International Journal on Future Revolution in Computer Science & Communication Engineering ISSN: 2454-4248
Volume: 4 Issue: 1 337 – 340

A Comparison of AODV Routing Protocols to Prevent Black Hole Attack in Manet

1* Saket2# Satish Kumar Negi3#Pushpendra Kumar Chandra

*Student (B. Tech _ 4th year), Department of Computer Science and Engineering (CSE), Institute of Technology, Guru Ghasidas Vishwavidyalaya, Bilaspur,Chattisgarh, India

Assistant Professor, Department of Computer Science and Engineering (CSE), Institute Of Technology, Guru Ghasidas Vishwavidyalaya, Bilaspur,Chattisgarh, India

*1*saketkumar2511@gmail.com 2#skn.ggv@gmail.com3#pushpendrachandra@gmail.com*

Absract Mobile ad hoc network (**MANET)** is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly.Due to limited power supply, physical infrastructure and absence of central base station, malicious nodes can easily disguise themselves among the legitimate nodes. So MANET is vulnerable to many security threats, among which one is the blackhole attack. In this attack, the malicious node misuses the protocols to advertise the shortest path to destination node and drops the data packets subsequently. It deterioates the performance of the network, which is based on many factors including Packet Delivery Ratio and End-to-End Delay. Many effective techniques for detecting the blackhole attack have been devised. Among them are the solutions based on Ad-hoc On demand Distance Vector (AODV) Routing. In this review paper a comparison is done between three such solutions- CBDAODV, MOSAODV and DPRAODV based on two performance criteria mentioned above.

Keywords *Mobile ad hoc network , AODV , CBDAODV , DPRAODV , End-to-End Delay , Packet Deivery Ratio*

*****

1 Introduction

I. MANET

A mobile ad hoc network (**MANET**), also known as wireless ad hoc network or ad hoc wireless network, is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly [1]. Because of dynamic movement of mobile nodes network topology is continuously changing. So a MANET can be considered as a highly dynamic, autonomous topology . MANETs are a kind of wireless ad hoc network (WANET) that usually has a routable networking environment on top of a link layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network. MANET has the following primary characteristics [2]: dynamic topology due to node mobility, resource constraints, limited physical security and no infrastructure.

A wide commercial implementation of MANET is yet to be achieved, due to the challenges involving various aspects such as security, reliability, power consumption, inter-networking and location-aided routing [3]. Various protocols used to implement MANETs are compared on basis of their performance, with varying parameters such as number of sensor nodes, number of sources, topology of network, mobility of nodes. The judging criteria are the factors such as packet delivery ratio , scalability, the routing overhead introduced, energy consumed by the network,etc.

With increasing deployment and usage on military operations, home networking, and vehicular traffic management systems, security of MANET has become an important issue. Since network management and operations in MANET are dependent on cooperation of all mobile nodes, it is very easy for a MANET to encounter security threats and various attacks.

II. Routing Protocols

MANET has a variety of routing protocols. On the basis of how routing information is distributed among nodes of the network, routing protocols are mainly classified into two types [4]:

a) Proactive Routing Protocol

It is also known as table-driven routing protocol. In this protocol the routing table of each node contains the list of adjacent nodes, reachable nodes and number of jumps needed. Thus each node has to store huge amount of information with every topology change. Thus, the limitation of this method is the drastic rise in the communication overhead with the increase in network size. But a major advantage is that the entry of any malicious node is immediately reflected in the network. One example of this type of protocol is the Destination Sequenced Distance Vector (DSDV) routing protocol.

b) Reactive Routing Protocol

Unlike the above protocol, this protocol starts when nodes need to transfer information to other nodes. The advantage of the method is that the communication overhead is less as compared to any proactive routing protocol. Two popular examples in this category are Ad-hoc On Demand Distance Vector(AODV) Routing and Dynamic Source Routing (DSR). AODV is one of the reactive protocols for MANET. It decreases routing load by constructing route only on demand [5]. The routing algorithm is location independent [6]. It allows dynamic and self-initialized routing between nodes longing to establish and maintain an ad-hoc network.

