created by destination node. The nodes communicate with each other by passing "hello" messages periodically to the neighboring nodes. If a node does not receive a reply then it deletes the node from its list and sends Route Error to all the members in the route.

. AODV is a hop by hop routing protocols developed for wireless ad-hoc networks. It offers quick adaptation to low processing, dynamic link conditions, and memory overhead. When a host wants to find a route to a destination it broadcast a route request (RREQ) message. The RREQ contains source addresses destination address, sequence number and a broadcast identifier. Nodes other than destination receiving RREQ message either re-broadcast or respond with route reply (RREP), depending on flags setting in RREQ message. When forwarding a RREQ, node stores broadcast identifier, source address and maintains a reverse route. In order to avoid loop, RREQ are re broadcasted only when a request with the same source address and broadcast identifier has not been processed before. Sequence number is used for updating route. Thus an intermediate host replies with a RREP when it has a fresh enough route to the destination.

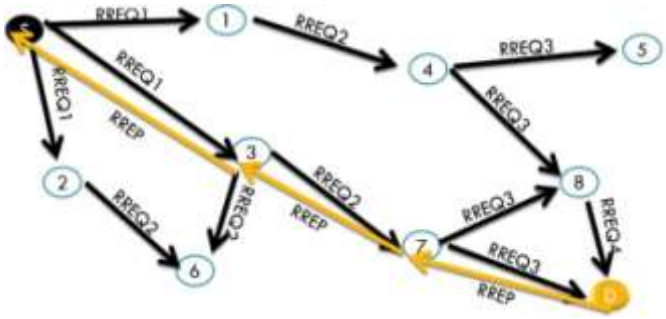

Figure 2. Route Discovery using AODV protocol

In Figure 2. Source node broadcasts RREQ message. Intermediate node creates and maintains a reverse route to the source node. On receiving RREQ, the destination node unicasts RREP to the source. It transmits RREP using the same path that was created during RREQ.

For every RREP control message received, the source node would first check whether it has an entry for the destination in the routing table. If it finds one, the source node would check whether the destination sequence number in the incoming control message is higher than one it sent last in the RREQ. If the destination sequence number is higher, the source node will update its routing table with the new RREP control message; otherwise the RREP control message will be discarded..

The AODV protocol has advantage compared to routing protocols like link-state and distance vector. AODV has greatly reduced the number of routing messages in the network. AODV uses reactive approach to achieve this goal. Reduction in number of routing messages is necessary in an ad-hoc network to get optimal performance when the topology is changing often. The sequence numbers represents the freshness of a route[11]. The sequence numbers avoids loops from being formed. AODV only supports one route for each destination. AODV can be easily modified, to support several routes per destination. When an old route becomes invalid, instead of requesting a new route, the next stored route to that destination could be tried.

The table 2 shows the comparative study of different protocols in MANET

S. N.	Protocol Property	DSDV	DSR	AODV
1	Table driven/ Source Routing	Table driven	Source Routing	Table driven and Source Routing
2	Need of Hello message	Yes	No	Yes
3	Route Discovery	Periodic	On Demand	On Demand
4	Route mechanism/ Maintenance in	Route table with next hop	Complete Route cached	Route table with next hop
5	Network Overhead	High	Low	Medium
6	Node overhead	Medium	High	Medium
7	Network Suitable for	Less number of nodes	Up to 200 nodes	Highly Dynamic
8.	Reactive/ Proactive	Proactive	Reactive	Reactive
9.	Packet size	Uniform	Non Uniform	Uniform

Table 2. Comparative study of routing protocols

From the above table we can conclude that AODV protocol is the most optimal routing protocol.

IV. BLACK HOLE ATTACK

In a black hole attack, malicious node attracts traffic to itself, and then drops those Packets [12]. The situation becomes worse when two or more nodes work as a black hole node.

