A Survey on AODV Protocol Performance with Black Hole Node in MANET

Alok Rao, Narendra Upadhyay, Vivek Kumar Rai

Abstract: Security is a main concern in any network communication. Because of MANETs special characteristics, it becomes vulnerable to security attacks. MANET has no fixed infrastructure and any centralized system. It has a dynamic topology which randomly changes itself. There are different kinds of security attacks in MANETs. In this we have discussed an attack known as Black Hole attack. In MANETs, AODV is the commonly used routing algorithm, in which black hole attack can easily take place. Black hole attack takes advantage of route discovery process in it and provide wrong route to the source node in MANETs. Many researchers have given different solutions for preventing and detecting this attack. We have discussed some of the proposed solutions in this survey.

Keywords: AODV, MANETs, Collaborative black hole attack, Single black hole attack.

I. INTRODUCTION

Mobile ad hoc networks are wireless self configuring networks. These are the collection of mobile nodes which come together to form a bigger network. MANETs has no fixed infrastructure and any central administration .This can be defined as autonomous system of mobile nodes. Every node here act as a router . MANETs are very easy to implement and have low cost of deployment with respect to other wired networks. MANETs has some special characteristic as limited bandwidth, computation power, changing topology in unpredictable manner, battery, lifetime for communicating to each other nodes. MANETs uses different routing protocols like DSDV, AODV, DSR etc. MANETs are vulnerable to the different security threats like black hole attack, denial of services Routing table overflow, impersonation, energy consummation, information disclosure etc.

II. PROTOCOL USED IN MANETS:

In MANETs nodes communicate with each other byusing some routing protocols. According the dynamic topology and characteristic there are three main routing protocol used in MANETs. These all are discussed below.

2.1 Proactive (table driven) routing protocol: This protocol is also called as table driven protocol because in this protocol each node in the network maintains its detailed routing table.

Manuscript received April, 2013.

Alok Rao, pursuing M.Tech in Information Technology from C-DAC Noida. His interest areas are wireless sensor networks, Mobile Ad hoc network and Operating Systems.

Narendra Upadhyay, pursuing M .Tech in Computer Science from C-DAC Noida. His interest areas are wireless sensor networks, Mobile Adhoc Networks and Vehicular Adhoc Networks

Vivek Kumar Rai, pursuing M.Tech in Information Technology from C-DAC Noida. His interest areas are image processing and networking.

In the routing table each node maintain complete path to the reachable node with its hop count. In this, each node periodically broadcast their routing information to the neighbors. Periodically update and large routing table generate large amount of overhead in the network which makes this protocol unusable. There are two main kind of this protocol optimized link state routing (OLSR) protocol and destination sequenced distance vector routing (DSDV) protocol.

2.2 Reactive (On-Demand) routing protocol: This protocol starts functioning whenever any node wants to transmit data to other node. In this protocol network bandwidth is not wasted and network is less congested. This protocol is less secure than the proactive protocols. Two kinds of protocols are there in it.

2.2.1 Ad hoc On Demand Distance Vector Protocol: AODV (ad hoc on demand distance vector) as the name suggests, it works when any node need to communicate or transmit data to other node. This routing protocol is developed by inheriting the property of DSDV protocol. The protocol uses four types of control messages RREQ, RREP, RERR and HELLO. The format of RREQ and RREP packets are in Fig 1.1 and 1.2 respectively.

Source_ address	Source_ sequence	Broadcas t_id	Destination_ address	Destination_ sequence	Hop_ count

Fig 1.1 RREQ

Packet format RREQ packet contains source address, destination address, source sequence number, destination sequence number and hop count.

Source_ad dress	Destination_ address	Destination _ sequence	Hop_ count	Lifetime

Fig 1.2 RREP

Packet format RREQ packet contains source address, destination address, destination sequence number, hop count and life time.

In this protocol every node only records next hop information in its routing table. When a node (sender) needs to send data to other node (Destination) and destination node is unreachable from sender then route discovery process is started. In this process first of all it will initialize a RREQ for getting the route. It broadcasts RREQ to all its neighbors, all the intermediate nodes receive RREQ. If there is any node which has fresh route to the destination then it sends RREP to the sender, when sender finds RREP it immediately starts sending data to that node which sent RREP to the sender .Whenever there is topology change or connection failure in network route maintenance process is started for it source node informed by the RERR packet then it utilizes routing information to decide other routing path or restart the route discovery process.