 ISSN: 2454-4248
337 – 340

Each node in AODV has a sequence number, which can be defined as a monotonously growing number which makes sure that there are no cycles in the routing path used.AODV defines 3 message types [7]:

1) Route Requests (RREQs)
i) Route discovery process begins when the source node creates the RREQ packet. The packet contains: source node's IP address, source node's current sequence number, destination IP address, destination sequence number. Besides this each packet also contains a broadcast ID number which is incremented by one every time source node generates RREQ.
ii) Each RREQ is uniquely identified by the broadcast ID and source IP address.

2) Route Replies (RREPs)
RREP packet is created by a node when it has a current route to respond to the RREQ packet sent by a source. RREP can be of two types:
i) RREP sent by destination : It will contain the following fields:Source IP address, Destination IP address, current sequence number of the destination, hop-count=0,life time.
ii) RREP sent by intermediate node : It will contain the following fields:Source IP address, Destination IP address, sequence number of the destination, hop-count=its distance from destination, life time. Here hop-count is the distance of the intermediate node from destination node.

3) Route Errors (RERRs)
i) RREP packet is generated by a source node if it detects a link failure in the network. The RERR message is delivered to all affected destinations.
ii) All the nodes that were using that link suffer the consequences of the failure and hence they are listed in the RERR message. Any node getting the RERR message marks that route the destination as invalid. A source node restarts the route discovery process upon receiving an RERR message.
AODV allows for the construction of routes to specific destinations and does not require that nodes keep these routes when they are not in active communication. AODV avoids the "counting to infinity" problem by using destination sequence numbers. This makes AODV loop free.
Apart from proactive and reactive protocols, there is a third type of routing protocol called hybrid routing protocol, which both of the above mentioned protocols. Zone Routing protocol is one example of hybrid protocol [8]. Ad-hoc networks, due to their improvised nature, are frequently established in insecure environments, which makes them susceptible to attacks [9]. One of the prominent attacks is the blackhole attack.

III. Blackhole Attack

In blackhole attack, the malicious node advertises that it has the shortest route to the destination node specified in the RREQ packet sent by the source node [10]. So, the source node sends its data packets to the malicious node which, in turn, drops all those packets continuously [11].When the source node sends RREQ packets to its in route discovery process, malicious nodes respond immediately by sending an RREP packet with high destination sequence number ,without referring the routing table.So, assuming that route discovery process is complete, the source node selects the path containing the malicious node to send its data packets which are dropped by it. So, this attack comes under a category of Denial of Service attack.

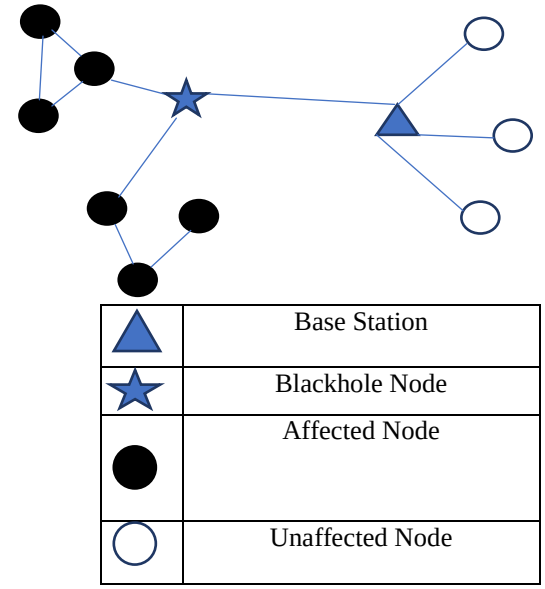

Fig1: Blackhole Attack

Cooperative black hole attack is the modified version of blackhole attack. However,this attack requires at least two malicious nodes to succeed. The two (or more) malicious nodes must be immediate neighbours. The node nearer to the source node is the first malicious node and the other one is the second malicious node. The attack begins when first malicious node secures a communication route with the source node. Thus a route connecting the source node,first malicious node and the second malicious node is formed and data packets sent through this route reach the first malicious node which in turn will forward the received data packets to the second malicious node through the directly connected wireless link.Then the received data packets are dropped by the second malicious node which marks the success of the attack .This attack is hard to detect because the data packets are transmitted normally by the first malicious node rather than being directly dropped. So any suspicion is not aroused against first malicious node for very long time .Meanwhile the second malicious node continuously keeps dropping the data packets [12].