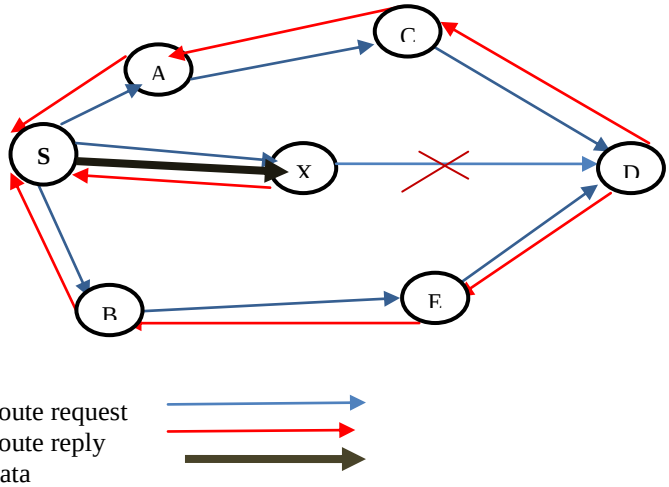

Fig 3. Black Hole Attack

Fig 3 shows how black hole problem arises, here node "S" wants to send data packets to node "D" and initiate the route discovery process to find out the valid route. So if node "X" is a malicious node then it will claim that it has active route to the specified destinations. It will then send the response to node "S" before any other node. In this way node "S" will think that this is the shortest route and thus route discovery is complete. Source node "S" will disregard all other replies and will start sending data packets to node "X" which will drop the received packets. In this way all the data packet will be lost [13].

V. RELATED WORK

M. Abdelshafy &J.B. King [1] proposed a solution for resisting black hole attacks in MANET, using fake RREQ. A node periodically sends fake RREQ from a non existing source node to a non-existing destination node. If a node receives a reply to one of its fake RREQs, The trust level of the node is changed its trust to threat. This solution has a drawback of flooding the entire Network with fake RREQ which increases routing overhead.

Pooja DCSA & R.K. Chauhan [2] proposed an assessment based approach to detect black hole attack in MANET. In this solution hint value of each node is calculated using connection start time and connection end time with the immediate neighboring node. The hint value is compared with a threshold value. The hint value if less than the threshold value, then the node is declared as a black hole node. The drawback of this solution is calculation of the hint value between the neighbouring nodes

Ashish Jain & Vrinda Tokekar [3] proposed a solution for mitigating the effects of Black hole attack by implementing RREP packet caching mechanism. All RREP packets are cached and counted. The first RREP packet is ignored as there is a possibility of Black hole involvement in the path of first RREP packet. The drawback of the solution is all the RREP packets have to be cached in the entire network.

L.Tamilselvanand & V. Sankaranarayan [8] proposed a solution for prevention of the black hole. In this solution they used following strategy: The source node waits for RREP messages from all other neighbor before sending data packets. The source node sets a timer for collecting the RREP messages from neighboring nodes. A table is maintained for all receiving RREP messages. When the assigned time gets over, source node considers and selects the most reliable route containing more repeated common nodes from the table. If repeated nodes are not there, then source node considers route as reliable if the replying node provides information about its next hop in the route. This solution has a drawback of processing delay and causes additional delay for waiting for reply from neighboring node; also if the next hop node is again Black hole then this may not be getting prevented.

M. Dasgupta, D. Santra [9] proposed a solution for preventing Black hole attack in MANET, using CPN model for providing anti Black hole mechanism .In this IDS is used to identify and isolate Black hole node. IDS node is set in the promiscuous mode in order to sniff all routing packets within its transmission range. Depending upon suspicious patterns the Black hole node is prevented from accessing the network. This solution has drawback of the placement of IDS nodes as they should cover entire network which is a difficult task i.e. the problem of placing the IDS node is open, also the suspicious patterns needs to be configured in advance.

Meenakshi Patel, S. Sharma[10] proposed a solution to detect and prevent flooding attacks in MANET using SVM. The system collects the behavior of every node in the network then using this data they are finding the malicious nodes with the predefined threshold set at the starting which is one of the drawback as much time will be wasted for the same .

Supriya Tayal, Viniti Gupta [11] proposed a survey of attacks in MANET on routing protocols mainly AODV. They mentioned AODV is improvement of DSDV and there are many security threats to AODV like active and passive attacks. One of the active attacks is Black hole attack. They concluded that the attacks are open for research.