2.2.2 Dynamic Source Routing Protocol: DSR (Dynamic source routing) This is based on source routing. In this each data packet contains the routing path from source to destination in their headers. In AODV protocol node records only next hop information in its routing table but in DSR every node records their route cache from source to destination node. In this routing path can be determined by source node. Performance of DSR decreases when mobility of node is increases.

2.3 Hybrid Routing Protocol: This protocol combines advantages of both proactive and reactive routing protocol. Two types are: Zone routing protocol (ZRP) and temporally ordered Routing protocol (TORA). At the initialization phase this follows proactive characteristic after that in between when network topology has changed it follows reactive characteristic

III. BLACK HOLE ATTACK:

Like matter disappears in black hole, in the same way data packets disappear at a node behaving as a black hole node in the MANETs. Black hole attack is a big problem in MANETs in which an intermediate node works as malicious and consumes data before reaching to the destination. Black hole attack works in two phases in first phase, it advertises that it has a fresh route to the destination to deliver data packets with intention to drop data packets. In second phase it drops data packets without forwarding it. In this whenever any intermediate node gets a RREQ it immediately generates a RREP with high destination sequence number and sends it to the initiator. (Source) source stops receiving RREP and starts sending data packet to that node which has sent RREP to the source there are two kind of black hole attack

3.1 Single black hole attack: In this malicious node individually works as a black bole node. This black hole is easy to detect in comparison with cooperative black hole attack.

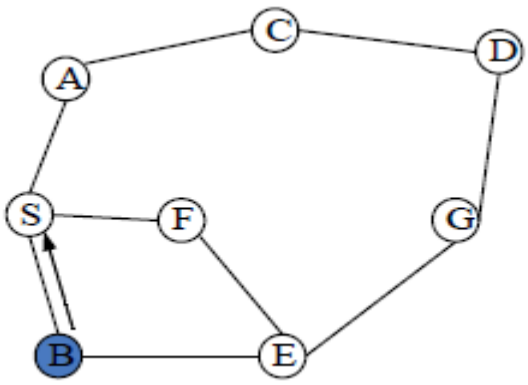

Fig 3.1

As shown in figure 3.1 B node is working as black hole node in the network. In this whenever source node S wants data to transmit to other node as D, it broadcasts RREQ to its neighbors and after it reaches B, B immediately sends RREP to S via route B-S. Source receives RREP and starts sending data packets to the node B which consumes data packets instead of forwarding it.

3.2 Cooperative black hole attack: In cooperative black hole attack, there are more than one black hole nodes working in group. It is more complex to detect cooperative black hole attack than single black hole attack. In the given figure node B1 and B2 are working in group. In this first black hole node B1 refers to B2 as next hop the source node sends further request (Frq) to B2 via different route other than via B1. Node S ask to B2 that it has a route to B1 and destination D.

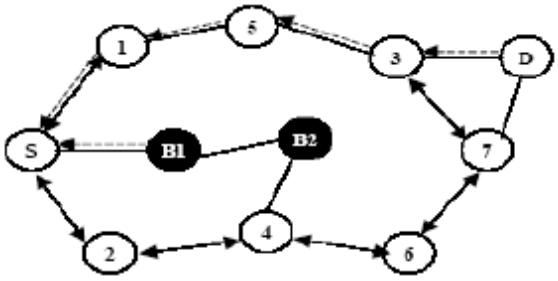

Fig 3.2

B2 and B1 are working in coordination so the answer will be yes and with further Reply (FRp). Now S starts sending data packets assuming that S-B1-B2 is secure route but data packets are finally dropped by black hole node B1.

3.3 Utilization of TCP characteristic with new layer (ATCP) insertion between TCP and IP [5].

Jian Leu and Suresh Singh proposed an approach for utilizing the TCP characteristic and network layer feedback. This approach is for using TCP in mobile ad hoc networks without any affect on the throughput And network performance. In this original TCP is not changed while inserting a new layer ATCP between IP and TCP. This monitors network state information provided by ECN and ICMP " Destination unreachable " messages and attach TCP at sender side.ECN is used as a mechanism by which sender is notified of impeding network congestion along the route followed by the TCP connection.

Nodes can interoperate with each other either by TCP or ATCP. But in this, a node having no ATCP faces same problem when using TCP in MANETs.

The main features of ATCP which are discussed in this approach are -

1. TCP/IP exists in its original form.
2. ATCP does not affect functions of original TCP.
3. End-to -End semantics are maintained.
4. This does not affect congestion control mechanism of TCP.
5. With use of large files the behavior of ATCP is ideal.