2 Overview of CBDAODV , MOSAODV and DPRAODV

In CBDAODV [12], a minimum of two RREP packets are received from all replying nodes; therefore, the source node knows two routes to reach the destination. The source node uses another routing path to verify the fidelity of selected path and changes the route if the fidelity of currently chosen route appears less. A confirmation control packet is invented by CBDAODV for the source node to send through another route, assumed to be slower than the selected one, to the destination node. The confirmation packet contains the

 ISSN: 2454-4248
337 – 340

name of the second malicious node which is observed and recorded by the source node when the first malicious node sends corresponding data packets to the second malicious node. Once receiving the confirmation packet, the destination node will reply it to indicate whether there exists a path connecting the destination node and the second malicious node. If the reply packet reveals that there is no route between the destination node and the second malicious node, then the source node will know the second malicious node is a malicious node and it is executing a black hole attack. Then the alternate path is used to retransmit the data packets. At the same time, the source node will put the first malicious node into observation; if this malicious node regularly uses the second malicious node as its next hop destination for all upcoming routing paths requested by the source node, then the source node can identify the first malicious node is belonging to the cooperative black hole attack group.

In MOSAODV [13], the source node collects all the RREP packets for a fixed interval and those packets having enormously high destination sequence number are discarded. But all these RREP packets are not stored directly in the routing table of the source node. A separate table is created for storing all RREPs which arrive until half the time for which the source node waits for RREP before regenerating RREQ. The source node after receiving first RREP control message waits for modified wait time. In the meanwhile , all incoming RREPs are feeded to a newly formed table. Afterwards, all these requests are examined by the source. The destination sequence number of all the collected RREP packets are compared among each other and the RREP packets which have unusually high destination sequence number are discarded. The node from which the RREP came is suspected to be a blackhole and any further packets sent by are discarded. This method is definitely an improvement over normal AODV, but it also increases the normalized routing overhead [14].

DPRAODV [15] is yet another method proposed to detect black hole attacks in ad-hoc networks. Usually in AODV , the sequence number of the received RREP packet is checked against the value of sequence number in routing table of the source. The RREP packet is acknowledged, in the event that it has RREP sequence number greater than the value stored in the sequence number field of the table. It is further checked whether the RREP sequence number is greater than an edge esteem (threshold value) and all such RREP packets are discarded. The threshold value is regularly modified in every time interval. The node from which is treated as malicious and is added to the discard list. Once a node is discarded an ALARM packet is sent to its neighbours ,containing the discarded node as a parameter. The neighbouring nodes after receiving the alarm packet identify the blackhole node and then all RREP packets sent from that node are ignored by them. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. This method is considered good because threshold number is updated with time. If the initial data regarding the threshold values of various nodes in the network are used throughout the mechanism without updating it, the adaptation of system to the changing topology and environment would be impossible. This will a major problem since in AODV the topology changes continuously as the new routes are forged regularly between sensor nodes along with the demolition of older and longer routes. Therefore updation is necessary so that any new node formed in the route which gets the RREP packet for the first time gets the latest value of threshold value. So this protocol also helps in preventing further blackhole attacks by updating the threshold value representing the real time environment. On the other hand, the routing overhead of the network is increased significantly due to the regular updation of threshold value at each interval [16].