VI. THE PROPOSED METHOD

In the proposed scheme the source node which is searching for the destination will broadcast the route request (RREQ) message in search of the destination, the source will wait for the multiple messages, then, the first route which is optimal is rejected and the second optimal route for data packets transmission after performing hash authentication is selected, as the first route is always provided by Black hole node present in the network. Black hole node identifies the target and launches the attack so when source node sends route request (RREQ) message to its neighbors the Black hole node without forwarding message to the next hop or destination gives back route reply (RREP) to the source immediately, so its reply reaches first to the source. In the proposed method when source will send the messages to the nearest node for delivering the data to the destination node it first performs the authentication of the nodes and the route which is optimal.

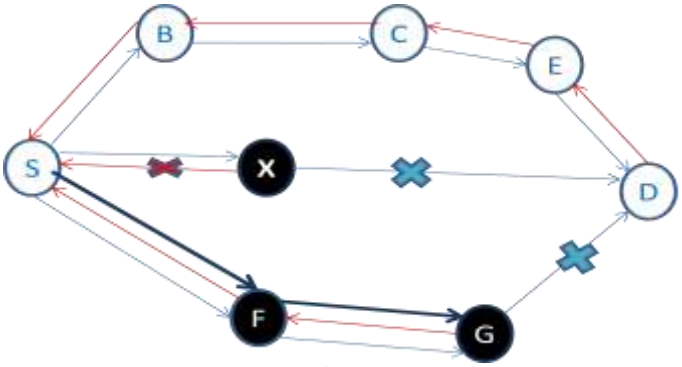

Figure. 4 proposed solution for avoiding black hole attack.

As shown in the figure source node 'S' will broadcast the Route Request (RREQ) message in search of destination node 'D' to all its neighboring nodes like 'B', 'X', 'F' in this figure. On receiving the RREQ from source, all the neighboring nodes will send back Route Reply (RREP) message to the source node. Source node will wait for the multiple RREP and then discards the first RREP thereby accepting the second optimal route to the destination

[3]. In the given figure node 'X' acts as the single black hole and nodes 'F' and 'G' acts as the cooperative black holes. In this the nodes 'X' and 'G' will send the RREP message to the source without looking into its table about the presence of active route to the destination, so its reply reaches the source node at the earliest. In the proposed method the first path is rejected as it's always given by the black hole if it is present. Now the second optimal route is selected i.e. S-F-G-D, but nodes 'F' and 'G' are co operative black holes. To overcome this problem authentication mechanism is provided i.e. node 'G' must give the address of its neighbor which is having active path to the destination node 'D'. In this example node 'G' is not having the active route to the destination so it will not provide address of destination node. Hence cooperative attack in the network is prevented.

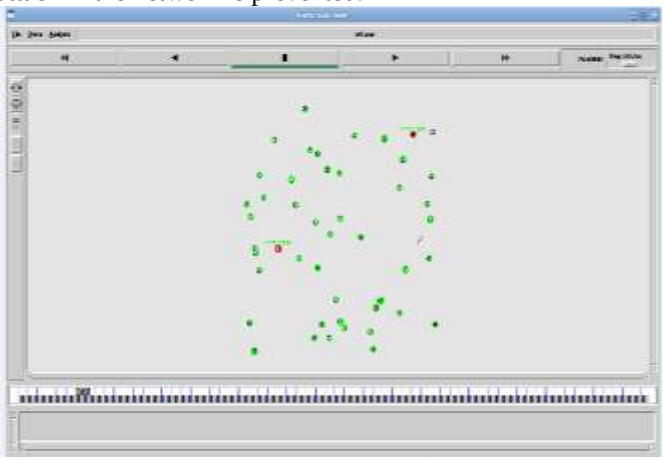

Figure. 5 simulated output of the different nodes.

As shown in the figure, the attacker nodes 14 and 46 works as the black hole for the network. AODV implementation is carried out to deliver the packets from source to destination, in this case source is 11 and destination is 32.