3.4 Black hole avoidance by new parameter generation based on previous property [19].

Houssein Hallani and Seyed A. Shahrestani proposed an approach in which a new routing protocol BAODV is proposed for MANETs. Here simulation studies are carried out by OPNET Modeler V11.5 in BAODV source node tries to find a secure route which is free from malicious node

It is generated by adding new parameter in old AODV protocol related with old property

This parameter is incremented and decremented based on node's packet transmission. The route discovery in BAODV is based on the parameter size. This selects a route from source to destination, in the same as the original AODV, but in this protocol a source node after receiving route reply packets from multiple nodes, selects the node which has the highest parameter which shows trustworthiness for a secure route. In BAODV, parameter is just updated without any

need of the acknowledgement of packet receiving. There is a possibility that an intermediate node may forward packet to the node which is not a member of the existing route. This is confirmed by checking the acknowledgement sent back from the destination to the source node. After acknowledgement packet is received by an intermediate node it extracts record corresponding IP address of the packet this record contains previous and next hop nodes of the packet IP address. If the information matches acknowledgement, it is forwarded to the previous node otherwise intermediate node decrements the parameter of the node that delivered acknowledgement and aborts the packet.

With this approach there is significant improvement in reliability and performance of the wireless ad hoc network in the presence of malicious or selfish node. When there are 40% malicious node present in the network in stationary or mobile state, the throughput increases by 11% and 13% respectively.

3.5 A Reverse AODV Routing Protocol [3].

Chonggun Kim, Elmurod Talipov, and Byoungchul Ahn proposed an approach which is called Reverse AODV protocol. They used ns-2 simulator for simulating the protocol. In this, recovery of route is different from original AODV protocol. In this protocol source and destination plays same role. In this when sender asked for route by flooding RREQ to its neighbor then this RREQ reaches to the destination node at the destination again Reverse RREQ is generated which follow the reverse path to the sender. When sender finds R-REQ immediately packet transmission is started. In this protocol when R-REQ is received by sender it compares the sequence number of the R-REQs when the sequence number is greater than already existed R-RREQ then It selects the path which has the less number of hop count.

The performance of this protocol is measured by analyzing four parameters. End to end delay in this protocol is lower than the existing protocol because R-AODV select routes based on reverse request. There is is less energy consumption in this protocol .packet delivery ratio is also increases by using this protocol. There is more overhead generated by control messages in this protocol.

3.6 Additional route maintenance method [13].

Rajib Das, Dr. Bipul Shyam Purkayastha, Dr. Prodipto Das proposed an approach to check whether intermediate node which generated RREP to the source node has a route to destination or not. Source node receives the FurtherReply (FRp) from next hop, It compares results from the reply packet. If it is yes then route establishment takes place and data packets are sent. If there is no route from next hop to inquired intermediate node and has a route to the destination, route reply packets will be discarded from inquired intermediate node. The new route through next hop to destination is followed. An alarm message to whole network will be sent out. If there is no route through next hop to the inquired intermediate node and to the destination a new RREQ will be generated at this stage for new route discovery process. And an alarm message is sent out to isolate the malicious node. Now whole network is prevented from black hole attack and black hole attack is avoided. This approach cannot be applied on cooperative black hole attack.

There is another method proposed in this paper to avoid cooperative black hole attack, the technique works with modified AODV protocol in which another data routing information (DRI) table is maintained.

NS-2 simulator is used in this for simulation of network, the parameter is used CBR (Constant Bit Rate), 30 mobile nodes, 500 by 500 square meter area, Node transmission power is 250 meter pause time is 30 seconds, packet size is 512 bytes. We have taken two metrics like Packet delivery Ratio, Throughput. These are measured with varying number of nodes. The simulation is done using ns-2.35 simulator. Results are discussed bellow –

1-**Packet Delivery ratio** for AODV protocol is measured with black hole and without black hole attack, while increasing node density. Packet delivery Ratio decreases when malicious node is present in the network. As Packet Delivery Ratio is 100% without black hole in network it decreases to 82% when there is one black hole node in network.

2- **Throughput** also decreases when there is black hole in network comparison with no black hole node in the network.

IV. CONCLUSION

This survey is aimed at finding performance of AODV under black hole attack in MANETs. We have reviewed and concluded many of the existing solutions with their pros and cons. AODV protocol is the most popular routing protocol for MANETs, but because of black hole presence, the performance of network decrease. In this paper, we have analyzed result of the solutions as Packet delivery Ratio, Packet loss, end-to-end Delay which is different in each of the proposed solution. Black hole problem is still in research work. This paper will help researchers to realize the current status of the black hole attack research and its effect on the AODV protocol used in MANETs.