3 Comparison and Results

A. Comparison Environment and Parameters

Based on the simulation results using networksimulator ns2, by varying the number of nodesfrom 10 to 70 , moving in an area of 800m x 800m , the comparison between the following two performance parameters is done, namely Packet Delivery Ratio and End to End Delay. Packet Delivery Ratio is defined as the ratio of the numberof data packets delivered to the destination to the number of data packets sent by the source.End to End Delay is the time it takes for a sent data packet to reach the destination.

B. Analysis and Results

Based on Packet Delivery Ratio

TABLE I : Comparison Based on Packet Delivery Ratio

METHOD MOBILITY (M/S)	MOSAODV	CBDAODV	DPRAODV
10	1	0.8	1
20	1	0.75	0.99
30	1	0.75	0.95
40	1	0.7	0.92
50	1	0.7	0.9
60	0.99	0.725	0.85

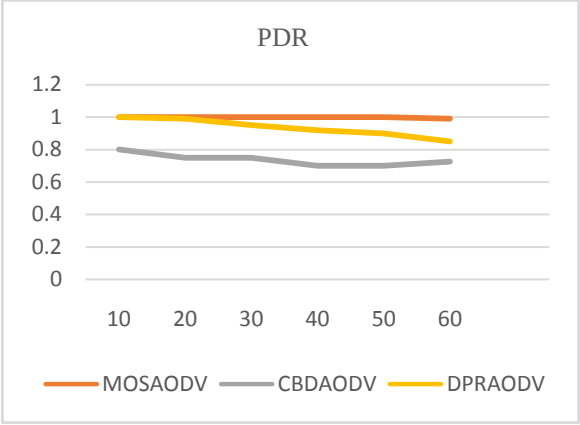

Fig. 2: Comparison of Packet Delivery Ratio

 ISSN: 2454-4248
337 – 340

From Fig. 2, we can see that in terms of Packet Delivery Ratio (PDR) , MOSAODV gives the best performance followed by DPRAODV while CBDAODV has the lowest PDR among the three methods. The average packet delivery ratio of MOSAODV is 35.36% and 6.77% higher than CBDAODV and DPRAODV respectively.

Based on End – to – End Delay(seconds)

TABLE II : Comparison Based on End to End Delay

METHOD / MOBILITY (M/S)	MOSAODV	CBDAODV	DPRAODV
10	0.055	0.0175	0.015
20	0.0575	0.025	0.04
30	0.06	0.0225	0.042
40	0.065	0.0225	0.05
50	0.0575	0.0225	0.059
60	0.08	0.027	0.06

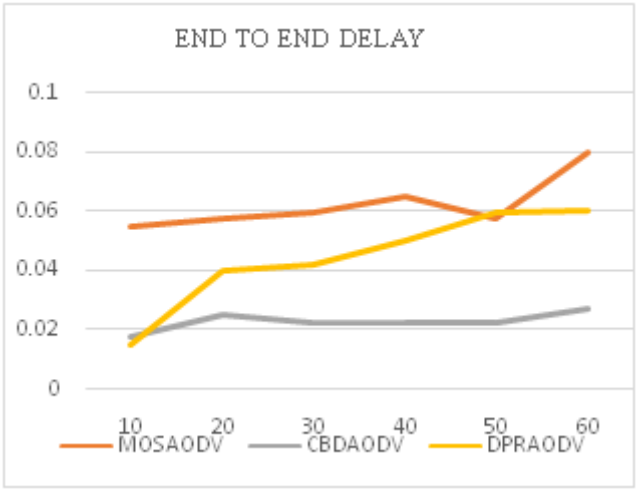

Fig 3: Comparison of End to End Delay

From Fig. 3, it is clear that CBDAODV has the least average End to End Delay, followed by DPRAODV whereas MOSAODV has the highest End to End Delay .The average End to End Delay of CBDAODV is 63.46% and 48.49% lower than the MOSAODV and DPRAODV respectively. This happens because in DPRAODV and MOSAODV the value of sequence number of packet has to be checked before accepting it, whereas in CBDAODV no checking is done.