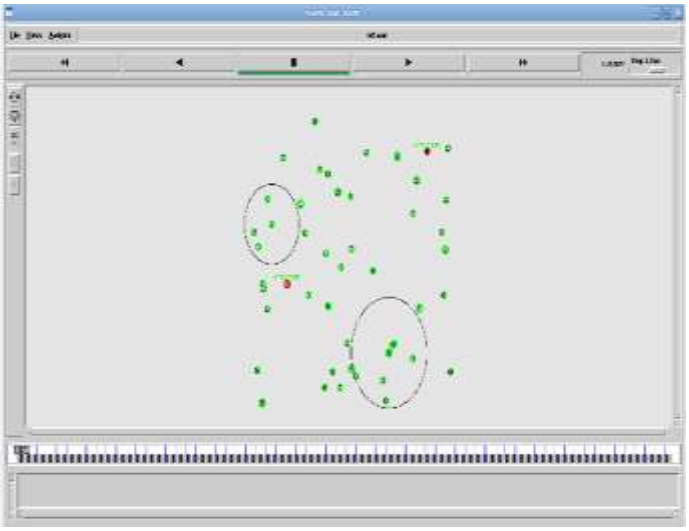

Figure. 6 mobility of the nodes in MANET

Above figure shows the dynamic reloaction of the nodes for one place to another place. Each node is having its own area of operation. The black hole is prevented by using the safest path from the source to destination with the help of hash authentication.

VII. CONCLUSION

In this work, the general working of MANET is shown followed by AODV routing protocol. Also the security issue in MANET been highlighted i.e. Black hole attack . The existing solutions along with their disadvantages are provided; some additional features are added in the proposed work.

The scheme has been proposed to provide better solution to the Black hole problem using AODV in MANET. Black hole attack is one of the major security issues for MANET, the security issue will be tackled here by using hash function. The use of this technique avoids single black hole and cooperative black hole attacks and provides safe route for the transmission of data packets from source to destination node. The mobility of the nodes and the black holes are simulated in the NS-2.

In the future work, the proposed scheme will be further improved related to the prevention of the black hole attack along with increasing the trust level estimate of each node by giving more authentications to each node.

REFERENCES

[1] Mohamed A. Abdelshafy, Peter J.B. King "Resisting Black hole attacks on MANET," IEEE Annual Consumer Communication and networking conference , May 2016.

[2] Pooja D, R.K Chauhan, " An Assessment Based Approach to detect Black Hole attack in MANET," IEEE International Conference on Computing , Communication and Automation, May-2015

[3] Ashish Kumar Jain , Vrinda Tokekar " Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile Ad Hoc Networks, "IEEE International Conference on Pervasive Computing (ICPC) ,May 2015.

[4] Renu Mishra, Dr.Sanjeev Sharma. "Vulnerabilities and security for ad-hoc networks"IEEEInternational Conference on networking and information technology, pp. 192-196, May-2010

[5] Piyush Agrawal and R. K. Ghosh: Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks www.stanford.edu/~piyushag/docs/icuimc08.pdf

[6] Y. Hu, A. Perrig and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, in Proceedings of ACM MobiCom Workshop - WiSe'03,2003

[7] LathaTamilselvan and Dr. V Sankaranarayanan, "Prevention of Black hole Attack in MANET" 2nd IEEE International Conference on Wireless Broadband and Ultra Wideband Communications, pp. 21, 2007.

[8] M. Dasgupta, D. Santra, "Network Modeling of a Black hole Prevention mechanism in MANET," IEEE International Conference on computational intelligence and communication networks, pp. 734-738, Nov-2012.

[9] Meenakshi Patel, S. Sharma. "Detection and Prevention of Flooding Attack Using SVM," IEEE International Conference on communication systems and Network Technology, pp.533-537, May-2013

[10] SupriyaTayal, Viniti Gupta. "A Survey of Attacks on MANET Routing Protocols," International Journal of Innovative Res. in Computer Science Eng. and Technology , Vol.2, Pg. 2280-2285, June-2013.

[11] S.Sun; Y. Guan; J.Chen; U.W. Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Networks," 5th European Personal Mobile Communications Conference, pp. 490-495, 2003.

[12] H. Deng, W. Li and D.P.Agrawal, "Routing security in wireless ad hoc networks," IEEE Communications Magazine, vo1.40, no. I 0, pp. 70- 75, Oct. 2002.

[13] M. Khalili, H. Taheri, S. Vakilinia, "Preventing black hole attack in AODV through use of hash chain", in Proc. of 19th Iranian Conference Electrical Engineering (ICEE), Iran, pp. 1- 6, 2011.