REFERENCES

[1] Naseer Ali Husieen, Osman B Ghazali, Suhaidi Hassan, Mohammed M. Kadhum "Route Cache Update Mechanisms in DSR Protocol – A Survey" *2011 International Conference on Information and Network Technology IACSIT Press, Singapore.*

[2]. IRSHAD ULLAH SHOAIB UR REHMAN " Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols" Master Thesis Electrical Engineering Thesis no: MEE 10:62 June, 2010.

[3] Chonggun Kim, Elmurod Talipov, and Byoungchul Ahn "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks" IFIP International Federation for Information Processing 2006.

[4] Rachit Jain1, Laxmi Shrivastava "Study and Performance Comparison of AODV & DSR on the basis of Path Loss Propagation Models" International Journal of Advanced Science and Technology Vol. 32, July, 2011.

[5]. Jian Liu, Member, IEEE, and Suresh Singh, Member, IEEE "ATCP: TCP for Mobile Ad Hoc Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 19, NO. 7, JULY 2001.

[6]. Saurabh Gupta,Subrat Kar, S Dharmaraja "BAAP: Blackhole Attack Avoidance Protocol for Wireless Network"International Conference on Computer & Communication Technology (ICCCT)-2011.

[7]. Manveen Singh Chadha, Rambir Joon, Sandeep "Simulation and Comparison of AODV, DSR and AOMDV Routing Protocols in MANETs" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[8]. Mr.Nirmal Singh1, Mrs.Mamta Katiyar "Performance Analysis of AODV and DSR Routing Protocols in MANET'S" International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 6, November 2012.

[9]. Sahil Gupta, Sunanda Arora, Gaurav Banga "Simulation Based Performance Comparison of AODV and DSR Routing Protocols in MANETS" International Journal of Applied Engineering Research, ISSN 0973-4562 Vol.7 No.11 (2012).

[10]. http://www.ietf.org/rfc/rfc3561.txt (last accessed 02/04/2013).
[11]. http://moment.cs.ucsb.edu/AODV/ (last accessed 30/03/2013).
[12]. Vikas Solomon Abel "Survey of Attacks on Mobile AdhocWireless Networks" International Journal on Computer Science and Engineering (IJCSE) ISSN: 0975-3397 Vol. 3 No. 2 Feb 2011.
[13]. Rajib Das, Dr. Bipul Shyam Purkayastha, Dr. Prodipto Das "Security Measures for Black Hole Attack in MANET: An Approach" International Journal of Engineering Science and Technology (IJEST) ISSN: 0975-5462 Vol. 3 No. 4 Apr 2011.
[14] Jhao Min, Zhou Jiliu "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks" 2009 International Symposium on Information Engineering and Electronic Commerce.
[15] Mehdi Medadian, Ahmad Mebadi, Elham Shahri "Combat with Black Hole Attack in AODV Routing Protocol" Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications 15 -17 December 2009 Kuala Lumpur Malaysia.
[16] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks" 2012 Second International Conference on Advanced Computing & Communication Technologies.
[17] U.Venkanna, R.Leela Velusami "BLACK HOLE ATTACK AND THEIR COUNTER MEASURE BASED ON TRUST MANAGEMENT IN MANET: A SURVEY" Proc. of1nt. Con/, on Advances in Recent Technologies in Communication and Computing 2011.
[18] Namhoon Kim, Saehoon Kang, Younghee Lee, and Ben Lee "Name-Based Autoconfiguration for Mobile Ad hoc Networks" ETRI Journal, Volume 28, Number 2, April 2006.
[19] Houssein Hallani and Seyed A. Shahrestani "Improving the Reliability of Ad-hoc on Demand Distance Vector Protocol" WSEAS TRANSACTIONS on COMMUNICATIONS, ISSN: 1109-2742 Issue 7, Volume 7, July 2008.

Alok Rao, pursuing M.Tech in Information Technology from C-DAC Noida. His interest areas are wireless sensor networks, Mobile Ad hoc network and Operating Systems.

Narendra Upadhyay, pursuing M .Tech in Computer Science from C-DAC Noida. His interest areas are wireless sensor networks, Mobile Adhoc Networks and Vehicular Adhoc Networks

Vivek Kumar Rai, pursuing M.Tech in Information Technology from C-DAC Noida. His interest areas are image processing and networking.