4 Conclusion

In this study, it was concluded that MOSAODV is better than the other two algorithms (namely CBDAODV and DPRAODV) if we compare the three on the basis of Packet Delivery Ratio.When we compare them on the basis of End-to-End Delay,CBDAODV has the lowest end to end delay . On the other hand, DPRAODV lies in between the two methods in case of both Packet Delivery Ratio and End-to-End Delay.So,we can say that if we are concerned only about the throughput then MOSAODV is the best choice among them but if we want to minimize End-to-End Delay ,then CBDAODV is the best choice. DPRAODV gives average reading on both the parameters.

References

[1] Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, "*Performance Analysis of AODV Routing Protocol in MANET under the Influence of Routing Attacks*", 2nd International Conference on Electrical and Information Technologies ICEIT, 2016

[2] H. Yang, H. Luo, F.Ye, S Lu, and L. Zhang, "*Security in Mobile Ad Hoc Networks: Challenges and Solutions*", IEEE Wireless Communications, Vol. 11, No. 1, 2004, pp. 38-47.

[3] Manoj Kumar Khinchi, Dr. Bharat Bhushan, " *Investigation on MANET Routing Protocols and Quality of Services Management Issues*", International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 04, Apr-2016.

[4] Sunil Kumar Jangir and Naveen Hemrajani , "*A Comprehensive Review and Performance Evaluation of Detection Techniques of Black Hole Attack in MANET"*, Journal of Computer Science. Volume 13, Issue 10, pp. 537-547

[5] C.E. Perkins, E.M. Royer, I.D. Chakeres, *"Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol"*, draft-perkinmanet-aodvbis-OO.txt, Oct. 2003.

[6] Q. Nadia, S. Fatin, A. Hamid, "*Mobile Ad Hoc Networking Protocols' Evaluation Through Simulation for Quality of Services*", IAENG International Journal of Computer Science, 36: 1, IJCS_36_1_10, Feb. 2009.

[7] H. P. Wang and L. Cui, "*An Enhanced AODV for Mobile Ad Hoc Network*" ,7th International Conference on Machine Learning and Cybernetics, Kunming, China, 12-15 July 2008, pp. 1135-1140.

[8] Ankita V. Rachh, Yatin V. Shukla, Tejas R. Rohit, *" A Novel Approach for Detection of Blackhole Attacks"* ,IOSR Journal of Computer Engineering (IOSR-JCE) , Volume 16, Issue 2, Ver. V , Mar-Apr. 2014 ,pp. 69-74

[9] A. A. Pirzada and C. McDonald, *"Secure Routing with the AODV Protocol" ,2005 Asia-Pacific Conference on Communications*, Perth, WA, 2005, pp. 57-61.

[10] Nital Mistry, Devesh C Jinwala, "*Improving AODV Protocol against Blackhole Attacks*", International MultiConference Of Engineers and Computer Scientists 2010 ,Vol 2 IMECS 2010,March 17 - 19, *2010*.

[11] J. CAI, P. YI, J. CHEN, Z. WANG, N. LIU, "*An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Networks* ", 2010 24th IEEE International Conference on Advanced Information networking and Application,2010.

[12] Nai-Wei Lo and Fang-Ling Liu *"A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET*",Vol 234, 2013, pp. 59-65

[13] Mistry N. H., Jinwala D. C., Zaveri M. A., "*MOSAODV: Solution to Secure AODV against Blackhole Attack", International Journal of Computer Science and Network Security*,Vol. 1, No. 3December 2009, pp. 42–45.

[14] Aditi Kumar, Parveen Thakur, *"Routing attacks and their Counter Strategies in MANET"* ,International Journal of Advanced Research in Computer Science and Software Engineering,Volume 4, Issue 5, May 2014.

[15] Raj P. N., Swadas P. B., DPRAODV*," A Dynamic Learning System against Blackhole Attack in AODV Based MANET "*, *International Journal of Computer Science Issues*, Vol. 2,2009, pp. 54-59.

[16] Bhoomika Patel, Khushboo Trivedi, *"Improving AODV Routing Protocol against Black Hole Attack based on MANET"*, International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014,pp.3586-3589